JAGAT GURU NANAK DEV
PUNJAB STATE OPEN UNIVERSITY, PATIALA

(Established by Act No. 19 of 2019 of the Legislature of State of Punjab)

The Motto of the University

(SEWA)

SKILL ENHANCEMENT EMPLOYABILITY WISDOM ACCESSIBILITY

Bachelor of Arts (BA)
Course Name: Fundamentals of Computer
Course Code: BAB32308T

ADDRESS: C/28, THE LOWER MALL, PATIALA-147001
WEBSITE: www.psou.ac.in

JAGAT GURU NANAK DEV
PUNJAB STATE OPEN UNIVERSITY PATIALA
(Established by Act No.19 of 2019 of Legislature of the State of Punjab)

PROGRAMME COORDINATOR :
Dr. Shifali Bedi
Assistant Professor, School of Social Sciences and Liberal Arts
Jagat Guru Nanak Dev Punjab State Open University, Patiala

COURSE COORDINATOR :
Dr. Monika Pathak
Assistant Professor, School of Sciences and Emerging Technologies
Jagat Guru Nanak Dev Punjab State Open University, Patiala

JAGAT GURU NANAK DEV
PUNJAB STATE OPEN UNIVERSITY PATIALA
(Established by Act No.19 of 2019 of Legislature of the State of Punjab)

PREFACE

Jagat Guru Nanak Dev Punjab State Open University, Patiala was established in Decembas 2019 by Act 19 of the Legislature of State of Punjab. It is the first and only Open Universit of the State, entrusted with the responsibility of making higher education accessible to all especially to those sections of society who do not have the means, time or opportunity to pursue regular education.

In keeping with the nature of an Open University, this University provides a flexible education system to suit every need. The time given to complete a programme is double the duration of a regular mode programme. Well-designed study material has been prepared in consultation with experts in their respective fields.

The University offers programmes which have been designed to provide relevant, skill-based and employability-enhancing education. The study material provided in this booklet is self instructional, with self-assessment exercises, and recommendations for further readings. The syllabus has been divided in sections, and provided as units for simplification.

The Learner Support Centres/Study Centres are located in the Government and Government aided colleges of Punjab, to enable students to make use of reading facilities, and for curriculum-based counselling and practicals. We, at the University, welcome you to be a part of this institution of knowledge.

Prof. G. S. Batra,
Dean Academic Affairs

Bachelor of Arts (BA)
Semester-III
BAB32308T: Fundamentals of Computer

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

INSTRUCTIONS FOR THE PAPER SETTER/EXAMINER

1. The syllabus prescribed should be strictly adhered to.
2. The question paper will consist of three sections: A, B, and C. Sections A and B will have four questions from the respective sections of the syllabus and will carry 10 marks each. The candidates will attempt two questions from each section.
3. Section C will have fifteen short answer questions covering the entire syllabus. Each question will carry 3 marks. Candidates will attempt any ten questions from this section.
4. The examiner shall give a clear instruction to the candidates to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.
5. The duration of each paper will be three hours.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt any two questions each from the sections A and B of the question paper and any ten short q questions from Section C. They have to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.

Section-A

Unit I: Introduction of Computer: Characteristics of the Computer, Block diagram of a Computer, Classification and Generations of Computer,Input Devices: Keyboard, Mouse, Trackball, Space ball, Joystick, Light pen, Touch screen, Digitizer, Data Glove, Scanner, Speech Recognition Devices, Optical Recognition Devices: OMR, OBR, OCR, MICR, Video Cameras, Output Devices: Monitors, Printers and its types, Plotters and its types, Speakers, Multimedia Projector.

Unit II: Computer languages: Machine language, assembly language, high level language, 4GL. Language Translators: Compiler, Interpreter, and Assembler. Software: Types of Software: System Software, Application Software, and Firmware. Memories: Memory Hierarchy, Memory Types: Magnetic core, RAM, ROM, Secondary, Cache, Overview of storage devices: floppy disk, hard disk, compact disk, tape.

Section –B

Unit III: Operating System: Functions of Operating System, Types of Operating System, Turning on a computer, desktop, taskbar, start menu, booting up, Desktop, Shortcut, Icons, Recycle Bin, Start Menu, My Computer, Computer's Devices and Drives, Storage, Removable Storage, CD/DVD Drive, floppy drive, and USB flash drive, Hard drive, Control Panel, The Window, Parts of Window, File Explorer, Files, Folders, Directories, Command, Menus, Keyboard, Function Keys, Normal Keys, Special keys, Direction keys, Numeric Keypad, Numeric Keys, Mouse: Left button, Right Button, Windows Accessories, Sharing Information between Programs. Virus, Antivirus, Peripherals can use with your computer.

Unit IV: Computer Networks: Components of data communication, modes of communication, standards and organizations, Network Classification, Network Topologies; Network Types,

Transmission media, network protocol; layered network architecture. Basic of Computer networks: LAN, MAN, WAN.

Suggested Readings:

1. "Computer Fundamentals" by P K Sinha
2. "Computer Fundamentals" by Goel
3. “Fundamentals of Computers” by V. Rajaraman
4. “Fundamentals of Computers” by E. Balagurusamy

Unit -I

1.1 Introduction of Computer

1.2 Characteristics of the Computer

1.3 Use of Computer

1.4 Block diagram of a Computer/Components of Computer

1.5 Generations of Computer

1.6 Input Output Devices (Peripheral Devices)

1.6.1 Input Devices

1.6.2 Output Devices

1.7 Classification of Computer

1.1 INTRODUCTION OF COMPUTER

The word "Computer" comes from the word "Compute", which means, "to calculate". In a layman language, a computer is a fast calculating device that can perform arithmetic operations. Although the computer was originally invented mainly for doing high speed and accurate calculation, it is not just a calculating device. The computer can perform any kind of work involving arithmetic and logical operations on data. It gets the data through an input device, processes at as per the instructions given and gives the information as output. We can define a computer as follows:-

"A computer is a fast electronic device that processes the input data according to the instructions given by the programmer/ uses and provides the desired information as output."

More accurately, we can define a computer as a device that operates upon data.

1.2 CHARACTERISTICS OF COMPUTER

Increasing popularity of computers has proved that it is very powerful and useful tool. The power and usefulness of this popular tool are mainly due to its following characteristics.

1) **Automatic:** Computers are automatic machines because once started on a job, they carry out the job (normally without any human assistance) until it is finished. However, computers being machines cannot start themselves and cannot go out and find there own problems and solutions. We need to instruct a computer using coded instructions that specify exactly how it will do a particular job.
2) **Speed:** A computer is a very fast device. It can perform in a few seconds, the amount of work that a human being can do in on entire year. A powerful computer is capable of performing several billing simple arithmetic operations per second.
3) **Accuracy:** In addition to being very fast, computer are very accurate. Accuracy of a computer is consistently high and degree of its accuracy depends upon its design. A computer performs every calculation with the same accuracy.
   However, errors can occur in a computer. These errors are mainly due to human rather than technological weaknesses.
4) **Diligence:** Unlike human beings, a computer is free from monotony, tiredness and lack of concentration. It can continuously work for hours without creating any error and without grumbling. If ten million calculation have to be performed, a computer will perform the last one with exactly the same accuracy and speed as the first one.
5) **Versatility:** Versatility is one of the most wonderful things about a computer. One moment it is preparing results of an examination, next moment it is busy preparing electricity bills, and in between, it may be helping an office secretary to trace an important letter. In brief, a computer is capable of performing almost any task.

6) **Power of Remembering:** As a human being acquires new knowledge, his/her brain subconsciously selects what it feels to be important and worth retaining in memory. The brain relegates unimportant details to back of mind or just forgets them. This is not the case with computers. A computers can store and recall any amount of information because of its secondary storage (a type of detachable memory) capability.

7) **No IQ:** A computer is not a magical device. It possesses no intelligence of its own. Its I.Q. is zero, at least until today. It has to be told what to do and in what sequence. A computer cannot take its own decision in this regard.

8) **No feelings:** Computers are devoid of emotions. They have no feelings because they are machines. No computer possesses the equivalent of a human heart and soul. Based on our feelings, taste,, knowledge, and experience we often make certain judgments in our day to day life but computer make judgments based on the instructions given to them in the form of program that are written by us (human beings).

1.3 USE OF COMPUTERS

Computers are being used in many areas of application like business, industry, scientific research, defense, space, communications, medicine, education etc. The utilization of computers in different fields is summarized as follows:-

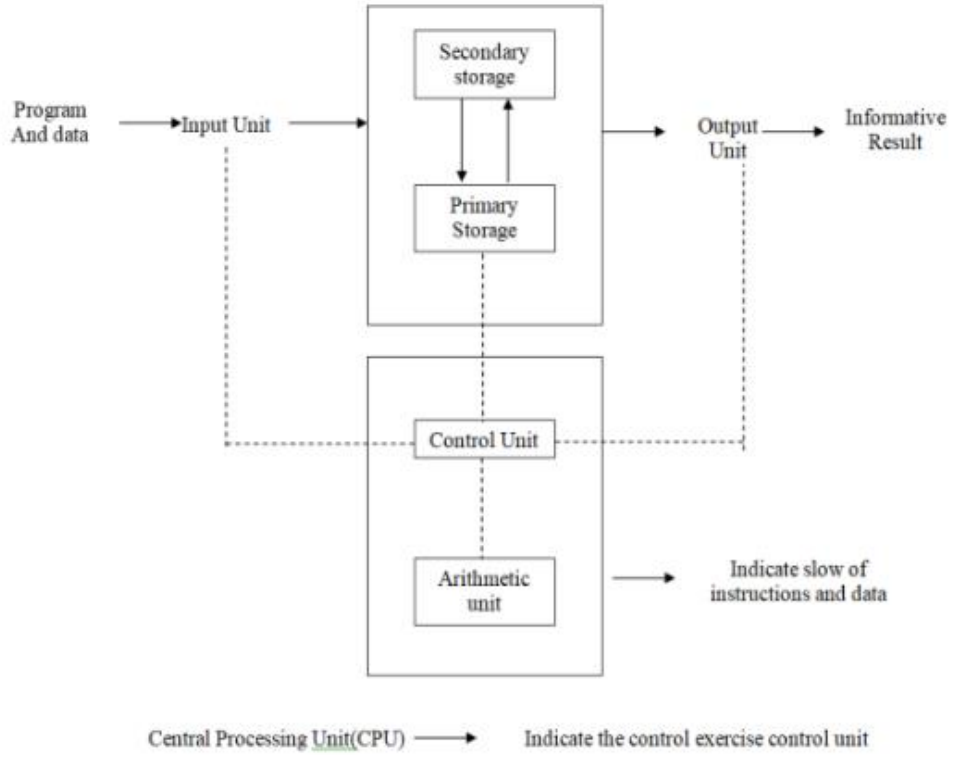
1) **Scientific Research:** Used to resolve complex scientific problems accurately in a short time.
2) **Industry:** Used in electricity, steel, paper, printing, engineering and other industries for production.
3) **Business:** Used in banks, airports, hotels, Govt. offices and others for computerizing business applications like financial accounting etc.
4) **Defense:** Used to computerize war planes, ships, radars etc.
5) **Space:** Used to design computerized space satellites, rockets and related technology.
6) **Data Communication:** Used to computerize geo-graphically separated offices through networking.
7) **Telecommunication:** Used in E-mail, Internet, Video Conferencing, Cellular phones etc.
8) **Medicine:** Used in hospitals and nursing home/clinics for maintaining medical records, prescription writing and computerized scanning etc.
9) **Education:** Used in development of CBT (Computer based teaching programmers for education.
10) **Law and order:** Used to records data of vehicles, criminals, finger prints etc.
11) **Libraries:** Used to develop library management systems.
12) **Publishers:** Used for designing and printing of books.
13) **Engineering:** Used for CAD (Computer aided designing) by engineering companies.
14) **Emerging Technologies:** Used in artificial intelligence like robotics.

1.4 BLOCK DIAGRAM OF COMPUTER:-

Computer has following components:-

1) Input unit
2) Output unit
3) Storage Unit
4) Arithmetic logic unit
5) Control Unit
6) Central Processing Unit.

The block diagram of basic computer organization is as follows:



In this figure, solid lines indicate flow of instruction and data, and dotted lines represent control exercised by control unit. These units correspond to the basic operations performed by all computer systems.

1) **Input Unit:** Data and instructing must enter a computer system before the computer can perform any computations on the supplied data. Data and instructions enter a computer through an input unit in a form that depends upon the input device used.

Input unit performs the following functions:

- It accepts instructions and data from outside world.
- It convert these instructions and data in computer readable form.
- It supplies the converted instructions and data to computer system for further processing.

2) **Output Unit:** An output unit performs the reverse operation of that of an input unit. It supplies information obtained from data processing to outside world means it present a data in a form people can understand.

An output unit performs following functions:

- It reads/accepts the results produced by a computer, which are in coded from and we cannot easily understand them.
- It converts these coded results to human readable form.
- It supplies the converted results to outside world.

3) **Storage Unit:** Data and instructions entered into a computer system through input units have to be stored inside the computer before actual processing starts. Similarly, results produced by a computer after processing have to be kept somewhere inside the computer system before being passed on to an output unit. Storage unit of a computer system caters to all these needs.

A storage unit holds:

- Data and instructions required for processing (received from input devices).
- Intermediate results of processing.
- Results for output before they are released to an output device.

Storage unit is of following two types :-

1) Primary Storage
2) Secondary Storage

Primary Storage:

- Primary storage of computer, also known as its main memory.
- It is used to hold pieces of program instructions and data and intermediate results of processing.
- However, primary storage can hold information only while computer system is on. As soon as the computer system switches off or resets, the information held in primary storage is erased.
- Primary storage normally has limited storage capacity because it is very experience.
- Primary storage of modern computer system is made of semiconductors devices.

Secondary Storage:

- It is also known as auxiliary storage.
- It is used to take care of the limitations of primary storage. It supplements the limited storage capacity and the volatile characteristic of primary storage.
- It is much cheaper then primary storage and it can retain information even when a computer system switches off or resets.

4) **Arithmetic Logic Unit:** It is the place where actual execution of instructions takes place during processing operation. Calculations are performed and all comparisons are made in arithmetic and logic unit. Data and instructions stored in primary storage before processing are transferred as and when needed to the arithmetic and logic unit (ALU) where processing takes place. Intermediate results generated in the ALU are temporarily transferred back to primary storage until needed later. In short, data may move firm primary storage to ALU and back again to storage many times before processing is over.

5) **Control Unit:** How does the ALU know what should be done with data once they are received? How it is that only results for output are sent to an output device and not the intermediate results? All this is possible due to the control unit of the computer system. It does not perform any actual processing on data. It manages and co-ordinates the entire computer system. It obtains instructions from the program stored in main memory, interprets the instructions, and issues signals causing other units of the system to execute them.

6) **Central Processing Unit:** Control unit and arithmetic logic unit of a computer system are together known as central processing unit (CPU). The CPU is brain of a computer system. In a computer system, all major calculations and comparisons take place inside the CPU and the CPU is responsible for activating and controlling the operations of other units of the computer system.

1.5 COMPUTER GENERATIONS

"Generation" in computer talk is a step in technology. It provides a framework for the growth of computer industry. There are total five computer generation known till today. Generations are major stages in the historical development of computing.

1) **<u>First Generations (1942-1955):</u>**

First Generation computer used thousands of *vacuum tubes*. A vacuum tube was a fragile says device, which used filaments and could control electronic signals. First generation computer were the only high speed electronic device available in these days. These vacuum tube computer could perform computations in milliseconds and known as first generation computers.

All data and instructions were fed into the system from punched cards. Only few specialists understand how to program these early computers. Machine and assembly languages are used.

Features:

1) They were too bulky in size, requiring large rooms for installation.
2) First generation computers used thousands of vacuum tubes that emitted large amount of heat. These computers were located had to be properly air conditioned.
3) They were the fastest calculating devices of their time.
4) Power consumption of these computers were very high because each vacuum tube consumed

about half a watt of power.

5) As vacuum tubes used filaments, they had a limited life. These computers were prone to frequent hardware failures.

6) Production of these computers was difficult and costly because thousands of components were assembled manually.

2) Second Generation (1955-1964):

The second generation computers were manufactured using *transistors* instead of vacuum tubes. Second generations computers were more powerful, more reliable, less expensive, smaller, and cooler to operate than the first generation computers.

Punched cards were still popular and widely used for entering data to these computers. High level programming languages (FORTAN, COBOL) were easier for people to understand and work with than assembly or machine languages.

Features:

1) Second generation computers were more than ten times faster than the first generation computers.
2) They were smaller than first generation computers and required smaller space.
3) They could switch much faster than tubes.
4) They were more reliable than first generation computers.
5) They had faster and larger primary and secondary storage as compared to first generation computers.
6) They consumed less power than first generation computers.
7) They were easier to use than the first generation computers.
8) They were less expensive to produce.

3) Third Generation (1964-1975):

Computers built using *integrated circuits* characterized the third generation. Integrated circuits are circuits consisting of several electronic components like transistors, resistors grown on a single chip of silicon.

Integrated circuits were smaller, less expensive to produce, more reliable, faster in operation, dissipated less heat, and consumed less power. Hence, third generation computers were more powerful, more reliable, less expensive, smaller and cooler to operate than second generation computers.

Features:

1) They are more powerful than second generation computers.
2) They were smaller than second generation computers. Hence requiring smaller space.
3) They consumed less power and dissipated less heat than second generation computers. Third generation computers were located still required to be properly air conditioned.
4) They were more reliable and less prone to hardware failures than second generation computers.
5) These had faster and larger primary and secondary storage as compared to second generation computers.
6) Commercial production of these systems were easier and cheaper because their manufacture did not require manual assembly of individual components.

4) <u>Fourth Generation (1975-1989):</u>

Fourth generation computers started a new social revolution *personal computer (PC) revolution.*During fourth generation, memories replaced by large random access memories with very fast access time. Hard disks became cheaper, smaller and larger in capacity. Magnetic takes became very popular as a portable medium for forting data from one computer to another.

Features:

1) PCs were smaller and cheaper than third generation computers.
2) No air conditioning was required for PCs.
3) They consumed less power than third generation computers.
4) They were more reliable and less prone to hardware failures than third generation computers.
5) They had faster and larger primary and secondary storage as compared to third generation computers.

6) They were general purpose machines.
7) Commercial production of these systems were easier and cheaper because their manufacturing did not require manual assembly of individual components.
8) Programs or data could be easily ported from one computer to another computer.
9) PCs were powerful tool for both office and home usage.

5) Fifth Generation (1989- Present):

During fifth generation, there was tremendous out growth of computer networks. Communication technologies become faster day by day and more and more computers were networked together. This trend resulted in emergence and popularity of the Internet and associated technologies and applications. The internet made it possible for computer were sitting across the globe to communicate with each other within minutes by use of e-mail (electronic mail) facility.

Features:

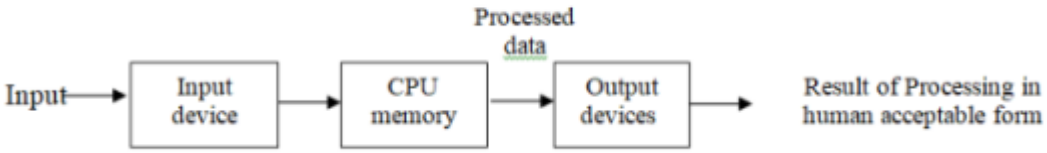
1. Portable computer (Notebook computers) are much smaller and handy than PCs of fourth generation computer.
2. Fifth generation computers are several times more powerful than PCs of fourth generation.
3. No air-conditioning is normally required for notebook computers.
4. They consume less power than fourth generation computers.
5. They are more reliable and less prone to hardware failures than fourth generation computers.
6. They have faster and larger primary and secondary storage as compared to fourth generation computers.
7. They are general purpose machines.
8. In fifth generation computers there are computers for almost any type of user whether the user is a child or a scientist.

1.6 INPUT- OUTPUT DEVICES (PERIPHERAL DEVICE)

The computers are useful only when these are able to communicate with users or external environment or operators. For this, input and output devices are used. These are also called as peripheral devices jointly. The term peripheral means all devices attached to computer.

Input device is used to enter data in computer. Output device display data form memory of computer.

Now a days, a variety of input and output device are available. User can use these device according to their need. Some devices are used for input as welt as output.



(a) **Input devices:**

An input device is an electromechanical device which is used to enter data or instructions from outside to computers main memory.

Input unit performs the following functions:-

1. It accepts instructions and data from outside world.
2. It converts these instructions and data in computer readable form.
3. It supplies the converted instructions and data to computer system for further processing.

Various types of input devices are as follows :-

1. Keyboard
2. Mouse
3. Trackball
4. Spaceball
5. Joystick
6. Light Pen
7. Touch Screen or Touch Pannel

8. Data Glove
9. Image Scanner

1. **Keyboard:** The most commonly used input device is keyboard the data is entered by pressing set of keys. All keys are labeled. A keyboard with 101 keys is called as qwerty keyboard. The keyboard has alphabetic as well as numeric keys some special keys are available.
2. **Mouse:** A mouse is small hand held box. Wheels are provided on bottom of mouse. Mouse is rotated on flat surface. Mouse can be picked and moved to other place without change the position of screen courser.Mouse can have two button or three button. Buttons are provided at top of mouse. Mouse is attached with CPU using wire.

   Advantages:

   1) It is simple to operate.
   2) It is low cost device
   3) It can select graphic object very fast.
   4) It is used for quick positioning of curser on an item.

   Disadvantage: Small rotation of mouse can cause error in readings.

3. **Trackball:** It also is a pointing device. It is similar to mouse except that you don't have to move the enter device like mouse rather only the ball is used for cursor movement. Ball is rolled with fingers. It requires less space for performing its operation. Sometimes it is fixed with mouse sometimes with keyboard.

   Due to limitation of space in laptop it is not suitable as part of keyboard.It can be rotated with palm also to produce curser movements on screen.
4. **Space Ball:** It is similar to trackball but it can move in six direction whereas trackball can move in two directions only. It can be pushed and pulled in various directions.
5. **Joystick:** It is a pointing device. Its working is same as that of trackball but instead of moving with hand ball is moving using stick. Ball is fixed in socket. On socket, stick is mounted. Stick can be moved in left, right, top, and down direction. The stick is also called as lever. The joystick can be mounted on keyboard. The stick is moved in any direction and amount of movement of cursor corresponds to amount of movement of stick. Joysticks are less expensive.

   Uses:

   - It is used to play video games.
   - Joystick is used by flight stimulators.
   - It is used for controlling industrial robots.

6. **Light Pen:** It also is a pointing device. Its shape is like pen or penal. It can detect light coming from points on CRT screen. Pen with not detect light emitted from background sources. When pen is on, it is pointed on screen than bean will light up that spot, it will generate pulse.

   Disadvantages:

   - It pen is used for longer period of time then it courses arm fatigue.
   - It gives false readings due to background light in room.

7. **Touch Screen or Touch Panel:** It allows display of objects using a touch of finger. Touch panel will select any icon as option from set of icons displayed on screen.

   Advantages:

   - It is a simple method of selecting graphical object.
   - It is an easy way of input.

   Applications:

   - These are used as information work for displaying information at hotel restaurants.
   - In public places like parks, these are used to guide people by displaying information.

8. **Data Glove:** It is a glove that you can wear in your hand. Glove can grasp virtual objects. Glove has a series of sensors. The seniors can detect movement of hand and fingers.
9. **Image Scanner:** It is an input device. The data or text is written on paper. The paper is feeded to scanner. The paper written information is converted into electronic format. This format is stored in computer. The input documents can contain text, handwritten material picture etc.

By storing the document in computer, it becomes safe for longer period of time. The document will be permanently stored for future. We can print the document when needed.

(b) Output devices:

An output device generally is an electromechanical device, which accepts data from a computer and translates them into a form understand able to users. It is as important as input device. It performs the reverse operation of that of in input unit.

Output unit performs the following functions:-

1. It accepts the results produced by a computer, which are in coded form and we cannot easily understand them.
2. It converts these coded results to human readable form.
3. It supplies the converted results to outside world.

There are many types of output devices. Some commonly used output devices are as follows:-

1. Monitors or VDU (Video display unit)
2. Printers
3. Plotters
4. Speakers.

An output device can be one of the following two types.

(a) Soft copy devices.
(b) Hard Copy devices.

Soft Copy Device: The output is produced on device not on paper. The output is temporary and erased when device is switched off. The output displayed on monitor is soft copy.

Hard Copy Device: It is output produced on paper. It can be touched. We can carry out paper to other place. It can be shown to other people also. It is not erasable. It can be stored permanently for future purposes. Output produced by platter and printer are example of these.

1. Monitors: It is most popular device for producing soft copy output. It is also called as VDU (Visual display Unit). A monitor is attached with keyboard and CPU. The keyboard will be used to enter data. The CPU will process the data. The output will be displayed on monitor.

2. Printers: A printer is an output device that produces text and graphics on paper. Printer is used to get the "Hard copy" of that documents. Printer is divided into two types.

(a) Impact Printers.
(b) Non Impact Printer.

(a) Impact Printers: The printers in which there is a mechanical contact between printer head and paper for printing are called impact printers. These are noisy printers. These are similar to typewriter.

For example :- 1. Dot Matrix
2. Line Printers

1.Dot Matrix: Dot matrix printer is an impact printer that produces text and graphics when tiny wire pins on the print head strike the ink ribbon. Higher number of pins means that the printer prints more dots per character thus resetting in higher print quality.

Advantages:

1. Low printing cost per page
2. Retable, colorable

Disadvantages :-

1. Noisy
2. Limited print quality
3. Low printing speed
4. Limited color printing.

2.Line Printers: Line printers are impact printers used with most medium and large computer systems for producing high volume paper output. They are fast printers having speeds in the range of 300 to 2500 lines per minute.

(b) Non-Impact Printers: The printers in which there is no mechanical contact between paper and printer are called non impact printers. These are not noisy.

For example:- 1. Inkjet Printers
2. Laser Printers.

1.Inkjet Printers: Inkjet printers are non impact printer which print text and images by spraying tiny droplets of liquid ink onto paper. They are most popular printers for home use. Inkjet printers

produce high quality output.

Advantages:

- Low cost
- Good for printing pictures
- High quality of output
- Easy to use
- Reasonably fast

Disadvantages:

- Ink bleeding causing blurred effects one some paper
- Ink is sensitive to water, even a small drop of water can cause blurring.

2.Laser Printers: Laser Printers are non impact printers which can print text and images in high speed and high quality resolution. Laser printer are page printers. An entire page is processed at a time. They use laser beam to produce an image of the page.

Advantages:

- High Print speed.
- Printout is not sensitive to water.
- Good for high volume printing.

Disadvantages:

- More expensive than inkjet printers
- Bulkier than inkjet printers.
- Laser printers are less capable of print high quality images such as photos.

3.Plotters: Plotters are output devices. They are used to produce good quality graphics and drawing under computers control. They use ink pen to draw graphics or drawings. Either single color or multicolor pens can be employed.

Pen plotters are slow devices. A pen plotter can take from several seconds (for simple drawings) to several minutes (for complex drawings) to produce a drawing. But it takes much less time as compared to traditional hand methods of producing drawing.

There are two types of plotters :-

1. Drum Plotter
2. Flat bed plotter

1.Drum Plotter: In drum plotter, the paper on which the graph is to be drawn is mounted on a rotating drum. The drum can rotate in either clockwise or anticlockwise direction under the control of the plotting instructions sent by the computers.

The pen can move left to right or right to left. The pen can also move up or down. The movement of the pen and drum are controlled by the graph plotting program.

2.Flat Bed Plotter: A flat bed plotter has a surface on which paper is fixed.The pen can be moved up or down. This type of plotter is called a flat bed plotter because it plots on paper which rests on a flat bed.

4.Speakers: Computer speakers or multimedia speakers are speakers external to a computer that disables the lower fidelity built in speaker. A voice response system has an audio response device i.e. speaker which produces audio output obviously the output is temporary soft copy output. Banking industry uses speaker in ATM .

1.7 CLASSIFICATION OF COMPUTERS

Today computers are classified based on their made of use. According to this classification computers are classified as notebook computers personal computers workstations, mainframe systems super computers and client and saver computers.

1. **Notebook Computers (LAPTOPS):** Notebook computers are portable computers use by people who need computing resource wherever they go notebook computers can easily fit in a briefcase. These are also called mini computers. Notebook computers are light in weight weighing around. 2 kg. They are also known as Laptop PCs (Laptop personal computers or simply Laptop) because they are as powerful as a moderate PC, and their size and weight allows them to be used comfortably.

   We can use laptop even at places where there is no eternal power source available (for example while traveling in a tram or airplane). Hence they are designed to operate with

chargeable batteries with a fully battery a laptop can operate for a few hours.

2. **Personal Computers (PCs):** A PC is a non portable general purpose computer that fits on a normal size office table and is used by one present at a time. Users use PCs for their personal computing needs either at their work places or at their homes. PCs have changed the work habits of organizations. An increasing proportion of office work now involves use of computers.

   Those employees who could not work during traditional office hours due to personal reasons can now work part of their time in office and remainder at home by having a PC at their homes. Several individuals also keep a PC at their homes to run business firm homes. Children use PCs for education and entertainment. Hence, PCs are now very common everywhere, and can be found in offices classrooms, homes, hospitals, shops. clinics etc. It is also know as microcomputers.

3. **Workstations:** A workstation is a powerful desktop computer designed to meet computing needs of engineers architects and other professionals who need greater processing power large storage and better graphics display facility than normal PCs provide for example workstations are used commonly for complex scientific and engineering problems. A workstation is almost similar to high end PC, and is used typically by one person at a time.

4. **Mainframe Computers:** Mainframe computers are computer system that are mainly used for handling data processing needs of large size organizations. There are several large size organizations such as banks hospital, railways etc, that need on line processing of large number of transactions.

   Mainframe computers are very large and fast computers. They are used in centralized location where many terminals (input/output devices) are connected with one CPU and thus allow different users to share the single CPU. They lave a very high memory and can support thousands of users. Mainframe systems are much bigger and several time more expensive than workstations.

5. **Super Computer:** Super computers are the most powerful and expensive computers available at any given time. They are mainly designed for complex scientific applications that require enormous processing power.

   Super computers have many CPUs which operate in parallel to make it as a fastest computer.

   It is mainly used for following applications :-

   1. Weather information
   2. Defence
   3. Medicine etc .

6. **Client and Server Computers:** With increased popularity of computer networks, it has become possible to interconnect several computers that can communicate with each other over the network.

Questions:

1. What is computer?
2. What is the need of the computer?
3. Explain the characteristics of computer.
4. Draw and discuss the block diagram of computer.
5. Discuss the input and output devices in detail.

UNIT-II

3.1 LANGUAGE CLASSIFICATION
3.3 SOFTWARE AND ITS CLASSIFICATION
3.3 MEMORY TYPES

3.1 LANGUAGE CLASSIFICATION

A language is a means of communication. We use a natural language such as English to communicate are idea and emotions to others. A language that is acceptable to a computer system is called a computer language. However all computer languages can be classified into the following three categories:

1. Machine Language
2. Assembly Language
3. High level Language
4. Fourth Generation Language (4GL)

1. MACHINE LANGUAGE:

There is only one language understood by the computer without using a translation program. This language is called the machine language of the computer. The machine language of a computer is normally written as strings of binary 1s and 0s.

A machine language instruction normally has a two part format. The first part of an instruction is the operation code, which tells the computer what function to perform. The second part is the operand, which tells the computer where to find or store the data or other instructions, which are to be manipulated.

Advantages: Programs curetted in machine language can be executed very fast by the computer. This is because machine instructions are directly understood by the computer, and no translation of the program is required.

Disadvantages:

1. *Machine dependent:* Because of internal design every type of computer is different from every other type of computer; the machine language also differs from computer to computer. It a company decides to change to another computer, its programmers will have to learn a new machine language and would have to write all the existing programs.
2. *Difficult to program:* Machine language programs a directly and efficiently executed by the computer, it is difficult to program in machine language. It is necessary for the programmer either to memorize the dozens of operation code numbers for the commands in the machines instruction set.
3. *Difficult to modify:* It is difficult to correct or modify machine language programs. Checking machine instructions to locate errors is very difficult and time consuming. Modifying a machine language program later is so difficult.

2. ASSEMBLY LANGUAGE:

It is also known as symbolic language. Assembly languages programming, was introduced in 1952, helped in overcoming the limitations of machine language programming in the following manner:

1. By using alphanumeric mnemonic codes, instead of numeric codes for the instructions in the instruction set. For example using ADD instead of 1110 (binary) 14.
2. A programmer can much easily remember and use the storage locations of the data and instructions used in an assembly language program. Assembler is used to convert assembly languages into machine language.

A language, which allows instructions and storage locations to be represented by letters and symbols, instead of numbers is called on assembly language or symbolic language. A program written in an assembly language is called an assembly language program or a symbolic program.

Advantages:

1. *Easier to understand and use:* Due to the use of mnemonics, instead of numeric op-codes, assembly languages programs are much easier to understand and use as compared to machine language programs.
2. *Easier to locate and correct errors:* Fewer errors are made while writing programs in assembly language and those that are made are easier to find and correct. Assemblers are designed to automatically detect and indicate errors for use of an invalid mnemonic op-code or a name that has never been defined.
3. *Easier to modify:* Since they are easier to understand it is easier to locate, correct and modify instructions of on assembly language program than a machine language program.
4. *No worry about addresses:* An important advantage of assembly language is that programmers need not keep track of the storage locations of the data and instructions while writing an assembly language program. Assembly languages programs can be easily moved from one section of the memory to another.
5. *Efficiency of machine language:* An assembly language program also enjoys the efficiency of its corresponding machine language program.

Limitations:

1. *Machine dependent:* Assembly languages differ from computer to computer and an assembly language program can be executed only on the computer in while assembly language it has been written. Hence, a decision to change to another computer will require learning a new language and the conversion of all existing programs into the assembly language of the new computer.
2. *Knowledge of hardware required:* Since assembly languages are machine dependent, an assembly language programmer must have a good knowledge of the characteristics and the logical structure of his /her computer to write good assembly language programs.
3. *Machine level coding:* In case of an assembly language, instructions an still written at the machine code level. That is one assembly language instruction is substituted for one machine language instruction. Hence, writing assembly language programs is still time consuming and not very easy.

3. HIGH LEVEL LANGUAGE:

High level programming languages were designed to overcome the limitations of machine language or assembly languages.

High level languages have the following features:

1. They are machine independent. That is, a program written in a high level language can be easily ported and executed on any computer.
2. They do not require the programmers to know anything about the internal structure of the computer on which the high level language program will be executed. Since high level languages are machine independent, a programmer writing a program in a high-level language may not even know on which computer will his/her program be executed.
3. They do not deal with the machine level coding. Rather, they deal with the high level coding enabling the programmers to write instructions using English words and familiar mathematical symbol sand expressions. Compiler and Interpreter are used to convert high level language into low level language (machine language).

The advent of high level languages has enabled the use of computers to solve problems even by non-expert users. This has allowed many users, without any background in computer science and engineering to become computer programmers.

Advantages:

1. **Machine Independence:** A program written in a high level language can be executed on many different types of computer with very little or no effort of porting it on different computers.

Hence, the time and effort spent on software development are better rewarded with high level language programming.

2. **Easier to learn and use:** High level languages are easier to learn, because they are very similar to the natural languages used by us in our day to day life. They are also easier to use, because a programmer need not know the internal details of the computer for programming in a high level language.

3. **Fewer errors:** A programmer need not worry about how and where to store the instructions and data of the program, and need not write machine level instructions for the steps to be carried out by the computer. This allows the programmer to concentrate more on the logic of the program under development.
   Hence, errors if any, in the program can be early located and corrected by the programmer.
4. **Lower program preparation cost:** Writing programs in high level languages require less time and effort which ultimately leads to lower program preparation cost.
5. **Better documentation:** The statements of a program written in a high level language are very similar to the natural language statements used by us in our day to day life. Hence, they can be easily understood by a programmer familiar with the problem domain.
6. **Easier to maintain:** Programs written in high level languages are easier to maintain than assembly language or machine language programs. This is because they are easier to understand, and hence, it is easier to locate correct and modify instructions as and when desired.

Limitations:

1. **Lower efficiency:** Programs written in high level languages take more time to execute and require more main memory space. Hence a program written in a high level language has lower efficiency then assembly language or machine language.
2. **Less flexibly:** High level languages are less flexible than assembly languages because some tasks cannot be done in a high level language or can be done only with great difficulty.

4. FOURTH GENERATION LANGUAGE (4GL)

The fourth generation languages, or 4GL, are languages that consist of statements similar to statements in a human language. Fourth Generation Languages (4GLs) are programming languages designed to simplify the process of writing programs and increase developer productivity. They are typically higher-level languages compared to earlier generations (such as machine language, assembly language, and third-generation languages). Examples of Fourth Generation Languages are SQL (Structured Query Language), Python etc. Fourth Generation Languages aim to boost productivity by reducing the complexity of traditional programming languages and focusing on solving specific problems efficiently. These languages are human friendly to understand.

Characteristics of Fourth Generation Languages:

- *Non-Procedural:* 4GLs are often non-procedural or declarative, meaning that programmers specify what needs to be done rather than how it should be done. This abstracts away low-level details and focuses on describing the desired outcome.
- *Database Oriented:* They are frequently designed with built-in capabilities for interacting with databases. This includes features like SQL (Structured Query Language) for querying and manipulating data, which simplifies database operations.
- *High-Level Abstraction:* 4GLs provide high-level abstractions that allow developers to work at a more conceptual level, using commands and statements that are closer to natural language or specific problem domains. This reduces the need for manual memory management and other low-level tasks.
- *Rapid Application Development (RAD):* They are often associated with RAD methodologies, enabling faster development cycles and quicker prototyping of applications. This is facilitated by their high-level nature and built-in support for common tasks.
- *Domain Specific:* Some 4GLs are designed for specific domains or industries, providing specialized features and libraries tailored to those needs. Examples include languages for financial modeling, scientific computation, or business process automation.
- *Code Generators and Wizards:* Many 4GL environments include tools such as code generators, wizards, and visual development interfaces that further automate and streamline the development process.

- *Graphical User Interface (GUI) Support:* They often provide built-in support for creating graphical user interfaces (GUIs), allowing developers to easily design and deploy user-friendly applications.

Advantages of 4GL:

- Easy to understand
- Less time required for application creation.
- It is less prone to errors.

Disadvantages of 4GL:

- Memory consumption is high.
- Has poor control over hardware.
- Less flexible.

3.2 SOFTWARE AND ITS CLASSIFICATION

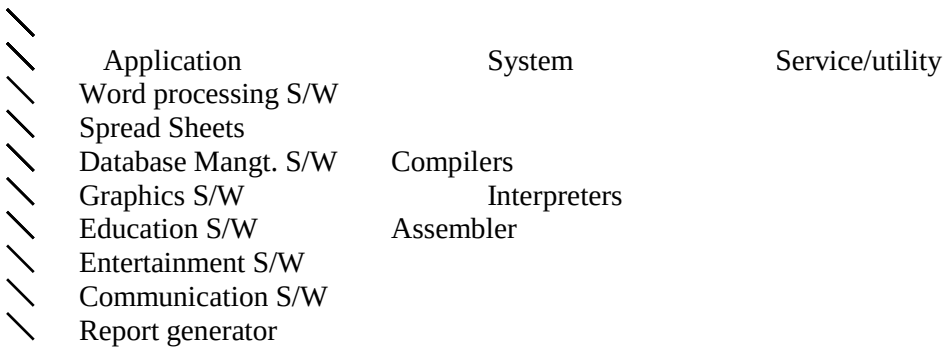
A computer cannot do anything on its own. It must be instructed to do a desired job. Hence, it is necessary to specify a sequence of instructions, which a computer must perform to solve a problem such a sequence of instructions, written in a language, which can be understood by a computer, is called a computer program.

The term software and hardware are frequently used in context with computers. Hardware is the term given to the machinery itself and to various individual pieces of equipment. It refers to the physical devices of the computer system. Thus, the input, storage, processing, control and the output devices are hardware.

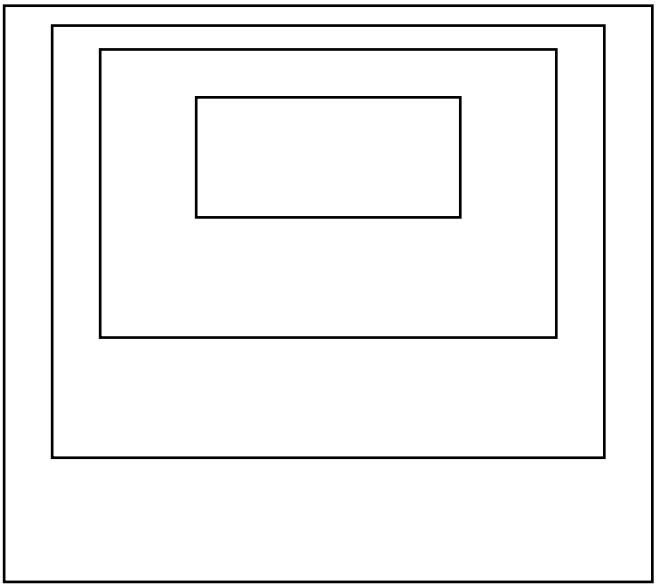
The term software refers to the set of computer programs, procedures, and associated documents (flowcharts, manuals etc.), which describe the programs, and how they are to be used. To be precise, software means a collection of programs, whose objective is to enhance the capabilities of the hardware. A software package is a group of programs, which solve a specific problem or perform a specific type of job.

Software or the program can be defined as the complete set of written instruction written by the programmer which enables the computer to obtain the solution of a problem with or without the data.

Relationship between the hardware, software and the user of the computer system is as shown.



Type of Software



There are two ways of obtaining software:Purchase on existing Package, or Develop own packages

TYPES OF SOFTWARE

(I) Application Software
(II) System Software
(III) Service or Utility Software

(I) APPLICATION SOFTWARE:

Application software is a set of one or more programs, designed to solve a specific problem, or do a specific task.

A program written by a scientist to solve his/her particular research problem is also application software. The programs included in an application software package are called application programs, and the programmers who prepare application software are referred to as application programmers.

These are literally millions of application software available for a wide range of applications, ranging from simple application, such as word processing, banking, hospital administration, insurance, publishing to complex scientific and engineering applications such as weather forecasting design of computer structures like aircrafts ships bridges etc.

With so many applications available, it is not possible to categorize them all, and to cover them. Some of the most commonly known applications software is:

(a) Word Processing Software
(b) Spreadsheets
(c) Database Management Software
(d) Graphics Software
(e) Education Software
(f) Entertainment Software
(g) Communication Software
(h) Report Generator

(a) Word Processing Software: These are software, which usually automate the day to day documentation work of an organization. It helps in creating texts, manipulating, formatting and printing of the text, so that the drafting, redrafting, typing again and again manually now becomes easy and less paper wastage as well as the time taken also is reduced a lot. Wordstar, Microsoft word etc. are some of the available word processors.

The word processing software is considered as a computerized version of a type writer. Most word processors allow user to make change and correction to the text easily. They also lot user change the grammar and the spellings in the document. Users can use a word processor to create almost any kind of the documents.

(b) Spreadsheets: Electronic spreadsheets are like sheets of paper with rows and columns. Electronic spreadsheets allow numbers, characters, formula and all other types of data which has to be entered in a tabular form rows or columns.

The areas where columns and rows meet are called cells. User can put text, numbers, or formulas into cells to create a worksheet. When entries are done into cells, user can change any of them. User can input different numbers into spreadsheets to generate graphics and charts to illustrate the relationship more emphatically.

Usage of electronic spreadsheet gives significant advantages and benefits over using paper spreadsheets. Some of the significant advantages:

(a) It provides flexibility and it is easy to incorporate changes.
(b) Automation of various calculations.
(c) Recalculating automatically on updating.
(d) Various built in functions are provided so that the user finds it conferment to work.
(e) Flexibility to size and resize columns.
(f) Spreadsheet is very vast, so that vast areas can be provided if required. The ease at which insertions and deletions can be made.
(g) Data can be formatted as per the requirement.

Most commonly available and used spreadsheets are MS-Excel, Super Calc etc.

(c) Database Management Software: Database is an organized collection of data, which is logically related. Database serves as the source from which desired information can be retrieved; conclusions can be drawn by processing the data.

The most commonly used database in our day to day life are the telephone directory, where the telephone numbers along with the name and address are arranged in alphabetical ardor and the dictionary, where words are arranged alphabetically along with their meanings.

The data has to be managed so that the retrieval of information is effective and easy. Managing data involves creating, deleting, updating, adding, modifying data in databases.

Database management software or system (DBMS) is a software package that allows a user to perform above function. It also allows multiple computers to sharing the data files.

(d) Graphics Software: Graphics program are those programs that manipulate the images to any extent. User can draw illustrations from the scratch, using an electronic pointing device such as mouse or light pen or pencil or brush. Such programs are referred to as either point or draw program.

The presentation graphic application is another type of graphic software that helps user to create professional looking visual aids for the presentation.

As graphical representation of data is much more easy to understand. It is also easier to represent relationships among data items graphically. Example of graphics generator is MS-Excel.

(e) Education Software: Education software allows a computer system to be used as a teaching and learning tool. A few examples of such application are those that teach going children to do Mathematics, Recognize alphabets, Read words and sentences.

(f) Entertainment Software: Entertainment software allows a computer system to be used as an entertainment tool. A good example of such an application is computer video games.

(g) Communication software: Communication software is used to connect the computers so that they can share information and resources. They use modems, the hardware devices used for sending the data across the telephone lines. A user can share information with another user with a modem and a piece of communication software. The communication software is also called a network software example of communication software is LINUX.

These can be an electronic data transfer between two different computers in a network. The concept of E-mail i.e. Electronic Mail has becomes the order of the day, where are can communicate with day one throughout the world by sending a mail electronically.

(I) Report Generator: There is always a need in day to day operations that timely reports of various activities have to be used, so as to depict a situation or helping decision making. If these reports are designed manually, it is very difficult task, therefore some software solutions have been designed so as to help a user to design his own report, with ease and even the time consumed is drastically reduced. Some of the commonly available report generating software are oracle reports, crystal reports etc.

(II) SYSTEM SOFTWARE:

System software is a set of one or more programs, designed to control the operation and extend the processing capability of a computer system. In general, computer system software performs one or more of the following functions:

- Supports the development of other application software
- Supports the execution of other application software.
  - Monitors the effective use of various hardware resources, such as CPU memory peripherals etc.
  - Communicates with and controls the operation of peripheral devices, such as printer, disk tape etc.

The efficient system software allows application software to be run on the computer with less time and effort system software makes the operation of a computer system more effective and efficient. It helps the hardware components work together and provides support for the development and execution of application software. The programs included in a system software package are called system software are referred to as system programmers.

Some of the most commonly known system software is as follows:

(a) Operating System: An operating system is software that runs on computer and manages the computer hardware. All computers must have an operating system used for starting the computer and to run other programs. It provides an interface between the user of a computer and computer hardware.

Operating system performs basic tasks, such as recognizing input from keyboard, sending output to the display screen, keeping tracks of files and controlling perspired devices such as printers. The operating system is also responsible for security ensuring that users do not access the system.

Functions:

1) It works as an interface between hard ware and software.
2) It manager memory and other storage.
3) Input/output management
4) Processor management assignment of processor to different tasks being performed by the computer system.
5) File management creation of a new file copying moving a file from one storage location to another
6) Priority system
7) Establishing data security and integrity.

The operating system can be classified as single user (DOS) and multi user (LINUX) depending on the number of users working on it at a given point of time.

(b) Language Processors: Language processors also known as language translators. Language processors are system software, which transform the instructions prepared by programmer in a programming language, into a form which can be interpreted and executed by a computer system. Translators are further classified into three categories which are given below:

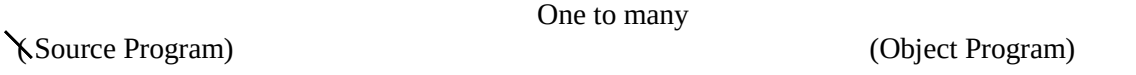
(1) Compilers
(II) Interpreters
(III) Assembler

(I) Compilers: A computer can execute only machine language programs directly. Hence, a high level language program must be converted (translated) into its equivalent machine language program before it can be executed on a computer. This translation is done with the help of a translator program called compiler.

A compiler is software that will accept the total program code (high level language) as input and then converts it into machine code (low level language). For every language, usually there is a compiler which interprets and converts the program in that language into machine understandable code.

Source code Input Object code output

As figure shows, input to the compiler is the high level language program, and its output is the machine language program.



Source program is not under execution, it is only converted into a form that can be executed by the computer.

Each compiler requires a separate compiler for each high level language that it supports. Compilers are large programs residing permanently on secondary storage. Compilers are more lengthy and complex software as compared to assembler and hence occupy more memory.

When the compiler is needed, it is called by the computer and loaded into the RAM of the system. To translate a source program, the compiler and the source program are loaded first from secondary storage into main memory of the computer. Compilers also detect and indicate certain types of errors in source programs automatically.

(II) Interpreters: Interpreter also does the same task of converting the program code into machine code like compiler but it is different from the compiler in sense the compiler takes the complete program as input, but interpreter takes the program code line by line and converts it to machine code. The interpreter takes one source program instruction, translates it into object code and executes it, then up the next instruction translates it and so on.

The input to an interpreter is a source program, but unlike a compiler its output is the result of program execution instead of on object program.

The interpreter program is small in size. Interpreters are easy to use and convenient. As compared to compliers, interpreters are easier to write because they are less complex programs than compilers.

The main disadvantage of interpreters is that they are slower than compilers when running a finished programs. This is because each statement is translated every time it is executed from the source program. In case of compiler, each statement is translated only once and saved in the object program.

When coming to operational efficiency, compiler is more efficient than an interpreter. Most of the translators of current day are compilers only.

(iii) Assembler: This is the third category of translator. It also works the same way as compiler and interpreter but here, the input programs are in assembly language. The output is in machine language.

This is system software that takes as an input a program written in assembly language and as an output generates the program written in machine level which can be directly executed on the computer.

Interpreter	Compiler
Translates program one statement at a time.	Scans the entire program and translates it as a whole into machine code.
Interpreters usually take less amount of time to analyze the source code. However, the overall execution time is comparatively slower than compilers.	Compilers usually take a large amount of time to analyze the source code. However, the overall execution time is comparatively faster than interpreters.
No Object Code is generated, hence are memory efficient.	Generates Object Code which further requires linking, hence requires more memory.
Programming languages like JavaScript, Python use interpreters.	Programming languages like C, C++, Java use compilers.

(c) Communication Software: In a network environment (where multiple computers are

interconnected together by communication networks), communication software enables transfer of data and programs from one computer system to another.

(d) Utility Programs: Utility programs (Utilities) are set of programs, which help users in system maintenance tasks, and in performing tasks of routine nature. Some of the tasks commonly performed by utility programs including formatting of hard disks or floppy disks, taking backup of files stored on hard disk on to a take on floppy disk, sorting of the records stored in a file in a particular order.

(iii) SERVICE OR UTILITY SOFTWARE:

The service or utility software or programs are those that are used to provide services to facilities the working of the operating systems. The operating systems have integrated many utilities into the system itself and some additional services that night help the user to take back up of data, scanning viruses, maintenance tools for the system, or retrieve the deleted files are called service software.

The service software is classified into the following categories:

(a) File defragmentation
(b) Data compression
(c) Backup software
(d) Data recovery software
(e) Antivirus utility
(f) Screen savers

(a) File defragmentation: A file defragmenter is a utility program that is used to defragment the files on the hard disk to speed up the working of the hard disk. It is now part of the windows operating system.

When user copies a file first time into a disk, the operating system allocates it one or more contiguous sectors. If some additions are to be carried out on that file later on, the sectors next to the file may not be available. In such a case the operating system stores the data some here else on the disk.

(b) Data Compression: Data compression is the ability to reduce the storage requirements of a file using mathematical algorithms. Thus data compression help helps to store more data on a disk.

Some utilities compress files on demand usually to store the data on a small disk or to reduce the space taken up on the hard disk by the files that are really accessed. The most widely used data compression software is easy zip and win zip.

(c) Backup Software: The backup software is designed to help user copy large group of files from hard disk to some other storage media such as floppy etc. Data compression is also build into the backup software.

(d) Data recovery software: Data recovery software or unease program is required when user erase or delete a file from a disk accidentally and then realize that file is still needed.

The unease software has the capability to get back the deleted files which are deleted by the user but are yet to be overwritten by the operating system.

(e) Antivirus utilities: A virus (Vital information resource under seize) is an infections program attached with another program. A virus can be programmed or carry out many tasks, including copying themselves to other programs, display information on screen and destroy the data files.

The antivirus utility software tracks the virus, eradicate and prevent their spread. The antivirus scans the sector on disk, identifies any virus and attempts to remove them. Some common antivirus programs are MacAfee, semantic antivirus and Norton antivirus.

(f) Screen savers: Screen saver is basically a program that displays moving images on the screen if no input is received from the user for several minutes. Programmers had become so creative with the types of images displayed by the screen savers that user began to purchase them to protect their data from being seen when they are away from their disks. Today a variety of screen savers are available ranging from flying windows to Hollywood personalities and desktop themes.

3.3 MEMORY TYPES:

The memory used by computers can be classified into various types, depending on the characteristics and functionality of it. One has to have a clear understanding of these memory types to understand the working of the computer memory.

The primary unit (storage) or memory is capable of storing data and computer instructions necessary

to direct the CPU during processing to solve a given problem. The computer's memory or primary storage consists of a large number of cells, each with a fixed capacity for storing data and each with a unique location or address. Each storage cell is capable of holding a specific amount of data.
The primary storage unit of some computer system also includes a small, very fast, very expensive storage area referred to as cache memory. This high speed storage area is used temporary to store instructions and data that will be accessed more frequently during execution of program. Some of the commonly available memory types as follows:

- **ROM:** Read only memory chips always retain the data they hold even when the computer is turned off this called non-volatile memory.

ROM is generally provided by the manufacturer of the computer and consists of small chips. The data and programs are "burned into" or permanently stored on the chip in computer manufacturing industry. The data in these chips can only read and used so the memory is called read only memory (ROM). There are different types of ROM which are as follows.

(i) **PROM (**Programmable ROM): As ROM is read only memory, the contents of ROM cannot be changed but for specialization use contents of ROM can be reprogrammed using special circuits. These ROMs are known as programmable read only memory (PROM). This is basically a blank ROM Chip that can be written to, but only once.

(ii) **EPROM (**Erasable Programmable ROM): It is that ROM that can be erased and reprogrammed to do this it has to be removed from the processor and exposed to write violet rays for some time, and then it can accept new contents.

(iii) **EEPROM (**Electrically Erasable and Programmable Read only Memory): It is also called flash BIOS. This ROM can be rewritten through the use of special electrical pulses or special software program.

ROM is slower than RAM.

- **RAM:** Random access memory chips do lose their contents when the computers power is shut off thus called volatile memory. The RAM is used for temporary storage of program data, allowing performance to be optimum.

  While a program is being executed it requires data, this data while is required which execution of the program is stored in RAM. Whenever new data is stored in RAM the previous data is erased. Thus RAM is used to store data and programs temporarily. The capacity of the RAM is one of the major factors for faster working of the computer.

  These are different types of RAM:

  (i) **SRAM (**Static RAM): This RAM will maintain its data as long as power is provided to the memory chips. It does not need to be se-written periodically. SRAM is very fast but is much more expensive than DRAM SRAM is often used s cache memory due to its speed.

  (ii) **DRAM** (Dynamic RAM): DRAM, unlike SRAM, must be continually re-written in order for it to maintain its data. DRAM is used for most system memory because it is cheap and small. There are several types of DRAM, complicating the memory scene even more. Today DRAM is mostly used.

- **Cache Memory:** Cache memory is a special very high speed memory used to increase the speed of processing by making current programs and a data available to the CPU at a rapid rate. Cache memory is similar to RAM, except that is extremely fast and used in a different way.

  When a program is running and the CPU needs data from the RAM, the CPU first checks to see whether the required data is in cache memory. If the data that it needs is not there, it reads the data from RAM into its registers but it also loads a copy of the data into cache memory. The next time the CPU needs the same data; it finds it in the cache memory and saves the time needed to load the data from RAM.

  Cache memory makes main memory appear to be faster and larger than it really is. It is very

expensive as compared to main memory and hence its size is normally very small.

- **Magnetic Core Memory:** This is the memory which uses small magnetic cores with wires running through then and electric current which flows through these wires, which generates magnetic field. Depending on direction of current and magnetic field, data is represented. But this form of memory is bulky; this problem has been overcome by newer technologies such as RAM and ROM.
- **Secondary Memory (Secondary Storage Media):** As the contents of RAM are temporary, if the data and programs are to be store permanently secondary memory is used. Floppy disks, magnetic tapes, CDs etc. are some of the secondary memory devices.
- **Bubble Memory:** This memory is non-volatile memory, but it not that widely used when compared to semiconductor memory (RAM and ROM) as it is expensive and slower. This memory is built on a thin piece of mineral garnet which produces bubble like areas and thus data is represented as presence or absence of these bubbles.

STORAGE DEVICES:

Secondary storage devices (Auxiliary Memory): This is a non volatile memory, which is external to a computer. It is a secondary media used for storing volumes of data permanently or long term. Apart from storing data permanently, the secondary storage devices are capable of storing volumes of data and instructions; the capacity of this secondary media in storage is for more than primary storage. Data from primary (main) memory takes beet the speed of accessing is slower than primary storage. Data from primary (main) memory takes just few non seconds for retrieval whereas it takes about few mili second for secondary storage. Virtually the size of secondary storage is unlimited it is even much cheaper than the main memory.

These secondary storage devices are external to CPU, they can be treated as peripheral device like any input/output device.

Features:

- **Permanent or non volatile storage:** The data which is stored in those devices is not lost when the power is switched off. The data is retained, which makes these devices more acceptable and useful.
- **Voluminous storage:** We can store volumes of data and instructions in these devices. This makes these devices very useful in almost every field where the data is bulky and voluminous.
- **Relatively cheaper:** These storage devices are relatively cheaper and cost effective than primary (main) memory of the CPU.
- **Computing capability:** These devices are not capable to handle any arithmetic and logic operations and neither executes a program. These are just storage devices.
- **Portable:** These devices act as portable media for transferring data from one system to other. The access to the data stored can be in serial order or random depending upon the type of secondary storage used.

The following are some of the commonly available categories of secondary storage devices.

(I) Magnetic Disks
- Fixed or Hard disks
  - Winchester
  - Cartridges
- Floppy disks

(II) Magnetic Topes

(III) Optical Disks
- Optical disk
- Optical card
- Optical tape

(IV) Modern Storage devices
- DVDs
- Pen drives OR flash drives
- External Hard disk drives
- Pocket Hard Drive

(I) Magnetic Disks:

Magnetic disk is the most popular storage medium for direct access secondary storage. A magnetic disk is thin, circular plate/platter made of metal or plastic, which is usually coated on both sides with

a magnetizable recording material such as iron oxide. Data are recorded on the disk in the form of tiny visible magnetized and non -magnetized spots (representing 1s and 0s) on the coated surfaces of the disk.

Magnetic disks can be erased and reused indefinitely. Old data on a disk are automatically erased as new data are recorded in the same area. However, the information stored can be read many times, without affecting the stored data.

The data can be accessed randomly from a disk, unlike magnetic tapes where data has to be accessed sequentially. These disks are capable to rotate at very high speeds of about 1860-3600 revolution per minute.

Principles (Storage Organization): For data recording, the surface of a disk is divided into a number of invisible concentric circles, called tracks. The tracks are numbered consecutively from outermost to innermost, starting from zero. The number of tracks varies greatly between disks.

Each track is further subdivided into sectors. There are eight such pie-shaped segments, each track will be divided into eight parts, and each of these eight portions of a track is called a sector.

Each sector of a disk is assigned a unique no. Before a disk drive can access a piece of data (a record) stored on a disk, it must specify the record's disk address. The disk address is comprised of the sector number, track number, and surface number (when double sided disks are used). That is, the disk address represents the physical location of the record on the disk.

Types of Magnetic Disks: All the magnetic disks are round and are coated with magnetic material. These disks come in various sizes. They can have varied storage capacities. These magnetic disks can be divided into the following broad categories.

(a) Floppy disks

(b) Fixed or hard disks

(a) Floppy disks: This is relatively new device used for secondary storage media for micro and mini computer system. This is small, flexible, faster and cheap alternative to storage using magnetic tape. This was developed in early 1970s, is one of the popular media for data storage.

It is also known as flexible floppy disk, diskette or floppy. The floppy disk is packed in protective paper or a plastic envelope.

Advantages:

- The data access is very fast.
- It can be re-used many times.
- No handing of bulky media.
- Moving files between computers that are not connected through communications hardware.
- Backing up data or programs.
- Loading new programs onto a system

Disadvantages:

- They are costly as compared to magnetic tapes.
- They are to be handled very carefully.

(b) Hard disks: Hard disks are the secondary storage device for most computer systems today. Unlike floppy disks, which are made of flexible plastic, hard disks are made of rigid metal (frequently aluminum).

Types of Hard Disks:

Winchester disks: These disks are made up of disk packs containing six or more disks each. The IBM developed it as a better way of storage and this technology enables greater precision of alignment, an increase in the number of tracks on the disk surface.

This disk is usually large. Any high capacity storage units which may be of any size if it sealed along with other devices are called Winchester disks. These disks are usually used in mini and personal computing (PC) systems.

The main difference between a Winchester disk and a disk pack is that Winchester disks are of fixed type. That is, the hard disk platters and disk drive are sealed together in a free container and cannot be separated from each other.

Removable Cartridges or Disk Packs:

Removable cartridges or disk packs refer to storage devices that consist of a collection of magnetic

disk platters housed within a protective cartridge. These were commonly used in older computer systems and mainframes, before the widespread adoption of smaller and more compact storage technologies like hard disk drives (HDDs) and solid-state drives (SSDs).

Characteristics of removable cartridges or disk packs:

- Physical Structure: A removable cartridge or disk pack typically contains multiple magnetic disk platters stacked on a spindle inside a protective casing or cartridge. The cartridge is designed for easy insertion and removal from the disk drive unit.
- Capacity: Each disk pack could hold several megabytes to tens or even hundreds of megabytes of data, depending on the size and number of disk platters. Compared to today's standards, their capacity was relatively small, but at the time, they offered significant storage capabilities.
- Use in Mainframes: Removable cartridges or disk packs were primarily used in large mainframe computers and minicomputers. They provided a convenient way to store and transfer large volumes of data between different systems or for backup purposes.
- Interchangeability: One of the advantages of removable disk packs was their interchangeability. Different systems from the same manufacturer or compatible models could often use the same type of disk pack, allowing for data interchange and system upgrades without requiring complete data migration.
- Access Speed: Access speeds for data retrieval from removable disk packs were significantly slower compared to modern HDDs or SSDs. This was due to the mechanical nature of the disk drives and the technology available at the time.
- Advancements and Decline: As technology progressed, the size and capacity of individual hard disk drives increased, while their physical size decreased. This led to the gradual obsolescence of removable disk packs as more compact and higher-capacity storage solutions became available.

Advantages of Magnetic Disks:

1) We can access data both sequentially and randomly.
2) We can update several online disk records by a single input transaction
3) It is re-usable, portable and easy to handle.
4) Accessibility: The magnetic disk provide for easy accessibility to the stored data. The time taken for the access is very less i.e. few milliseconds.
5) Long life: The disk has longer life than tapes; the data on the disk is less likely to be lost due to mishandling.
6) Due to its random access property, magnetic disks are often used simultaneously by multiple users as a shared device. A tape is not suitable for such type of usage, due to its sequential access property.
7) Data transfer rate for a magnetic disk system is normally higher than a tape system.

Disadvantage of Magnetic Disks:

1) It is bit costlier than magnetic tapes.
2) Data may be lost in case when new records are written on the disk or incase of drive failures.
3) Special backup procedures are to be adopted so that data can be protected.
4) The data is less secure than magnetic tape.
5) They must be stored in a dust free environment.

(II) Magnetic Tapes:

Magnetic tape is the most popular storage medium for large data, which are sequentially accessed and processed. These tapes are to be accessed serially i.e. we need to turn the tape till we get required point. It is same as playing an audio cassette in a tape recorder, i.e. whenever we like to hear a particular part, we need to either forward or rewind the tape. This tape is usually made of a plastic material known as Mylar. The deck is connected to the CPU permanently and the information stored into or read from the tape by processor.

Its widespread use is due to its high transfer rate (characters that can be read or written per second), storage density mass storage capability, and compact size and relatively low cost of operation.

The IBM magnetic tape sub system, for example, has transfer rate of three million characters, or bytes, per second, this is extremely fast. The magnetic tape medium is a plastic ribbon, which is

usually 1/2 inch or 1/4 inch wide, and 50 to 2400 feet long. Tape reels are used with mini computers and micro/personal computers.

The magnetic tape used in computer systems can be erased and re-used indefinitely. Old data on a tape is automatically erased as new data is recorded on the same area. However, the information stored can be read many times, without affecting the stored data.

These tapes have their own coding formats to store data. Usually magnetic tapes are divided into seven to nine tracks. The code which is used for 7 tracks tape is known as binary coded decimal (BCD). The 9 track arrangement is called "extended binary coded decimal interchange code (EBCDIC)".

Advantages of Magnetic Tape:

1) The tape is very easy and convenient to handle.
2) The tape is very economical i.e. it is reductively very cheap.
3) The tape is re-usable i.e. the tape can be erased and new data stored on it.
4) It is fast and saves time.
5) Large amount of data can be stored onto a small length of magnetic tape i.e. the high density of the tape allows us to store volumes of data in small areas.
6) The life of magnetic tape is very high, permitting long term storage.
7) Due to this compact size and light weight, magnetic tape reels are easily portable from one place to another. They are often used for transferring data and programs from are computer to another, which are not linked together.

Disadvantages of Magnetic Tape:

1) Humans cannot read the data directly as it is recorded as polarized magnetic particles.
2) Access being sequentially, searching becomes difficult.
3) It is sensitive to dust, temperature, moisture and other environmental factors.
4) Variations in density of tapes usually create problems as data cannot be read effectively by some tape drives.

(III) Optical Disks:

Optical Disks have been used for music videos and audio recording for some time. The optical disk is different from magnetic disk in the method used to record the data. The recording techniques most commonly used with optical disk prohibit new data from being recorded over the old.

An optical storage technique performs reading and writing operations by focusing laser became on the surface of spinning disk. A laser (light implication by stimulated emitted radiations) is a concentrated, narrow beam of light, focused and directed with lenses, prisms and mirrors. Due to the laser of laser beam technology, optical disks are also known as laser disks or optical laser disks.

The reading data from on optical disk is relatively simple while writing data again and again is not possible. A serious shortcoming of currently available optical disk systems is that they are permanents storage devices. Data once recorded, cannot be erased and hence the disk cannot be reused.

It is particularly suitable for the archival storage of data such as large business data bases, medical, legal other professional reference, libraries, music and videos, all reuse tremendous amount of data that is not normally altered. The storage density of optical disks is enormous the storage cost is extremely low, and the access time is relatively fast.

There are two types of optical technology:

(a) **CD-ROM:** CD-ROM stands for Compact Disk Read only Memory. It is a spinoff of music CD technology, and woks much like the music CDs used in music systems.

The CD-ROM disk is a shiny, silver color metal disk of 12 cm (5 ¼ inch) diameter. It has a storage capacity of about 650 MB. It is so called, because of its enormous storage capacity on a computer size disk and because it is a read only storage medium. That is, these disks come pre-recorded, and the information stored on them cannot be altered.

(b) WORM DISK: It stands for write once, read many. WORM disks allow the users to create their own CD-ROM disks by using a CD recordable (CD-R) drive, which can be attached to a computer as a regular peripheral device. WORM disks, which look like standard CD-RAM disks, are purchased blank and encoded using a CD-R drive.

As the name implies, data can be written only once on a WORM disk, but can be read many times. Once data has been etched on the surface of a WORM disk, it becomes permanent. Moreover,

writing on a WORM disk, cannot be done in multiple sessions, and all the data to be recorded have to be written on the disk surface in a single recording session.

Erasable Optical Disk: These are the disks which are erasable and can be re-used. These disks are bit expensive. We can use CD-writer to write into these CD's.

A new recording technique that combines optical and magnetic technologies has produced an erasable optical disk. This recording technique utilizes a laser beam to heat a minute spot on the surface of the disk.

Optical Card: These are similar to credit cards, in size and they have on optical laser encoded strip. These cards can store about 2 MB of data. These cards are becoming more and more popular with growing uses like storing credit records, medical histories. These cards can be used to replace all cash transactions as well as cheque transactions, these by moving towards cashless environment. This is done by storing all the transactions on cards and updating the financial status for every transaction.

Some of the users can be tracking medical histories, bank transactions, academic performance, etc.

Optical Tape: This is quite similar to the magnetic tape in looks, the difference being that the date is stored using optical technology. These tapes come in cassettes, and can store about 8 Giga bytes (GB). These tapes are read by using optical take drives; these drives are capable of holding about 128 cassettes. These tapes are also read only as other optical storage devices.

Advantages of Optical Disks:

1) The cost per bit of storage for optical disks is very low, because of their low cost and enormous storage density.
2) Optical disks are more reliable storage medium than magnetic tapes or magnetic disks.
3) Optical disks have a data storage life in excess of 30 years. This makes them a better storage medium for data archiving as compared to magnetic tapes or magnetic disks.
4) Since data once stored on optical disk becomes permanent, the danger of stored data getting erased or overwritten is not there with optical disks.
5) Due to their compact size and light weight, optical disks one easy to handle, store and port from one place to another.

Disadvantages of Optical Disks:

1) The data access speed for optical disks is slower than magnetic disks.
2) It is a read only (permanent) storage medium. Data once recorded, cannot be erased, and hence, the optical disks cannot be re-used.
3) Optical disks require a more complicated drive mechanism than magnetic disks.

(IV) Modern Storage Devices:

Let us look into some of modern storage devices.

(a) DVDs: DVD was originally used as an abbreviation for "Digital Video Disk" since the DVDs were first used for storing movies and video. DVDs today are also commonly known as "Digital Versatile Disk" owing to the fact that a DVD is used today to store just not movies but almost any data, which has to be stored digitally. The storage capacity of a DVD disk is quite high, which can store up to 4-7 GB on a single layer disk and 8.5 GB on a dual layer disk.

A DVD is similar in design and appearance to a CD but the differentiating factor is that the DVDs have a much higher capacity for holding data. DVDs are also available in double sided as well. One has to have a DVD reader/writer to work with the DVDs.

(b) Pen Drives/Flash Drives: A pen drive or a flash drive is a small and portable storage device, which does not have any moving parts, like a hard drive. These drives are very flexible and are usually plug and play devices, which connect to the computer with the help of an built in USB port. The storage capacity is highly flexible; it ranges from almost 16 MB to as high as 64 GB and more.

These drives can be written and re-written to an almost unlimited number of times. These are used to quickly transfer audio, video and data files from the hard drive of one computer to another. The size being quite small which fits into a pocket. These drives are an improvement on both the older floppy drive disks and the more modern compact disks are often used to copy data and reload the files on.

One can store any type of data, may it be photos, spreadsheets, word documents, movie clips, music tracks, and any other type of file.

(c) External Hard Disk Drives: An external hard disk drive refers to a hard drive disk which is outside the computer cabinet. These drives are outside computer and are highly portable and secure

devices since one can store them under lock and key. They are slightly bigger is size than the hard drive itself.

These external hard drives can be connected to the computer system with the help of single high speed interface cable, and these devices are like pen drives, which are also plug and play and can be connected using interface such as USB.

(d) Pocket Hard Drive: These are the handy external hard drives, which are mini external hard drives, which one can easily carry in his pocket, which gives it the name "Pocket Hard Drive". Pocket hard drives take the best of the traditional hard disk storage with the convenient sizes and USB connections.

These devices are a bit larger than the flash drives; they are still convenient for storing and transferring large amounts of data without much hassle, which makes them one of the popular storage devices. Pocket hard drives usually have a capacity of many Gigabytes.

Note: Computer based training **(CBTs)** has become one of the most popular ways of self learning, where each and every step is given in sequential order, so that one can self learn the concepts easily using the graphical interface, which simulates the real time learning process. This is usually done using CDs.

Questions:

1. Discuss computer languages in detail.
2. Compare and contrast the computer languages.
3. What do you mean by language translator? Explain the language translators in detail with suitable example.
4. What is software? Discuss the types of software with suitable examples.
5. Discuss memory management in detail.

Unit-III
OPERATING SYSTEM

4.1 OPERATING SYSTEM

An operating system is a software program that acts as an intermediary between computer hardware and user applications. It provides essential services and manages resources such as memory, processors, storage devices, and input/output devices. The operating system enables users to interact with the computer through a user interface, which may include graphical user interfaces (GUIs) or command-line interfaces (CLIs). Its primary functions include managing the execution of programs, facilitating communication between hardware components and software applications, and providing a platform for running various types of software. Additionally, the operating system handles tasks such as file management, security, multitasking, and device driver management. Overall, the operating system plays a crucial role in enabling computers to function efficiently and providing users with a seamless computing experience.

All computers must have an operating system used for starting the computer and to run other programs. It provides an interface between a user of a computer and the computer hardware.

Operating system perform basic tasks, such as recognizing input from keyboard, sending output to the display screen, keeping track of files and controlling peripheral devices such as printers.

The operating system is also responsible for security, ensuring that unauthorized users do not access the system. It is like a traffic cop, it makes sure that different program and users running at the same

time do not interferes each other.
So, it can be concluded that An operating system (OS) is software that manages computer hardware and provides a user interface. It facilitates communication between software and hardware components, allocates system resources, and coordinates tasks. Operating systems come in various types, including real-time, multi-user, and embedded systems, tailored to different computing needs. They serve as the backbone of computing devices, enabling efficient and seamless operation

4.2 FUNCTIONS OF OPERATING SYSTEM

The operating system performs a variety of essential functions to manage computer resources and facilitate user interactions. Some of the key functions of an operating system include:
Process Management: The OS manages processes, which are instances of running programs. It allocates resources to processes, schedules their execution on the CPU, and facilitates communication and synchronization between processes.

- **Memory Management:** It manages system memory, allocating memory space to processes, and ensuring efficient use of available memory. This includes virtual memory management, which allows the OS to use secondary storage (such as hard drives) as an extension of RAM.
- **File System Management:** The operating system manages files stored on storage devices such as hard drives, solid-state drives, and network storage. It provides functions for creating, deleting, reading, and writing files, as well as organizing them into directories or folders.
- **Device Management:** This involves managing input and output devices such as keyboards, mice, printers, and network interfaces. The OS controls device communication, handles device interrupts, and provides device drivers to facilitate interaction between software and hardware components.
- **User Interface:** The operating system provides a user interface that allows users to interact with the computer system. This can include graphical user interfaces (GUIs) with windows, icons, menus, and pointers, as well as command-line interfaces (CLIs) where users type commands to perform tasks.

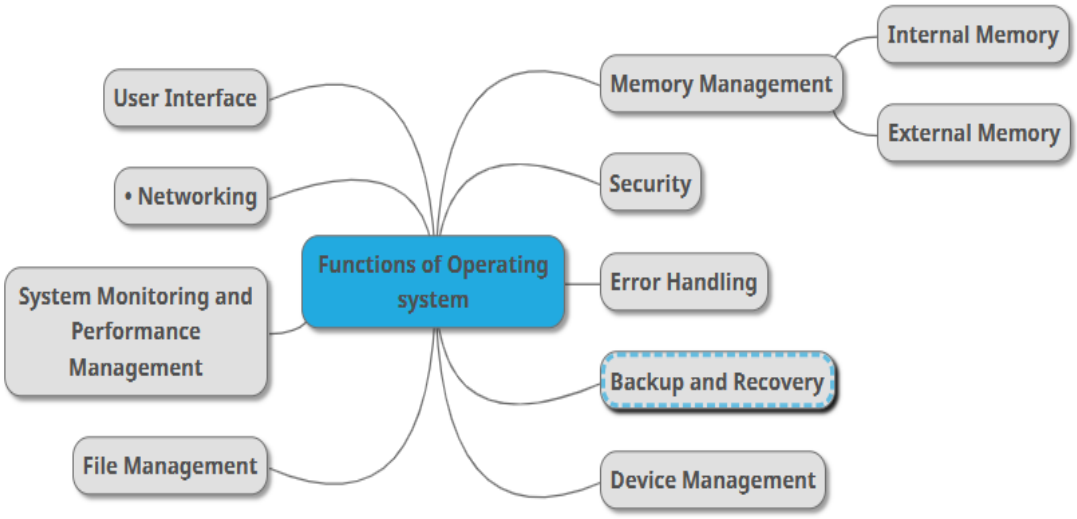


Figure4.1: Functions of Operating system

- **Security:** OS ensures system security by controlling access to system resources, enforcing user authentication and authorization, and implementing security mechanisms such as encryption, firewalls, and antivirus software.
- **Networking**: It provides networking capabilities, allowing computers to connect to networks and communicate with other devices over local area networks (LANs), wide area networks

(WANs), and the internet. This includes managing network protocols, configuring network settings, and supporting network services.

- **Error Handling:** The operating system handles errors and exceptions that occur during system operation, such as hardware faults, software crashes, and user mistakes. It may provide error messages, log events, and attempt to recover from errors to ensure system stability and reliability.
- **System Monitoring and Performance Management:** OS monitors system performance, resource usage, and system health. It provides tools for administrators to monitor system activity, diagnose performance issues, and optimize system performance through tasks such as tuning resource allocation and adjusting system settings.
- **Backup and Recovery:** The operating system facilitates backup and recovery processes to protect data from loss or corruption. It may provide built-in backup utilities or integrate with third-party backup solutions to create backups of files, applications, and system configurations, and restore them in case of data loss or system failure.

These functions collectively enable the operating system to manage computer resources efficiently, provide a platform for running applications, and facilitate user productivity and interaction with the computer system.

4.3 TYPES OF OPERATING SYSTEM

Types of operating systems provides a framework for understanding the diverse range of operating systems and their respective functionalities and applications.The following are the types of operating systems:

1. **Batch Processing Operating Systems:**
   Name of Operating system: IBM OS/360, IBM z/OS, UNIVAC EXEC I
2. **Multiprogramming Operating Systems:**
   Name of Operating system: IBM MFT/MVT, IBM VM/370, CDC Kronos
3. **Time Sharing Operating Systems:**
   Name of Operating system: Unix (Various flavors like Linux, FreeBSD, macOS), Windows (Various versions like Windows 10, Windows Server), IBM TSS/360
4. **Multiprocessing Operating Systems:**
   Name of Operating system: Windows NT, Linux (supports multiprocessing), Unix variants like Solaris and AIX.
5. **Network Operating Systems:**
   Name of Operating system: Novell NetWare, Windows Server, Linux distributions configured for server use (e.g., Ubuntu Server, CentOS).
6. **Real-Time Operating Systems:**
   Name of Operating system: VxWorks, FreeRTOS, QNX,

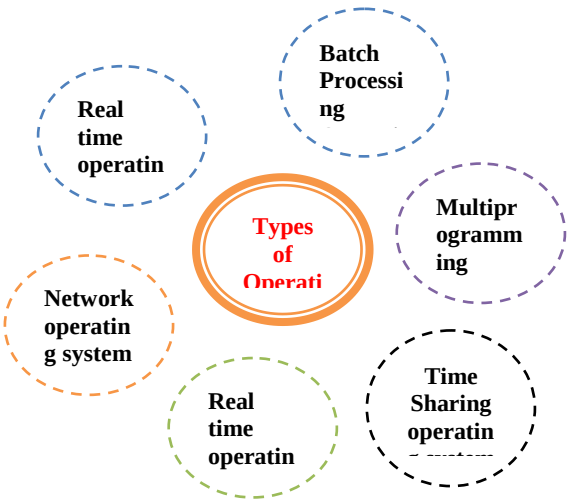


Figure 4.2: Types of Operating System

1. Batch Processing Operating System: In earlier computers, the users did not interact directly with the system, instead, a user prepared a job, which consisted of program, data and some control information about the nature of the job and submit it to the computer operator.

This method of job execution was known as manual loading mechanism because the jobs had to be manually loaded one after another by the computer operator in the computer system. In this method, job to job transition was not automatic.

The manual transition from one job to another caused lot of computer time to be wasted since the computer remained idle while the operator loaded and unloaded job and prepared the system for a new job.

In new method, known as a batch processing system, when one job is finished, the system control is automatically transferred back to the operating system which automatically performs the other jobs (such as clearing the memory to remove any data remaining from previous job) needed to load and run the next job.

Jobs in the batch processing operating system executed in the following manner:

i. Programmers would prepare their programs and submitted them to the computer operator at computer centre.
ii. The operator would periodically collect all the submitted programs and would batch them together and then load them all into the input devices of the system at one time.
iii. The operator would give a command to the system to start executing the jobs.
iv. The jobs then automatically loaded from the input device and executed by the system one by one without any operator intervening.
v. Then all the jobs in the submitted batch were processed the operator would separate and keep the printed output of each job at the reception courts for the programmers to collect them later.

Advantages:

i. The batch processing mechanism helped in reducing the idle time of a computer system because transition from one job to another did not require any operator intervening. It avoids idling the computing resources.
ii. It allows sharing of computer resources among many users and programs.

Disadvantages:

i. While the jobs were collected, the CPU is left idle and wasting its potential.
ii. Once the processing starts, the system processes efficiently without wasting time and user intervention but till the processing starts jobs has to wait and this effects the turnaround time as the job has to wait till it is completed.

Batch processing is also known as serial sequential, off-line or stacked job processing.

2. **Multiprogramming Operating System:**Multi programming operating system is the name given to the execution of two or more different and independent programs by the same computer. It is an efficient way to improve the system performance. Multi programming approach permits more than one job to utilize the CPU time at any moment by applying the scheduling technique like first come first serve, shortest job first etc. The more the number of programs requesting for system resources, utilization would be better. The operating system picks up any of the programs as scheduled and starts execution.

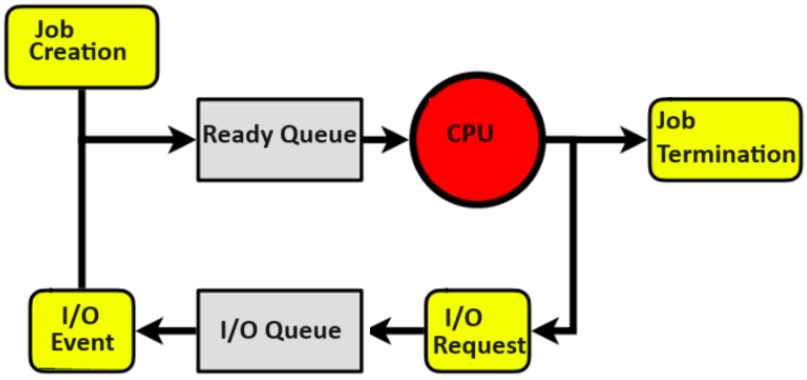


Figure4.3: Logical diagram of Multiprogramming Operating System

The CPU is capable of executing only one instruction at a time. Hence at any given time only one of the programs has control of the CPU and is emerging instructions. (Simultaneous execution of more than one program with single CPU is impossible in the diagram job a is not utilizing the CPU since it is busy writing output data on to disk (I/O operation). Hence CPU is being utilized to execute job B which is also present in the main memory. Job C also residing in the main memory is waiting for the CPU to become free.

Advantages of Multiprogramming:

- Increased through put
- Shorter response time
- Ability to assign priorities of jobs.
- Improved primary storage allocation.

Disadvantages of Multiprogramming:

- Large main memory
- Proper job mix
- CPU subduing

3. **Time Sharing operating system**: The sharing is a technique of allocation of computer resources in a time dependent fashion to several programs simultaneously. It helps to provide a large number of user's direct access to the main memory. Time sharing provides indication with computer system by many users in such a way that each is given the impression that he/she has his/her own computer.

The special CPU scheduling used in a time sharing system allocates a very short period of CPU time one by one to each user process beginning from the first user process and proceeding through the last one and again beginning from the first one. The short period of time during which a user process gets the attention of the CPU is known as time slice" "time slot" or" quantum. It is very from 10 milliseconds to 100 milliseconds. When the CPU is allocated to a user process the user process will use the CPU unit the allotted time expires or until the process needs to per from some I/O operation.

These real-time operating systems are designed to meet strict timing requirements and provide predictable behavior, making them essential for applications where timely processing and response are critical, such as control systems, medical devices, and industrial automation.

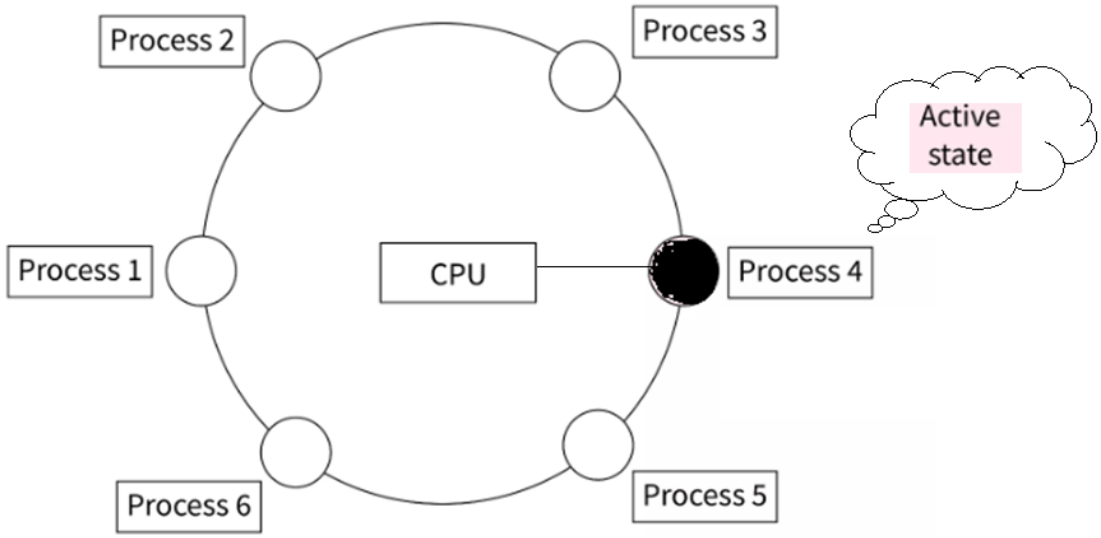


Figure4.4: Time Sharing operating system

Advantages of Time Sharing Operating System

- Effective utilization and sharing of resources
- Reduces CPU idle time.

- Since time slice is of few milliseconds users can get the output of programs move quickly in comparison on other models which are expensive also

Disadvantages of Time Sharing Operating System

- Security
- Data transmission charges are very high in comparison to other methods.
- Since regular soaping needs to done. This results in poor response.

4. **Multiprocessing operating system**: In a multiprogramming system executes more than one program using a single CPU. But in Multiprocessingoperating system unlike multiprogramming one program is processed by more than one CPU.

A multi processing operating system allows a program to run on more than one central processing unit (CPU) at a time. If one of the CPU breaks down the other CPU will automatically takes over its job. The instructions are executed simultaneously because the available CPU's can execute different instructions of the same program or different program at any given time. Multi processing data processing capabilities are not present when only one CPU is used. Many complex operations can be performed at the same time.

In multiprocessing instructions from different and independent programs can be processed simultaneously by different CPU's or the CPU's may simultaneously execute different instructions from the same program.

Multiprocessingsystems are of two types

- Tightly coupled system: There is a single system-wide primary memory which is shared by all the processors.
- Loosely coupled systems: The processors do not share memory and each processor has it's won local memory.

Advantages of Multiprocessing:

- Improves performance
- Provides backup

Disadvantages of Multiprocessing

- A large amount of main memory is required.
- Use of multiple CPU's makes it is very expensive

5. **Network operating system**: A network operating system is a software that runs on a server and enables the driver to manage data users groups security applications and other networking functions. NOS is based on a client/server architecture in which a server enables multiple clients to share resources.

NOS (Network operating system) typically are used to run computers that act as servers. They provide the capabilities required for network operations. Network operating systems provide the following functions:

- Account administration for users
- Security.

Characteristics of Network Operating System:

- Secure access to a network
- Allow users to connect to a network like the internet
- Allow for simple additions of clients and resources.
- Back up data and make sure it is always available.
- Monitor the status and functionality of network elements.
- Online Processing Operating System.

In an online processing operating system, the processing is performed under the direct control of the CPU white at the same time the user remains in the communication with the computer.

The systems which play online processing need high-capacity memory so that user data operating system elements and programs can be stored and accused quickly.

Online processing systems perform random and rapid input of transactions and provide immediate access to the records. Each user is provided direct access to the CPU on time sharing basis only a little CPU time is needed for each user.

6.**Real time operating system**: A read time operating system is a multitasking operating system that aims at executing read time applications. The main objective of read time operating system is their

quick and predictable response to events. They have an event driven or time sharing design and often aspects of both.
An event driven system switches between tasks based on their priorities. An external events while time sharing operating system switch tasks based on clock interrupts.

A real time operating system responds to input instantly. They are designed to handle events as they occur. General purpose operating system such as DOS and UNIX are not real time because they can take a few seconds or even minutes to read "Lynx" is an example of a real time operating system.

4.4 TURNING ON A COMPUTER

"Turning on a computer" refers to the process of starting up a computer system from a powered-off or standby state. This involves supplying power to the computer's components, initiating the boot-up sequence, and loading the operating system into memory so that the user can interact with the computer and perform tasks such as running applications, accessing files, and connecting to the internet. Turning on a computer is typically done by pressing the power button.Turning on a computer is usually a straightforward process. Here are the general steps:

- *Plug in the Power:* Make sure your computer is plugged into a power source. This could be a wall outlet or a surge protector.

- *Press the Power Button:* Locate the power button on your computer case or laptop. It's usually located on the front panel of a desktop computer or on the side or back of a laptop. Press this button to turn on the computer.

- *Wait for Boot-up:* After pressing the power button, your computer will start the boot-up process. This involves loading the operating system (like Windows, macOS, or Linux) into memory and initializing hardware components.

- *Login (if required):* Depending on your computer's settings, you may need to enter a username and password to access the system. This is typical for user accounts with password protection.

- *Desktop Interface:* Once the boot-up process is complete and you've logged in (if required), you'll be greeted by the desktop interface of your operating system. From here, you can start using your computer for various tasks.

- *Shutdown/Restart:* When you're finished using your computer, it's important to shut it down properly to avoid data loss and to conserve power. You can do this by selecting the shutdown or restart option from the operating system's menu.

The very first step is to turn on the computer. Make sure all the cables are plugged in correctly. and locate the power button. Press the power button symbol

Once turned on, your computer takes time before it's ready to use. You may see a few different displays flash on the screen. This process is called booting up, and it can take anywhere from 15 seconds to several minutes. Once the computer has booted up, it is ready to use.

You interact with a computer mainly by using the keyboard and mouse, or a trackpad on laptops. The keyboard allows you to type letters, numbers, and words into the computer Whenever you see a flashing vertical line called the cursor you can start typing. The mouse controls the pointer on the screen. Whenever you move the mouse across the desk, the pointer will move in a similar manner. A mouse usually has two buttons, which are referred to as the left button and the right button. You will often interact with the computer by moving the mouse pointer over something on the computer screen, then clicking one of the buttons.

Turning off a computer

Click the Start button, then the Power icon, then click Shut down.

Restarting mode

If your computer has become unresponsive, you can choose Restart to quickly turn it off and on agam.

Sleep mode

You can also choose to put your computer into sleep mode. This turns off most of your computer's processes, but it remembers which applications and files are open. It allows the computer to start up more quickly because you won't have to wait for the operating system and applications to load. Note that your computer may go into Sleep mode automatically if you haven't used it for more than a few minutes.

To wake the computer from Sleep mode, click the mouse or press any key on the keyboard.

4.5 COMPUTER DRIVERS

A driver is a program that enables communication between an operating system and a hardware component or software application. Every computer uses multiple drivers to control the various installed hardware components and software applications.

Without these drivers, the hardware and software will not function properly, and in some cases may not be able to function at all.

Operating system sends some files to hardware component or software application to instruct them on how to function. These files are known as drivers.

There are two primary types of drivers: device drivers and software drivers.

Device driver: Device drivers are designed to communicate between an operating system and a device. Some devices which require drivers are: printers, scanners, digital camera, modems, card readers etc. Without device drivers, the computer could not send and receive data correctly to hardware devices, such as a printer, scanner etc.

Software driver: Software drivers are designed to communicate between an operating system and software applications. Software drivers only associated with software applications not hardware components. The main purpose behind software drivers is to enable or disable access to protected data.

4.6 TASKBAR

The taskbar is a graphical user interface (GUI) element present in various operating systems, including Microsoft Windows and some Linux desktop environments. It typically appears as a horizontal bar located at the bottom of the screen, although its position can be customized in some systems.

Features of Taskbar:

- *Program Launching:* The taskbar often includes a section for pinning frequently used applications. Users can click on these icons to quickly launch their favorite programs without navigating through menus or searching for shortcuts.

- *Window Management:* When multiple applications or windows are open, the taskbar displays icons or thumbnails representing each open window. Users can click on these icons to switch between windows or bring a particular window to the foreground.

- *System Tray:* The taskbar usually includes a section known as the system tray or notification area, located on the far right. This area displays system icons representing active processes, background services, and system notifications. Users can interact with these icons to adjust system settings, view notifications, or access running applications.

- *Start Menu:* In Windows operating systems, the taskbar typically incorporates the Start button, which provides access to the Start menu. The Start menu allows users to search for files, launch applications, access system settings, and shut down or restart the computer.

- *Customization:* Users can customize the appearance and behavior of the taskbar according to their preferences. This may include changing its size, position, color, and transparency, as well as adding or removing specific features such as the system tray or Cortana search bar (in Windows).

Overall, the taskbar serves as a central hub for launching applications, managing open windows, and accessing system-related functions, providing users with convenient access to essential features and enhancing their overall productivity and user experience.

4.7 BOOTING UP

Booting up, also known as booting, is the process of starting or initializing a computer system. When you turn on a computer or restart it, the boot process begins, during which the computer's hardware and software components are activated and initialized to prepare the system for use.
During the booting up process, the computer undergoes several steps, including a power-on self-test (POST), initialization of hardware components, execution of the boot loader program, loading of the operating system into memory, and finally presenting the user with a login screen or desktop environment.
In simpler terms, "booting up" refers to the time it takes for a computer to go from being powered off to being fully functional and ready for the user to interact with it. This term is commonly used in everyday language to indicate the process of starting a computer. Here's a basic overview of the boot process:

- *Power-On Self-Test (POST):* When you turn on a computer, the hardware components (such as the processor, memory, and storage devices) undergo a self-diagnostic test called the POST. This test checks for hardware errors and ensures that essential components are functioning correctly. If any issues are detected during the POST, the computer may display error messages or emit audible alerts.

- *Initialization of Hardware Components*: Once the POST completes successfully, the computer's hardware components are initialized. This includes identifying and configuring devices such as the CPU, RAM, storage drives, graphics card, and peripherals like keyboards and mice.

- *Boot Loader Execution:* After the hardware initialization, the system loads the boot loader program. The boot loader is responsible for loading the operating system (OS) into memory from the storage device (typically a hard drive, solid-state drive, or network location). In systems running Windows, the boot loader is often the Windows Boot Manager or NTLDR (for older versions). In Linux systems, GRUB (Grand Unified Bootloader) is commonly used.

- *Operating System Initialization:* Once the boot loader loads the operating system into memory, the OS begins its initialization process. This involves loading essential system files,

initializing device drivers, and configuring system settings. The operating system then presents the user with a login screen or desktop environment, indicating that the boot process is complete.

- *User Interaction:* Finally, the user can interact with the computer through the operating system's user interface, launching applications, accessing files, and performing various tasks.

The booting process may vary slightly depending on the computer's hardware configuration and the operating system installed. In modern computers, especially those with solid-state drives (SSDs), the boot process can be very fast, often completing in a matter of seconds.

4.8 DESKTOP

A desktop computer, often simply referred to as a "desktop," is a personal computer designed to be used at a single location, typically a desk or table. It consists of separate components, including a central processing unit (CPU), monitor, keyboard, mouse, and often other peripherals such as speakers and printers. Unlike laptops or tablets, which are portable and compact, desktops are stationary and offer greater performance and customization options.

The term "desktop" can refer to both the physical hardware and the graphical user interface (GUI) environment provided by the operating system. In the context of hardware, a desktop computer typically comprises a tower or chassis housing the CPU, motherboard, RAM, storage drives, and other internal components. These components are connected to an external monitor, keyboard, and mouse for user interaction.

Desktop computers are commonly used for a wide range of tasks, including productivity work (such as word processing, spreadsheet management, and presentations), multimedia consumption (such as watching videos, listening to music, and viewing photos), gaming, programming, graphic design, video editing, and more. They are favored by users who prioritize performance, customization, and expandability over portability.

Once your computer has started, the first thing you'll see is the desktop. Desktop is the main workspace for your computer. From here, you can view and manage your files, applications access the Internet, and much more.

Customize desktop background: Image appears behind the icons on the computer's desktop is known as wallpaper or desktop background. We can change the desktop background by right-clicking the desktop and selecting personalize.

Select Background. By default, you'll see the images that were included with your computer. When you find an image you like, just select it and choose view image. Then click and drag the picture to your desktop. You can now set the image as your desktop background.

4.9 ICONS

An icon in computing refers to a small graphical symbol or image that represents an object, action, or concept on a computer's graphical user interface (GUI). Icons are used extensively in various software applications, operating systems, websites, and digital interfaces to visually communicate information and interact with users.

Here are some key points about icons:

- *Visual Representation:* Icons are visual representations of objects, such as files, folders, applications, or system functions. They convey meaning through graphical symbols, making it easier for users to understand and interact with digital content.
- *Simplification:* Icons simplify complex concepts or commands by using graphical symbols instead of text-based descriptions. This simplification enhances usability and makes interfaces more intuitive, especially for users who may not be familiar with technical terminology.

- *User Interaction:* Icons are interactive elements that users can click, tap, or interact with to perform actions. For example, clicking on an application icon launches the corresponding program, while clicking on a file icon opens the file in the associated application.
- *Consistency:* Icons often follow design standards and conventions to ensure consistency across different applications and platforms. Standardized iconography helps users recognize familiar symbols and understand their meaning, even when using different software or operating systems.
- *Customization:* Users can often customize icons by changing their appearance, arrangement, or functionality to suit their preferences. For example, users can rearrange icons on a desktop, change icon sizes or styles, or create custom icons for specific applications or tasks.
- *Accessibility:* Icons play a crucial role in making digital interfaces accessible to users with disabilities. They can be designed with contrasting colors, distinct shapes, and descriptive labels to improve visibility and usability for users with visual impairments or cognitive disabilities.

Icons are used to represent the different files, applications, and commands on your computer. An icon is a small image which gives you an idea about what file represents. Double-clicking an icon on the desktop will open that file or application.

Icons help users to quickly identify the type of file. For example: the recycle bin is represented by the image of a small trash bin.

Steps for Changing the Icon: Right-click on a program icon, select Properties, go to the shortcut tab, and click the "change icon" button. Some programs include a number predefined icons you can choose from, or you can select any other icon you have stored on your computer. Click the icon that you want to use, click OK, and then click OK.

Overall, icons are fundamental elements of graphical user interfaces, enhancing usability, accessibility, and user engagement in computing environments. They provide a visual language that helps users navigate, understand, and interact with digital content more effectively.

4. 10 FILES

A file is an object on a computer that stores data, information, settings, or commands used with a computer program.

Computer files are stored on a drive (eg.. the hard drive), dise (e.g., DVD), and a diskette (e.g., floppy disk) and may be in a folder (directory) on that medium.

There are three types of files:

Application files: An application file is used to describe a file that a program puts on a computer after it gets installed. They're more often called program files and might use the EXE file extension.

Data files: A data file is any file containing information, but not code; it is only meant to be read or viewed and not executed. For example: text file, letter written in a word processor

System files: A file critical to the proper function of an operating system which, if deleted or modified, may cause it to no longer work. Often these files are hidden and cannot be deleted because they are in use by the operating system.

File Extension: A file extension or file name extension is the ending of a file that helps to identify the type of file. File extension is often followed by three characters. For example, the file name "myfile.txt" has a file extension of ".txt," which is a file name extension associated with text files.

There are thousands of file extensions associated with one or more applications.

File type

Text

File extension

Image

asc .doc .docx .rtf.msg, .pdf .txt .wpd.wps

Sound

bmp.eps gif.jpg .pict.png.psd .tifaac au mid mp3 rasnd wma wav

Video

avi.mp4 .mpg .mov.wmv

Program

bat.com.exe

Compressed

arearjgzhqx .rar sit tar z zip

Web page

.htm, .html

You can convert a file in one format into a different format. For example, an MP3 audio file can be converted to M4R so that an iPhone will recognize it as a ringtone file.

File Path: A file path is the location of a file based on a computer's file system. There are two types of file path: First one is absolute file path which contains the root directory and include the volume, directory, and file name. Second one is relative file path which list only part of the entire file path.

PDF File: Portable document format file is one of the most used file types today. Whenever you see a file that ends with .pdf that means it's a PDF file.

We can open, edit, and convert PDFs in Adobe Acrobat Reader and other PDF readers. Manuals, eBooks, and other documents come in this format, which holds images, text, and other elements.

Need of PDF Files:

Word documents are meant to be edited, there's a chance that some of the formatting and text in your document may be shifted around. But PDF files are primarily meant for viewing, not editing. One reason they're so popular is that PDFs can preserve document formatting, which makes them more shareable and helps them to look the same on any device.

Creating PDF Files: There are several ways to create PDF files, but the method will largely depend on the device

you're using. We can go to the Print dialog box, and then select PDF from the list of printers at

the top. This allows in creating a PDF of anything.

The simplest method is to use software that supports a PDF export, such as Microsoft Office or Google Chrome.

4.11 FOLDERS

A folder helps in organizing files. We can put files inside a folder.

Basically, a folder or directory is a collection of files. Files that contain text are often called documents.

A directory (folder) is an area on the computer containing other directories and files and helps keep the computer organized. A folder holds

one or more files, and a folder can be empty until it is filled. A folder can also contain other folders, and there can be many levels of folders within folders. Folders are created on the hard drive or solid state drive when the operating system and applications are installed. Files are always stored in folders. In fact, even the computer's desktop is a special kind of folder that displays its contents across the screen

4.12 FILE EXPLORER

You can view and organize files and folders using a built-in application known as File Explorer or Window Explorer.

To open File Explorer, click the File Explorer icon on the taskbar, or double-click any folder on your desktop. A new File Explorer window will appear. Now we can start work with your files and folders.

After double-click on a folder, we can see all of the files stored in that folder.

We can also see the location of a folder in the address bar near the top of the window.

To open a file:

There are two main ways to open a file:

Find the file on your computer and double-click on it.

OR

We can go to the File menu at the top of the window and select Open.

To move a file:

It's easy to move a file from one location to another.

1. Click and drag the file to the desired location.

2. Release the mouse. The file will appear in the new location.

To create a new folder:

1. Right-click where we want the folder to appear, then select New Folder.

2 The new folder will appear. Type the desired name for the folder and press Enter.

To rename a file or folder:

1. Right-click on the file or folder, then select Rename from the menu that appears. 2. Type the desired name on your keyboard and press Enter. The name will be changed.

To delete a file or folder:

1. Right-click on the file or folder, then select delete from the menu that appears. File w

delete. When you delete a file, it is moved to the Recycle Bin. If you change your min you can move the file from the Recycle Bin back to its original location.

2. To permanently delete the file, right-click the Recycle Bin icon and select Empty Recycc Bin. All files in the Recycle Bin will be permanently deleted.

Selecting all files:

If you want to select all files in a folder at the same time, press Ctrl+A. All of the files in the folder will be selected.

4.13 START MENU

Menus are organized collections of commands and shortcuts. Click a menu to open it. Commands and shortcuts are displayed within the menu. If you want to execute any item displayed in the menu, then just click that item.

Start menu is the important feature in the Windows. Start menu is used to open apps and commonly used folders. We can customize the Start menu according to our needs.

To open a program using the Start menu:

1. Click Start

2. Click All Programs, and slide your mouse pointer until you've selected the program you want to open.

3. Click to open the program you've selected.

4. To close a program, click the X button located at the top-right of the window.

4.14 WINDOW EXPLORER

Windows Explorer is a file management tool that helps you to create, rename, and move folders. It also allows you to copy, print, move, delete, and rename files.

To open Windows Explorer:

1. Click Start.

2. Choose Programs, Then Click Windows Explorer.

3. A list of folders appears in the left pane.

4. Scroll until you see the Control Panel icon in the left pane.

5. After viewing the contents, close the Windows Explorer window.

4.15 MY COMPUTER

My Computer icon on the desktop is another tool used to manage files on the computer. We can create, rename, and move folders and copy, print, move, delete, and rename files with this tool. We can also access to other system tools such as printers.

To open My Computer:

1. Double-click the My Computer icon on the desktop.

2. A list of the folder's content appears: your local drives, printers, and Control Panel folders

3. After viewing the contents, close the window.

Note: Windows Explorer is more text-based, while My Computer is more picture-based,

4.16 WINDOW

Windows makes it possible to complete all types of everyday tasks on your computer. The rectangular work area for an application, folder, file, or other task is called a window.

When you open an application or folder, it is displayed in its own window. Whenever you open a file, folder, or application, it will appear in a new window. A window has its own menus specific to that program. We can rearrange multiple windows at the same time on the desktop and switch between them. We are using window all the time. It is important to know how to switch between open windows, how to move and resize windows, and how to close windows after using them.

Parts of the window:

There are three buttons in the upper-right corner of almost every window. These buttons allow us to perform several functions, including these below.

Minimize Button: Click the Minimize button to hide the window. The window will be minimized to the taskbar. You can then click the icon for that window on the taskbar to

make it reappear. Maximize Button: Click the Maximize button to make the window fill the entire screen.

Restore Button: If the screen is maximized, the Maximize button will be temporarily replaced by the Restore button. Just click it to return the window to its original size.

Close Button: Click the Close button to close the window.

4.17 RECYCLE BIN

Recycle Bin is a folder or directory where deleted items are temporarily stored in Windows unless they are permanently deleted. The Icon of Recycle Bin is wastebasket.

When we delete any file, it does not remove permanently from the system. The deleted file goes to Recycle Bin. The files cannot be used directly while they are in the Recycle Bin. We have to recover files first to use them. We can restore that deleted file from Recycle Bin if necessary. The files in the Recycle Bin are restored to their original location. If a file is deleted from the

Recycle Bin, it is permanently deleted and cannot be recovered. If we want to prevent to go files in the Recycle Bin and delete files permanently, and then use a shortcut key Shift + delete the key from the keyboard.

To move an item to the Recycle Bin:

1. Right click on the File or Folder which you want to delete.

2. When the pop-up menu appears. Choose Delete option. Click Yes. OR

Drag the file or folder to the Recycle Bin.

Retrieving an item from the Recycle Bin:

1. Double-click on the Recycle Bin. Right click on the File or Folder which you

want to restore. 2. Choose Open Restore, Click Ok.

OR

Double-click on the Recycle Bin, and drag the file or folder onto the desktop.

To permanently delete all files or folder from the Recycle Bin:

1. Right click on the Recycle Bin.

2. Press the Empty Recycle Bin option.

To permanently delete one or few files or folders from the Recycle Bin:

1. Double-click on the Recycle Bin. Right click on the File or Folder which you want to permanently delete.

2. Press ok.

4.18 UNDO & REDO

UNDO:

Undo is a function performed to reverse the action of an earlier action. It erases the last change done to the document, reverting it to an older state. We can undo many times but depends on the program we are using.

The Undo function is most commonly found in the Edit menu.

We can click Undo on the Quick Access Toolbar also. Press Undo repeatedly if want to undo multiple

steps.

Ctrl+Z is a common keyboard shortcut for Undo.

Note: If you make changes and then close the document or program, any changes that were made earlier cannot be undone.

REDO:

The opposite of undo is redo. The redo command reverses the undo or advances the buffer to a more recent state.

Redo function will undo your last undo. If we have used Undo but then realize we didn't want to Undo the most recent change, then use Redo, Redo will restore it.

For example: we undo but after sometimes we realize there was no requirement of undo and you want previous changes then you use redo. Redo reverses the undo.

Click Redo on the Quick Access toolbar.

Ctrl+Y is a common keyboard shortcut for Redo.

4.19 SHORTCUTS

If you have a file or folder you use frequently, you can save time by creating a shortcut on the

desktop. Instead of navigating to the file or folder cach time you want to use it, you can simply

double-click the shortcut to open it. A shortcut will have a small arrow in the lower-left corner of the icon Note that creating a shortcut does not create a duplicate copy of the folder, it's simply a way to access the folder more quickly. If you delete a shortcut, it will not delete the actual folder or the files it contains.

To create a shortcut:

In the right pane of Windows Explorer, click the file, program, or folder for which you want to make a shortcut. The item darkens when you select it.

Choose File, and then click on Create Shortcut.

The mouse pointer over the shortcut icon, holds down the left mouse button, and drags the shortcut onto desktop (in the left pane).

The word Desktop will darken when you drag the icon over it. Release the left mouse button, and a shortcut is moved to the desktop.

1. Locate and right-click the desired folder, then select Send to Desktop (create shortcut)

A shortcut to the folder will appear on the desktop. Notice the arrow in the lower-left

comer of the icon. 2. You can also hold the Alt key on your keyboard, then click and drag the folder to the desktop to create a shortcut.

4.20 PERIPHERALS WITH YOUR COMPUTER

We can plug many different types of devices into the extra ports on the computer. These devices are called peripherals.

The following are some peripherals:

1. Printers: A printer is used to print documents, photos, and anything else that appears on your screen. There are many types of printers, including inkjet, laser, and photo printers. There are even all-in-one printers, which can also scan and copy documents.

2. Scanners: A scanner allows you to copy a physical image or document and save it to your computer as a digital (computer-readable) image. Many scanners are included as part of an all-in-one printer, although you can also buy a separate flatbed or handheld scanner.

3. Speakers/headphones: Speakers and headphones are output devices, which means they send information from the computer to the user in this case, they allow you to hear

sound and music. Depending on the model, they may connect to the audio port or the USB port. Some monitors also have built-in speakers.

4. Microphones: A microphone is a type of input device, or a device that receives information from a user. You can connect a microphone to record sound or talk with someone else over the Internet. Many laptop computers come with built-in microphones. 5. Web cameras: A web camera or webcam is a type of input device that can

record videos and take pictures. It can also transmit video over the Internet in real time,

which allows for video chat or video conferencing with someone else. Many webcams

also include a microphone for this reason. 6. Game controllers and joysticks: A game controller is used to control computer games. There are many other types of controllers you can use, including joysticks, although you can also use your mouse and keyboard to control most games.

7. Digital cameras: A digital camera lets you capture pictures and videos in a digital format. By connecting the camera to your computer's USB port, you can transfer the images from the camera to the computer.

8. Mobile phones, MP3 players, tablet computers, and other devices: Whenever you buy an electronic device, such as a mobile phone or MP3 player, check to see if it comes with a USB cable. If it does, this means you can most likely connect it to your computer.

4.20 STORAGE

When you're working on a document or other computer file, you can always save it to your computer's hard drive.

I. HARD DRIVE

The hard drive is where your software, documents, and other files are stored. The hard drive is long-term storage, which means the data is still saved even if you tum the computer off or unplug it.

When you run a program or open a file, the computer copies some of the data from the hard drive onto the RAM. When you save a file, the data is copied back to the hard drive. The faster the hard drive, the faster your computer can start up and load programs.

II. EXTERNAL HARD DRIVE

One of the easiest ways to back up your files is to copy them to an extemal hard drive. External hard drive is not a part of computer. We need to purchase an extemal drive to get started.

Keep in mind that an extemal hard drive have same risks as the computer, including fire, theft, and accidental damage. It is important to keep the external hard drive in a secure location when not in use. We can use a small fireproof safe for greater protection of external hard drive.

USB drive: USB drive or flash drives are small, removable hard drives that plug into

the USB ports on your computer. They are relatively inexpensive (usually less than $20) and

can be purchased at any store with an electronics section.

Cloud storage: Cloud storage means you save your files on servers on the Internet using an account with a cloud service. With cloud storage, you can access your files from any computer with Internet access without having to keep track of a physical device.

Google Drive

Google Drive is a cloud storage service from Google, offering 15GB of free storage. From Drive, you can also access Google Docs, which allows you to create, share, and collaborate on documents, spreadsheets, presentations, and more. Visit our Google Drive and Docs tutorial to learn more.

OneDrive

OneDrive (previously called SkyDrive) is a cloud-based storage service from Microsoft, offering 5GB of free storage. You'll also have access to Office Online, a free online version of Microsoft Office that includes Word, Excel, PowerPoint, and OneNote. Visit our OneDrive and Office Online tutorial to learn more.

III. CD/DVD Drive

A CD/DVD drive, also known simply as an optical drive, is a hardware device found in computers and other electronic devices that is used for reading and writing data to optical discs. These discs include:
Compact Discs (CDs): These were initially used for storing music and later expanded to include data storage capabilities.
Digital Versatile Discs (DVDs): DVDs offer higher storage capacity than CDs and are commonly used for storing movies, software, and large amounts of data.

Functions of a CD/DVD Drive:
Reading: The primary function of a CD/DVD drive is to read data from optical discs. This includes retrieving files, music tracks, videos, or any other data stored on CDs or DVDs.

Writing (Burning): Some CD/DVD drives are capable of writing data onto blank discs. This process is known as burning, and it allows users to create their own CDs or DVDs by copying files, creating music CDs, or backing up data.

Uses of a CD/DVD Drive:
Installing software: Many software programs are distributed on CDs or DVDs for installation onto computers.
Playing media: CDs for music and DVDs for movies can be played directly from the drive.
Data backup: Users can create backup copies of important files and documents onto CDs or DVDs for

archival purposes.

IV. Floppy Drive

A floppy drive is a hardware device used to read and write data to floppy disks, which are a type of magnetic storage media.

Floppy Disk:A floppy disk is a thin, flexible disk made of a magnetic storage medium enclosed in a square or rectangular plastic casing. It typically has a capacity of 1.44 MB (megabytes) for the most common 3.5-inch disks used in PCs.

Floppy Drive: A floppy drive is the hardware component installed in a computer that reads and writes data to floppy disks. It consists of a motorized mechanism to spin the disk and a read/write head that magnetically reads and writes data on the disk's surface.

A floppy drive is a hardware device used in older computers to read and write data to floppy disks, which were once a common form of portable data storage before being largely replaced by more advanced technologies.

V. FLASH DRIVE

A flash drive is a small, removable hard drive that plugs into a USB port on your computer. You can purchase a flash drive for less than $20 at just about any retail store with an electronics department, and even at some grocery stores and pharmacies. Flash drives are a convenient way to bring your files with you and open them on a different computer. You could also use a flash drive to back up important documents and other files. In this lesson, we'll show you how to use a flash drive with your computer.

Insert the flash drive into a USB port on your computer. You should find a USB port on the front, back, or side of your computer (the location may vary depending on whether you have a desktop or a laptop).

Depending on how your computer is set up, a dialog box may appear. If it does, select Open folder to view files.

If a dialog box does not appear, open Windows Explorer and locate and select the flash drive on the left side of the window. Note that the name of the flash drive may vary.

To safely remove a flash drive:

When you're done using a flash drive, don't remove it from the USB port just yet! You'll need to make sure to disconnect it properly to avoid damaging files on the drive. Right-click the flash drive, then select Disconnect (or Eject).

You can now safely remove the flash drive from the USB port.

4.22 CONTROL PANEL

At some point, We may want to adjust your computer's settings. The Control Panel enables a user to change various computer hardware and software features in Windows. Settings for the mouse, display, sound, network, and keyboard represent a few examples of what may be modified in the Control Panel.

For example, we might want to change your desktop background or modify the Internet settings. We can change these settings and more from the Control Panel.

Steps to Open the Control Panel

1. Open the Start Menu.

2. Scroll down to W, click Windows System, then click Control Panel.

OR

1. Click the bottom-left Start button to open the Start Menu

2. Type Control Panel in the search box and select Control Panel in the results.

Main Areas of Control Panel

There are eight main areas on the Control Panel, containing different tools designed to optimize your computer.

System and Security - A section to check your computer's status, backup and restore, and

others. Network and Intemet - View network status.

Hardware and Sound - View which devices are on your computer and add devices.

Programs - Uninstall programs

User Accounts - Change user accessibility.

Appearance and Personalization - Change desktop options, like fonts and screen readers.

Clock and Region-Change date and time.

Ease of access - Optimize your display settings

PROTECTING YOUR COMPUTER

Your computer faces many potential threats, including viruses, malware, and hard drive failure. This is why it's important to do everything you can to protect your computer and your files.

Safeguarding against malware:

Malware is any type of software that is designed to damage your computer or gain unauthorized access to your personal information. It includes viruses, worms, Trojan horses, and spyware. Most malware is distributed over the Internet and is often bundled with other software.

It's also important to stay smart when you're browsing the Web or using email. If a website or email attachment looks suspicious, trust your instincts. Keep in mind that your antivirus program may not catch everything, so it's best to avoid downloading anything that might malware,

4.23 VIRUS

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

Malware is any type of software that is designed to damage your computer or gain unauthorized access to your personal information. It includes viruses, worms, Trojan horses, and spyware. Most malware is distributed over the Internet and is often bundled with other software.

The full form of VIRUS is "Vital Information Resource Under Seize".

A computer virus is a kind of malicious computer program, which when executed, replicates itself and inserts its own code. When the replication is done, this code infects the other files and program present on your system.

These computer viruses are present in various types and each of them can infect a device in a different manner. A computer virus is a program which can harm our device and files and infect them for

no further use. When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding. This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.

The following are certain indications which can help to analyse that a device is virus-hit:

Speed of the System - In case a virus is completely executed into your device, the time taken to open applications may become longer and the entire system processing may start working slowly

Pop-up Windows-One may start getting too many pop up windows on their screen which may be virus affected and harm the device even more

Self Execution of Programs Files or applications may start opening in the background. of the system by themselves and you may not even know about them

Log out from Accounts In case of a virus attack, the probability of accounts getting hacked increase and password protected sites may also get hacked and you might get logged out from all of them

* Crashing of the Device - In most cases, if the virus spreads in maximum files and programs, there are chances that the entire device may crash and stop working

Computer viruses can be dangerous and should be taken seriously, The best way to guard against virus is to install antivirus software, Bitdefender, Norton, or Kaspersky.

4.24 ANTIVIRUS

Antivirus software helps to prevent malware from being installed, and it can also remove malware from your computer.

It's also important to stay smart when you're browsing the Web or using email. If a website or email attachment looks suspicious, trust your instincts.

Once you've verified that your antivirus program is running, begin a scan.

Some programs offer several types of scans, and you may want to run the most thorough type, usually called a full system scan. This may take several hours.

Either during the course of the scan or when it's complete, the antivirus program will notify you of discovered threats and recommend various courses of action. Usually, the recommended

action for each threat is the best choice. If no viruses or malware are found but you are still

experiencing problems with your computer,

try your computer assessed by a support professional. Keep in mind that your antivirus program may not catch everything, so it's best to avoid downloading anything that might contain malware. But keep in mind that it may still be necessary to hire a technical support professional to completely remove the virus and repair your computer.

4.25 BACKING UP YOUR COMPUTER

Imagine what would happen if your computer suddenly stopped working. Would you lose any important documents, photos, or other files? It may be possible to repair your computer, but your files may be lost forever. Luckily, you can prevent this by creating backup copies of all of your files (or just the important ones) on an external hard drive or an online backup service. External hard drives: You can purchase an external hard drive and copy the contents of your computer to it. Follow-up backups should be conducted on a regular basis. One drawback is that an external hard drive can be lost, damaged, or stolen-just as your computer might be. This is why it's important to keep your drive in a secure location when not in use.

Online backup services:Backup your data on cloud, which means you'll be able to recover them from any computer with an Internet connection. The amount of storage provided by these sites varies, and you will probably need to pay a fee for adequate storage space.

Questions:

1. What is the primary function of an operating system?
2. Define an operating system and explain its significance in computer systems.
3. How would you describe the role of an operating system in managing computer hardware and software resources?
4. Discuss the core purpose of an operating system in the context of modern computing.
5. List and explain three fundamental features of an operating system.
6. Describe the role of process management as a feature of operating systems.
7. How does memory management contribute to the efficiency of an operating system?
8. Discuss the significance of file system management in operating systems.
9. Explain the importance of device management as a feature of operating systems.
10. What distinguishes real-time operating systems from other types of operating systems?
11. Provide examples and describe the characteristics of batch processing operating systems.
12. Explain the key differences between single-user and multi-user operating systems.
13. Compare and contrast embedded operating systems with general-purpose operating systems.
14. Discuss the advantages and applications of network operating systems in modern computing environments.
15. How do time-sharing operating systems enable multiple users to interact with a computer system simultaneously?
16. What are the main characteristics of multiprocessing operating systems, and how do they differ from single-processor systems?

Unit-IV

5.1 Data Communication
5.2 Components of Data Communication
5.3 Modes of Communication
5.4 Standards and Organizations
5.5 Network Classification
5.6 Network Topologies
5.7 Network Types
5.8 Transmission Media
5.9 Network Protocol
5.10 Layered Network Architecture
5.10.1 OSI Model
5.10.2 TCP/IP Model

5.1 Data Communication

Data communication refers to the exchange of information between two devices or systems through various transmission media, such as cables, optical fibers, or wireless channels. It encompasses the processes of encoding, transmitting, receiving, and decoding data to facilitate communication between devices or users. Key components and concepts related to data communication include the following:

- **Data:** Information that is represented in a digital format, such as text, images, audio, or video.
- **Sender:** The device or system that initiates the transmission of data.
- **Receiver:** The device or system that receives the transmitted data.
- **Transmission Medium:** The physical pathway through which data is transmitted, such as wires, fiber optic cables, or wireless radio waves.
- **Protocols:** Rules and conventions that govern the format and behavior of data communication, ensuring compatibility and reliability between communicating devices.
- **Modulation and Demodulation:** Modulation is the process of encoding digital data onto an analog signal suitable for transmission over a communication channel, while demodulation is the reverse process of extracting the digital data from the received analog signal.
- **Error Detection and Correction:** Techniques used to detect and correct errors that may occur during data transmission, ensuring data integrity and reliability.
- **Bandwidth:** The maximum data transfer rate of a communication channel, typically measured in bits per second (bps) or its multiples (e.g., kilobits per second, megabits per second).
- **Latency:** The time delay between the transmission and reception of data, influenced by factors such as the distance between sender and receiver, transmission medium, and processing time.
- **Networking:** The interconnection of multiple devices or systems to enable communication and resource sharing, often facilitated by networking devices such as routers, switches, and gateways.

Data communication is essential in fields such as telecommunications, computer networking, and the Internet, facilitating information exchange and the operation of numerous applications and services.

5.2 Components of Data Communication

Data communication involves various components that work together to enable the efficient and reliable exchange of data between devices or systems over communication networks. Here are the key components:

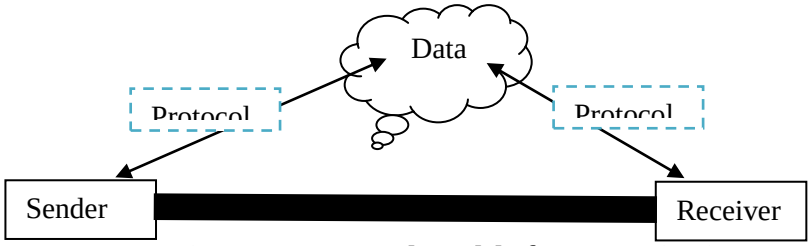


Figure 5.1: General Model of Communication

I. **Sender/Transmitter:**

In data communication, the sender, also known as the transmitter, is the device or entity that originates and transmits data to a recipient or receiver. This could be a computer, smartphone, sensor, or any device capable of generating and sending data. The sender's primary function is to encode the data into a suitable format for transmission and send it through a communication channel, such as cables, optical fibers, or wireless signals, to the intended recipient. Additionally, the sender interacts with other components of the communication system, such as protocols and networking hardware, to ensure accurate and efficient data delivery to the receiver.

II. **Receiver:** The device or system that receives the transmitted data. It processes the received data and delivers it to the intended destination.

In data communication, the receiver is the counterpart to the sender/transmitter. It's the device or entity that receives the data transmitted by the sender. The receiver's primary function is to decode the received data and deliver it to the intended destination, which could be another device, application, or system.

Similar to the sender, the receiver interacts with various components of the communication system, such as protocols and networking hardware, to ensure that the transmitted data is received accurately and reliably. The receiver typically performs tasks such as error checking, data buffering, and interpreting the received data according to the agreed-upon communication protocols.

In summary, while the sender initiates and transmits the data, the receiver receives, decodes, and processes the transmitted data to make it usable by the recipient system or application.

III. **Communication Channel/Medium:** The physical pathway through which data is transmitted from the sender to the receiver. This can include wired mediums such as copper wires, fiber optic cables, or wireless mediums such as radio waves or infrared signals.

In data communication, the communication channel, also known as the communication medium, refers to the physical or logical path through which data is transmitted from the sender to the receiver. Communication channels can vary widely in their characteristics, including transmission medium, bandwidth, capacity, and reliability.

Effective communication channel selection depends on factors such as data transmission requirements, distance, cost, and environmental considerations. Different applications and scenarios may require specific types of communication channels to ensure reliable and efficient data transfer. Here are some common types of communication channels:

- **Wired Communication Channels:** These channels use physical cables or wires to transmit data. Examples include:

Twisted Pair Cable: Used in Ethernet networks and telephone lines.

Coaxial Cable: Commonly used in cable television (CATV) and broadband internet.

Fiber Optic Cable: Utilized for high-speed data transmission over long distances, offering high bandwidth and immunity to electromagnetic interference.

- **Wireless Communication Channels**: These channels transmit data without the use of physical cables, typically utilizing electromagnetic waves. Examples include:

Radio Frequency (RF) Transmission: Used in Wi-Fi, Bluetooth, and cellular networks.

Infrared Transmission: Found in remote controls, wireless keyboards, and some short-range communication systems.

Satellite Communication: Involves communication via satellites orbiting the Earth, commonly used for long-distance and global communication.

- Guided vs. Unguided Channels: Guided channels, such as cables, provide a physical path for data transmission, while unguided channels, such as wireless signals, do not require a physical medium and propagate through space.
- **Point-to-Point vs. Multipoint Channels**: Point-to-point channels connect two specific endpoints, while multipoint channels allow communication between multiple devices simultaneously. Ethernet and Wi-Fi networks are examples of multipoint channels.
- **Analog vs. Digital Channels:** Analog channels transmit data in continuous waves, while digital channels encode data into discrete binary signals. Digital communication is more common in modern data transmission due to its reliability and noise immunity.
- **Physical vs. Logical Channels:** Physical channels refer to the actual physical medium used for transmission, while logical channels represent the conceptual paths defined by protocols for data transfer.

IV. **Protocol:** A network protocol is a set of rules and conventions that govern the communication between devices in a computer network. Protocols define how data is encoded, transmitted, received, and interpreted by devices to ensure interoperability and reliability.

Some common network protocols are:

- **Transmission Control Protocol (TCP):** A connection-oriented protocol used for reliable, ordered, and error-checked delivery of data packets over IP networks.
- **Internet Protocol (IP):** A network-layer protocol responsible for addressing and routing packets across interconnected networks.
- **User Datagram Protocol (UDP):** A connectionless protocol that provides simple datagram delivery service without the reliability features of TCP.
- **Ethernet:** A family of protocols and standards for wired LANs, specifying the physical and data link layers of network communication.
- **HTTP (Hypertext Transfer Protocol):** A protocol for transmitting hypermedia documents, such as web pages and files, over the Internet.
- **Simple Mail Transfer Protocol (SMTP**): A protocol used for sending and receiving email messages.
- **File Transfer Protocol (FTP):** A protocol used for transferring files between a client and a server on a computer network.

V. **Modem (Modulator-Demodulator):** In cases where digital data needs to be transmitted over analog communication channels, a modem is used to modulate the digital signals into analog signals for transmission and demodulate them back into digital signals upon reception.

Modems are essential for connecting computers and other digital devices to communication networks, such as telephone lines, cable systems, or wireless networks.

Modems can also perform other functions, such as error detection and correction, compression, and protocol conversion, depending on their capabilities and the requirements of the communication system.

Here's how modems work:

- **Modulation:** When sending data, the modem converts digital signals from the computer into analog signals suitable for transmission over the communication channel. Modulation techniques vary depending on the type of channel used. For example:

For telephone lines, modems typically use frequency-shift keying (FSK) or phase-shift keying (PSK) modulation.

For cable systems, modems may use quadrature amplitude modulation (QAM).

For wireless communication, modems may use techniques like phase-shift keying (PSK), quadrature amplitude modulation (QAM), or frequency-shift keying (FSK), depending on the wireless standard being used (e.g., Wi-Fi, cellular).

- **Transmission:** The modulated analog signals are transmitted over the communication channel, such as a telephone line or cable.
- **Demodulation:** At the receiving end, another modem demodulates the incoming analog signals back into digital data. The demodulation process is extracting the original digital signal from the received analog waveform.

- **Data Communication:** Once the digital data is recovered, it can be processed by the receiving device, typically a computer or network device, for further use or transmission.

VI. **Multiplexers/Demultiplexers:** Multiplexers (mux) and demultiplexers (demux) are essential components in data communication systems, particularly in scenarios where multiple signals need to be transmitted over a single communication channel. These devices play a crucial role in efficiently utilizing available bandwidth and sharing communication resources. They enable efficient utilization of available bandwidth, reduce hardware complexity, and facilitate the transmission of multiple data streams over shared communication channels. Here's an overview of multiplexers and demultiplexers:

- **Multiplexers (MUX):** A multiplexer is a device that combines multiple input signals into a single output signal for transmission over a shared communication channel.

It selects one of the input signals based on control inputs and then routes that selected signal to the output.

Multiplexers are commonly used in scenarios where multiple data sources need to share a common communication medium, such as telephone lines or optical fibers. Multiplexing techniques include time-division multiplexing (TDM), frequency-division multiplexing (FDM), wavelength-division multiplexing (WDM), and code-division multiplexing (CDM).

- **Demultiplexers (DEMUX):** A demultiplexer is the counterpart of a multiplexer. It takes a single input signal that contains multiple channels of data and separates them into individual output signals.

Demultiplexers use control inputs to determine which channel of data to extract from the input signal and route to the corresponding output.

Demultiplexers are crucial at the receiving end of a communication link to separate and distribute the incoming data streams to their respective destinations. Demultiplexing techniques mirror those of multiplexing, such as time-division demultiplexing (TDDM), frequency-division demultiplexing (FDDM), and so on, corresponding to the multiplexing method used.

VII. **Switches/Routers:** Devices that facilitate the routing and switching of data between different devices or networks. Both devices play critical roles in directing data traffic within and between networks, facilitating efficient and reliable data communication. They serve different purposes and operate at different layers of the OSI model. Switches operate at the data link layer of the OSI model and are used to connect devices within the same network, while routers operate at the network layer and are used to connect multiple networks and facilitate inter-network communication.

Switches: A switch is a networking device that operates at the data link layer (Layer 2) of the OSI model. It is used to connect multiple devices within a local area network (LAN) and selectively forward data frames between them based on the Media Access Control (MAC) addresses.

Switches maintain a MAC address table, also known as a forwarding table or content addressable memory (CAM) table, which maps MAC addresses to the corresponding switch ports.

When a switch receives a data frame, it examines the destination MAC address and forwards the frame only to the port where the destination device is connected, improving network efficiency by reducing unnecessary traffic.

Switches can operate in various modes, including unmanaged switches (plug-and-play), managed switches (configurable and monitorable), and layer 3 switches (combining switching and routing capabilities).

Routers: A router is a networking device that operates at the network layer (Layer 3) of the OSI model.

It is used to connect multiple networks together and forward data packets between them based on network layer addresses, such as IP addresses.

Routers maintain a routing table, which contains information about the available paths to different network destinations and the associated next-hop routers.

When a router receives a data packet, it examines the destination IP address and determines

the best path to forward the packet based on its routing table.

Routers can perform functions such as packet forwarding, packet filtering, and network address translation (NAT), enabling communication between devices on different networks.

Routers are essential for interconnecting LANs, WANs, and the Internet, enabling end-to-end communication across diverse network infrastructures.

VIII. **Repeaters/Amplifiers:** Repeaters and amplifiers are both used in data communication to enhance the quality and extend the reach of signals transmitted over communication channels. Repeaters are typically used for digital signals and operate at the physical layer, while amplifiers are used for analog signals and operate at the electrical level to increase signal power.

Repeaters: Repeaters are devices used to regenerate and retransmit digital or analog signals to extend the distance over which the signals can travel without significant degradation.

In digital communication, repeaters are placed at intervals along a communication link to compensate for signal attenuation caused by transmission loss over long distances.

Repeaters operate at the physical layer (Layer 1) of the OSI model and regenerate the original signal to its original strength before retransmitting it.

They are commonly used in communication networks such as Ethernet, fiber optic networks, and long-distance telecommunication links to extend the reach of signals and improve communication reliability.

Amplifiers: Amplifiers are electronic devices used to increase the strength or power level of electrical signals, typically analog signals, without significantly affecting their other characteristics.

Amplifiers are commonly used in analog communication systems, such as audio and radio frequency (RF) transmission systems, to boost signal strength and improve signal-to-noise ratio (SNR).

Unlike repeaters, which regenerate digital signals, amplifiers amplify analog signals directly without decoding and re-encoding them.

Amplifiers can be placed at various points along a communication link to compensate for signal attenuation and ensure that the signal remains above the noise floor.

They are used in applications such as audio amplification, RF amplification in wireless communication systems, and signal boosting in cable TV distribution networks.

IX. **Error Detection and Correction Mechanisms:** Techniques employed to detect and correct errors that may occur during data transmission, ensuring data integrity and reliability. Here are some common error detection and correction techniques:

- **Parity Checking:** Parity checking is a simple error detection technique that involves adding an extra parity bit to each transmitted character or byte.

The parity bit is set such that the total number of bits (including the parity bit) is always even (even parity) or odd (odd parity), depending on the desired parity scheme.

At the receiving end, the parity of the received data is checked. If the parity doesn't match the expected parity, an error is detected.

- **Checksums:** Checksums are error detection codes calculated from the data bits in a message. A checksum algorithm computes a checksum value by summing or applying a mathematical function to the data bits.

The sender appends the checksum to the message before transmission.

At the receiver, the checksum is recomputed using the received data. If the computed checksum matches the received checksum, the data is assumed to be error-free. Otherwise, an error is detected.

- **Cyclic Redundancy Check (CRC):** CRC is a more robust error detection technique commonly used in data communication protocols such as Ethernet, Wi-Fi, and digital communication standards like HDLC and ATM.

CRC uses polynomial division to generate a checksum, which is appended to the data before transmission.

At the receiver, the same CRC polynomial is applied to the received data, and the resulting checksum is compared with the received checksum. If they match, the data is considered error-free.

- **Forward Error Correction (FEC):** FEC is an error correction technique that adds redundant data (error-correcting codes) to the transmitted message.

The redundant data allows the receiver to detect and correct errors without needing to request retransmission of the data.

Reed-Solomon codes and convolutional codes are examples of FEC techniques used in communication systems like digital television, satellite communication, and optical communication.

- **Automatic Repeat reQuest (ARQ):** ARQ is an error detection and correction strategy that relies on retransmission of damaged or lost packets.

When the receiver detects an error, it sends a request to the sender to retransmit the corrupted data. ARQ protocols include Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ, each with different mechanisms for managing retransmissions.

X. **Terminal Equipment:** Devices such as computers, terminals, printers, and other peripherals that generate, process, or display data in a human-readable format, serving as the endpoints of data communication. Terminal equipment can take various forms, ranging from simple devices such as telephones and modems to more sophisticated equipment like computers, servers, and networking devices.

5.3 Modes of Communication

Communication modes define how data is exchanged between devices or systems. In the context of data communication, there are several modes of communication that describe how data is transferred between devices or systems. These modes define the directionality of data flow and the relationship between the communicating entities. The primary modes of communication are:

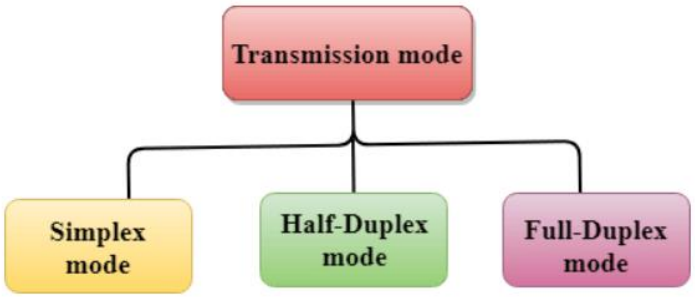


Figure 5.2 Types of Transmission modes

I. **Simplex Mode:** In simplex mode, communication occurs in only one direction, meaning data flows from one device to another without any acknowledgment or response. One device is the transmitter, and the other is the receiver. However, the receiver cannot send any data back to the transmitter.

Examples of simplex mode communication include radio broadcasting and television broadcasting, where the sender (the broadcaster) sends information to multiple receivers (listeners or viewers), but the receivers cannot send data back to the sender through the same channel.

Advantages of Simplex Mode:

Simplex mode offers advantages in scenarios where unidirectional communication is sufficient and can provide efficient, reliable, and cost-effective solutions for various applications:

- **Simplicity:** Simplex mode communication systems are often simpler to design, implement, and operate compared to duplex or half-duplex systems. This simplicity can lead to lower costs and easier maintenance.

- **Unidirectional Transmission:** In situations where data only needs to flow in one direction, simplex mode is highly efficient. This can be advantageous in broadcasting scenarios, such as radio and television transmissions, where a single sender needs to reach multiple receivers.
- **Resource Conservation**: Since simplex mode systems do not require the overhead of managing bidirectional communication, they can conserve resources such as bandwidth, power, and processing capacity. This efficiency can be crucial in scenarios where resources are limited or need to be allocated carefully.
- **Reduced Complexity:** By eliminating the need for bidirectional communication, simplex mode systems can be less complex. This simplicity can lead to increased reliability and decreased susceptibility to errors or interference.
- **High Throughput:** In scenarios where data transmission is the primary concern and feedback or interaction from the receiver is unnecessary, simplex mode can achieve high throughput rates. This can be beneficial for applications such as data streaming or broadcasting.
- **Broadcasting:** Simplex mode is well-suited for broadcasting applications, where a single source needs to transmit information to multiple recipients simultaneously. This includes radio and television broadcasting, as well as one-way data transmission in industrial monitoring systems or weather stations.

Disadvantages of Simplex Mode:

While simplex mode offers certain advantages, it also comes with several disadvantages:

- Lack of Feedback: One of the most significant drawbacks of simplex mode is the inability to receive feedback from the receiver. In scenarios where real-time feedback or interaction is necessary, such as in telecommunications or interactive systems, simplex mode is inadequate.
- **Limited Versatility:** Simplex mode communication is inherently unidirectional, which restricts its versatility. It is not suitable for applications that require bidirectional or interactive communication, such as telephony, video conferencing, or online gaming.
- **Reduced Flexibility**: Due to its one-way nature, simplex mode may not adapt well to dynamic environments or changing communication requirements. Systems operating in simplex mode are less flexible compared to duplex or half-duplex systems, which can dynamically adjust the direction of communication.
- **Potential for Data Loss:** Since simplex mode does not provide mechanisms for error detection and correction in the transmitted data, there is a risk of data loss or corruption. Without the ability to verify the integrity of received data or request retransmissions, reliability can be compromised.
- **Limited Interactivity:** Simplex mode precludes direct interaction between the sender and receiver. This limitation can be a significant disadvantage in applications where real-time interaction or response is essential, such as in control systems or collaborative environments.
- **Dependency on Infrastructure:** Simplex mode communication relies heavily on the infrastructure and transmission medium used. Any disruptions or failures in the transmission path can result in complete loss of communication, without the possibility of recovery through feedback mechanisms.
- **Reduced Efficiency in Some Cases:** In scenarios where bidirectional communication is required, simplex mode may lead to inefficiencies. For example, in systems where both data transmission and acknowledgment are necessary, simplex mode would require separate channels or additional mechanisms to achieve reliability, which can increase complexity and resource usage.

II. Half-Duplex Mode: In half-duplex mode, communication can occur in both directions, but not simultaneously. Data can be transmitted and received, but not at the same time. Typically, devices take turns sending and receiving data. This mode is commonly used in walkie-talkies and some forms of radio communication.

Advantages of Half-Duplex Mode:

- **Bidirectional Communication:** Half-duplex mode allows devices to both transmit and receive data. This bidirectional capability enables interactive communication, where participants can send and receive messages.

- **Single Communication Channel:** Devices operating in half-duplex mode typically share a single communication channel. They take turns transmitting and receiving data, switching between the two functions as needed.
- **Simplex Channel with Reversal:** Half-duplex mode can be thought of as utilizing a simplex channel (where communication is unidirectional) but with the ability to reverse the direction of transmission. This enables two-way communication without the need for separate channels.
- **Efficiency in Certain Scenarios:** Half-duplex mode can be more efficient than simplex mode in scenarios where bidirectional communication is required but simultaneous transmission and reception are not necessary. Examples include walkie-talkies, where users take turns speaking and listening, or Ethernet networks using Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- **Reduced Complexity Compared to Full Duplex:** Half-duplex mode is simpler to implement and manage compared to full-duplex mode, which allows simultaneous bidirectional communication. This simplicity can lead to cost savings and easier deployment, especially in scenarios where full duplex is not required.

Disadvantages of Half-Duplex Mode:

- Reduced Throughput: Since data transmission and reception cannot occur simultaneously, the effective throughput of a half-duplex channel is lower compared to full-duplex communication. This can lead to slower data transfer rates, especially in high-demand environments.
- Potential for Collisions: In half-duplex communication, devices must share the communication medium. This can lead to collisions, where two or more devices attempt to transmit data simultaneously, resulting in data corruption or loss. Collision detection and avoidance mechanisms are typically employed to mitigate this risk.
- Increased Latency: Because devices must wait for their turn to transmit data, half-duplex communication can introduce additional latency compared to full-duplex communication. This delay may impact real-time applications or interactive communication systems.

III. **Full-Duplex Mode:** In full-duplex mode, communication can occur simultaneously in both directions. Both devices can transmit and receive data at the same time, enabling more efficient communication. This mode is commonly used in telephone conversations and most modern data communication systems, including Ethernet networks and Internet connections.

Table 5.1 Advantages of Full Duplex Mode

nultaneous Bidirectiona l Communica tion	ll-duplex mode allows devices to transmit and receive data simultaneously. This capability enables seamless two-way communication, similar to a natural conversation, where participants can both speak and listen at the same time.
reased Throughput	cause data transmission and reception can occur simultaneously, full-duplex communication offers higher throughput compared to half-duplex or simplex modes. This leads to faster data transfer rates and improved efficiency, especially in high-demand environments
w Latency	ll-duplex communication typically results in lower latency compared to half-duplex or simplex modes. Since devices can transmit and receive data concurrently, there is no need to wait for turnarounds, reducing communication delays and improving responsiveness.
w Latency	ll-duplex communication typically results in lower latency compared to half-duplex or simplex modes. Since devices can transmit and receive data concurrently, there is no need to wait for turnarounds, reducing communication delays and improving responsiveness.
w Latency	ll-duplex communication typically results in lower latency compared to half-duplex or simplex modes. Since devices can transmit and receive data concurrently, there is no need to wait for turnarounds, reducing communication delays and improving responsiveness.

ficiency in Interactive Application s	ll-duplex mode is well-suited for interactive applications, such as voice and video calls, online gaming, and real-time collaboration tools. Users can communicate in real-time without experiencing delays or disruptions, enhancing the user experience.
xibility	ll-duplex mode provides flexibility in communication, allowing devices to send and receive data as needed without strict scheduling or coordination. This flexibility simplifies the design and implementation of communication systems and improves overall system performance.

Disadvantages of Full Duplex Mode:

- **Complexity and Cost:** Implementing full-duplex communication requires more sophisticated hardware and protocols compared to half-duplex or simplex modes. This increased complexity can lead to higher costs and resource requirements, especially in large-scale or high-speed communication systems.
- **Sensitivity to Interference:** Full-duplex communication may be more susceptible to interference and noise compared to half-duplex or simplex modes, especially in wireless or shared-medium environments. Effective interference mitigation techniques, such as error correction and signal processing, are necessary to ensure reliable communication.
- **Infrastructure Requirements:** Full-duplex communication often requires dedicated communication channels or separate frequency bands for transmission and reception to avoid self-interference. This may impose additional infrastructure requirements and constraints, particularly in wireless or congested environments.

These modes of communication are fundamental in designing and implementing data communication systems, allowing for efficient and reliable transfer of information between devices or systems. The choice of mode depends on factors such as the requirements of the application, the capabilities of the devices involved, and the characteristics of the communication medium.

5.4 Standards and Organizations

Computer networks rely on standards and organizations to ensure interoperability, compatibility, and the smooth operation of communication technologies. Here are some key standards and organizations in the field of computer networks:

- **IEEE (Institute of Electrical and Electronics Engineers):** IEEE is a professional organization dedicated to advancing technology in various fields, including computer networking. It develops and publishes standards for networking technologies, such as Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), and others.
- **ISO (International Organization for Standardization):** ISO is an international standard-setting body that develops and publishes standards for various industries, including computer networking. ISO's networking standards cover aspects such as network architecture, protocols, and network management.
- **IETF (Internet Engineering Task Force):** IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It develops and promotes voluntary Internet standards, in particular, the standards that comprise the Internet protocol suite (TCP/IP).
- **ITU (International Telecommunication Union):** ITU is a specialized United Nations agency responsible for issues related to information and communication technologies (ICT). It develops global telecommunications standards, including those for networking technologies such as DSL (Digital Subscriber Line) and ISDN (Integrated Services Digital Network).
- **Wi-Fi Alliance:** A global nonprofit organization that promotes and certifies interoperability of Wi-Fi products based on IEEE 802.11 standards. It develops testing protocols and certification programs to ensure compatibility and quality of Wi-Fi products.

- **Ethernet Alliance:** A global industry consortium dedicated to the promotion and advancement of Ethernet technologies. It collaborates with industry stakeholders to develop and promote Ethernet standards, interoperability testing, and education.
- **3GPP (3rd Generation Partnership Project):** A collaboration between telecommunications standards organizations to develop globally applicable specifications for third-generation (3G) mobile communication systems and beyond, including standards for mobile networking technologies such as LTE (Long-Term Evolution) and 5G.
- **W3C (World Wide Web Consortium):** W3C is an international community that develops open standards to ensure the long-term growth of the Web. It focuses on standards related to web technologies, including HTML, CSS, and various web protocols.

These standards and organizations play a crucial role in shaping the development and adoption of networking technologies, ensuring compatibility, interoperability, and the seamless functioning of computer networks on a global scale.

5.5 Network Classification

Networks can be classified based on various criteria, including their size, topology, technology, and geographical scope. Here are some common classifications of networks:

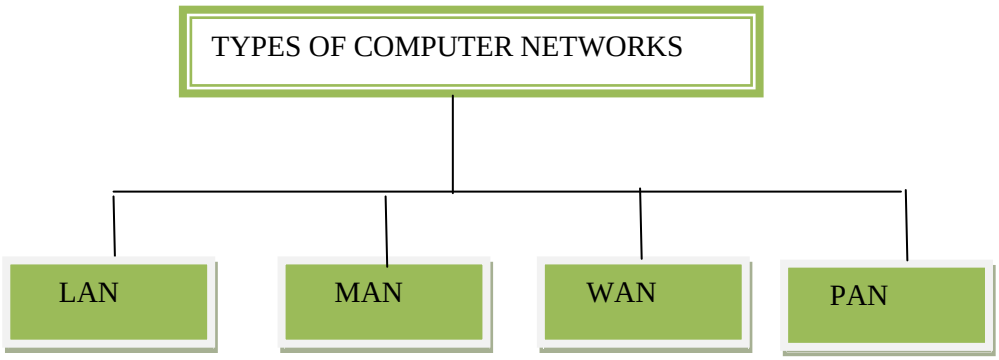


Figure 5.3: Types of Network

I. Based on Scale:

- **LAN (Local Area Network):** A Local Area Network (LAN) is a network that connects computers and other devices in a relatively small geographic area, such as a home, office building, school, or campus. LANs are commonly used for connecting devices like computers, printers, and servers within an office or home.

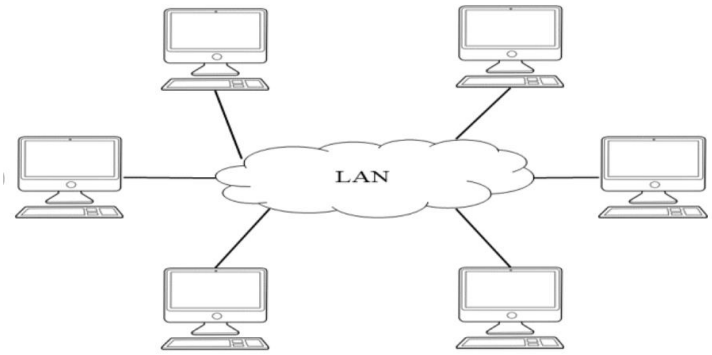


Figure 5. 4: Logical diagram of LAN

LANs typically cover a small area, such as a single building or a group of buildings in close proximity.

- High Data Transfer Rates: LANs are designed for high-speed data transfer, allowing devices within the network to communicate with each other quickly and efficiently.
- Private Ownership and Control: LANs are privately owned and controlled by the organization or individual that sets them up. This provides greater control over network security and access permissions.
- Use of Ethernet or Wi-Fi: LANs commonly use Ethernet cables or wireless technologies (such as Wi-Fi) to connect devices to the network infrastructure.
- Common Protocols: LANs typically use standard networking protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol), for communication between devices.
- Shared Resources: Devices connected to a LAN can share resources, such as files, printers, and internet connections, making it easier for users to collaborate and access information.
- Scalability: LANs can be easily scaled to accommodate additional devices or expanded coverage by adding more network infrastructure components, such as switches, routers, and access points.

Advantages of LAN:

- Resource Sharing: LANs allow devices connected to the network to share resources such as printers, scanners, storage devices, and internet connections. This facilitates collaboration and improves efficiency by reducing the need for duplicate equipment.
- Data Transfer Speed: LANs provide high-speed data transfer rates compared to wide-area networks (WANs) or the internet. This enables fast communication and access to shared resources within the local network.
- Cost-Effectiveness: LANs are cost-effective solutions for connecting devices within a relatively small geographic area, such as a home, office, or campus. They require less infrastructure and maintenance compared to larger networks like WANs.
- Centralized Management: LANs allow for centralized management of network resources, including user accounts, permissions, and security settings. This simplifies network administration and ensures consistent access control across all connected devices.
- Improved Communication: LANs facilitate real-time communication between users through features like instant messaging, video conferencing, and VoIP (Voice over Internet Protocol). This enhances collaboration and productivity among individuals and teams.
- Enhanced Security: LANs offer greater control over network security compared to public networks like the internet. Network administrators can implement security measures such as firewalls, encryption, access control, and intrusion detection systems to protect sensitive data and prevent unauthorized access.
- Scalability: LANs can be easily scaled to accommodate additional devices or expanded coverage by adding more network infrastructure components, such as switches, routers, and access points. This flexibility allows organizations to adapt to changing business needs and growth requirements.
- High Reliability: LANs are typically more reliable than internet-based connections because they operate within a controlled environment with fewer external factors that can affect network performance. Redundant components and backup systems can be implemented to minimize downtime and ensure continuous operation.
- Support for Multimedia Applications: LANs support multimedia applications such as video streaming, online gaming, and multimedia content sharing with minimal latency and high-quality performance. This makes them ideal for environments where multimedia communication and entertainment are important.
- Local Control: LANs provide local control over network infrastructure and services, allowing organizations to customize their network environment to meet specific requirements and preferences without relying on external service providers.

Disadvantages of LAN:

- Limited Coverage: LANs are designed for small-scale networking within a limited geographic area, such as a single building or campus. They are not suitable for connecting devices over long distances, which may require the use of wide-area network (WAN) technologies.

- High Initial Setup Cost: Setting up a LAN infrastructure, including networking equipment such as switches, routers, cables, and servers, can involve significant upfront costs. This initial investment may be prohibitive for small businesses or individuals with limited budgets.
- Maintenance and Management Complexity: LANs require ongoing maintenance and management to ensure optimal performance and security. Network administrators must configure and monitor network devices, troubleshoot issues, apply software updates, and implement security measures, which can be time-consuming and resource-intensive.
- Security Risks: LANs are vulnerable to security threats such as unauthorized access, data breaches, malware infections, and insider attacks. Without proper security measures in place, sensitive information stored on LAN-connected devices may be at risk of compromise.
- Single Point of Failure: LANs rely on a centralized infrastructure, which can become a single point of failure if critical components, such as switches or servers, experience downtime or malfunction. Redundancy and backup systems can mitigate this risk but may add complexity and cost to the network.
- Limited Mobility: Devices connected to a LAN are typically stationary and must be physically connected to the network infrastructure via cables or wireless access points. This limits the mobility of users and devices within the local area covered by the network.
- Bandwidth Limitations: LANs may experience bandwidth limitations, especially in shared network environments where multiple devices compete for network resources. This can lead to congestion and decreased performance, particularly during peak usage periods.
- Dependency on Physical Infrastructure: LANs rely on physical infrastructure such as cables, switches, and routers to transmit data between devices. Any damage to this infrastructure, such as cable cuts or equipment failure, can disrupt network connectivity and require timely repairs.
- Compatibility Issues: Different devices and operating systems may have compatibility issues when connected to the same LAN, leading to interoperability challenges and potential performance issues. Network administrators must ensure compatibility and consistency across all networked devices.
- Scalability Constraints: While LANs can be scaled to accommodate additional devices or expanded coverage, there are practical limitations to their scalability. Adding too many devices or extending the network beyond its intended capacity may result in performance degradation and increased complexity.
- **MAN (Metropolitan Area Network):**

A Metropolitan Area Network (MAN) is a type of network that spans a larger geographic area than a Local Area Network (LAN) but is smaller than a Wide Area Network (WAN). MANs typically cover a metropolitan area such as a city or a large campus, connecting multiple LANs and other network devices over a wide geographical area.

MANs often connect multiple LANs and provide high-speed connectivity over longer distances than LANs.

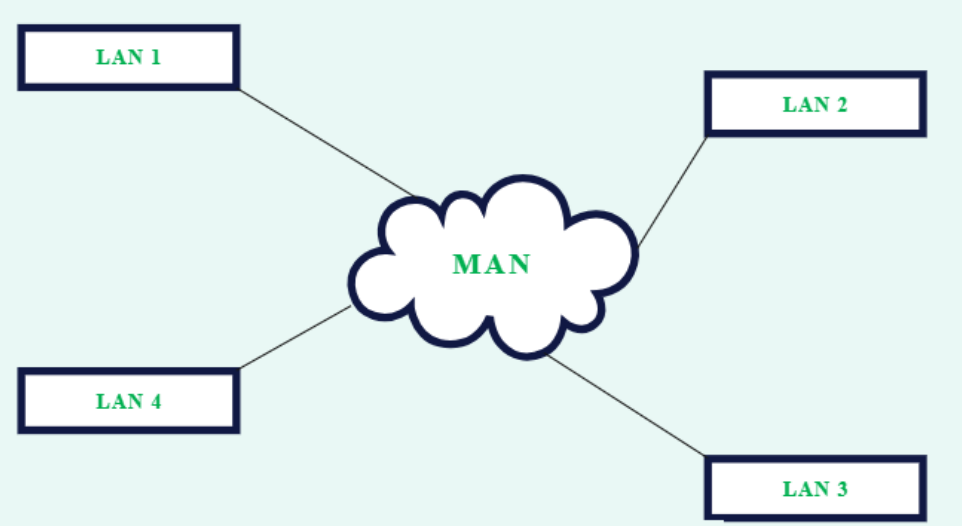


Figure 5.5: Logical diagram of MAN

- Geographic Coverage: MANs cover a larger geographic area than LANs but are typically confined to a single metropolitan area or city. They may encompass multiple buildings, campuses, or office locations within the same city or urban area.
- High-Speed Connectivity: MANs provide high-speed connectivity between connected LANs and other network devices within the metropolitan area. This allows for efficient data transfer and communication over the network.
- Ownership and Control: MANs may be owned and operated by a single organization, such as a municipal government, a telecommunications provider, or a large corporation. Alternatively, they may be built and maintained through collaboration between multiple entities.
- Fiber Optic Backbone: MANs often rely on fiber optic cables as the primary transmission medium for data communication. Fiber optic technology allows for high bandwidth and long-distance transmission, making it well-suited for MAN deployments.
- Scalability: MANs are designed to be scalable, allowing for expansion to accommodate additional users, devices, and network services as needed. This scalability enables MANs to grow alongside the evolving needs of the metropolitan area they serve.
- Interconnection of LANs: One of the primary purposes of a MAN is to interconnect multiple LANs located within the same metropolitan area. This enables seamless communication and resource sharing between different sites or buildings connected to the MAN.
- Redundancy and Reliability: MANs often incorporate redundancy and failover mechanisms to ensure high availability and reliability. Redundant network links, backup systems, and disaster recovery plans help minimize downtime and ensure continuous operation of critical network services.
- Support for Various Applications: MANs support a wide range of applications and services, including internet access, VoIP (Voice over Internet Protocol), video conferencing, cloud computing, and enterprise resource planning (ERP) systems. These applications require high-speed, reliable connectivity, which MANs can provide.
- Service Level Agreements (SLAs): MAN providers may offer service level agreements to guarantee certain levels of network performance, uptime, and customer support. SLAs help ensure that businesses and organizations relying on the MAN receive the quality of service they require for their operations.
- Cost Considerations: Building and maintaining a MAN can involve significant upfront costs, including infrastructure deployment, equipment purchases, and ongoing maintenance expenses. However, MANs offer cost-effective solutions for interconnecting multiple LANs and providing high-speed connectivity within a metropolitan area.

Advantages of MAN:

- High-Speed Connectivity: MANs provide high-speed data transmission within the metropolitan area, enabling fast communication and data transfer between different locations, such as office buildings, campuses, or government facilities.
- Scalability: MANs are designed to accommodate growth and expansion, allowing organizations to easily add new users, locations, and network services as needed. This scalability ensures that the network can adapt to evolving business requirements and technological advancements.
- Resource Sharing: MANs enable efficient resource sharing among connected locations, including shared internet access, file servers, printers, and other network resources. This promotes collaboration and productivity among users within the metropolitan area.
- Improved Communication: MANs facilitate seamless communication between employees, departments, and organizations located across different sites within the metropolitan area. Features such as VoIP, video conferencing, and unified communications enhance real-time communication and collaboration.
- Centralized Management: MANs allow for centralized management and administration of network resources, including user accounts, permissions, security policies, and network configurations. This centralized approach simplifies network management and ensures consistency across multiple locations.
- Enhanced Reliability: MANs often incorporate redundancy and failover mechanisms to ensure high availability and reliability. Redundant network links, backup systems, and disaster recovery plans help minimize downtime and ensure continuous operation of critical network services.
- Support for Critical Applications: MANs support a wide range of applications and services, including mission-critical business applications, cloud services, and multimedia applications. The high-speed connectivity and reliability of MANs ensure that these applications can operate efficiently and effectively within the metropolitan area.
- Business Continuity: MANs enable organizations to implement disaster recovery and business continuity strategies by replicating data and services across multiple locations within the metropolitan area. This ensures that essential business operations can continue in the event of a localized disruption or disaster.
- Cost-Effective Connectivity: MANs offer cost-effective solutions for interconnecting multiple locations within a metropolitan area, reducing the need for expensive leased lines or wide-area network (WAN) services. This cost savings can be particularly beneficial for businesses and organizations with distributed operations.
- Community Benefits: MANs can benefit the broader community by providing high-speed internet access, digital services, and connectivity to schools, libraries, healthcare facilities, and government offices. This helps bridge the digital divide and promotes economic development and social inclusion within the metropolitan area.

Disadvantages of MAN

- High Initial Setup Cost: Building and deploying a MAN infrastructure can involve significant upfront costs, including the installation of network equipment, fiber optic cables, and other infrastructure components. This initial investment may be prohibitive for smaller organizations or communities with limited financial resources.
- Complexity of Deployment: Deploying a MAN infrastructure requires careful planning, coordination, and technical expertise. It may involve navigating regulatory requirements, obtaining permits, and negotiating access to rights-of-way, which can add complexity and delay the deployment process.
- Maintenance and Management Challenges: MANs require ongoing maintenance, monitoring, and management to ensure optimal performance and reliability. Managing a distributed network infrastructure spanning multiple locations within a metropolitan area can be complex and resource-intensive, requiring skilled IT personnel and adequate support resources.
- Dependency on Physical Infrastructure: MANs rely on physical infrastructure such as fiber optic cables, switches, routers, and other networking equipment. Any damage to this

infrastructure, such as cable cuts, equipment failure, or natural disasters, can disrupt network connectivity and require timely repairs, resulting in downtime and service interruptions.

- Security Vulnerabilities: MANs are susceptible to security threats, including unauthorized access, data breaches, malware infections, and insider attacks. The distributed nature of MANs and the interconnectedness of multiple locations within the metropolitan area can increase the attack surface and pose challenges for ensuring consistent security across all network segments.
- Limited Coverage Area: MANs cover a larger geographic area than Local Area Networks (LANs) but are still limited to a single metropolitan area or city. This may pose challenges for organizations with operations or facilities located outside the coverage area of the MAN, requiring additional networking solutions or reliance on external service providers.
- Bandwidth Limitations: MANs may experience bandwidth limitations, especially in densely populated urban areas where multiple users and organizations share the same network infrastructure. This can result in congestion and decreased performance, particularly during peak usage periods.
- Regulatory and Compliance Requirements: MAN operators may be subject to regulatory requirements and compliance standards governing telecommunications, data privacy, and network security. Ensuring compliance with these regulations can add administrative overhead and regulatory costs to MAN operations.
- Dependency on Service Providers: Organizations relying on MAN services may become dependent on external service providers for network connectivity, support, and maintenance. This dependency can pose risks in terms of service reliability, vendor lock-in, and potential disruptions due to changes in service provider policies or business practices.
- Obsolescence and Technology Evolution: MANs are subject to technological obsolescence and evolution, requiring periodic upgrades and investments to keep pace with advancements in networking technology and changing business requirements. Failure to adapt to emerging technologies and market trends may result in the depreciation of MAN infrastructure and the loss of competitive advantage.
- **WAN (Wide Area Network):**

A Wide Area Network (WAN) is a telecommunications network that extends over a large geographic area, typically connecting multiple local area networks (LANs) or other WANs. WANs are used to connect computers and other devices across long distances, often spanning cities, countries, or even continents.

WANs use various communication technologies such as leased lines, satellite links, microwave links, or digital subscriber lines (DSL) to transmit data over longer distances. WANs are commonly used by businesses, governments, and organizations to enable communication and data exchange between remote locations, branch offices, and headquarters. They provide the infrastructure for services like the internet, corporate intranets, and wide-reaching applications such as online banking and video conferencing.

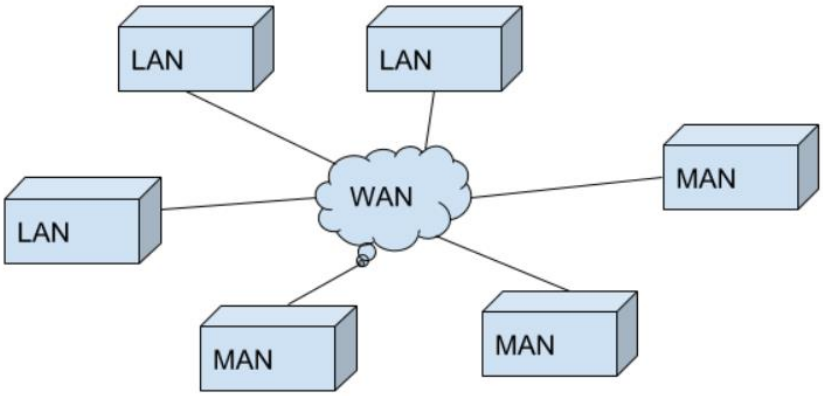


Figure 5.6: Logical diagram of WAN

- Geographic Scope: WANs cover a wide geographic area, connecting devices and networks across cities, regions, countries, or continents. They enable communication over long distances.
- Connectivity Technologies: WANs utilize various technologies for connectivity, including leased lines, fiber optic cables, satellite links, microwave links, and wireless connections like 4G/5G. These technologies differ in terms of speed, reliability, and cost.

Internet Backbone: The internet itself is a prime example of a WAN. It consists of a vast network of interconnected WANs operated by internet service providers (ISPs) and telecommunications companies.

- Data Transmission: WANs facilitate the transmission of data between different locations. They employ protocols such as TCP/IP for reliable data delivery over diverse networks.
- Centralized Management: WANs often have centralized management, allowing administrators to oversee and control network resources, security policies, and access privileges across distributed locations.
- Scalability: WANs are designed to scale efficiently to accommodate growing network demands. They can support a large number of users, devices, and applications across diverse locations.
- Security Challenges: Securing WANs presents challenges due to their extensive reach and reliance on public infrastructure. Encryption, firewalls, virtual private networks (VPNs), and other security measures are used to protect data transmitted over WANs.
- Reliability and Redundancy: WANs require redundancy and failover mechanisms to ensure continuous operation and minimize downtime. Redundant links and backup connections help maintain connectivity in case of network failures.
- Cost Considerations: Building and maintaining WANs can be costly due to infrastructure expenses, ongoing operational costs, and the need for specialized equipment and skilled personnel.
- Business Applications: WANs enable various business applications such as email, file sharing, remote access to corporate resources, video conferencing, and cloud-based services. They support collaboration and facilitate efficient workflows across distributed teams and locations.

Advantages of WAN

- Geographic Reach: WANs allow connectivity across vast geographical areas, enabling communication and data exchange between remote offices, branches, and facilities regardless of their location.
- Centralized Resources: WANs facilitate centralized management and access to shared resources such as servers, databases, and applications. This centralization promotes efficiency, consistency, and easier maintenance of IT infrastructure.
- Improved Collaboration: WANs enable real-time collaboration among geographically dispersed teams through tools like video conferencing, VoIP, instant messaging, and shared document repositories. This fosters teamwork, innovation, and knowledge sharing.
- Cost Efficiency: Despite initial setup costs, WANs can be cost-effective in the long run by consolidating resources, reducing the need for duplicate infrastructure at multiple locations, and enabling economies of scale in purchasing network services.
- Scalability: WANs are designed to scale according to the evolving needs of organizations. They can accommodate additional users, devices, and network traffic without significant architectural changes, allowing businesses to grow without major disruptions to their network infrastructure.
- Enhanced Disaster Recovery: WANs support disaster recovery and business continuity efforts by enabling data replication, backup, and failover mechanisms across multiple locations. In the event of a localized outage or disaster, critical operations can continue from unaffected sites.
- Global Connectivity: WANs provide access to global communication networks such as the internet, enabling organizations to connect with customers, partners, and suppliers worldwide.

This global connectivity opens up opportunities for international collaboration, market expansion, and business growth.

- Flexible Access: WANs offer flexible access options, allowing users to connect from various devices and locations, including remote offices, mobile devices, and telecommuting setups. This flexibility enhances productivity and supports modern work practices like remote work and Bring Your Own Device (BYOD) policies.
- Resource Optimization: WAN optimization technologies, such as caching, compression, and traffic shaping, help optimize bandwidth usage, reduce latency, and improve application performance over the network. This leads to a better user experience and more efficient use of network resources.
- Competitive Advantage: By providing reliable and efficient communication capabilities, WANs can confer a competitive advantage to organizations, enabling them to respond quickly to market changes, customer demands, and business opportunities.

Disadvantages of WAN

- Cost: Setting up and maintaining a WAN can be expensive due to the need for specialized equipment, dedicated leased lines, and ongoing operational expenses. Costs can include equipment purchases, subscription fees for internet services, and hiring skilled personnel for network management.
- Complexity: WANs are inherently more complex than Local Area Networks (LANs) due to their extensive reach and reliance on diverse technologies and infrastructure. Managing and troubleshooting WANs require expertise in networking protocols, routing, security, and performance optimization.
- Security Risks: WANs are susceptible to security threats such as hacking, data breaches, malware attacks, and unauthorized access. Transmitting data over public networks increases the risk of interception and eavesdropping. Securing WANs requires robust encryption, firewalls, intrusion detection systems, and regular security updates.
- Reliability Concerns: WANs may experience downtime, latency, or packet loss, especially when relying on public internet connections or shared infrastructure. Network outages can disrupt business operations, impact productivity, and lead to financial losses. Implementing redundancy, failover mechanisms, and Service Level Agreements (SLAs) with service providers can mitigate reliability concerns.
- Performance Limitations: WAN performance may vary based on factors such as distance, network congestion, bandwidth limitations, and the quality of connectivity technologies. Latency-sensitive applications like VoIP, video conferencing, and virtual desktops may experience degraded performance over WANs, requiring optimization techniques such as Quality of Service (QoS) prioritization.
- Regulatory Compliance: Organizations operating WANs across multiple jurisdictions must navigate regulatory compliance requirements related to data privacy, consumer protection, and telecommunications regulations. Compliance obligations may differ between regions, leading to additional administrative burdens and legal risks.
- Dependency on Service Providers: Organizations relying on third-party service providers for WAN connectivity are vulnerable to disruptions caused by provider outages, maintenance windows, or service degradation. Limited competition in certain regions may result in monopolistic practices and reduced bargaining power for customers.
- Scalability Challenges: Scaling WAN infrastructure to accommodate growing bandwidth demands and expanding geographical coverage can be challenging. Upgrading equipment, adding new network links, and adjusting configurations require careful planning and investment to ensure seamless scalability.
- Management Overhead: Managing a distributed WAN environment with multiple sites, devices, and users entails significant administrative overhead. Tasks such as provisioning, configuration management, performance monitoring, and troubleshooting require coordination and resources across the organization.
- Interoperability Issues: Integrating disparate network technologies, equipment vendors, and software platforms within a WAN environment can lead to interoperability issues.

Compatibility issues, protocol mismatches, and vendor lock-in may hinder seamless communication and collaboration between different network components.

- **PAN (Personal Area Network):**

A Personal Area Network (PAN) is a type of network used for communication among devices close to one person. PANs can be used for connecting devices in proximity, such as smartphones, tablets, laptops, wearable devices, and personal computers.

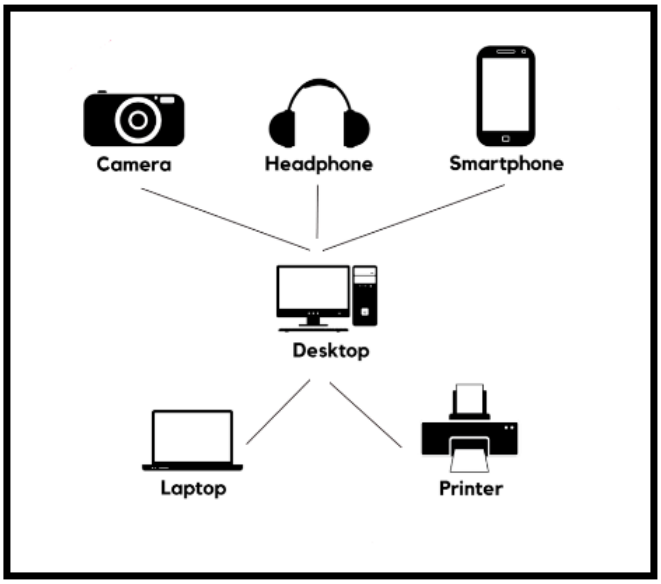


Figure5.7: Logical diagram of PAN

Features of PAN:

- Proximity: PANs typically cover a small area, usually within a range of a few meters. Devices in a PAN are typically located within the immediate vicinity of the user.
- Wireless Connectivity: PANs often use wireless technologies such as Bluetooth, Zigbee, Wi-Fi Direct, or Near Field Communication (NFC) to enable communication between devices without the need for physical cables.
- Device Interconnection: The primary purpose of a PAN is to facilitate communication and data sharing between personal devices, allowing users to synchronize data, share files, stream media, and control devices seamlessly.
- Applications: PANs support a wide range of applications, including wireless file sharing, audio streaming, gaming, wireless printing, remote control of smart home devices, and wearable health monitoring.

Advantages of PAN:

- Convenience: PANs offer convenience and flexibility by allowing users to connect and interact with their personal devices wirelessly, without the constraints of physical cables. This enables seamless integration and communication between devices, enhancing user experience and productivity.
- Mobility: PANs support mobility, allowing users to move freely within the coverage area while maintaining connectivity with their personal devices. This mobility is especially beneficial for users who frequently switch between different devices or work on the go.
- Versatility: PANs support a wide range of devices and applications, making them versatile and adaptable to various user needs and preferences. Users can easily connect and interoperate different types of devices, such as smartphones, tablets, laptops, wearables, and smart home devices.
- Ease of Setup: Setting up a PAN is typically straightforward and requires minimal configuration, especially for wireless PANs using technologies like Bluetooth or Wi-Fi Direct. Users can quickly establish connections between devices without the need for complex network configurations.

Disadvantages of PAN:

- Limited Range: PANs have a limited coverage range, typically extending only a few meters from the user. This limited range restricts the distance over which devices can communicate and may require users to remain close to their devices for effective connectivity.
- Interference: Wireless PANs may experience interference from other nearby wireless devices operating on the same frequency band. Interference can degrade signal quality, reduce data transfer speeds, and cause connectivity issues, impacting the reliability and performance of the PAN.
- Security Risks: Wireless PANs are susceptible to security risks such as unauthorized access, data interception, and device hijacking. Without adequate security measures such as encryption, authentication, and access control, sensitive information transmitted over a PAN may be vulnerable to exploitation by attackers.
- Dependency on Battery Power: Many devices in a PAN, such as smartphones, tablets, and wearables, rely on battery power for operation. The dependency on battery power means that devices may need to be recharged regularly to maintain connectivity, especially during prolonged use.

II. Based on Ownership:

- **Private Network:**

In network classification, a private network refers to a network infrastructure that is restricted in access and usage, typically limited to a specific organization, group of users, or a closed community. Owned and operated by a single organization for its internal use. Examples include corporate networks, educational institution networks, and government networks.

Key points of Private Network:

- Access Restrictions: Private networks enforce access restrictions to control who can connect to the network and access its resources. Access is usually limited to authorized users or devices within the organization or community.
- Security: Private networks prioritize security to protect sensitive information and resources from unauthorized access, interception, and tampering. Security measures may include encryption, authentication, access controls, firewalls, intrusion detection/prevention systems, and virtual private networks (VPNs).
- Ownership and Control: Private networks are owned, operated, and controlled by the organization or entity that establishes them. This ownership allows for customization, configuration, and management according to the specific needs and policies of the organization.
- Dedicated Infrastructure: Private networks often use dedicated infrastructure, including physical cables, routers, switches, servers, and other networking equipment. This dedicated infrastructure provides greater control over network performance, reliability, and security compared to shared or public networks.
- Performance: Private networks typically offer better performance and reliability compared to public networks, as they are not subject to the congestion and variability associated with shared infrastructure. Organizations can prioritize and optimize network traffic to meet their performance requirements.
- Privacy: Private networks afford greater privacy for communication and data exchange compared to public networks. Users can communicate securely within the private network without the risk of interception or monitoring by external parties.
- Costs: Establishing and maintaining a private network can be costly due to the need for dedicated infrastructure, equipment, maintenance, and operational expenses. However, the investment may be justified by the increased security, control, and performance benefits offered by a private network.
- Use Cases: Private networks are commonly used in business environments, government agencies, educational institutions, healthcare facilities, and other organizations that require secure, reliable, and controlled communication and data exchange. They support internal

communication, file sharing, application access, and collaboration among employees or members.

- **Public Network:**

In network classification, a public network refers to a network infrastructure that is openly accessible to a wide range of users, typically without access restrictions or membership requirements.

Owned and operated by service providers and made available to the general public for a fee. The Internet is the most prominent example of a public network.

Key Points of Public Network:

- Open Access: Public networks are accessible to anyone with the necessary equipment and connection capabilities, such as computers, smartphones, or other internet-enabled devices. Users do not need to be members of a specific organization or community to access the network.
- Shared Infrastructure: Public networks often rely on shared infrastructure, including telecommunications networks, internet service provider (ISP) networks, and wireless communication technologies. Multiple users and organizations share the same network resources, such as bandwidth and network infrastructure.
- Security Considerations: Public networks pose security risks due to their open access nature. Users may be vulnerable to threats such as eavesdropping, data interception, malware attacks, and unauthorized access to sensitive information. Security measures such as encryption, authentication, and secure communication protocols are essential for protecting users' data and privacy on public networks.
- Internet: The internet is the most prominent example of a public network. It consists of interconnected networks operated by ISPs, telecommunications companies, governments, and other organizations. The internet provides a global platform for communication, information exchange, and access to online services and resources.
- Global Connectivity: Public networks enable global connectivity, allowing users to communicate and exchange data with individuals, organizations, and resources worldwide. The internet's interconnected nature facilitates international collaboration, commerce, education, entertainment, and social interaction.
- Service Availability: Public networks offer a wide range of services and resources accessible to users, including websites, email services, social media platforms, online shopping, streaming media, and cloud-based applications. Users can access these services from anywhere with internet connectivity.
- Performance Variability: Performance on public networks can vary based on factors such as network congestion, bandwidth limitations, geographic distance, and the quality of network infrastructure. Users may experience fluctuations in network speed, latency, and reliability, particularly during peak usage periods or in areas with limited connectivity.
- Costs: Access to public networks may incur costs, such as subscription fees for internet service, data usage charges, and fees for premium services or content. However, many public networks offer free or subsidized access to basic internet services in public spaces, libraries, and community centers.
- Regulatory Oversight: Public networks are subject to regulatory oversight and governance by governments, regulatory agencies, and international bodies. Regulations may address issues such as network neutrality, privacy protection, data security, and consumer rights related to internet access and usage.
- Use Cases: Public networks are widely used for a variety of purposes, including communication, information dissemination, entertainment, education, e-commerce, telecommuting, and remote access to resources. They serve as a vital infrastructure for modern society, supporting economic, social, and cultural activities on a global scale.

III. Based on Connectivity:

- **Point-to-Point Network:** A network topology where devices are connected directly to each other. Each connection links only two devices. A point-to-point network refers to a network architecture where each node (or device) in the network is connected directly to another node,

forming a direct link between them. Point-to-point networks are often used in various applications, including telecommunications, computer networking, and transportation systems.

Advantages of Point to Point Network:

- Efficiency: Point-to-point connections can provide efficient data transfer because there are no intermediate devices or nodes between the sender and the receiver.
- Scalability: These networks are often scalable since adding more nodes typically involves establishing additional point-to-point connections rather than reconfiguring the entire network.
- Reliability: Point-to-point connections can offer greater reliability since failures or disruptions in one connection typically do not affect others.
- Dedicated Bandwidth: Each point-to-point connection can offer dedicated bandwidth between the connected nodes, which can be beneficial for applications requiring high-speed data transfer.
- Security: Point-to-point connections can be more secure since data is transmitted directly between the communicating nodes without passing through intermediate devices where it could be intercepted.

Disadvantages of Point to Point Network:

- Potentially higher infrastructure costs due to the need for multiple direct connections and potential scalability challenges in extremely large networks.
- Managing and maintaining numerous individual connections can become complex as the network grows.
- **Broadcast Network:** A broadcast network is a type of network architecture where data transmitted by one node is received by all other nodes in the network. This broadcasting of data allows for efficient communication and dissemination of information to multiple recipients simultaneously.

A network topology where multiple devices are connected to a shared communication medium, and data sent by one device is received by all other devices on the network. Ethernet LANs are an example of a broadcast network.

Advantages of Broadcast Network:

- Efficient Data Distribution: One of the primary advantages of broadcast networks is their ability to efficiently distribute data to multiple recipients simultaneously. Instead of sending individual messages to each recipient, a single broadcast message can reach all nodes connected to the network.
- Simplicity: Broadcast networks often have a simpler architecture compared to point-to-point networks because they do not require establishing and maintaining individual connections between every pair of nodes. This simplicity can lead to easier network management and reduced overhead in terms of configuration and maintenance.
- Scalability: Broadcast networks can be highly scalable, allowing for the addition of new nodes without significant changes to the network infrastructure. As long as the network medium can support the increased traffic load, new nodes can easily join the network and participate in data broadcasts.
- Resource Sharing: In broadcast networks, resources such as printers, servers, or shared storage devices can be easily accessed by multiple nodes. This facilitates resource sharing and collaboration among network users without the need for complex point-to-point connections or dedicated access mechanisms.
- Real-time Communication: Broadcast networks can support real-time communication applications where timely dissemination of information to multiple recipients is crucial. For example, in multimedia streaming or live broadcasting scenarios, a broadcast network can efficiently deliver data to all viewers simultaneously.
- Redundancy and Fault Tolerance: The broadcast nature of the network can provide inherent redundancy and fault tolerance. If one node fails or becomes unreachable, other nodes can still receive broadcast messages from alternative paths or neighboring nodes, reducing the impact of single-point failures.

- Broadcast-based Protocols: Certain network protocols and services are designed specifically for broadcast networks, leveraging the broadcast nature to enhance efficiency or provide unique functionalities. For example, Address Resolution Protocol (ARP) in Ethernet networks uses broadcast messages to resolve IP addresses to MAC addresses.
- Cost-effectiveness: In some cases, broadcast networks can be more cost-effective than point-to-point networks, especially in scenarios where the infrastructure costs of establishing individual connections between every pair of nodes are prohibitive. The shared medium in broadcast networks can allow for cost savings in cabling and network equipment.

Disadvantages of Broadcast Network:

- Broadcast Storms: One of the major drawbacks of broadcast networks is the potential for broadcast storms. A broadcast storm occurs when a large volume of broadcast traffic overwhelms the network, causing congestion and performance degradation. This can happen if multiple nodes continuously rebroadcast broadcast messages, leading to a vicious cycle of increased traffic.
- Bandwidth Consumption: Broadcast messages consume bandwidth on the network medium, and since these messages are received by all nodes, they can lead to inefficient use of available bandwidth. In scenarios where broadcast traffic is excessive, it can monopolize network resources and adversely affect the performance of other network communication.
- Security Risks: Broadcast networks can pose security risks due to the inherent openness of the broadcast medium. Since broadcast messages are accessible to all nodes on the network, sensitive information transmitted in broadcast packets can be intercepted by unauthorized users. Without proper encryption or access control mechanisms, confidential data may be compromised.
- Limited Privacy: In broadcast networks, data transmitted by one node is visible to all other nodes on the network. This lack of privacy can be a concern in environments where data confidentiality is important. For example, in shared LAN environments, users may inadvertently access or intercept data intended for other users.
- Collision Domain: In shared media networks like Ethernet, all nodes connected to the same segment share the same collision domain. When multiple nodes attempt to transmit data simultaneously, collisions can occur, leading to retransmissions and degraded network performance. Broadcast networks may experience higher collision rates compared to point-to-point networks, especially in densely populated or heavily utilized networks.
- Difficulty in Network Troubleshooting: Due to the broadcast nature of the network, diagnosing and troubleshooting network issues can be more challenging compared to point-to-point networks. Identifying the source of excessive broadcast traffic or pinpointing specific network problems may require more sophisticated monitoring and analysis tools.
- Scalability Challenges: While broadcast networks can be scalable to a certain extent, there are limitations to the number of nodes that can efficiently share the broadcast medium. As the network grows larger or becomes more congested, scalability challenges may arise, necessitating network segmentation or other scalability solutions.
- Management Overhead: Managing broadcast networks, especially in large-scale deployments, can involve significant overhead. Administrators may need to implement traffic management policies, monitor network performance, and optimize broadcast traffic to ensure efficient operation and mitigate potential issues.

IV. Based on Architecture:

Client-Server Network: A client-server network is a common architectural model where individual devices, called clients, request services or resources from centralized servers.

Servers provide resources such as files, applications, or databases to clients upon request. This architecture is prevalent in various computing environments, from small-scale setups like home networks to large-scale infrastructures such as enterprise networks and the internet.

Components of Client Server Network:

- Client: A client is typically a device or application that initiates communication with a server to request services or data. Examples of clients include personal computers, smartphones, tablets, and IoT devices. Clients are often end-users or end-user devices.

- Server: A server is a centralized computing system or application that provides services or resources to clients upon request. Servers are designed to handle multiple client requests simultaneously, making them capable of serving numerous clients concurrently. Examples of servers include web servers, email servers, file servers, and database servers.
- Communication: Communication in a client-server network typically follows a request-response model. Clients send requests to servers, specifying the desired service or resource, and servers process these requests and respond accordingly. This communication is often facilitated through network protocols such as HTTP, FTP, SMTP, and TCP/IP.
- Centralized Control: In a client-server network, servers act as centralized points of control for managing resources and providing services. This centralized control facilitates administration, security enforcement, and resource management within the network.
- Scalability: Client-server architectures are inherently scalable, allowing organizations to accommodate growing numbers of clients and increasing demands for services by adding additional servers or upgrading existing server hardware.
- Reliability and Redundancy: Client-server networks can be designed with redundancy and fault tolerance mechanisms to ensure high availability and reliability. This may include deploying redundant servers, implementing load balancing techniques, and employing backup and recovery strategies.
- Security: Security is a critical consideration in client-server networks, as they often involve transmitting sensitive data between clients and servers. Security measures such as encryption, authentication, access control, and firewalls are commonly employed to protect data confidentiality, integrity, and availability.

Advantages of Client-Server Network

- Centralized Management: In client server network, network resources and services are centrally managed on servers. This centralized management simplifies administration tasks such as software updates, security configurations, and user access control. Administrators can efficiently monitor and control the network from a central location, enhancing overall network management.
- Scalability: Client-server networks are highly scalable, allowing organizations to accommodate growing numbers of clients and increasing demands for services. Additional servers can be added to the network infrastructure to distribute the workload and handle additional client requests effectively. This scalability ensures that the network can adapt to changing business requirements and support future growth without significant disruptions.
- Resource Sharing: In a client-server network, resources such as files, printers, and databases are shared centrally through servers. This enables efficient resource utilization and facilitates collaboration among users. Clients can access shared resources as needed, enhancing productivity and streamlining workflows within the organization.
- Improved Performance: Client-server architectures often result in improved network performance compared to peer-to-peer networks. Servers are typically equipped with high-performance hardware and optimized software to handle client requests efficiently. Additionally, centralized management and resource allocation strategies help minimize network congestion and latency, resulting in faster response times for client applications.
- Enhanced Security: Client-server networks offer enhanced security features compared to peer-to-peer networks. Security mechanisms such as authentication, access control, encryption, and firewall protection can be implemented at the server level to safeguard sensitive data and prevent unauthorized access. Centralized security management allows administrators to enforce consistent security policies across the network, reducing the risk of security breaches and data loss.
- Reliability and Fault Tolerance: Client-server architectures can be designed with redundancy and fault tolerance mechanisms to ensure high availability and reliability. Multiple servers can be deployed in a redundant configuration, allowing for failover and load balancing to distribute traffic evenly across servers. This redundancy minimizes the impact of server failures and helps maintain continuous access to network resources and services.

- Support for Specialized Services: Client-server networks support a wide range of specialized services and applications tailored to specific business needs. Servers can be dedicated to hosting specialized software applications such as web servers, email servers, database servers, and file servers. This enables organizations to deploy custom-tailored solutions that meet their unique requirements and optimize performance for specific tasks.

Disadvantages of Client-Server Network

- Dependency on Server: Client-server networks rely heavily on servers to provide services and resources to clients. If the server experiences downtime or malfunctions, clients may be unable to access essential resources, resulting in disruptions to productivity and workflow.
- Single Point of Failure: Since client-server networks centralize resources and services on servers, these servers become single points of failure. If a server fails or becomes inaccessible, it can affect multiple clients simultaneously, leading to widespread service interruptions and downtime.
- Cost of Implementation and Maintenance: Setting up and maintaining a client-server network can be costly, particularly for small businesses or organizations with limited budgets. The initial investment in server hardware, software licenses, and infrastructure components, as well as ongoing maintenance and support costs, can be significant.
- Complexity: Client-server networks tend to be more complex than peer-to-peer networks, especially in large-scale deployments. Managing multiple servers, configuring network services, and ensuring compatibility between client and server components require specialized knowledge and expertise. This complexity can pose challenges for network administrators and increase the risk of configuration errors or security vulnerabilities.
- Network Bottlenecks: In client-server architectures, network traffic must pass through the network infrastructure to reach the server and back to the client. This centralized communication pattern can create bottlenecks, particularly in networks with high client-server interaction or limited bandwidth. Network congestion and latency can degrade performance and responsiveness, impacting user experience.
- Security Vulnerabilities: While client-server networks offer enhanced security features, they are also susceptible to security vulnerabilities and attacks. Servers represent lucrative targets for hackers seeking to exploit vulnerabilities in server software or gain unauthorized access to sensitive data. Additionally, centralizing resources on servers increases the potential impact of security breaches, as a successful attack can compromise multiple clients' data and systems.
- Scalability Challenges: While client-server networks are generally scalable, scaling them efficiently can be challenging, particularly as the network grows in size or complexity. Adding additional servers and expanding infrastructure to accommodate growing numbers of clients requires careful planning and coordination to maintain performance, reliability, and security.
- **Peer-to-Peer (P2P) Network:** A decentralized network architecture where all devices are considered equal peers and can act as both clients and servers. Peers share resources directly with each other without the need for centralized servers.

Components of Peer to Peer Network:

- Peers: Peers are individual devices (such as computers, smartphones, or IoT devices) connected to the network. Each peer has equal status and can initiate requests for resources or services as well as respond to requests from other peers. Peers in a P2P network communicate with one another directly, without relying on centralized servers.
- Resource Sharing: One of the primary features of peer-to-peer networks is resource sharing. Peers can share various types of resources, including files, storage space, processing power, and internet connections. This distributed sharing allows peers to leverage each other's resources and collaborate without relying on centralized servers.
- Decentralization: Peer-to-peer networks are decentralized, meaning there is no central authority or single point of control. Instead, control and decision-making are distributed among the network's peers. This decentralization promotes resilience and fault tolerance, as the network can continue to function even if some peers are unavailable or disconnected.

- Dynamic Topology: Peer-to-peer networks often have dynamic topologies, with peers joining and leaving the network dynamically. Peers can connect to or disconnect from the network at any time, and the network topology adjusts accordingly. This dynamic nature enables flexible scalability and adaptability to changing network conditions.
- Self-Organization: Peer-to-peer networks typically rely on self-organization mechanisms to facilitate resource discovery, routing, and communication among peers. Peers may use protocols such as Distributed Hash Tables (DHTs) or gossip protocols to maintain network connectivity and locate resources efficiently without central coordination.
- Scalability: Peer-to-peer networks are inherently scalable, as the addition of new peers does not impose a significant burden on the network infrastructure. The distributed nature of resource sharing and communication allows peer-to-peer networks to scale organically as more peers join the network.
- Security and Privacy Challenges: Peer-to-peer networks face unique security and privacy challenges due to their decentralized and distributed nature. Ensuring data confidentiality, integrity, and authenticity can be challenging, as peers may not fully trust each other. Additionally, malicious peers may attempt to exploit vulnerabilities or launch attacks, such as Distributed Denial of Service (DDoS) attacks or Sybil attacks, to disrupt the network or compromise its integrity.
- Performance Considerations: While peer-to-peer networks offer benefits such as resource sharing and decentralization, they may also face performance limitations, particularly in large-scale deployments or networks with high churn rates. Ensuring efficient resource discovery, routing, and communication while minimizing latency and network overhead requires careful design and optimization.

Advantages of Peer to Peer Network:

Table: 5.2 List of advantages of Peer to Peer Network

centralization:	P networks operate without a central server or authority, distributing control and decision-making among network peers. This decentralization promotes resilience and fault tolerance, as the network can continue to function even if individual peers fail or leave the network.
alability:	P networks are inherently scalable, as the addition of new peers does not impose a significant burden on the network infrastructure. The distributed nature of resource sharing and communication allows P2P networks to scale organically as more peers join the network.
source Sharing:	e of the primary advantages of P2P networks is resource sharing. Peers can share various types of resources, including files, storage space, processing power, and internet connections, directly with one another. This distributed sharing allows peers to leverage each other's resources and collaborate without relying on centralized servers.
duced Infrastructure Costs:	nce P2P networks do not require centralized servers, they can significantly reduce infrastructure costs compared to client-server architectures. Peers in a P2P network contribute their resources, such as storage space and bandwidth, to the network without the need for costly server hardware and maintenance.
xibility and Adaptability:	P networks offer flexibility and adaptability to changing network conditions. Peers can join or leave the network dynamically, and the network topology adjusts accordingly. This dynamic nature enables P2P networks to accommodate

Disadvantages of Peer to Peer Network:

- Security Risks: P2P networks are susceptible to security risks and vulnerabilities due to their decentralized nature. Malicious peers can exploit security flaws, launch attacks, or distribute malware across the network. Additionally, P2P networks may lack robust authentication and

access control mechanisms, making it easier for unauthorized users to gain access to sensitive information or resources.

- Legal Concerns: P2P networks are often associated with copyright infringement and illegal file sharing activities. Since peers in a P2P network can freely share files with one another, it can be challenging to enforce copyright laws and prevent the unauthorized distribution of copyrighted content. As a result, P2P networks have faced legal scrutiny and regulatory challenges in various jurisdictions.
- Reliability and Quality of Service: The reliability and quality of service in P2P networks can be variable, depending on factors such as peer availability, network topology, and resource availability. P2P networks may experience performance degradation or service interruptions if key peers become unavailable or if network conditions deteriorate. Additionally, ensuring consistent data availability and integrity can be challenging in decentralized environments.
- Scalability Challenges: While P2P networks are inherently scalable, achieving efficient scalability can be challenging, particularly in large-scale deployments. As the number of peers increases, managing network topology, resource discovery, and communication becomes more complex. Ensuring optimal performance and efficiency while maintaining network scalability requires careful design and optimization.
- Network Overhead: P2P networks can generate significant network overhead due to peer discovery, resource indexing, and data transfer activities. As peers communicate directly with one another, network traffic may increase, leading to congestion, latency, and bandwidth consumption. Managing network overhead and optimizing communication protocols are essential for maintaining network performance and efficiency.
- Lack of Centralized Control: The decentralized nature of P2P networks means there is no central authority or control mechanism governing network behavior. While this decentralization promotes resilience and fault tolerance, it can also lead to coordination challenges, conflicts of interest, and difficulties enforcing network policies or standards.
- Complexity and Management: P2P networks can be more complex to design, deploy, and manage compared to centralized architectures. Ensuring interoperability, compatibility, and security among diverse peer devices and software implementations requires specialized knowledge and expertise. Additionally, troubleshooting and resolving issues in decentralized environments can be more challenging due to the lack of centralized visibility and control.

V. Based on Technology:

- **Wireless Network:** A wireless network is a type of computer network that utilizes wireless communication technology such as Wi-Fi, Bluetooth, or cellular networks to enable devices to connect and communicate with each other without the need for physical wired connections. Instead of using cables or wires, wireless networks rely on radio waves, infrared signals, or microwave signals to transmit data between devices.

Components of Wireless Network

- Wireless Access Points (APs): Wireless access points are devices that serve as central hubs for connecting wireless devices to a wired network or the internet. They transmit and receive wireless signals, allowing devices such as laptops, smartphones, tablets, and IoT devices to connect to the network wirelessly.
- Wireless Network Interface Cards (NICs): Wireless network interface cards, also known as wireless adapters, are hardware components that enable devices to connect to wireless networks. These cards are typically integrated into devices such as laptops, smartphones, and tablets or can be added externally via USB adapters or expansion cards.
- Wireless Standards and Protocols: Wireless networks use various standards and protocols to govern communication between devices and access points. Common wireless standards include Wi-Fi (IEEE 802.11), which encompasses different versions such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6 and Wi-Fi 6E). Each standard specifies different frequencies, data rates, and modulation techniques for wireless communication.
- Frequency Bands: Wireless networks operate within specific frequency bands allocated by regulatory authorities. The most common frequency bands for Wi-Fi networks are 2.4 GHz

and 5 GHz. The 2.4 GHz band offers better range but may suffer from more interference, while the 5 GHz band provides higher data rates and less interference but has shorter range.

- Security: Security is a critical consideration in wireless networks due to the inherent vulnerability of wireless communication to interception and unauthorized access. Common security measures include Wi-Fi Protected Access (WPA) and WPA2/WPA3 encryption protocols, which encrypt data transmitted over the network, as well as authentication mechanisms such as WPA-Enterprise and Extensible Authentication Protocol (EAP).
- Range and Coverage: The range and coverage of a wireless network depend on various factors, including the transmit power of access points, antenna design, environmental obstacles, and interference from other devices or networks. Range extenders or repeaters can be used to extend the coverage area of a wireless network in large or multi-story buildings.
- Mobility: One of the key advantages of wireless networks is mobility, allowing users to connect to the network and access resources from anywhere within the coverage area. Mobile devices such as smartphones and tablets can seamlessly roam between different access points without losing connectivity, enabling users to stay connected while on the move.
- Application Areas: Wireless networks are widely used in various applications and industries, including home networking, business environments, education, healthcare, hospitality, transportation, and telecommunications. They enable convenient and flexible connectivity for devices and users in both indoor and outdoor settings.

Advantages of Wireless Network

- Mobility: Perhaps the most significant advantage of wireless networks is mobility. Users can connect to the network and access resources from anywhere within the coverage area without being tethered to a specific location by cables or wires. This mobility enables users to work, communicate, and access information conveniently, whether they are at home, in the office, or on the go.
- Flexibility and Convenience: Wireless networks provide flexibility and convenience in network deployment and access. Users can easily connect devices to the network without the need for physical cabling, allowing for quick setup and configuration. Additionally, wireless networks support a wide range of devices, including laptops, smartphones, tablets, IoT devices, and wearable technology, making it easy to integrate new devices into the network.
- Scalability: Wireless networks are inherently scalable, allowing organizations to expand or reconfigure their network infrastructure easily. Additional access points can be deployed to increase coverage area or accommodate growing numbers of users and devices. This scalability enables businesses to adapt to changing requirements and scale their network infrastructure as needed without significant disruptions.
- Cost Savings: Wireless networks can offer cost savings compared to wired networks, particularly in terms of infrastructure deployment and maintenance. Eliminating the need for physical cabling reduces installation costs and eliminates the ongoing expenses associated with cable management, maintenance, and replacement. Additionally, wireless networks can support Bring Your Own Device (BYOD) policies, allowing organizations to leverage existing employee devices rather than purchasing dedicated hardware.
- Improved Productivity: Wireless networks can enhance productivity by enabling seamless connectivity and collaboration among users. Employees can access network resources and communicate with colleagues from anywhere within the coverage area, facilitating flexible work arrangements and remote collaboration. This improved connectivity can lead to increased efficiency, faster decision-making, and greater responsiveness to customer needs.
- Ease of Installation and Expansion: Setting up a wireless network is generally easier and faster than deploying a wired network. Wireless access points can be installed quickly without the need for extensive cable runs or infrastructure modifications. Additionally, wireless networks can be easily expanded or reconfigured to accommodate changes in network topology, user requirements, or environmental conditions.
- Accessibility: Wireless networks provide accessibility to users in various locations and environments, including homes, offices, public spaces, and outdoor areas. Users can connect to the network from multiple devices simultaneously, enabling seamless access to

applications, services, and online resources. This accessibility enhances connectivity and communication, allowing users to stay connected wherever they are.

- Integration with Mobile Devices: Wireless networks seamlessly integrate with mobile devices such as smartphones, tablets, and laptops, allowing users to take advantage of their mobility and functionality. Mobile devices can connect to the network via Wi-Fi, enabling users to access the internet, email, social media, and other online services while on the move. This integration enhances user experience and productivity, supporting modern mobile lifestyles.

Disadvantages of Wireless Network

- Interference and Signal Degradation: Wireless networks are susceptible to interference from various sources, including other wireless devices, electronic appliances, and physical obstacles such as walls and buildings. Interference can degrade signal quality, reduce network performance, and cause connectivity issues for users, particularly in crowded or congested environments.
- Limited Range and Coverage: Wireless networks have limited range and coverage compared to wired networks. The range of wireless signals is affected by factors such as transmit power, antenna design, and environmental conditions. Users located at the edge of the coverage area may experience weaker signals, slower data rates, or intermittent connectivity, especially in large or obstructed spaces.
- Security Vulnerabilities: Wireless networks are inherently vulnerable to security threats, including eavesdropping, unauthorized access, and data breaches. Without proper security measures, wireless communication can be intercepted or compromised by attackers, potentially leading to the theft of sensitive information or unauthorized access to network resources. Common security risks in wireless networks include Wi-Fi eavesdropping, rogue access points, and man-in-the-middle attacks.
- Bandwidth Limitations: Wireless networks have limited bandwidth compared to wired networks, which can impact network performance and user experience, especially in high-traffic environments. Shared wireless channels may become congested, leading to slower data rates, increased latency, and reduced throughput for users accessing network resources simultaneously. Bandwidth limitations can be particularly challenging for applications requiring high-speed data transfer or real-time communication.
- Reliability and Stability: Wireless networks may be less reliable and stable than wired networks, especially in environments with fluctuating signal conditions or interference sources. Wireless connections are more susceptible to disruptions due to factors such as signal attenuation, environmental changes, and device mobility. Users may experience dropped connections, packet loss, or network downtime, affecting productivity and user experience.
- Complexity of Management: Managing and troubleshooting wireless networks can be more complex than wired networks due to factors such as interference, signal propagation, and device compatibility. Wireless networks require careful planning, configuration, and optimization to ensure optimal performance, coverage, and security. Additionally, diagnosing and resolving issues in wireless environments may require specialized expertise and tools, increasing the complexity of network management.
- Cost of Infrastructure: While wireless networks can offer cost savings in terms of installation and maintenance, the initial cost of infrastructure deployment can be higher than wired networks, especially for large-scale deployments. Wireless access points, antennas, and network controllers may require significant investment, particularly for organizations with extensive coverage requirements or specialized deployment scenarios.
- Health Concerns: Although scientific research has not conclusively proven adverse health effects from wireless networks, some individuals express concerns about potential health risks associated with prolonged exposure to electromagnetic radiation emitted by wireless devices and infrastructure. While regulatory agencies establish safety guidelines and standards for wireless technology, ongoing research and public debate continues regarding the long-term health impacts of wireless networks.
- **Wired Network:** A wired network is a type of computer network that uses physical cables or wires such as twisted pair, coaxial cable, or fiber optic cable to connect devices and enable

communication between them. Unlike wireless networks, which rely on wireless communication technology, wired networks utilize physical connections to transmit data between devices. Wired networks offer several advantages, making them suitable for various applications and environments.

Components of Wired Network

- Ethernet Cables: Ethernet cables are the most common type of cables used in wired networks to connect devices such as computers, routers, switches, and printers. Ethernet cables come in various categories, including Cat5e, Cat6, and Cat6a, each offering different levels of performance and bandwidth.
- Network Interface Cards (NICs): Network interface cards, also known as network adapters, are hardware components installed in devices to enable them to connect to a wired network. NICs interface with the device's motherboard and facilitate communication between the device and the network via Ethernet cables.
- Switches and Hubs: Switches and hubs are networking devices used to connect multiple devices within a wired network. Switches operate at the data link layer (Layer 2) of the OSI model and forward data packets only to the intended recipient, improving network efficiency and bandwidth utilization. Hubs, on the other hand, operate at the physical.

Advantages of Wired Network

- Speed and Performance: Wired networks typically offer higher data transfer speeds and lower latency compared to wireless networks. Ethernet cables can support Gigabit Ethernet and even higher speeds, providing fast and reliable connectivity for data-intensive applications such as file transfer, video streaming, and online gaming.
- Reliability: Wired connections are generally more reliable and stable than wireless connections. Since data is transmitted over a physical cable, it is not susceptible to interference from external sources such as electromagnetic interference (EMI), radio frequency interference (RFI), or environmental obstacles. This reliability ensures consistent network performance and minimizes the risk of connectivity issues or signal disruptions.
- Security: Wired networks are inherently more secure than wireless networks due to the physical nature of the connections. Since data is transmitted over a physical cable, it is more difficult for unauthorized users to intercept or eavesdrop on network traffic compared to wireless communication, which can be intercepted over the airwaves. Additionally, wired networks can implement security measures such as VLANs, port security, and physical access controls to enhance network security further.
- Immunity to Interference: Wired networks are less susceptible to interference from external sources compared to wireless networks. Since data is transmitted over a physical medium (cables), it is not affected by factors such as electromagnetic interference (EMI), radio frequency interference (RFI), or environmental obstacles that can degrade wireless signals. This immunity to interference ensures stable and consistent network performance, even in challenging environments.
- Lower Cost of Infrastructure: While the initial cost of infrastructure deployment may be higher for wired networks due to the purchase and installation of cables, switches, and other networking equipment, the long-term cost of maintenance and operation is generally lower compared to wireless networks. Wired networks require less ongoing maintenance and troubleshooting, as they are less susceptible to signal interference, connection issues, and security vulnerabilities.
- Scalability and Bandwidth: Wired networks offer greater scalability and bandwidth compared to wireless networks. Ethernet cables can support higher data rates and accommodate more devices simultaneously, making it easier to scale the network infrastructure to support growing numbers of users and devices. Additionally, wired networks can use technologies such as Ethernet bonding or link aggregation to combine multiple network links for increased bandwidth and redundancy.
- Ease of Installation and Management: Setting up and managing a wired network is generally easier and more straightforward than a wireless network. Ethernet cables can be easily installed and routed through buildings or structured cabling systems, and network devices

such as switches and routers can be centrally located and managed. **Disadvantages of Wired Network**

- Limited Mobility: One of the primary disadvantages of wired networks is limited mobility. Since devices are connected to the network via physical cables, users are tethered to a specific location and cannot move freely while connected to the network. This limitation can restrict flexibility and mobility, especially in environments where users need to move around or access network resources from multiple locations.
- Cost of Infrastructure: The initial cost of infrastructure deployment for wired networks can be higher compared to wireless networks. Setting up a wired network requires purchasing and installing cables, switches, routers, and other networking equipment, as well as labor costs for installation and configuration. Additionally, the cost of cabling may vary depending on factors such as cable type, length, and installation complexity.
- Complexity of Installation: Installing a wired network can be more complex and labor-intensive than setting up a wireless network, especially in existing buildings or structures where running cables may require drilling holes, pulling cables through walls or ceilings, and routing cables around obstacles. The complexity of installation can increase deployment time and cost, particularly in large-scale or multi-story environments.
- Maintenance and Flexibility: Wired networks may require more maintenance and management compared to wireless networks. Maintaining and troubleshooting physical cables, connectors, and network devices such as switches and routers can be time-consuming and labor-intensive. Additionally, wired networks may lack the flexibility to accommodate changes in network topology, user requirements, or environmental conditions without significant reconfiguration or infrastructure modifications.
- Physical Constraints: Wired networks are subject to physical constraints such as cable length limitations and environmental restrictions. Ethernet cables have maximum length limitations, typically ranging from 100 meters for twisted-pair cables (e.g., Cat5e, Cat6) to longer distances for fiber optic cables. Exceeding these cable length limits can result in signal degradation and reduced network performance. Additionally, wired networks may be less suitable for environments where physical cabling is impractical or prohibited, such as historic buildings or outdoor spaces.
- Disruption and Damage: Physical cables used in wired networks are susceptible to disruption and damage from factors such as construction work, accidental cuts or breaks, and environmental hazards (e.g., water, heat, pests). Disruptions or damage to network cables can result in network downtime, connectivity issues, and data loss, requiring costly repairs and maintenance.
- Limited Flexibility for Expansion: Expanding or reconfiguring a wired network may be more challenging and costly compared to wireless networks. Adding new network devices or extending network coverage may require running additional cables, installing new infrastructure components, and reconfiguring network settings, which can increase deployment time and complexity.

VI. Based on Topology:

- **Bus Network:** Devices are connected to a single communication line, called a bus. Data is transmitted to all devices on the network, and each device checks whether the data is intended for it.
- **Star Network:** Devices are connected to a central hub or switch. Data flows through the hub, which manages communication between devices.
- **Ring Network:** Devices are connected in a closed loop or ring configuration. Data travels around the ring from one device to the next until it reaches its destination.
- We will discuss topologies in detail in 5.6

These classifications provide a framework for understanding the different types of networks and their characteristics, helping to design, deploy, and manage network infrastructures effectively.

5.6 Network Topologies

Network topology refers to the arrangement of devices and connections in a computer network. It defines how devices are interconnected and the paths along which data flows within the network.

Different network topologies offer various advantages and disadvantages in terms of performance, scalability, reliability, and ease of maintenance.

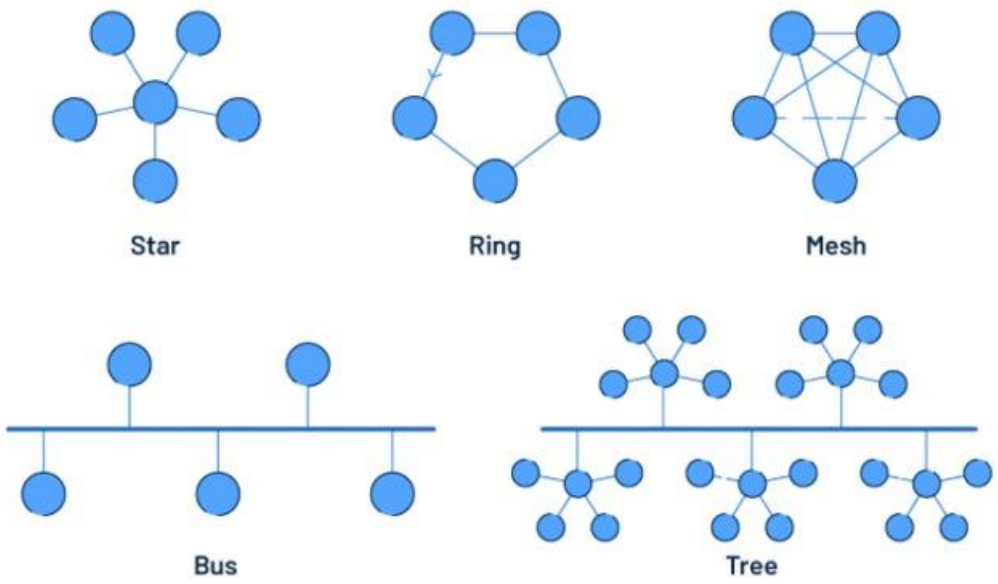


Figure 5.8: Types of Network Topologies

Common Network Topologies:

Bus Topology:

In a bus topology, all devices are connected to a single communication line or "bus."

Data is transmitted along the bus, and all devices receive the transmitted data. Bus topology is simple to implement and cost-effective for small networks but prone to collisions and difficult to troubleshoot. Bus topology has limited scalability, a single point of failure (the bus), and potential performance issues as the network grows.

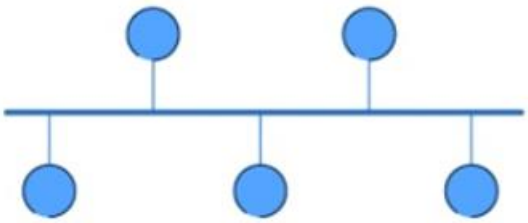


Figure 5.9: Star Network Topology

Key Points of Bus Topology:

- Single Communication Line: In a bus topology, all devices are connected to a central cable or bus, which serves as the communication medium for transmitting data between devices.
- Terminators: The ends of the bus cable are terminated with resistors to prevent signal reflection and ensure proper signal transmission.
- Shared Medium: All devices on the bus share the same communication medium, meaning that data transmitted by one device is received by all other devices on the bus.
- Ethernet Networks: Bus topology was commonly used in early Ethernet networks, where devices were connected to a coaxial cable using BNC connectors.

Advantages of Bus Topology:

- Simplicity: Bus topology is simple to implement and understand, making it suitable for small networks with a limited number of devices.

- Cost-Effective: Bus topology requires less cabling compared to other topologies, reducing installation costs, and making it cost-effective for small-scale deployments.
- Easy to Expand: Adding new devices to a bus topology is relatively easy—all that's required is connecting the new device to the bus cable.

Disadvantages of Bus Topology:

- Single Point of Failure: The bus cable represents a single point of failure—if the bus cable is damaged or fails, the entire network becomes inoperable.
- Limited Scalability: Bus topology is not easily scalable, especially as the number of devices increases. Adding too many devices can lead to signal degradation and performance issues.
- Performance Issues: As the number of devices on the bus increases, the bandwidth available to each device decreases, leading to potential performance issues such as data collisions and network congestion.
- Difficulty in Troubleshooting: Identifying and troubleshooting network issues in a bus topology can be challenging, as a fault in any part of the bus cable can disrupt communication for all devices connected to the bus.

Star Topology:

In a star topology, all devices are connected to a central hub or switch. Devices communicate with each other through the hub/switch, which acts as a central point of control. Star topology is easy to install and maintain, scalability, fault tolerance (failure of one device does not affect others) but if the hub fails, all connected devices lose connectivity.

Figure 5.10: Star Network Topology

Key Points of Star Topology:

- Central Hub or Switch: In a star topology, all devices are connected to a central hub or switch through individual point-to-point connections.
- Point-to-Point Connections: Each device has a dedicated connection to the central hub or switch, forming a star-like structure.
- Centralized Control: The central hub or switch acts as a central point of control for data transmission, facilitating communication between devices.
- Fault Isolation: In star topology, if one device or connection fails, it does not affect the operation of other devices on the network. The fault is isolated to the affected device or connection.

Advantages of Star Topology:

- Scalability: Star topology is highly scalable, allowing for easy expansion by adding new devices or connections to the central hub or switch. This scalability makes it suitable for both small and large networks.
- Ease of Installation and Maintenance: Star topology is easy to install and maintain compared to other topologies. Adding or removing devices requires minimal disruption to the network, and troubleshooting is simplified due to the centralized structure.
- Reliability: Star topology offers better reliability compared to other topologies, as the failure of one device or connection does not affect the operation of other devices on the network. This fault tolerance improves network uptime and reliability.
- High Performance: Each device has a dedicated connection to the central hub or switch, providing high bandwidth and minimizing data collisions. This results in better network performance and faster data transmission speeds.

Disadvantages of Star Topology:

- Dependency on Central Device: The central hub or switch represents a single point of failure in star topology. If the central device fails, the entire network becomes inoperable until the issue is resolved.
- Cost of Infrastructure: Star topology requires additional cabling and networking equipment, such as hubs or switches, compared to other topologies like bus or ring. The cost of infrastructure can be higher, especially for large-scale deployments.
- Limited Scalability with Shared Medium: While star topology is scalable, the bandwidth available to each device is limited by the capacity of the central hub or switch. Adding too many devices can lead to network congestion and performance issues.
- Performance Degradation with Network Traffic: As the number of devices connected to the central hub or switch increases, network traffic may become congested, leading to performance degradation and slower data transmission speeds.

Ring Topology:

In a ring topology, each device is connected to two other devices, forming a closed loop or ring.
Data circulates around the ring in one direction, with each device receiving and forwarding the data. Ring topology is simple and easy to install, each device has equal access to the network, no central point of failure but susceptible to single-point failures and difficult to expand. Failure of a single device can disrupt the entire network, limited scalability, and potential performance issues as the network grows.

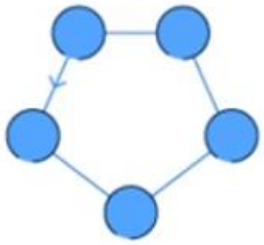


Figure5.11: Ring Network Topology

Key Points of Ring Topology:

- Closed Loop Structure: In a ring topology, each device is connected to exactly two other devices, forming a closed loop or ring.
- Unidirectional Data Flow: Data circulates around the ring in one direction, passing through each device until it reaches its destination.
- Token Passing: To avoid data collisions, ring topologies often use a token passing mechanism, where a special token is circulated around the ring to control data transmission.
- Equal Access: Each device on the ring has equal access to the network, and there is no central point of control or single point of failure.

Advantages of Ring Topology:

- Equal Access and Fairness: Ring topology provides equal access to all devices on the network, ensuring fairness in data transmission. Each device has the opportunity to transmit data without being prioritized over others.
- No Central Point of Failure: Unlike star topology, ring topology does not have a central hub or switch, meaning there is no single point of failure. If one device or connection fails, data can still circulate around the ring in the opposite direction.
- Simple and Easy to Implement: Ring topology is relatively simple and easy to implement, making it suitable for small to medium-sized networks. Devices can be connected in a logical ring structure without the need for additional networking equipment.
- Efficient Use of Network Bandwidth: In ring topology, data circulates around the ring in one direction, minimizing data collisions and maximizing the efficient use of network bandwidth. This can result in better network performance and faster data transmission speeds.

Disadvantages of Ring Topology:

- Single Point of Failure with Token: While ring topology does not have a single point of failure in terms of network connectivity, the token passing mechanism represents a potential

single point of failure. If the token is lost or corrupted, data transmission may be disrupted until the issue is resolved.

- Limited Scalability: Ring topology is not easily scalable, especially as the number of devices increases. Adding new devices to the ring may require reconfiguring the entire network, and the addition of too many devices can lead to performance issues and signal degradation.
- Complex Troubleshooting: Identifying and troubleshooting network issues in ring topology can be challenging, especially if a device or connection fails. Locating the source of a problem may require systematically testing each device and connection in the ring.
- Performance Issues with Network Traffic: As the number of devices on the ring increases or network traffic becomes congested, performance issues such as latency and data collisions may occur. This can lead to slower data transmission speeds and reduced network efficiency.

Mesh Topology:

In a mesh topology, each device is connected to every other device in the network, forming a fully interconnected mesh. Provides redundancy and fault tolerance, as data can take multiple paths to reach its destination. Mesh topology is complex and expensive to implement, especially in large networks, but offers high reliability and performance. Issues are high cost due to the large number of connections, and potential performance issues due to increased network traffic.

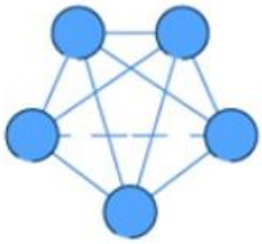


Figure5.12: Mesh Network Topology

Key Points of Mesh Topology:

- Fully Interconnected: In a mesh topology, each device has a direct point-to-point connection to every other device in the network, creating multiple communication paths.
- Redundancy: Mesh topology provides redundancy and fault tolerance, as there are multiple paths for data to travel between devices. If one path fails, data can be rerouted through alternate paths, ensuring continuity of communication.
- Scalability: Mesh topology is highly scalable, allowing for easy expansion by adding new devices or connections to the network. As the number of devices increases, the number of communication paths also increases, maintaining connectivity and performance.
- Reliability: Mesh topology offers high reliability and robustness, as there are no single points of failure in the network. Even if one or more devices or connections fail, data can still be transmitted through alternative paths.

Advantages of Mesh Topology:

- High Reliability and Fault Tolerance: Mesh topology provides high reliability and fault tolerance due to its redundant connections. If one path fails, data can be rerouted through alternate paths, ensuring uninterrupted communication.
- Scalability: Mesh topology is highly scalable and flexible, allowing for easy expansion by adding new devices or connections to the network. As the network grows, the number of communication paths increases, maintaining connectivity and performance.
- Performance: Mesh topology offers high performance and throughput, as multiple communication paths allow for efficient data transmission and load balancing. This can result in faster data transmission speeds and improved network efficiency.
- Privacy and Security: Mesh topology can offer enhanced privacy and security, as data transmitted between devices may not pass through intermediate nodes or network infrastructure. This can reduce the risk of unauthorized access or interception of sensitive information.

Disadvantages of Mesh Topology:

- Complexity: Mesh topology can be complex to design, implement, and manage, especially in large-scale networks with numerous devices and connections. Configuring and maintaining the network requires careful planning and coordination to ensure optimal performance and reliability.
- Cost: Mesh topology can be costly to deploy and maintain, as it requires a large number of cables, switches, and networking equipment to establish redundant connections between devices. The cost of infrastructure and equipment can be prohibitive for some organizations, especially for small-scale deployments.
- Overhead: Maintaining redundant connections in a mesh topology can result in increased overhead and network traffic, as devices exchange routing information and monitor the status of alternative paths. This can consume network resources and bandwidth, affecting overall network performance.
- Physical Space Requirements: Mesh topology may require additional physical space to accommodate the large number of cables and networking equipment needed to establish redundant connections between devices. This can be challenging in environments with limited space or infrastructure constraints.

Hybrid Topology:

A hybrid topology combines two or more different types of network topologies, such as a combination of star and bus, star and ring, or any other combination. It combines two or more different network topologies into a single network. It provides flexibility and scalability while leveraging the strengths of multiple topologies. Issues are complexity in design and implementation, increased cost and maintenance requirements.

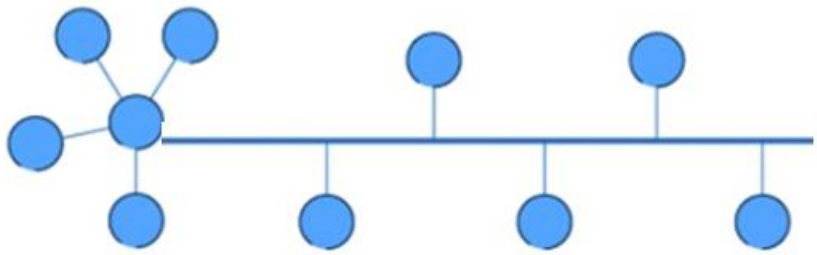


Figure 5.13: Hybrid Network Topology(Star & Bus Topologies)

Key Points of Hybrid Topology:

- Combination of Topologies: Hybrid topology combines two or more different types of network topologies to form a single network infrastructure. For example, a hybrid topology may include a combination of star and mesh topologies or a combination of bus and ring topologies.
- Flexibility: Hybrid topology offers flexibility in design and implementation, allowing organizations to tailor the network to meet specific requirements and optimize performance. Different parts of the network can be configured with different topologies based on factors such as scalability, reliability, and cost.
- Scalability and Redundancy: By combining multiple topologies, hybrid topology provides scalability and redundancy, enabling organizations to expand the network and maintain connectivity even in the event of device or connection failures.

Advantages of Hybrid Topology:

- Optimized Performance: Hybrid topology allows organizations to optimize network performance by selecting the most suitable topology for each part of the network. For example, star topology may be used for local area networks (LANs) within departments or offices, while mesh topology may be used for backbone connections between buildings or remote locations.

- Flexibility and Customization: Hybrid topology offers flexibility and customization, allowing organizations to design a network infrastructure that meets their specific requirements and preferences. Different topologies can be combined and tailored to address factors such as scalability, reliability, security, and cost-effectiveness.
- Scalability and Redundancy: By combining multiple topologies, hybrid topology provides scalability and redundancy, enabling organizations to expand the network and maintain connectivity even in the event of device or connection failures. This redundancy enhances network reliability and fault tolerance, reducing the risk of downtime and data loss.

Disadvantages of Hybrid Topology:

- Complexity: Hybrid topology can be complex to design, implement, and manage, especially in large-scale networks with diverse topologies and configurations. Configuring and maintaining the network requires expertise and coordination to ensure optimal performance and reliability.
- Cost: Hybrid topology may involve higher costs compared to single-topology networks, as it requires a combination of networking equipment, cables, and infrastructure to support multiple topologies. The cost of deployment, maintenance, and management may be prohibitive for some organizations, especially for small-scale deployments.
- Overhead: Maintaining multiple topologies in a hybrid network can result in increased overhead and complexity, as devices exchange routing information and monitor the status of connections across different topologies. This can consume network resources and bandwidth, affecting overall network performance and efficiency.

Tree (Hierarchical) Topology:

Tree topology, also known as hierarchical topology, is a type of network topology that combines characteristics of both bus and star topologies. Hierarchical arrangement of devices in multiple levels or layers. Typically consists of a root node (such as a main switch or router) connected to multiple secondary nodes, which in turn connect to additional devices.Provides scalability and centralized management but can be complex to design and implement.

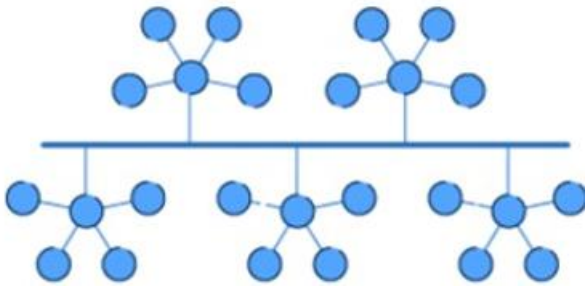


Figure 5.14: Tree Network Topology

Key Points of Tree Topology

- Hierarchical Structure: In a tree topology, network devices are organized in a hierarchical structure resembling a tree, with multiple levels or layers of interconnected nodes.
- Root Node: At the top of the hierarchy is a central node called the root node, which serves as the main point of communication and control for the entire network.
- Branches: The root node is connected to multiple intermediate nodes or branch nodes, which in turn are connected to other nodes, forming branches or sub-networks.
- Leaves: At the bottom of the hierarchy are the leaf nodes, which represent end devices such as computers, printers, and other peripherals.

Advantages of Tree Topology

- Scalability: Tree topology is highly scalable, allowing for easy expansion by adding new branches or nodes to the network. As the organization grows, additional branches can be added to accommodate new departments, offices, or locations.
- Centralized Control: The root node in a tree topology provides centralized control and management of the network. Administrators can configure and manage network settings, access control, and security policies from the root node, ensuring consistency and uniformity across the network.

- Segmentation and Isolation: Tree topology allows for segmentation and isolation of network traffic within different branches or sub-networks. Each branch can operate independently, with its own dedicated resources and connectivity, reducing the risk of network congestion and improving performance.
- Redundancy and Fault Tolerance: Tree topology provides redundancy and fault tolerance by allowing multiple paths for data transmission between nodes. If one branch or connection fails, data can be rerouted through alternative paths, ensuring continuity of communication.

Disadvantages of Tree Topology

- Complexity: Tree topology can be complex to design, implement, and manage, especially in large-scale networks with multiple branches and nodes. Configuring and maintaining the network requires careful planning and coordination to ensure optimal performance and reliability.
- Single Point of Failure: While tree topology provides redundancy and fault tolerance, the root node represents a single point of failure in the network. If the root node fails, communication between branches may be disrupted until the issue is resolved.
- Cost: Tree topology may involve higher costs compared to simpler topologies such as bus or star, as it requires additional networking equipment, cables, and infrastructure to support multiple branches and nodes. The cost of deployment, maintenance, and management may be prohibitive for some organizations, especially for small-scale deployments.
- Performance Issues: As the number of branches and nodes in the network increases, network performance may degrade due to increased traffic and congestion. This can lead to slower data transmission speeds and reduced network efficiency, especially during peak usage periods.

Point-to-Point Topology:

Point-to-point topology, also known as a point-to-point connection, is a simple network topology where two devices are directly connected by a dedicated communication link. It connects two devices directly without any intermediary devices. It is used in simple setups like connecting a computer to a printer or a router to a modem. Provides a dedicated connection between devices but lacks scalability and fault tolerance.

Key Points of Point-to-Point Topology

- Direct Connection: Point-to-point topology consists of a single communication link between two devices, allowing for direct communication without the need for intermediate devices or network infrastructure.
- Dedicated Link: Each connection in point-to-point topology is dedicated to the two connected devices, providing exclusive communication between them.
- Common examples of point-to-point connections include telephone lines, leased lines, serial connections, and point-to-point wireless links (e.g., microwave links, satellite links).

Advantages of Point-to-Point Topology

- Simplicity: Point-to-point topology is simple and easy to implement, requiring minimal configuration and management. It is suitable for connecting two devices over short or long distances without the need for complex networking equipment or infrastructure.
- Dedicated Bandwidth: Each connection in point-to-point topology provides dedicated bandwidth for communication between the two devices. This ensures consistent and reliable data transmission without interference from other devices or network traffic.
- Security: Point-to-point connections offer inherent security benefits, as data transmitted over the dedicated link is less susceptible to interception or eavesdropping compared to shared network connections. This is particularly important for transmitting sensitive or confidential information.
- Predictable Performance: Point-to-point connections provide predictable performance characteristics, such as low latency and minimal packet loss, making them suitable for real-time applications such as voice and video communication, remote monitoring, and control systems.

Disadvantages of Point-to-Point Topology

- Limited Connectivity: Point-to-point topology is limited to connecting only two devices at a time. While this simplicity is advantageous for direct communication between specific devices, it may not be suitable for scenarios requiring connectivity between multiple devices or network segments.
- Scalability: Point-to-point topology is not easily scalable, as each connection requires a dedicated communication link between two devices. Adding more devices to the network would require additional point-to-point connections, which can be costly and impractical for large-scale deployments.
- Maintenance Overhead: Managing and maintaining multiple point-to-point connections can be cumbersome, especially in environments with numerous connections or remote locations. Each connection may require individual monitoring, troubleshooting, and maintenance, leading to increased overhead and complexity.
- Cost: Point-to-point connections can be costly to deploy and maintain, especially for long-distance or high-speed links that require specialized equipment or infrastructure. The cost of leasing dedicated lines or acquiring wireless spectrum can also be a significant factor in the overall cost of implementing point-to-point connections.

Each network topology has its advantages and disadvantages, and the choice of topology depends on factors such as the size and requirements of the network, budget constraints, and the need for scalability and fault tolerance.

5.7 Network Types

Computer networks can be classified into various types based on their size, purpose, and geographical coverage. Here are some common types of computer networks:

- **Local Area Network (LAN):**

A LAN is a network that covers a small geographical area, such as a single building, office, or campus. Typically used to connect devices like computers, printers, and servers within an organization. LANs often use Ethernet or Wi-Fi technologies for communication.

- **Wide Area Network (WAN):**

A WAN is a network that spans a large geographical area, such as a country, continent, or even worldwide. Connects multiple LANs and MANs over long distances using telecommunications links, such as leased lines, fiber optic cables, or satellite links. The Internet is the largest WAN, connecting millions of networks and devices globally.

- **Metropolitan Area Network (MAN):**

A MAN is a network that covers a larger geographical area than a LAN but smaller than a WAN, such as a city or metropolitan area. Often used by service providers to provide high-speed connectivity to businesses and organizations within a city.

- **Personal Area Network (PAN):**

A PAN is a network used for communication among devices within the immediate vicinity of an individual, typically within a range of a few meters.
Examples include Bluetooth networks used to connect smartphones, tablets, and wearable devices.

- **Client-Server Network:**

A client-server network is a network architecture where client devices request services or resources from centralized servers. Servers provide resources such as files, applications, or databases to clients upon request. Commonly used in business environments for centralized data storage, application hosting, and resource management.

- **Peer-to-Peer Network (P2P):**

A peer-to-peer network is a decentralized network where all devices have equal status and can act as both clients and servers. Devices share resources directly with each other without the need for centralized servers. Commonly used for file sharing, collaborative applications, and distributed computing.

- **Virtual Private Network (VPN):**

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over

a less secure network, such as the internet. Used to enable secure remote access to an organization's network resources for remote users or branch offices. Provides encryption and authentication mechanisms to ensure privacy and data security.

These are some of the primary types of computer networks, each serving specific purposes and catering to different networking needs.

5.8 Transmission Media

Transmission media, also known as communication channels, are the physical pathways through which data is transmitted from one device to another in a communication network. Different types of transmission media have distinct characteristics, such as data transfer rates, distances, and susceptibility to interference. Here are some common types of transmission media:

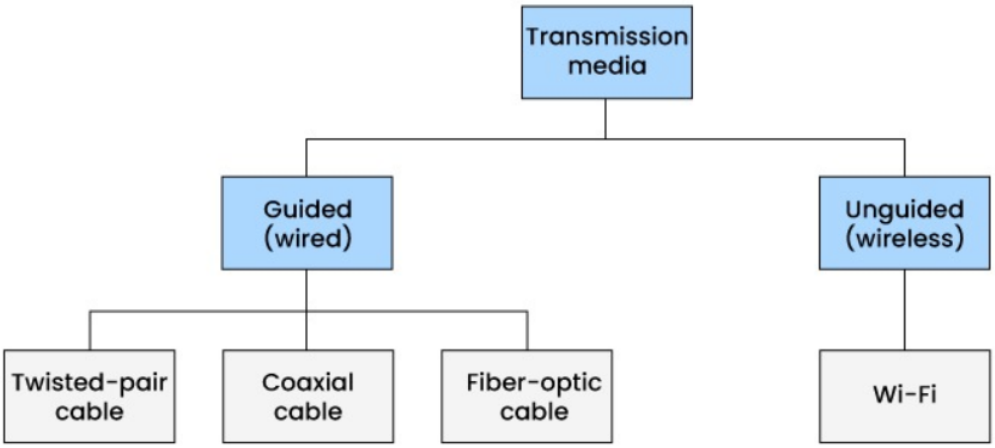


Figure 5.16: Types of Transmission Media

I. **Guided Transmission Media (Wired):** Guided transmission media, also known as wired transmission media, are physical pathways or cables through which data signals are transmitted from one device to another in a communication network. These cables provide a guided path for the transmission of electromagnetic signals, which can be in the form of electrical or optical signals

a. **Twisted Pair Cable:**

Twisted pair cable is commonly used in telecommunications and computer networking.
It consists of pairs of insulated copper wires twisted together.
Two types: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).
Used in LANs for Ethernet connections, telephone lines, and in-home networking.
Affordable, easy to install, and flexible, but susceptible to electromagnetic interference (EMI) and limited in distance compared to other media.

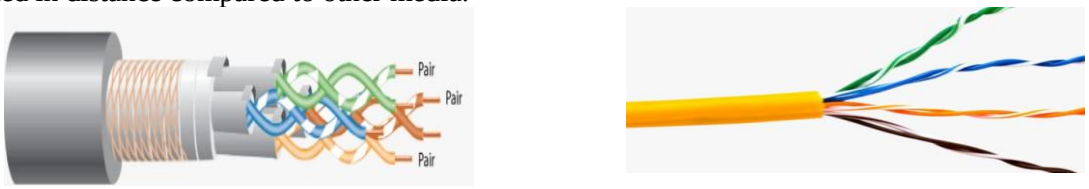


Figure 5.17: Shielded twisted pair and Unshielded twisted pair

Key Points of Twisted Pair Cable

- Twisting: The wires in twisted pair cable are twisted together in pairs to reduce electromagnetic interference (EMI) and crosstalk from adjacent pairs. The twisting pattern helps to cancel out interference and maintain signal integrity.

- Insulation: Each wire in the twisted pair cable is insulated to prevent short circuits and electrical interference. The insulation material can vary depending on the cable's application and environmental conditions.
- Categories: Twisted pair cable is classified into different categories (e.g., Cat 5e, Cat 6, Cat 6a) based on performance specifications such as bandwidth, attenuation, and crosstalk. Higher category cables generally support higher data rates and better performance.
- Termination: Twisted pair cable is terminated with connectors (e.g., RJ45 connectors for Ethernet) to connect to network devices such as computers, switches, and routers. Proper termination is essential for maintaining signal quality and reducing signal loss.

Types of Twisted Pair Cable

- Unshielded Twisted Pair (UTP): Consists of twisted pairs of copper wires without any additional shielding. Commonly used in telephone lines, Ethernet networks, and residential wiring. Available in various categories (e.g., Cat 5e, Cat 6, Cat 6a) with different specifications for bandwidth and performance.
- Shielded Twisted Pair (STP): Similar to UTP but with additional shielding to protect against electromagnetic interference (EMI) and radio frequency interference (RFI). Shielding can be made of foil or braided metal around the twisted pairs. Provides better performance in noisy environments and over longer distances compared to UTP.

Advantages of Twisted Pair Cable

- Cost-Effective: Twisted pair cable is relatively inexpensive compared to other types of transmission media such as fiber optic cable or coaxial cable, making it cost-effective for both residential and commercial applications.
- Easy to install and maintain: Twisted pair cable is flexible and easy to install, allowing for easy routing around corners, through walls, and in tight spaces. It can be installed using simple tools and techniques, making it suitable for DIY installations.
- Widely Available: Twisted pair cable is widely available and compatible with a wide range of networking equipment and devices. It is the most common type of cable used in Ethernet networks and telecommunications infrastructure.
- Immunity to External Interference: Twisted pair cable is less susceptible to external interference such as electromagnetic interference (EMI) and radio frequency interference (RFI) compared to unshielded cables. Shielded twisted pair (STP) provides additional protection against interference in noisy environments.

Disadvantages of Twisted Pair Cable

- Limited Distance: Twisted pair cable has limited transmission distances compared to other transmission media such as fiber optic cable. Signal strength degrades over long distances, limiting the maximum cable length for reliable communication.
- Susceptible to Crosstalk: Despite the twisting pattern, twisted pair cable is still susceptible to crosstalk, especially in high-density cabling environments. Crosstalk occurs when signals from adjacent pairs interfere with each other, leading to signal degradation and performance issues.
- Bandwidth Limitations: Twisted pair cable has bandwidth limitations compared to fiber optic cable, which can support much higher data rates over longer distances. Higher category cables (e.g., Cat 6, Cat 6a) offer higher bandwidth and better performance but may be more expensive.
- Vulnerability to Damage: Twisted pair cable is vulnerable to damage from environmental factors such as moisture, temperature extremes, and physical stress. Care must be taken during installation and maintenance to protect the cable from damage and ensure reliable operation.

b. Coaxial Cable:

Coaxial cable is commonly used for transmitting high-frequency signals, such as those used in cable television (CATV), broadband internet, and networking applications.

It consists of a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer.

It offers higher bandwidth and longer distances than twisted pair cable, but more expensive and less

flexible.

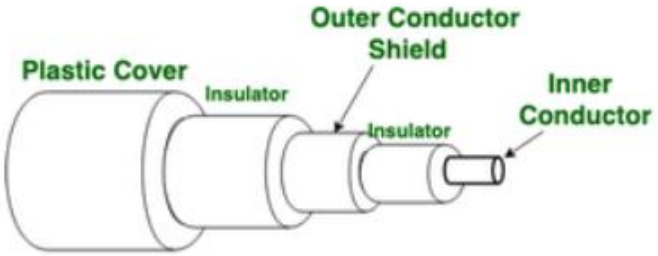


Figure 5.18: Coaxial Cable

Key Points of Coaxial Cable

- Construction: Coaxial cable consists of a central conductor, an insulating layer (dielectric), a metallic shield (usually made of braided wire or foil), and an outer insulating layer (jacket). The central conductor carries the signal, while the shield provides protection against electromagnetic interference (EMI) and radio frequency interference (RFI).
- Impedance: Coaxial cable is characterized by its impedance, which is the resistance to the flow of electrical signals. Common impedance values for coaxial cable are 50 ohms (used in data communications) and 75 ohms (used in video and CATV applications).
- Transmission Distance: Coaxial cable can support longer transmission distances compared to twisted pair cable, especially for higher-frequency signals. Thicker cables typically support longer distances due to lower signal attenuation.
- Termination: Coaxial cable is terminated with connectors such as BNC (Bayonet Neill-Concelman) or F-type connectors. Proper termination is essential for maintaining signal integrity and minimizing signal loss.

Advantages of Coaxial Cable

- Bandwidth: Coaxial cable offers higher bandwidth compared to twisted pair cable, making it suitable for transmitting high-frequency signals such as those used in cable television, broadband internet, and networking applications.
- Immunity to Interference: Coaxial cable provides better protection against electromagnetic interference (EMI) and radio frequency interference (RFI) compared to twisted pair cable, thanks to its metallic shield.
- Longer Transmission Distances: Coaxial cable can support longer transmission distances compared to twisted pair cable, especially for higher-frequency signals. This makes it suitable for use in applications where long-distance transmission is required.
- Durable Construction: Coaxial cable is more durable and less susceptible to damage from environmental factors such as moisture, temperature extremes, and physical stress compared to twisted pair cable.

Disadvantages of Coaxial Cable

- Cost: Coaxial cable is generally more expensive than twisted pair cable, especially for high-performance or specialized applications. The cost of installation and termination can also be higher due to the need for specialized tools and equipment.
- Limited Flexibility: Coaxial cable is less flexible and more difficult to bend compared to twisted pair cable, which can make it challenging to install in tight spaces or around corners.
- Signal Attenuation: Coaxial cable experiences signal attenuation, or loss of signal strength, over long distances. Thicker cables and higher-quality materials can help reduce attenuation, but it is still a limiting factor for long-distance transmission.
- Obsolete Technology: Some types of coaxial cable, such as Thinnet and Thicknet, are considered obsolete and have been largely replaced by newer technologies such as twisted pair and fiber optic cables. However, coaxial cable is still widely used in certain applications such as cable television and broadband internet.

c. Fiber Optic Cable:

Fiber optic cable commonly used for transmitting data using light signals

It consists of a core made of glass or plastic fibers that transmit data using light signals.
Two types: Single-mode fiber (SMF) for long-distance transmissions and multimode fiber (MMF) for shorter distances.
Provides high bandwidth, long distances, and immunity to electromagnetic interference.
Commonly used in high-speed networks, such as backbone connections in WANs and MANs, and in telecommunications systems.

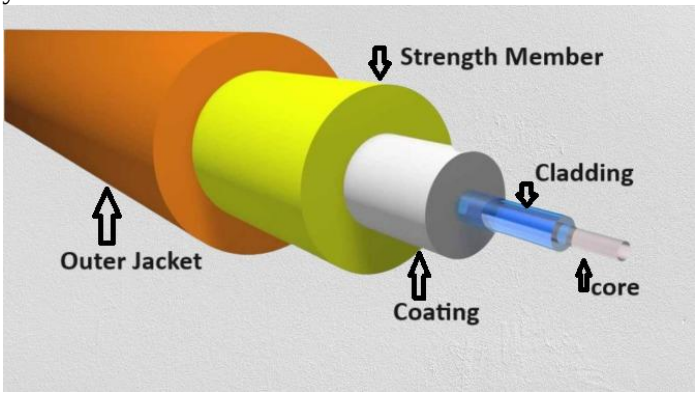


Figure 5.19: Optical Fiber Cable

Key Points of Fiber Optic Cable

- Light Transmission: Fiber optic cable transmits data using light signals, allowing for high-speed transmission over long distances without signal degradation. Light signals travel through the core of the fiber by bouncing off the walls due to total internal reflection.
- Immunity to Interference: Fiber optic cable is immune to electromagnetic interference (EMI) and radio frequency interference (RFI), making it ideal for use in environments with high levels of electrical noise and interference.
- Bandwidth: Fiber optic cable offers extremely high bandwidth, allowing for the transmission of large amounts of data over long distances at high speeds. This makes it suitable for applications requiring high-speed data transmission, such as internet access, video streaming, and cloud computing.
- Security: Fiber optic cable offers enhanced security compared to other types of transmission media, as it is difficult to tap or intercept light signals without physically accessing the cable. This makes it ideal for transmitting sensitive or confidential information.

Types of Fiber Optic Cable

- Single-Mode Fiber (SMF):Has a small core diameter (typically around 9 microns) and uses a single beam of light to transmit data. Designed for long-distance transmission with minimal signal loss and dispersion. Used in long-haul telecommunications networks, high-speed internet backbone, and intercontinental data links.
- Multi-Mode Fiber (MMF): Has a larger core diameter (typically around 50 or 62.5 microns) and allows multiple beams of light to propagate simultaneously. Designed for shorter-distance transmission within buildings, campuses, and data centers. Used in local area networks (LANs), storage area networks (SANs), and short-distance telecommunications applications.

Advantages of Fiber Optic Cable

- High Bandwidth: Fiber optic cable offeHigh Bandwidth: Fiber optic cable offers significantly higher bandwidth compared to copper-based cables such as twisted pair and coaxial cable. This allows for faster data transmission rates and greater capacity for handling large volumes of data.
- Low Signal Loss: Fiber optic cable experiences minimal signal loss (attenuation) over long distances compared to copper-based cables. This allows for longer transmission distances without the need for signal boosters or repeaters.
- Immunity to Interference: Fiber optic cable is immune to electromagnetic interference (EMI), radio frequency interference (RFI), and crosstalk, providing reliable and interference-free transmission even in noisy environments.

- Lightweight and Thin: Fiber optic cable is lightweight and thin compared to copper-based cables, making it easier to install and handle. It also takes up less space in cable trays and conduits, reducing installation costs and space requirements.

Disadvantages of Fiber Optic Cable

- Cost: Fiber optic cable is generally more expensive than copper-based cables, both in terms of initial installation costs and equipment costs. The cost of fiber optic transceivers, connectors, and termination equipment can also be higher.
- Fragility: Fiber optic cable is more fragile and prone to damage from bending, twisting, or crushing compared to copper-based cables. Care must be taken during installation and handling to prevent damage to the cable and maintain signal integrity.
- Complexity: Fiber optic cable installation and termination require specialized tools, equipment, and training. Proper installation techniques are essential to ensure optimal performance and reliability, which may require additional time and resources.
- Compatibility: Fiber optic cable may not be compatible with existing infrastructure or equipment designed for copper-based cables. This may require additional investment in equipment upgrades or adapters to support fiber optic connectivity.

II. Unguided Transmission Media (Wireless): Unguided transmission media, also known as wireless transmission media, are communication channels that transmit electromagnetic signals through the air or space without the use of physical cables or conductors. Unlike guided transmission media, which rely on physical pathways such as cables, unguided transmission media propagate signals through free space.

a. **Radio Waves (Wireless LAN):** The most common form of unguided transmission media is radio waves, which are electromagnetic waves used for wireless communication. Radio waves are a type of electromagnetic radiation with wavelengths ranging from about one millimeter to hundreds of meters. They are used extensively in various wireless communication technologies, including radio broadcasting, television broadcasting, cellular networks, Wi-Fi, Bluetooth, and many others.

Key Points of Radio Waves:

- Electromagnetic Spectrum: Radio waves are part of the electromagnetic spectrum, which also includes other forms of electromagnetic radiation such as microwaves, infrared, visible light, ultraviolet, X-rays, and gamma rays. Radio waves have the longest wavelengths and lowest frequencies among all forms of electromagnetic radiation.
- Propagation: Radio waves propagate through free space by oscillating electric and magnetic fields. They can travel long distances without the need for physical conductors, making them suitable for wireless communication over large areas.
- Modulation: Information is transmitted over radio waves by modulating the amplitude, frequency, or phase of the carrier wave. Different modulation techniques are used depending on the application and desired characteristics of the communication system.
- Antennas: Antennas are used to transmit and receive radio waves. Transmitter antennas convert electrical signals into radio waves for transmission, while receiver antennas capture radio waves and convert them back into electrical signals for processing.

Advantages of Radio Waves:

- Long Range: Radio waves can travel long distances without the need for physical cables, making them suitable for long-range communication over large areas.
- Penetration: Radio waves can penetrate through obstacles such as buildings, walls, and vegetation, allowing for communication in urban and rural environments.
- Versatility: Radio waves can be used for a wide range of applications, including broadcasting, cellular communication, wireless networking, satellite communication, and remote sensing.
- Mobility: Wireless communication using radio waves allows for mobility and flexibility, enabling communication on the move and in remote locations.

Disadvantages of Radio Waves:

- Interference: Radio waves are susceptible to interference from other electronic devices, atmospheric conditions, and man-made sources such as power lines and electronic equipment. Interference can degrade signal quality and affect communication reliability.
- Limited Bandwidth: The available bandwidth for radio communication is limited, especially in congested frequency bands. This can result in limited data rates and capacity for wireless communication systems.
- Security: Wireless communication using radio waves is vulnerable to interception, eavesdropping, and unauthorized access. Encryption and authentication mechanisms are required to secure wireless communication channels.
- Propagation Effects: Radio wave propagation is affected by factors such as atmospheric conditions, terrain, and distance. Signal attenuation, fading, and multipath propagation can degrade signal quality and affect communication performance.

b. Microwave Transmission: Microwave transmission refers to the use of electromagnetic waves in the microwave frequency range for communication purposes. It uses microwave frequencies (above 1 GHz) to transmit data through the atmosphere. Microwave transmission is often used for point-to-point communication over long distances, such as microwave links between cellular towers or satellite communication.

Key Points of Microwave Transmission

- Frequency Range: Microwave frequencies typically range from 1 gigahertz (GHz) to 300 gigahertz (GHz). These frequencies fall in the part of the electromagnetic spectrum between radio waves and infrared waves.
- Line-of-Sight Communication: Microwave transmission requires a clear line of sight between the transmitter and receiver. Any obstruction such as buildings, mountains, or atmospheric conditions can degrade the signal.
- High Bandwidth: Microwave transmission can offer high bandwidth, making it suitable for transmitting large amounts of data quickly. This makes it ideal for applications like long-distance telecommunications and high-speed internet.
- Point-to-Point Communication: Microwave links are often used for point-to-point communication, connecting two fixed points directly without the need for intermediate infrastructure.
- Common Applications: Microwave transmission is commonly used for long-distance communication links, satellite communication, cellular networks, and wireless backhaul.

Advantages of Microwave Transmission:

- High Data Rates: Microwave transmission can support high data rates, making it suitable for applications requiring fast data transfer, such as broadband internet access and digital television broadcasting.
- Low Cost: Once the initial infrastructure is set up, the operational costs of microwave transmission can be relatively low compared to other communication technologies like fiber optics.
- Quick Deployment: Microwave links can be deployed relatively quickly compared to laying cables or fiber optics, making them suitable for temporary communication needs or in areas where infrastructure deployment is challenging.
- Versatility: Microwave links can be used for various applications, including point-to-point communication, backbone networks, and mobile backhaul.

Disadvantages of Microwave Transmission:

- Line-of-Sight Limitations: Microwave signals require an unobstructed line of sight between the transmitter and receiver. Any obstacles in the path, such as buildings or terrain features, can block or weaken the signal.
- Susceptibility to Weather Conditions: Atmospheric conditions such as rain, fog, or snow can attenuate microwave signals, leading to degradation in signal quality and reliability.
- Limited Range: Microwave signals are subject to attenuation over long distances, limiting the range of transmission without the use of repeaters or amplifiers.

- Interference: Microwave links can be susceptible to interference from other microwave sources, such as nearby communication links or industrial equipment operating in the same frequency band.
- Security Concerns: Because microwave signals can be intercepted with specialized equipment, there are security concerns regarding the confidentiality of transmitted data. Encryption and other security measures are often required to mitigate this risk.

c. **Infrared Waves:** Infrared waves are used for short-range wireless communication, typically within a confined area such as a room or building. Infrared transmission is commonly used in remote controls, IrDA (Infrared Data Association) devices, and proximity sensors.

Key Points of Infrared Waves

- Wavelength Range: Infrared waves have wavelengths ranging from approximately 700 nanometers to 1 millimeter, lying between the visible and microwave portions of the electromagnetic spectrum.
- Heat Sensing: Infrared radiation is commonly associated with heat sensing. Objects emit infrared radiation in proportion to their temperature, allowing for thermal imaging and heat detection applications.
- Applications: Infrared waves have diverse applications across various fields, including communication, heating, remote sensing, security systems, spectroscopy, and medical diagnostics.
- Invisibility to Human Eye: Infrared radiation is invisible to the human eye but can be detected and utilized with specialized equipment, such as infrared cameras or sensors.
- Interaction with Matter: Infrared radiation interacts differently with different materials. Some materials are transparent to infrared waves, while others absorb or reflect them.

Advantages of Infrared Waves:

- Thermal Imaging: One of the significant advantages of infrared waves is their ability to detect heat signatures, enabling thermal imaging for various applications such as search and rescue, building inspections, and military surveillance.
- Non-Destructive Testing: Infrared radiation can be used for non-destructive testing of materials and structures, allowing for the detection of defects, leaks, or anomalies without causing damage.
- Remote Sensing: Infrared sensors are used in remote sensing applications to gather information about Earth's surface temperature, vegetation health, and atmospheric conditions from satellites and aircraft.
- Security Systems: Infrared sensors are integral to security systems, such as motion detectors and burglar alarms, as they can detect the presence of intruders based on changes in infrared radiation.
- Energy Efficiency: Infrared heating systems can be more energy-efficient compared to traditional heating methods, as they directly transfer heat to objects and people without heating the surrounding air.

Disadvantages of Infrared Waves:

- Limited Range: Infrared waves have limited range compared to other forms of electromagnetic radiation. They are primarily used for short-range communication and sensing applications.
- Atmospheric Absorption: Infrared radiation can be absorbed or scattered by gases, water vapor, and particulate matter in the atmosphere, which can reduce its effectiveness for long-distance communication or remote sensing.
- Interference: Infrared communication systems can be susceptible to interference from ambient infrared sources or sunlight, which can affect signal quality and reliability.
- Line-of-Sight Requirement: Like microwave transmission, infrared communication typically requires a clear line of sight between the transmitter and receiver, which can be challenging in environments with obstacles or atmospheric conditions.
- Limited Penetration: Infrared radiation has limited ability to penetrate certain materials, limiting its effectiveness for certain applications, such as imaging through dense fog or thick walls.

d. **Satellite Transmission:** Unguided transmission media can be used for both terrestrial and satellite communication. Terrestrial communication involves communication between devices on the Earth's surface, while satellite communication involves communication between devices and satellites orbiting the Earth.
Used for long-distance communication in remote areas, mobile communication (satellite phones), and satellite television (direct-to-home). Provides wide coverage area but suffers from latency and susceptibility to weather conditions.

Each type of transmission medium has its advantages and disadvantages, and the choice depends on factors such as data transfer requirements, distance, cost, environmental conditions, and network architecture.

5.9 Network Protocol

Network protocols are sets of rules that define communication between devices in a network. These protocols define the format, timing, sequencing, and error control of data exchange, ensuring that devices can communicate effectively and reliably. Each protocol has its own strengths and weaknesses, and the choice of protocol depends on factors such as the specific requirements of the application, security concerns, and network conditions.

Key Points of Network Protocol:

- **Data Formatting:** Protocols define how data is formatted before transmission, including the structure of headers, data fields, and trailers. This formatting ensures that devices can understand and interpret the data correctly.
- **Addressing:** Protocols specify how devices are addressed within a network, allowing data to be sent to specific destinations. This includes the format of network addresses (such as IP addresses) and the rules for routing data to the correct destination.
- **Handshaking:** Protocols often include mechanisms for establishing and terminating communication sessions between devices. Handshaking protocols define how devices negotiate parameters, synchronize their communication, and acknowledge the receipt of data.
- **Error Detection and Correction:** Many protocols include mechanisms for detecting and correcting errors that may occur during data transmission. This can involve adding checksums or error-correcting codes to transmitted data and requesting retransmission of corrupted or lost data.
- **Flow Control:** Protocols may include flow control mechanisms to regulate the flow of data between devices, preventing one device from overwhelming another with data. Flow control can involve techniques such as buffering, sliding window protocols, and congestion control.
- **Multiplexing and Demultiplexing:** In networks where multiple devices share a communication channel, protocols define how data from different sources is multiplexed for transmission and demultiplexed upon reception. This allows multiple communication streams to be carried over the same channel.
- **Security:** Some protocols include provisions for securing data transmission and protecting network resources from unauthorized access or attacks. This can involve encryption, authentication, access control, and other security measures.

Common Network Protocols:

- **Transmission Control Protocol (TCP):** It is a connection-oriented protocol used for reliable, ordered, and error-checked delivery of data packets over IP networks. TCP/IP is the foundation of the internet. It enables reliable communication by breaking data into packets and ensuring they reach their destination.

It is a widely adopted, platform-independent, robust error handling, supports various types of networks. It can be slower due to overhead, may not be suitable for real-time applications

where low latency is crucial. Transmission Control Protocol (TCP) is a core protocol in the Internet Protocol Suite (TCP/IP).

Key Points of Transmission Control Protocol

- Connection-Oriented: TCP establishes a connection between the sender and receiver before transmitting data. This ensures reliable communication with error checking and retransmission of lost packets.
- Reliable: TCP guarantees that data will be delivered in the correct order and without errors. It uses acknowledgment mechanisms and flow control to achieve reliability.
- Full Duplex: TCP supports simultaneous data transmission in both directions, allowing for efficient bidirectional communication.
- Stream-oriented: TCP treats data as a continuous stream of bytes, breaking it into smaller segments for transmission over the network.
- Flow Control: TCP regulates the rate of data transmission to prevent overwhelming the receiver. It uses sliding window mechanisms to manage the flow of data.

Advantages of Transmission Control Protocol

- Reliability: TCP ensures reliable delivery of data by retransmitting lost packets and detecting errors through checksums.
- Ordered Delivery: Data transmitted via TCP is received in the same order it was sent, ensuring integrity for applications that require sequential data delivery.
- Error Detection and Recovery: TCP detects errors and retransmits lost packets, enhancing data integrity and reducing the need for error handling at higher protocol layers.
- Connection Management: TCP handles connection establishment, maintenance, and termination, simplifying application development by abstracting network complexities.

Disadvantages of Transmission Control Protocol

- Overhead: TCP introduces overhead due to its reliability mechanisms, including acknowledgment packets, sequence numbers, and flow control, which can affect performance, especially in low-bandwidth networks.
- Latency: The connection-oriented nature of TCP requires establishing and maintaining connections before data transmission, leading to increased latency compared to connectionless protocols like UDP.
- Complexity: TCP's comprehensive features and mechanisms make it more complex to implement and configure compared to simpler protocols. This complexity can lead to higher development and maintenance costs.
- Not Suitable for Real-Time Applications: While TCP ensures reliable delivery, its emphasis on reliability and ordered delivery may not be suitable for real-time applications like streaming media or online gaming, where low latency is critical.

- **Internet Protocol (IP):** A network-layer protocol responsible for addressing and routing packets across interconnected networks.

IP is commonly paired with TCP to form TCP/IP, the overall internet protocol suite. Together, IP sends packets to their destinations, and TCP arranges the packets in the correct order, as IP sometimes sends packets out of order to ensure the packets travel the fastest ways.

IP functions similarly to a postal service. When users send and receive data from their device, the data gets spliced into packets. Packets are like letters with two IP addresses: one for the sender and one for the recipient. After the packet leaves the sender, it goes to a gateway, like a post office, that directs it in the proper direction. Packets continue to travel through gateways until they reach their destinations.

Internet Protocol (IP) is the principal communications protocol used for relaying datagrams across network boundaries. It's essentially the backbone protocol of the Internet.

Key Points of Internet Protocol

- Version: There are two main versions of IP in use today: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). IPv4 is the older version and is still widely used, while IPv6 is gradually being adopted to address the limitations of IPv4.
- Addressing: IP addresses are used to uniquely identify devices on a network. In IPv4, addresses are 32 bits long, represented in dotted-decimal notation (e.g., 192.168.1.1). In IPv6, addresses are 128 bits long, represented in hexadecimal notation.
- Routing: IP enables routers to forward packets between networks based on the destination IP address. Routers use routing tables to determine the best path for packet delivery.
- Connectionless Protocol: IP is a connectionless protocol, meaning it does not establish a direct connection between sender and receiver before sending data. Each packet is treated independently and can take different paths to reach its destination.
- Best Effort Delivery: IP provides best-effort delivery, meaning it does not guarantee delivery or provide mechanisms for error recovery. It relies on higher-layer protocols (e.g., TCP) to ensure reliable data transmission if needed.

Advantages of Internet Protocol

- Global Connectivity: IP enables communication between devices across the globe, forming the basis of the Internet's interconnected network.
- Scalability: IP's hierarchical addressing scheme allows for the scalability of the Internet, accommodating the addition of new devices and networks without major infrastructure changes.
- Flexibility: IP supports various types of network topologies and technologies, including wired and wireless networks, making it adaptable to diverse networking environments.
- Interoperability: IP facilitates interoperability between different types of networks and devices, regardless of their underlying hardware or software platforms.
- Decentralization: IP's distributed nature decentralizes control over the Internet, promoting resilience and robustness against failures or attacks.

Disadvantages of Internet Protocol

- Security Concerns: IP itself does not provide inherent security mechanisms, leaving data vulnerable to interception or tampering. Additional protocols such as IPsec are often required for secure communication.
- Quality of Service (QoS) Challenges: IP's best-effort delivery model does not guarantee timely or reliable delivery of packets, which can be problematic for real-time applications like voice and video streaming.
- Complexity in Network Management: Managing large IP-based networks can be complex, requiring skilled administrators and sophisticated network management tools.
- Fragmentation Overhead: Packet fragmentation may occur when data packets are too large to be transmitted over a network without being divided into smaller packets. This can introduce additional overhead and decrease network performance.

- **User Datagram Protocol (UDP):**

UDP is a connectionless protocol that provides simple unreliable datagram delivery service but fast communication. Advantages are low overhead, suitable for real-time applications like video streaming or online gaming. Disadvantages are no error checking or retransmission of lost packets, less reliable than TCP for critical data transmission.

Key Points of User Datagram Protocol

- Connectionless Communication: UDP provides a connectionless communication service, meaning it does not establish a connection before sending data and does not guarantee delivery or order of packets.
- Minimal Overhead: UDP has minimal overhead compared to connection-oriented protocols like TCP (Transmission Control Protocol), making it lightweight and efficient for certain types of applications.

- Unreliable Delivery: UDP does not provide mechanisms for error detection, correction, or acknowledgment, so it does not guarantee delivery of packets.
- Simple Header Format: UDP headers are smaller and simpler compared to TCP headers, consisting of only source and destination port numbers and a length field.
- Low Latency: Because UDP does not perform extensive error checking or ensure delivery, it can offer lower latency compared to TCP, making it suitable for real-time applications like video streaming and online gaming.

Advantages of User Datagram Protocol

- Low Overhead: UDP has minimal overhead because it does not require establishing and maintaining a connection, making it efficient for transmitting small packets of data.
- Suitable for Real-Time Applications: UDP's connectionless nature and low latency make it suitable for real-time applications where maintaining a continuous flow of data is more important than ensuring every packet is delivered, such as VoIP (Voice over Internet Protocol) and online gaming.
- Broadcast and Multicast Support: UDP supports broadcasting and multicasting, allowing a single packet to be sent to multiple recipients simultaneously.
- Simplicity: UDP is simpler than TCP, making it easier to implement and requiring fewer system resources.

Disadvantages of User Datagram Protocol

- Unreliable Delivery: UDP does not guarantee delivery or order of packets, making it unsuitable for applications that require reliable data transmission, such as file transfer or email.
- No Flow Control or Congestion Avoidance: UDP does not provide flow control or congestion avoidance mechanisms, so it can potentially overwhelm network resources in situations of high traffic.
- No Error Detection or Correction: UDP does not include mechanisms for error detection or correction, so corrupted or lost packets are not automatically retransmitted.
- Limited Support for Large Data Transfers: UDP's maximum packet size is limited, which can pose challenges for applications that require large data transfers, such as file downloads or database queries.

- **HTTP (Hypertext Transfer Protocol):** A protocol for transmitting hypermedia documents, such as web pages and files, over the Internet.

HTTP is used for transmitting web pages, while HTTPS encrypts data for secure communication. It is simple and widely supported, allows for efficient retrieval of web resources. Issues are lack of security in HTTP, HTTPS can introduce additional overhead due to encryption.

Key Points of Hypertext Transfer Protocol

- Client-Server Protocol: HTTP follows a client-server model, where a client (such as a web browser) sends requests to a server (such as a web server) and receives responses containing web content.
- Stateless Protocol: HTTP is stateless, meaning each request-response cycle is independent of previous ones. The server does not retain information about past requests from the same client.
- Text-Based Protocol: HTTP messages are text-based, making them human-readable and easy to interpret. HTTP requests and responses consist of headers and, optionally, a message body.
- Standardized Protocol: HTTP is standardized by the Internet Engineering Task Force (IETF) and defined in RFC 7230.
- Supports Secure Version (HTTPS): HTTPS (HTTP Secure) is a secure version of HTTP that encrypts data exchanged between the client and server using SSL/TLS protocols, providing confidentiality and integrity.

Advantages of Hypertext Transfer Protocol

- Universal Compatibility: HTTP is widely supported by various platforms, devices, and web browsers, making it accessible for users across different environments.
- Simple and Lightweight: HTTP is a simple and lightweight protocol, making it efficient for transmitting web pages and other hypermedia content over the Internet.
- Caching Support: HTTP supports caching, allowing web browsers and proxy servers to store copies of previously accessed web content, which can improve performance and reduce bandwidth usage.
- Flexible: HTTP supports various methods (such as GET, POST, PUT, DELETE) for interacting with web resources, providing flexibility for different types of web applications.
- Easy to Debug: HTTP messages are human-readable, making it easier for developers to debug and troubleshoot issues with web applications using tools like browser developer consoles or network sniffers.

Disadvantages of Hypertext Transfer Protocol

- Security Concerns: Traditional HTTP is not encrypted, so data transmitted over HTTP is vulnerable to interception and tampering by malicious actors. This lack of security can compromise the confidentiality and integrity of sensitive information.
- Limited Performance: HTTP is not optimized for high-performance applications that require low latency and high throughput, as it may introduce overhead due to its text-based nature and stateless design.
- No Built-in Authentication: HTTP does not provide built-in mechanisms for user authentication or access control, requiring developers to implement additional security measures, such as session tokens or OAuth.
- No Support for Binary Data: HTTP is primarily designed for transmitting text-based data, so handling binary data efficiently may require additional encoding or encapsulation techniques.
- Potential for Content Spoofing: Without proper security measures, HTTP responses can be manipulated by attackers to inject malicious content or perform content spoofing attacks, leading to phishing or malware distribution.

- **Simple Mail Transfer Protocol (SMTP)**: SMTP is used for sending emails between servers. A protocol used for sending and receiving email messages over the internet. It is simple and efficient for sending emails. Issues are lack of encryption by default, susceptible to spam and phishing attacks.

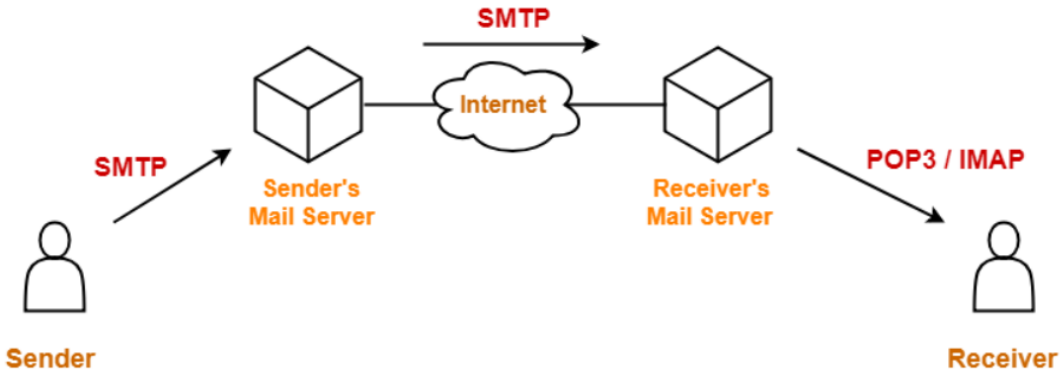


Figure 5.20 Simple Mail Transfer Protocol

Key Points of Simple Mail Transfer Protocol

- Message Transmission: SMTP is primarily used for transmitting email messages between mail servers.
- Text-Based Protocol: SMTP commands and responses are text-based, making it human-readable and easy to understand.

- Client-Server Communication: SMTP follows a client-server architecture, where an email client (such as Outlook or Gmail) communicates with an SMTP server to send outgoing messages.
- Message Routing: SMTP is responsible for routing email messages between mail servers, using domain names to identify the destination server.
- Port: SMTP typically uses port 25 for communication, though encrypted variants like SMTPS (SMTP Secure) or STARTTLS (which upgrades a plain text connection to an encrypted one) can use different ports.

Advantages of Simple Mail Transfer Protocol

- Universal Compatibility: SMTP is widely supported by email servers and clients, making it a standard protocol for sending and receiving emails across different platforms and networks.
- Reliability: SMTP provides reliable delivery of email messages by employing error detection, retransmission, and acknowledgment mechanisms to ensure messages reach their intended recipients.
- Simple Configuration: Setting up and configuring SMTP servers and clients is relatively straightforward, making it accessible for both individuals and organizations.
- Text-Based Communication: SMTP commands and responses are text-based, allowing administrators to troubleshoot and debug email-related issues more easily.
- Customization: SMTP allows for customization of email headers and message content, enabling users to personalize their email messages and add additional information such as attachments or MIME types.

Disadvantages of Simple Mail Transfer Protocol

- Spam and Abuse: SMTP's open nature can be exploited by spammers and malicious actors to send unsolicited bulk emails (spam) or distribute malware through phishing attacks, leading to abuse of email systems.
- Security Concerns: Traditional SMTP does not provide encryption for email transmission, making it susceptible to eavesdropping and interception of sensitive information. However, SMTP can be secured using protocols like SMTPS or STARTTLS to encrypt communication between email servers.
- Potential for Email Spoofing: SMTP does not include built-in mechanisms for sender authentication, allowing attackers to spoof email addresses and impersonate legitimate senders, which can lead to phishing or fraud.
- Message Size Limitations: Some SMTP servers impose limits on the size of email messages that can be sent or received, which can be a limitation for users sending large attachments or multimedia content.
- Complex Routing: SMTP routing relies on domain names to identify destination mail servers, which can lead to routing issues or delays if domain name resolution fails or if mail servers are misconfigured.

- **File Transfer Protocol (FTP):** A protocol used for transferring files between a client and a server on a computer network.

FTP is efficient for large file transfers, supports various authentication methods. Issues are lacks encryption, prone to security risks such as data interception or unauthorized access.

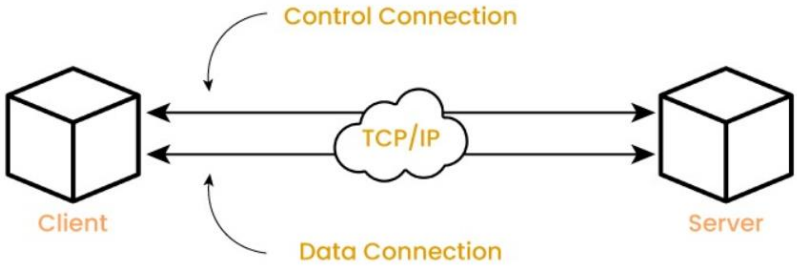


Figure 5.21: FTP Protocol working

Key Points of File Transfer Protocol

- Client-Server Architecture: FTP operates on a client-server architecture, where a client connects to an FTP server to perform file transfers.
- Two Modes of Operation: FTP supports two modes of operation: active mode and passive mode. In active mode, the client initiates connections to the server, while in passive mode, the server opens a port for data transfer, and the client connects to it.
- Authentication: FTP typically requires user authentication using a username and password to access files on the server.
- Commands: FTP uses a set of commands to perform file operations such as uploading, downloading, renaming, deleting, and listing files and directories.
- Port: FTP typically uses port 21 for control connections and port 20 for data connections, though passive mode may involve additional ports.

Advantages of File Transfer Protocol

- Widespread Support: FTP is supported by a wide range of operating systems, servers, and clients, making it a versatile and widely used protocol for file transfer.
- Simple Configuration: Setting up an FTP server and client is relatively straightforward, requiring minimal configuration compared to more complex protocols.
- Efficient File Transfer: FTP is designed for efficient bulk file transfer, making it suitable for scenarios where large files or large numbers of files need to be transferred.
- Resume Capability: FTP supports resuming interrupted file transfers, allowing users to resume downloads or uploads from where they left off in case of network failures or interruptions.
- Anonymous Access: FTP servers can be configured to allow anonymous access, allowing users to connect and download files without requiring authentication.

Disadvantages of File Transfer Protocol

- Security Concerns: Traditional FTP transmits data in plain text, making it vulnerable to eavesdropping and interception by malicious actors. Sensitive information such as usernames, passwords, and file contents can be compromised.
- Limited Firewall Compatibility: FTP's use of multiple ports for data transfer (especially in active mode) can pose challenges for firewall configuration and may require opening a wide range of ports, which can introduce security risks.
- No Encryption: FTP does not provide encryption for data transmission, exposing transferred files to potential interception or tampering. However, secure variants like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) address this limitation by encrypting data using SSL/TLS or SSH protocols.
- Data Integrity: FTP does not include built-in mechanisms for ensuring data integrity during file transfer, such as checksum verification or error detection and correction.
- Limited Support for NAT: FTP's use of IP addresses in its protocol can complicate network address translation (NAT) setups, especially in active mode, where the server initiates data connections to the client.

5.10 Layered Network Architecture

Layered network architecture, also known as the layered protocol stack or protocol layering, is a conceptual framework used to organize and structure the various protocols and functionalities within a computer network.

This architecture divides the complex task of network communication into a series of distinct layers, each responsible for specific functions and interactions.

The layered network architecture promotes modularity, scalability, and interoperability by separating the network functionality into discrete layers, allowing for easier development, maintenance, and troubleshooting of network systems. It also facilitates the implementation of new technologies and protocols without disrupting existing layers, fostering innovation and evolution in network design and communication.

5.10.1 OSI Model

The most widely adopted layered network architecture model is the OSI (Open Systems Interconnection) model, developed by the International Organization for Standardization (ISO).

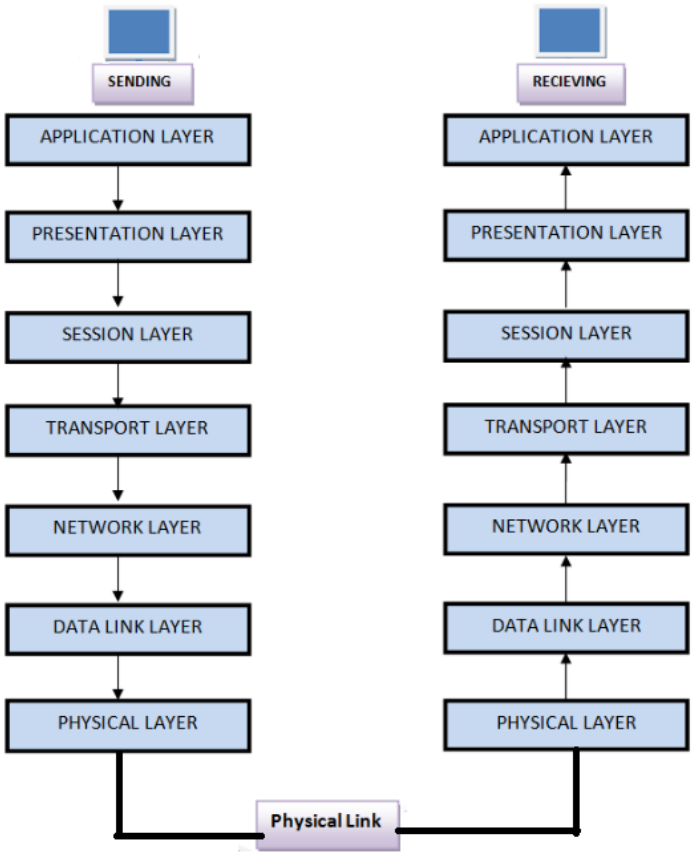


Figure 5.22: ISO Reference Model

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize how different networking protocols and technologies interact within a network.

Key Points of OSI Model

- Modularity: The OSI model divides network communication into seven distinct layers, each with its own set of functions and responsibilities, which allows for easier troubleshooting, maintenance, and interoperability.
- Standardization: The OSI model provides a standardized framework for understanding and designing network protocols and architectures, facilitating compatibility and interoperability between different networking technologies and vendors.

- Abstraction: Each layer of the OSI model abstracts the complexities of lower layers, allowing network engineers and developers to focus on specific aspects of network communication without having to understand the entire system in detail.
- Layered Communication: Communication between devices in an OSI-based network occurs through interactions between corresponding layers, where data is encapsulated, transmitted, and decapsulated at each layer as it traverses the network.
- Encapsulation: Data sent over a network is encapsulated with header information at each layer of the OSI model, providing addressing, error detection, and control information necessary for successful transmission and delivery.

Layers of OSI Model:

The OSI model consists of seven layers, each with its own set of protocols and responsibilities:

- **Physical Layer (Layer 1):** This layer deals with the physical transmission of data over the network medium. It defines the hardware specifications, such as cables, connectors, and signaling, required for transmitting raw bits over the network.

The lowest layer of the OSI model. Responsible for transmitting raw data bits over the physical medium. Defines characteristics such as voltage levels, timing, and physical connections. Examples of protocols: Ethernet, Wi-Fi, DSL, Fiber optic.

- **Data Link Layer (Layer 2):** The data link layer is responsible for establishing and maintaining reliable data transfer between adjacent network nodes. It handles framing, error detection, and flow control, ensuring error-free transmission of data frames over the physical layer.

Responsible for providing error-free transmission of data frames between adjacent nodes over a physical link. Performs functions such as framing, error detection and correction, and flow control. Divided into two sublayers: Media Access Control (MAC) and Logical Link Control (LLC). Examples of protocols: Ethernet, Wi-Fi (MAC sublayer), HDLC, PPP (LLC sublayer).

- **Network Layer (Layer 3):**The network layer is responsible for routing and forwarding data packets between different networks. It provides logical addressing, packet forwarding, and routing functions, enabling communication between devices on different networks.

Responsible for routing and forwarding packets between different networks to reach their destination. Provides logical addressing, routing, and traffic control. Examples of protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

- **Transport Layer (Layer 4):** The transport layer ensures reliable end-to-end communication between hosts. It manages data segmentation, flow control, error recovery, and retransmission, providing reliable data delivery services to higher-layer protocols.

Responsible for end-to-end communication between hosts, ensuring data reliability, flow control, and error recovery. Divides data into segments, manages connections, and provides reliable data delivery. Examples of protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Control Transmission Protocol).

- **Session Layer (Layer 5):** The session layer establishes, manages, and terminates communication sessions between devices. It handles session establishment, synchronization, and teardown, allowing applications on different hosts to communicate with each other.

Responsible for establishing, managing, and terminating sessions or connections between applications. Manages dialogue control, synchronization, and checkpointing. Examples of protocols: NetBIOS, PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call).

- **Presentation Layer (Layer 6):** The presentation layer is responsible for data formatting, encryption, and decryption. It ensures that data exchanged between applications is in a format that can be understood by both sender and receiver, handling tasks such as data compression and encryption.

Responsible for translating, encrypting, and formatting data to ensure compatibility between different systems. Handles data representation, encryption, and compression. Examples of protocols: SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, GIF, ASCII.

- **Application Layer (Layer 7):** The application layer provides network services directly to end-users and application processes. It includes protocols for services such as email (SMTP), web browsing (HTTP), file transfer (FTP), and remote access (SSH), enabling users to interact with network resources.

The highest layer of the OSI model. Provides network services directly to end-users and applications.

Supports user-level processes and applications such as web browsers, email clients, and file transfer protocols. Examples of protocols: HTTP, FTP, SMTP, DNS, DHCP.

Advantages of OSI Model

- Interoperability: The OSI model promotes interoperability between different networking technologies and devices by providing a common framework for communication protocols and architectures.
- Modularity: The layered architecture of the OSI model allows for easier troubleshooting, debugging, and maintenance of network systems by isolating issues to specific layers.
- Flexibility: The modular design of the OSI model allows for the development and implementation of new protocols and technologies within existing network infrastructures without affecting other layers.
- Standardization: The OSI model provides a standardized reference model for network communication, which helps ensure consistency, compatibility, and reliability in networking implementations.
- Understanding: The OSI model serves as a conceptual framework for understanding how network protocols and technologies interact and operate within a network environment.

Disadvantages of OSI Model

- Complexity: The OSI model can be overly complex for practical implementation, especially in real-world network environments where network protocols and technologies may not strictly adhere to the model's layered architecture.
- Rigid Structure: The rigid layering of the OSI model may not always reflect the dynamic nature of modern network architectures and protocols, leading to limitations in flexibility and scalability.
- Overlap: Some functions and responsibilities may overlap between adjacent layers of the OSI model, leading to potential confusion and ambiguity in protocol design and implementation.
- Resource Overhead: The encapsulation and decapsulation processes at each layer of the OSI model can introduce additional processing overhead and latency, impacting network performance.
- Incompatibility: Despite efforts to standardize network protocols and architectures, differences in interpretation and implementation of the OSI model may lead to compatibility issues between different networking technologies and vendors.

5.10.2 TCP/IP Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a networking protocol suite that is widely used for communication over the Internet and local area networks (LANs).

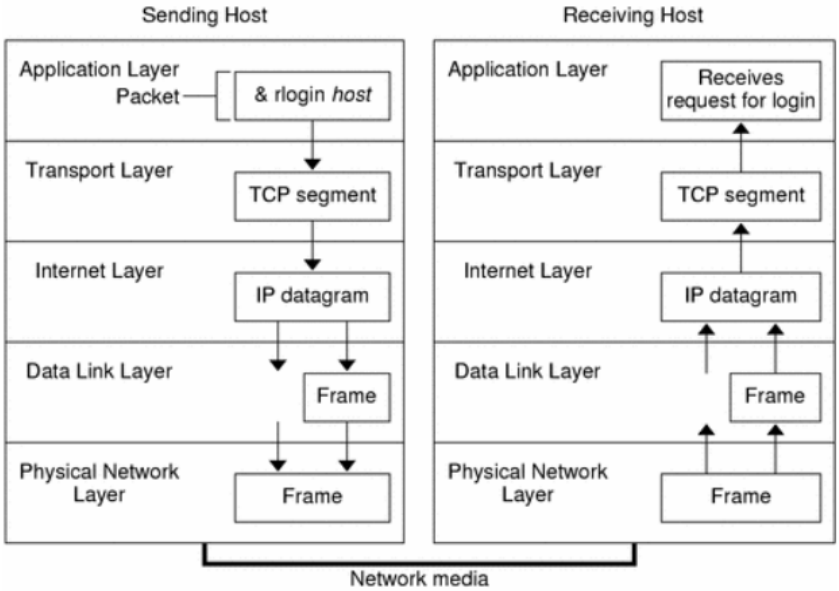


Figure 5.23: TCP/IP Model

Key Points of TCP/IP Model

- De Facto Standard: The TCP/IP model is the de facto standard for networking communications, forming the basis for the Internet and most modern network architectures.
- Flexible and Scalable: TCP/IP is designed to be flexible and scalable, allowing it to adapt to various networking environments and accommodate the growth of the Internet.
- Modular Architecture: The TCP/IP model is organized into a set of modular protocols, each responsible for specific functions related to networking communication.
- Open Standards: TCP/IP protocols are open standards developed and maintained by various organizations, promoting interoperability and compatibility between different network technologies and vendors.
- Robustness: TCP/IP is known for its robustness and reliability, providing mechanisms for error detection, correction, and congestion control to ensure the efficient and reliable transmission of data.

Layers of TCP/IP Model

The TCP/IP model consists of four layers:

- Application Layer: This layer provides network services directly to end-users and application processes. It includes protocols such as HTTP, SMTP, FTP, DNS, and DHCP, which enable various application-level functions such as web browsing, email communication, file transfer, and domain name resolution.
- Transport Layer: The transport layer is responsible for end-to-end communication between hosts and provides reliable or unreliable data delivery services to upper-layer protocols. It includes protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), which handle segmentation, flow control, error recovery, and multiplexing/demultiplexing of data streams.
- Internet Layer: This layer is responsible for routing packets between different networks and hosts on the Internet. It includes the IP (Internet Protocol), which provides logical addressing and packet forwarding services, enabling internetwork communication and routing.
- Link Layer: The link layer is responsible for the transmission of data between directly connected network devices, such as Ethernet switches and wireless access points. It includes protocols such as Ethernet, Wi-Fi, and PPP (Point-to-Point Protocol), which handle framing, addressing, and error detection for data transmission over physical media.

Advantages of TCP/IP Model

- Scalability: TCP/IP is highly scalable, allowing it to accommodate the growth of the Internet and support a large number of interconnected devices and networks.
- Interoperability: TCP/IP protocols are open standards that promote interoperability and compatibility between different network technologies, platforms, and vendors.
- Robustness: TCP/IP includes mechanisms for error detection, correction, and congestion control, making it robust and reliable for transmitting data over diverse network environments.
- Flexibility: TCP/IP is flexible and adaptable, supporting a wide range of applications and services through its modular architecture and layered design.
- Global Reach: TCP/IP is the foundation of the Internet and enables communication across global networks, facilitating worldwide connectivity and information exchange.

Disadvantages of TCP/IP Model

- Complexity: TCP/IP protocols can be complex to configure and manage, especially in large-scale network environments with diverse technologies and configurations.
- Security Concerns: TCP/IP does not inherently provide strong security mechanisms, leaving data vulnerable to interception, tampering, and unauthorized access. Additional security measures such as encryption, authentication, and firewalls are often required to secure TCP/IP-based networks.

- Overhead: TCP/IP introduces overhead due to the encapsulation and processing of data at each layer, which can impact network performance and efficiency, especially in bandwidth-constrained environments.
- Fragmentation: TCP/IP packet fragmentation may occur when data packets are too large to be transmitted over a network without being divided into smaller packets, leading to inefficiencies in data transmission and potential performance degradation.
- Reliance on IP Addresses: TCP/IP relies heavily on IP addresses for host identification and routing, which can lead to scalability challenges and potential conflicts in IP address allocation, especially with the depletion of IPv4 addresses and the transition to IPv6.

Questions:

1. Explain the components of data communication with a diagram.
2. Discuss the role of the message in the data communication process.
3. What is simplex communication?
4. Describe full-duplex communication.
5. Compare and contrast simplex, half-duplex, and full-duplex modes of communication.
6. Discuss the advantages and disadvantages of full-duplex communication.
7. What is the purpose of standards in data communication?
8. Explain the importance of standards in data communication.
9. Discuss the role of the International Organization for Standardization (ISO) in data communication.
10. How are networks classified?
11. What distinguishes a WAN from a LAN?
12. Describe the different classifications of networks based on size and geographical area.
13. Compare and contrast LAN, MAN, and WAN.
14. List three types of network topologies.
15. Describe a star topology.
16. What is a mesh topology?
17. Explain the different types of network topologies with diagrams.
18. Discuss the advantages and disadvantages of a star topology.
19. Describe the characteristics of PAN, LAN, MAN, and WAN.
20. Explain how network types influence the choice of transmission media.
21. Compare guided and unguided transmission media with examples.
22. Discuss the advantages and disadvantages of fiber optic cables.
23. Describe the role of the Application layer in the OSI model.
24. Compare the TCP/IP model to the OSI model.
25. Describe the layers of the TCP/IP model and their functions.