Draft Study Material

JOB ROLE

CYBER SECURITY ASSISTANT

Qualification Pack
QG-03-IT-00350-2023-V1-NIELIT

Sector: IT-ITeS
Grades: IX

विद्यया ऽमृतमश्नुते

एन सी ई आर टी
NCERT

PSS CENTRAL INSTITUTE OF VOCATIONAL EDUCATION
(a constituent unit of NCERT, under Ministry of Education, Government of India)
Shyamla Hills, Bhopal- 462 002, M.P., INDIA
www.psscive.ac.in

Cyber Security Assistant

Grade – IX

Qualification Pack
QG-03-IT-00350-2023-V1-NIELIT

विद्यया ऽ मृतमश्नुते

एन सी ई आर टी
NCERT

PSS Central Institute of Vocational Education

(A constituent unit of NCERT, under the Ministry of Education, Government of India)

Shyamla Hills, Bhopal - 462 002, Madhya Pradesh, India

www.psscive.ac.in

DISCLAIMER
This material is only a reference study material and has been prepared by experts. Care has been taken to acknowledge the information with suitable references.

CHIEF PATRON
Prof. Dinesh Prasad Saklani
Director
National Council of Educational Research and Training (NCERT), New Delhi

PATRON
Dr. Deepak Paliwal
Joint Director
PSS Central Institute of Vocational Education, Bhopal

PROGRAMME COORDINATOR
Dr. Munesh Chandra
Professor (CSE), Head, ICT Centre
Department of Engineering and Technology,

Published by:
Joint Director
PSS Central Institute of Vocational Education, NCERT,
Shyamla Hills, Bhopal

PREFACE

The National Education Policy, 2020, emphasizes removing hard distinctions between arts, science, and commerce; and between curricular, co-curricular, and extracurricular activities; and between vocational and general education. NEP focuses on flexible curricular structure and multidisciplinary learning. The secondary stage is for students aged between 14 and 18 and is divided into two phases: Phase 1 — Grades 9 and 10, and Phase 2 – Grades 11 and 12. The secondary stage for students aged 14-18 is divided into two phases, with the guidelines presented for grades 11 and 12. The National Curriculum Framework for School Education (NCFSE) 2023 advocates for choice-based courses, aiming to provide flexibility, remove separations between disciplines, and align with industry needs. Vocational education in the secondary stage will be an integral part of the educational system designed to provide students with practical skills and knowledge that directly prepare them for specific careers or trades. The focus should be on the holistic development of each child, addressing not only vocational skills but also social, emotional, and life skills. In schools, vocational courses are expected to align with the National Skill Qualifications Framework (NSQF), falling within NSQF levels 3 and 4. The NSQF is a quality assurance framework that organizes qualifications in a series of eight levels, in increasing order of complexity and competency. These levels are defined in terms of learning outcomes, which are an explicit description of what a learner should know, understand, and be able to do as a result of learning, regardless of whether these competencies were acquired through formal, non-formal, or informal learning.

The NEP underscores the importance of vocational education, preparing students with practical skills aligned with industry needs. In the context of web development, this translates to equipping learners with not just theoretical knowledge but also hands-on experience. We should strive to provide comprehensive training that empowers individuals to tackle real-world challenges in the digital landscape.

Just as the NEP emphasizes the holistic development of students, our approach to web development should extend beyond technical skills. Let's prioritize the development of essential soft skills such as problem-solving, collaboration, and adaptability, ensuring that learners are well-rounded professionals capable of thriving in diverse environments.

I thank all other members for completing this task on time and in such an admirable way. I am also thankful to all the institutions and organisations that have generously extended their help and assistance in making this possible. As an organisation committed to reforming school education in Bharat and continuously improving the quality of all learning and teaching material that it develops, NCERT looks forward to critical comments and suggestions from all its stakeholders to further improve upon this textbook.

Professor Dinesh Prasad Saklani

Director

National Council of Educational Research and Training

New Delhi

Foreword

Vocational Education and Training (VET) plays a significant role in preparing youth for relevant occupations and meeting the skill demand of the changing labour market. This is even more relevant, as India is witnessing an accelerated youth population and the need for preparing a skilled workforce for the growing economy. The strong partnership with the industry partners characterises India's National Skills Qualification Framework (NSQF). The Vocationalisation of Education in Schools under *Samagra Shiksha* by the Ministry of Education, Government of India, is spearheading and catalysing the role of vocational education and training in equipping young people with skills.

The recent reforms through the National Educational Policy (NEP) 2020 have focused on making the VET system more coherent and flexible to both the needs of the labour market and social challenges. Improving the learning pathways and bridging the gap between vocational and general education, and avoiding dead ends, is another goal. The ultimate goal is to ensure flexibility and responsiveness to the needs through education and training, and to provide a strong framework for lifelong learning.

Reflecting on vocational education and training priorities, and recent developments in the system, priority has to be placed on developing vocational teachers of trainers to act as the link between education and training and employment. Preparing a cadre of professionally trained. Vocational teachers is vital for imparting quality vocational education and developing skilled workforce in different sectors In this perspective, the PSS Central Institute of Vocational Education (PSSCIVE), Bhopal has introduced a 'Diploma in Vocational Education and Training' through distance mode, to develop a pool of trained vocational teachers or resource persons in spearheading the effective, Implementation of the scheme an vocationalization of education in schools across India, The Diploma in VET is a one year programme, which will be taught in four blocks of tri-semester. It aims to provide the learners with the latest knowledge, skills, and competencies in the field of vocational education and training. Among others, the programme will also enable the learners to appreciate the ethical dimension of teacher professionalism in Vocational Education. The goal is to. Equip the learners with a strong theoretical and practical understanding of VET while integrating ICT in their teaching.

I acknowledge the contributions of the material development team, reviewers, and the support team for their contributions in the development of this self- learning material. We would welcome suggestions, which would help us to improve further the quality of this programme.

Wish you all the very best in this endeavor.

Dr. Deepak Paliwal

Joint Director

PSSCIVE, Bhopal

About the Textbook

"Junior Cyber Security Assistant for Class 9th" is a concise and practical textbook designed to introduce students to the fundamentals of computer networks, operating systems, and cyber security. It provides clear explanations and hands-on exercises that help learners understand how data travels through networks, how systems operate, and how to protect digital environments effectively.

The book covers key topics such as Introduction to Computer Networks, OSI and TCP/IP Models, IP Addressing and Subnetting, TCP/IP Utilities and Troubleshooting, Exploring Windows Operating System, and Exploring Linux Operating System. Each chapter combines theory with practical tasks, enabling students to apply concepts in real-world scenarios and strengthen their problem-solving and troubleshooting skills.

By studying this textbook, students gain a strong foundation for future learning and careers in IT and cybersecurity. It nurtures essential technical skills in network configuration, system management, and digital safety, preparing learners to adapt confidently to today's technology-driven world.

Dr. Munesh Chandra

Professor

Department of Engineering and Technology

PSSCIVE, NCERT, Bhopal

Textbook Development Team

1. Dr. Digvijay Singh Rathore, National Forensic Science University, Gandhi Nagar
2. Dr. Virendra Kumar Yadav, Indian Institute of Technology, Delhi
3. Mr. Desh Deepak Pathak, Directorate of Education, GNCT, Delhi
4. Ms. Yogita Goyal, Gurukul The School, Ghaziabad
5. Dr. Monika Sharma, PSSCIVE, Bhopal
6. Ms. Soumya Trivedi, AKG Engineering College, Ghaziabad

MEMBER-COORDINATOR

Dr. Munesh Chandra,

PSSCIVE, NCERT, Bhopal

Acknowledgement

On behalf of the team at the PSS Central Institute of Vocational Education (PSSCIVE), Bhopal, we are grateful to the officials of the Ministry of Education, Government of India, for the guidance and support at all times and levels.

We are obliged to the Director, NCERT, for his care and leadership. We are indebted to the PAC NCERT for financial support.

We acknowledge the contributions of our colleagues at PSSCIVE and other experts for their academic support, untiring efforts, and contributions to the development of this material. The names of all the experts are acknowledged in the list of contributors.

The contributions made by the Administration and the supporting staff of PSSCIVE are duly acknowledged.

TEAM PSSCIVE

Table of Contents

Chapter-1

Introduction to Computer Networks

At Sunnydale High, students often waited in long lines to use the computer lab and printers. The principal asked Mr. Sharma, the computer teacher, to find a solution. He connected all the computers using cables and Wi-Fi, linking them to the printer and the internet. Suddenly, students could share files, access online resources, and print from any computer. Riya said excitedly, "It's like all the computers are talking to each other!" The network made learning faster, easier, and more fun, and the school realized the true power of computer networks.

1.1. Introduction to computer networks

A computer network is a system where two or more computers are connected together to share information, resources, and services. These connections can be made using wires (like cables) or without wires (using Wi-Fi).

In everyday life, computer networks allow us to do many things, such as browsing the internet, sending emails, chatting with friends, or sharing files and printers. The most common and largest computer network in the world is the Internet, which connects millions of computers globally.

Real-life Example:

In a school computer lab, all the computers are connected to a printer. This connection is a computer network. It allows students to access the same internet connection, share files, and even take printouts from a single printer.

Did You Know?

- In a computer network, you can share not just files but also devices like printers and scanners. Computer networks make communication faster, save time, and help people work together more easily.

Need for a Computer Network

A computer network is important because it allows computers and devices to work together. The main needs of a computer network are:

- **Sharing of Resources –** Networks allow sharing of printers, scanners, and storage devices, which saves cost.

- **Sharing of Data and Files –** Information, documents, and media can be easily shared between computers.
- **Communication –** Networks make it possible to send emails, messages, or video calls quickly.
- **Access to the Internet –** Through networks, users can browse websites, use apps, and learn online.
- **Centralized Data Management –** In schools, offices, or banks, networks help store and manage data in one central place, making it secure and easy to update.
- **Collaboration –** People can work on the same project together even if they are in different places.

Example: In a school, a computer network helps teachers and students share notes, access study materials, and use one printer for the entire class.

1.2. History and Evolution of Computer Networks

i. Global Evolution of Computer Networks

1960s – Beginning of Networking:
The concept of connecting computers started in the 1960s. In 1969, the U.S. Department of Defense created a project called ARPANET (Advanced Research Projects Agency Network). This was the first successful computer network and the foundation of today's Internet.

1970s – Email and Early Networking:
In 1971, the first email was sent over ARPANET. Networks grew in universities and research centers, connecting scientists and researchers.

1980s – Expansion and Internet Protocols:
A set of rules called TCP/IP (Transmission Control Protocol/Internet Protocol) was developed. These rules allowed different networks to connect, creating the "network of networks" – the Internet. In 1983, the word Internet began to be used.

1990s – World Wide Web (WWW):
In 1991, Tim Berners Lee invented the World Wide Web (WWW), which made the Internet easy to use with websites, links, and browsers. This started the growth of email services, search engines, and online businesses.

2000s – Broadband and Wireless Internet:
The Internet became faster with broadband and Wi-Fi. Social media platforms like Facebook, YouTube, and Twitter appeared, making global communication very easy.

2010s to Present – Smart Era:
With the rise of 4G, 5G, cloud computing, and IoT (Internet of Things), computer networks are now everywhere—connecting not just computers, but also smartphones, smart TVs, cars, and even household appliances.

ii. Evolution of Computer Networks in India

1980s – Early Developments:
India started with small research networks in institutions. The National Informatics Centre (NIC) launched NICNET in 1987, which was India's first nationwide satellite-based computer network. It connected government offices across the country.

1990s – Internet Comes to India:
The Internet was officially launched in India on 15th August 1995 by VSNL (Videsh Sanchar Nigam Limited). At first, it was very slow and costly, and only a few people could access it.

2000s – Growth of Internet and Mobile Networks:
Internet services expanded quickly with the spread of broadband. The rise of mobile phones brought internet access to more people. Cyber cafés also became popular in cities and towns.

2010s – Digital India Revolution:
With the launch of affordable smartphones and 4G internet (especially after 2016), India became one of the largest consumers of mobile internet in the world. The government's Digital India program promoted e-governance, online education, and digital payments.
Present and Future:
India is now rapidly adopting 5G networks, cloud computing, and AI-based applications. Projects like BharatNet aim to connect even rural areas with high-speed internet, making India a digitally connected nation.

Did You Know?

- Globally, computer networks evolved from ARPANET (1969) → Internet (1980s) → World Wide Web (1990s) → High-speed and wireless networking (2000s) → Smart connected world (2010s onwards).
- In India, computer networks began with NICNET (1987) → Internet launch (1995) → Broadband and mobile internet (2000s) → Digital India and 4G/5G (2010s onwards).

1.3. Client–Server Model

The client–server model is one of the most common ways computers communicate over a network. It is based on the idea that one computer (the server) provides services, while other computers or devices (the clients) request and use those services.

i. Client

- A client is a computer, laptop, or smartphone that sends a request to the server.
- Clients are usually used by end-users (students, office workers, etc.) to access information or services.
- They depend on the server to get resources like web pages, files, or emails.
- Example: When you open a web browser (like Chrome or Firefox) and type in a website, your computer is the client.

ii. Server

- A server is a powerful computer that stores data, applications, or services.
- It waits for requests from clients and responds by providing the required information.
- Servers are always connected and running so that clients can access them anytime.
- Example: Google's servers store billions of web pages. When you search for something, they send the results to your device.

Working of the Client–Server Model
The Client–Server model works on the principle of request and response. Clients request a service, and the server responds with the required result.
Here's how it works step by step:
1. Connection Setup

- A client (like a computer, laptop, or smartphone) connects to the network (LAN, Wi-Fi, or Internet).
- The server (a powerful computer) is already connected and running, waiting for requests.

2. Request from Client

- The client sends a request to the server.
- Example: When you type 'www.wikipedia.org' in a web browser, your browser (client) sends a request to Wikipedia's server asking for the web page.

3. Processing by Server

- The server receives the request.
- It searches for the required data or performs the necessary task.
- Example: Wikipedia's server searches its database for the homepage content.

4. Response from Server

- Once the data is ready, the server sends a response back to the client.
- Example: Wikipedia's server sends back the homepage (text, images, and links).

5. Display at Client Side

- The client receives the response and displays it for the user.
- Example: The homepage of Wikipedia appears in your browser.

6. Continuous Interaction

- This process of request → processing → response happens repeatedly whenever you click a link, send a message, or download a file.
- The server can handle requests from many clients at the same time.

Real-Life Examples of Working

- Web Browsing: Browser (client) requests a webpage → Web server responds.
- Email: Email app (client) requests new messages → Mail server provides them.
- Online Games: Player's device (client) requests game updates → Game server sends data.

Advantages of Client–Server Model

- Centralized Data: Data and files are stored in one place (server), making it easy to manage.
- Security: The server can control access with passwords and security settings.
- Resource Sharing: Printers, files, and applications can be shared across clients.
- Scalability: New clients (computers or devices) can be added easily.

Disadvantages of Client–Server Model

- Single Point of Failure: If the server crashes, clients cannot access resources.
- Cost: Setting up and maintaining a server requires money and skilled staff.
- Overload: Too many requests from clients can slow down the server.

Did You Know?

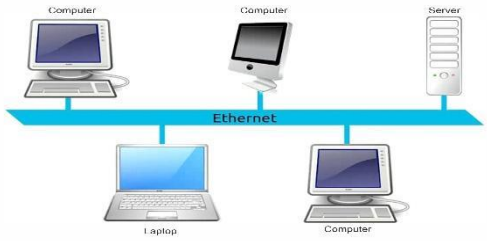
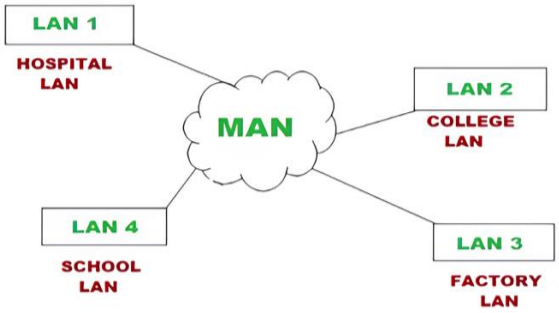
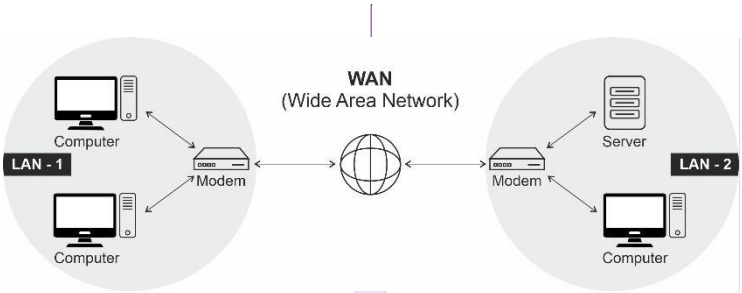
- India got Internet access for the first time on 15th August 1995.
- The first email was sent in 1971, and it was simply the text: "QWERTYUIOP."

Assignment 1.1.

1. Define a computer network in your own words.
2. Write two real-life examples of computer networks.

1.4. Types of Computer Network

Computer networks are categorized based on their size, coverage area, and purpose. The major types include:

Local Area Network (LAN): • A high-speed network covering a small area, such as homes, offices, or schools. It uses Ethernet or Wi-Fi for communication.	
Metropolitan Area Network • **Metropolitan Area Network (MAN):** A network that connects multiple LANs within a city, often used by businesses, government agencies, or cable TV providers (e.g., cable TV networks).	
Wide Area Network • **Wide Area Network (WAN):** A large-scale network covering vast distances, such as the Internet, which connects multiple cities or countries via leased lines, satellites, or fiber optics.	

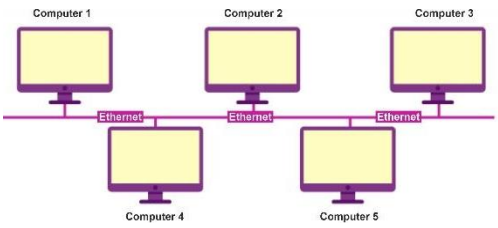
[1]

Table 1.1: Types of Computer Networks

1.5. Network Topologies

Network topology defines the structural layout of devices in a network. Common topologies include:

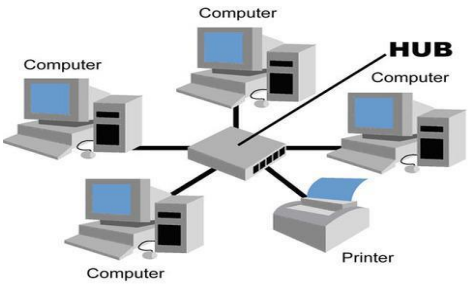
1. Bus Topology



In a bus topology, all the computers are connected to a single main cable called the backbone. The data sent by one computer travels through this backbone, and every computer on the network receives the data, but only the intended device accepts it. This topology is simple and requires fewer cables, which makes it cost-effective. However, the entire network depends on the backbone cable, and if it fails, the whole network stops working. Bus topology is suitable for small networks.

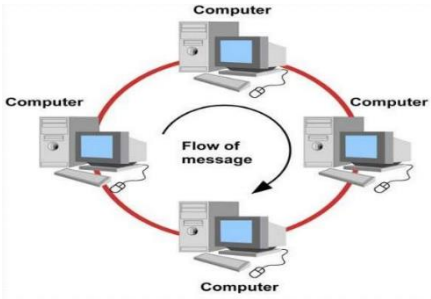
2. Star Topology:

In a star topology, all computers are connected to a central device such as a switch or a hub. The central device manages the flow of data between different computers. This topology is easy to set up and expand, and the failure of one computer does not affect the others. However, if the central hub or switch fails, the entire network stops working. Star topology is one of the most commonly used topologies in schools, offices, and organizations.



3. Ring Topology:

In a ring topology, each computer is connected to exactly two other computers, forming a circular path for the flow of data. The data travels around the ring in one direction (or sometimes both) until it reaches the correct destination. This arrangement ensures that each computer has equal access to the network. However, the failure of one computer or cable can disrupt the whole network, making it difficult to troubleshoot. Ring topology is less common today, but was widely used in earlier networks.



4. Mesh Topology:

In a mesh topology, every computer is directly connected to every other computer in the network. This provides multiple paths for data to travel, making the network highly reliable. If one connection fails, data can take another route to reach its destination. Mesh topology offers excellent performance and security, but it is very expensive because it requires a large number of cables and ports. It is mostly used in critical systems where reliability is very important, such as in military or banking networks.

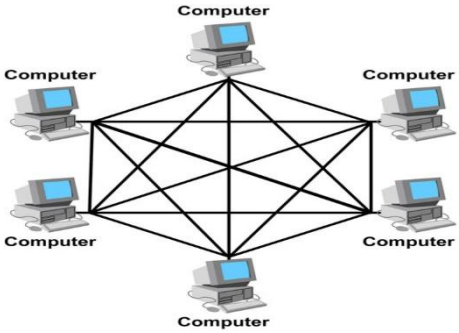


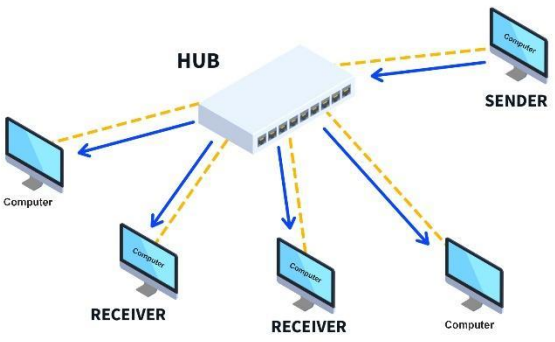
Table 1.2: Topologies Used in Networking

1.6. Networking Devices

When computers are connected to form a network, different devices are needed to manage the flow of data. These devices act like helpers that control how data is sent, received, and directed to the correct place. The most common networking devices are hub, switches, router, and bridges.

Hub

A hub is a basic networking device that connects multiple computers in a network and transmits data to all connected devices, regardless of the destination. It operates at the physical layer of the OSI model and does not filter or manage traffic. Hubs are cost-effective and simple, but lead to network congestion and collisions due to unnecessary data broadcasting. While once common in small networks, they are now largely replaced by more efficient switches, which offer better traffic management and performance.



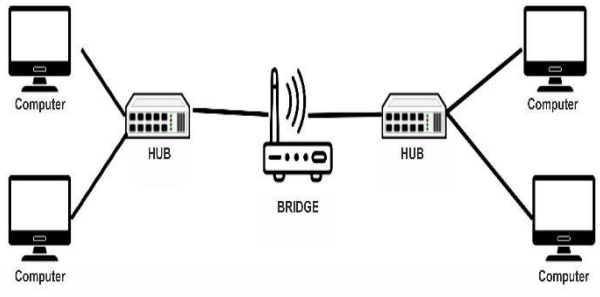
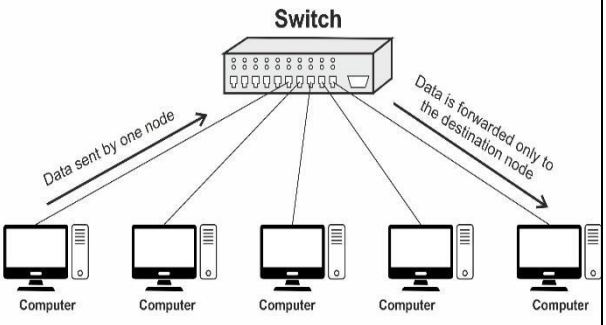
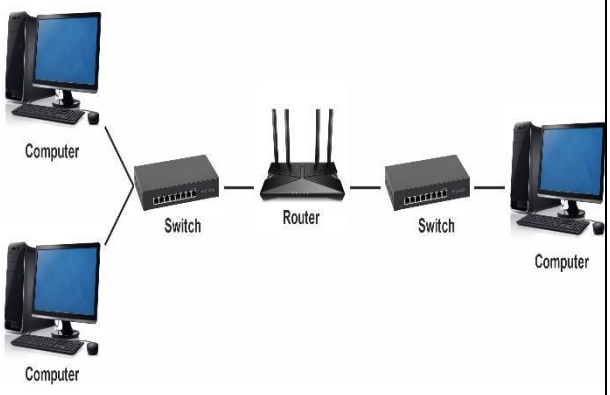
Bridge A bridge is a networking device that connects and filters traffic between two or more LAN segments, improving network efficiency. It operates at the data link layer (Layer 2) and uses MAC addresses to forward or block data, reducing congestion. Bridges enhance performance by segmenting traffic, preventing unnecessary data flow. Unlike repeaters, they analyze data before forwarding. Commonly used in large networks, bridges help in network expansion while maintaining seamless communication and reducing collisions between connected segments.	
Switch A switch is an intelligent networking device that connects multiple devices within a LAN and efficiently manages data traffic. It operates at the data link layer (Layer 2), using MAC addresses to forward data only to the intended recipient, reducing congestion. Unlike hubs, switches improve network performance by enabling simultaneous data transfers. Advanced switches also function at Layer 3 (network layer) for routing. They enhance speed, security, and scalability, making them essential for modern enterprise and home networks.	
Router A router is a networking device that directs data packets between different networks, enabling internet connectivity and efficient communication. It determines the best path for data transmission using IP addresses and routing protocols. Routers enhance security with firewalls, support multiple devices, and enable network segmentation. They connect LANs to WANs, ensuring seamless data flow. Unlike switches, routers operate at the network layer, making intelligent forwarding decisions. Essential for both home and enterprise networks, routers optimize performance, security, and scalability.	

Table 1.3: Networking Devices Overview

Did You Know?

A switch is smarter than a hub because it sends data only to the computer that actually needs it.

1.7. Transmission Media

When data is transferred in a computer network, it needs a medium (path) through which it can travel. This medium is called Transmission Media. It is the physical or wireless channel that carries data signals from one device to another. Transmission media can be divided into two main types: Wired Media and Wireless Media.

1. Wired Media

Wired media uses physical cables to connect computers and other devices in a network. Data travels in the form of electrical signals or light through these cables. Wired media is reliable, secure, and less affected by interference, but it requires a lot of cabling.

Types of Wired Media:

- **Twisted Pair Cable:** Made up of pairs of copper wires twisted together. It is commonly used in telephone lines and local area networks (LANs).
- **Coaxial Cable:** A thick cable with better protection against interference, often used in cable TV and early computer networks.
- **Optical Fiber Cable:** Uses light signals instead of electricity to carry data. It provides very high speed and can carry data over long distances, making it popular in modern networks and Internet connections.

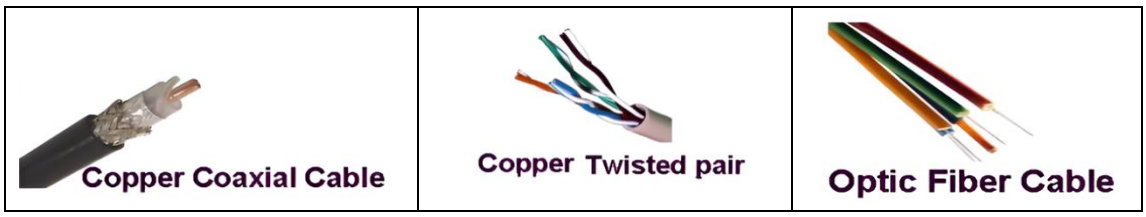


Fig: 1.1. Wired Media

2. Wireless Media

Wireless media does not use cables. Instead, it uses radio waves, microwaves, or infrared signals to transmit data through the air. It allows devices to connect without physical wiring, making it flexible and convenient. However, wireless signals can be affected by distance and interference.

Types of Wireless Media:

- **Radio Waves:** Used in Wi-Fi, mobile networks, and FM radio. They can cover both short and long distances.
- **Microwaves:** Used in satellite communication and long-distance data transfer.
- **Infrared:** Used for very short-range communication, like remote controls.

Assignment 1.2

1. List any two advantages and one disadvantage of the client–server model.
2. What is the function of a router?

Practical Activity 1.1: Demonstrating the Client–Server Concept

Materials Required

- At least two computers (one as server, one as client) connected in a LAN (Local Area Network) or using Wi-Fi.
- Basic software (e.g., Notepad for writing a simple webpage, and a web browser such as Chrome/Edge).

Steps

Step 1: Set up the Server

- On Computer 1, open Notepad and type a simple HTML page:

  <html>

  <head><title>Server Test</title></head>

  <body><h2>Hello, this is the Server!</h2></body>

  </html>

- Save the file as index.html in a folder.
- Use a simple web server tool (e.g., XAMPP or Python HTTP server) to host the page.
- (For example, in Python: open Command Prompt → type python -m http.server inside the folder where the file is saved.)

Step 2: Find the Server Address

- Check the IP address of Computer 1 (server) using the command: "ipconfig."
- Note down the IP address (e.g., 192.168.1.10).

Step 3: Set up the Client

- On Computer 2 (client), open a web browser.
- In the address bar, type the server's IP address followed by the port number (e.g., http://192.168.1.10:8000).

Step 4: Observe the Result

- The webpage created on the server (Computer 1) will be displayed on the client (Computer 2).

This shows that the client requested the page and the server responded by sending the page back.

Practical Activity 1.2: Network Topology Simulation

Materials Required

- Computer with Cisco Packet Tracer software installed.
- Basic understanding of using Packet Tracer tools (PCs, Switches, Hubs, and Connections).

Steps

A. Creating a Star Topology

- Open Cisco Packet Tracer.
- From the device list, drag and drop one switch and four PCs onto the workspace.
- Use the "Connections" tool → select Copper Straight-Through Cable.
- Connect each PC to the switch using the cable.
- Assign IP addresses to each PC:

  PC1: 192.168.1.1

  PC2: 192.168.1.2

  PC3: 192.168.1.3

  PC4: 192.168.1.4

- Test connectivity using the Ping command from one PC to another (e.g., PC1 → PC3).

- Observe that all communication passes through the central switch.

B. Creating a Bus Topology

- Place four PCs and one Hub on the workspace.
- Connect all PCs to the Hub using Copper Straight-Through Cables.
- Assign IP addresses in the same range as before.
- Test communication between PCs using Ping.
- Observe that the hub sends data to all devices, even if only one PC is the intended recipient.

C. Creating a Ring Topology

- Place four PCs in a circular arrangement.
- Connect them using Copper Cross-Over Cables in a closed loop.

  (PC1 → PC2 → PC3 → PC4 → back to PC1).
- Assign IP addresses in the same range.
- Ping from PC1 to PC3 and observe data flow around the ring.

D. Creating a Mesh Topology

- Place four PCs on the workspace.
- Connect every PC to every other PC using Copper Cables.

  (Each PC will have 3 connections).
- Assign IP addresses in the same range.
- Ping between different PCs and observe multiple paths for data.

Observation

- Star Topology: Communication depends on the central switch.
- Bus Topology: All data travels through the single backbone hub.
- Ring Topology: Data moves in a circular path until it reaches the destination.

Mesh Topology: Provides multiple paths, making the network more reliable.

Practical Activity: Identifying Network Devices and Transmission Media through real/virtual labs

Materials Needed

- Real Lab: Hub, Switch, Router, Bridge, Cables (Twisted Pair, Coaxial, Optical Fiber), Wi-Fi Router
- Virtual Lab (Cisco Packet Tracer): Devices and cables available in the software library

Procedure

Step 1: Open Lab Setup

- If working in a real lab, visit the networking section and collect the available devices and cables.
- If working in Cisco Packet Tracer, open the software and go to the Device List Panel to view available networking devices.

Step 2: Identify Networking Devices

Hub

- Real: Check for ports where cables can be plugged in.
- Virtual: Select hub from the "Network Devices → Hubs" category.
- Function: Broadcasts data to all connected devices.

Switch

- Real: Looks similar to a hub but is smarter in function.
- Virtual: Available under "Switches" in Packet Tracer.
- Function: Sends data only to the intended destination device.

Router

- Real: Small device with antenna (Wi-Fi router) or bigger industrial routers.
- Virtual: Found under "Routers" in Packet Tracer.
- Function: Connects different networks and manages traffic using IP addresses.

Bridge

- Real: Rarely seen in modern labs, but can be identified as a simple two-port device.
- Virtual: Found in "Switches/Bridges" section.
- Function: Connects two LAN segments and filters data.

Step 3: Identify Transmission Media

Twisted Pair Cable

- Real: Color-coded twisted wires inside plastic covering.
- Virtual: Available under "Connections → Copper Straight-through/Cross-over Cable."
- Function: Common LAN connection cable.

Coaxial Cable

- Real: Thick cable with one copper core.
- Virtual: Shown in "Connections" list.
- Function: Used in older networks and cable TV.

Optical Fiber Cable

- Real: Thin, glass-like cable for very fast communication.
- Virtual: Represented as a fiber cable in "Connections."
- Function: Long-distance, high-speed communication.

Wireless Media

- Real: Wi-Fi router and connected devices.
- Virtual: Use a Wireless Router and PCs with Wi-Fi in Packet Tracer.

Function: Uses radio waves for data transfer without cables.

Summary

- A computer network connects two or more computers to share data, resources, and applications.
- Networks are needed for file sharing, hardware sharing, communication, and cost efficiency.
- ARPANET was the first network in the 1960s, and the Internet became public in India in 1995.
- In the client–server model, the client requests services and the server provides them.
- In a bus topology, all devices share one backbone cable.

- In a star topology, all devices are connected to a central hub or switch.
- In a ring topology, devices are connected in a closed loop where data moves in one direction.
- In a mesh topology, every device is connected to every other device.
- A hub broadcasts data to all devices, while a switch sends it only to the correct device.
- A router connects different networks, and a bridge connects two LAN segments.
- Wired media include twisted pair cable, coaxial cable, and optical fiber.
- Wireless media include Wi-Fi, Bluetooth, radio waves, and infrared.
- Tools like Cisco Packet Tracer can be used to simulate and practice network setups.
- Optical fiber is the fastest transmission medium because it uses light signals.

ASSESSMENT

A. Multiple Choice Questions

1. Which is the largest computer network in the world?
   a) LAN
   b) MAN
   c) Internet
   d) WAN

2. ARPANET, the first successful computer network, was created in:
   a) 1960
   b) 1969
   c) 1975
   d) 1983

3. Which protocol formed the foundation of the Internet?
   a) HTTP
   b) TCP/IP
   c) FTP
   d) SMTP

4. The World Wide Web (WWW) was invented by:
   a) Charles Babbage
   b) Vint Cerf
   c) Tim Berners-Lee
   d) Dennis Ritchie

5. In which year was the Internet officially launched in India?
   a) 1987
   b) 1991
   c) 1995
   d) 2000

6. In the client–server model, the client's role is to:
   a) Store data
   b) Provide services
   c) Request services
   d) Manage networks

7. Which topology connects all computers to a central hub or switch?
   a) Bus
   b) Star

c) Ring
d) Mesh

8. Which device directs data packets between different networks?
   a) Hub
   b) Switch
   c) Router
   d) Bridge

9. Optical fiber cables transmit data using:
   a) Electrical signals
   b) Light signals
   c) Radio signals
   d) Infrared signals

10. Which wireless medium is used in remote controls?
    a) Radio waves
    b) Microwaves
    c) Infrared
    d) Bluetooth

B. Fill-in-the-blanks

1. A computer network allows computers to share _____, _____, and _____.
2. The first successful computer network was _____, created in 1969.
3. The first email was sent in the year _____.
4. The set of rules that allow networks to connect with each other is called _____.
5. The Internet was officially launched in India on _____.
6. In the client–server model, a _____ provides services while a _____ requests services.
7. In _____ topology, all devices are connected to a single main cable called backbone.
8. A _____ is smarter than a hub because it sends data only to the intended computer.
9. _____ cable uses light signals to transmit data over long distances.
10. _____ waves are used in Wi-Fi and mobile networks.

C. True/False questions

1. The Internet is also called the “network of networks.”
2. ARPANET was launched in India in 1969.
3. Email was first introduced in the year 1971.
4. TCP/IP is the protocol that connects different networks together.
5. The World Wide Web (WWW) was invented in 1991 by Vint Cerf.
6. In a star topology, if the central hub fails, the entire network stops working.
7. A hub is more intelligent than a switch.
8. Routers operate at the network layer of the OSI model.
9. Optical fiber cables are slower than twisted pair cables.
10. Wireless media uses radio waves, microwaves, or infrared signals.

D. Short Answer Questions

1. Define a computer network with one real-life example.
2. Why do we need computer networks in schools or offices?
3. Write two differences between a client and a server.
4. Name any three major milestones in the global evolution of computer networks.
5. When was NICNET launched in India, and what was its purpose?
6. Explain the working principle of the client–server model.
7. Differentiate between LAN, MAN, and WAN with one example each.
8. What are the main advantages and disadvantages of a star topology?
9. Write the functions of a router and a switch.
10. Explain the difference between wired and wireless transmission media with examples.

Answer Key

A. Multiple Choice Questions

1. c), 2. b), 3. b), 4. c), 5. c), 6. c), 7. b), 8. c), 9. b), 10. c)

B. Fill-in-the-blanks

1. information, resources, and services, 2. ARPANET, 3. 1971, 4. TCP/IP, 5. 15th August 1995, 6. server, client, 7. Bus, 8. Switch, 9. Optical fiber, 10. Radio

C. True/False questions

1. True, 2. False, 3. True, 4. True, 5. False, 6. True, 7. False, 8. True, 9. False, 10. True

Chapter-2

OSI & TCP/IP Protocol Models

In a small town, a group of computers wanted to send messages to each other. But there was a problem—each computer spoke a different language! Sometimes, messages get lost or misunderstood. One day, a wise computer named OSI said, "Let's follow a set of rules so everyone can understand each other." OSI divided the communication into seven steps, from sending raw bits to showing the final message on the screen. Later, another computer called TCP/IP simplified the process into four layers to make communication faster over the Internet. Soon, all computers could send and receive messages correctly. Maya, a student watching this, said, "It's like computers are talking to each other using secret steps!" From that day, the town's computers worked together smoothly, showing how important rules and layers are in network communication.

2.1. Introduction of IAB, ICANN, Internet, Intranet

IAB (Internet Architecture Board)

The Internet Architecture Board (IAB) is a committee that oversees the technical and engineering development of the Internet. It ensures that the Internet runs smoothly by creating and maintaining global standards for communication protocols. The IAB supervises Internet-related activities, reviews new proposals, and guides researchers and developers. It plays an important role in ensuring that computers, devices, and applications developed by different companies can communicate effectively across the world.

Advantages of IAB:

- Maintains global technical standards for smooth Internet functioning.
- Encourages research and development in networking technologies.
- Provides technical direction for the long-term growth of the Internet.

Disadvantages of IAB:

- Works more at a policy and technical guidance level, so ordinary users may not see its impact directly.
- Decisions sometimes take time due to the involvement of multiple committees.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is an international organization that manages the Internet's Domain Name System (DNS). It ensures that every website has a unique domain name and that these names are correctly mapped to IP addresses. Without ICANN, there would be confusion as multiple users could try to register the same domain name. ICANN also distributes IP addresses globally, making sure that each device on the Internet has a unique identity.

Advantages of ICANN:

- Ensures that websites and domains are unique and easy to access.
- Provides global management of IP addresses.
- Makes Internet browsing user-friendly (users type names instead of complex numbers).

Disadvantages of ICANN:

- Centralized control can sometimes create issues of power and dependency.
- Domain registration and renewal fees can be costly for some organizations or individuals.

Internet

The Internet is the world's largest network that connects millions of computers, devices, and users globally. It uses the TCP/IP protocol to allow communication and data transfer. The Internet makes it possible to send emails, browse websites, attend online classes, shop online, and connect with people through social media. It has become a necessity for education, business, government, and entertainment.

Figure 2.1: Internet

Advantages of the Internet:

- Provides instant access to vast information and knowledge.
- Enables easy global communication through email, video calls, and messaging.
- Supports e-learning, e-commerce, banking, and online entertainment.
- Encourages global collaboration and sharing of ideas.

Disadvantages of the Internet:

- It can expose users to cyber threats like hacking, phishing, and viruses.
- Leads to over-dependence and sometimes addiction (e.g., social media).
- Privacy and security risks due to data tracking and misuse.
- Requires stable infrastructure, which may not be available in rural areas.

Intranet

An Intranet is a private network that uses Internet technologies but is restricted within an organization. It allows employees or members to share internal documents, information, and applications securely. Intranets are commonly used in schools, colleges, offices, and government departments to ensure smooth internal communication. Unlike the Internet, outsiders cannot access an intranet without permission, which makes it more secure.

Advantages of Intranet:

- Provides secure communication within an organization.
- Allows easy sharing of internal resources like documents, notices, and applications.
- Reduces printing and communication costs by digitizing information.
- Increases productivity by centralizing information in one place.

Disadvantages of Intranet:

- Limited access (only within the organization).
- Setup and maintenance require cost and technical expertise.
- It can become outdated if not regularly updated.
- It may be less useful if employees are working remotely without proper access.

2.2. Open Systems Interconnection (OSI) Model

The OSI model is a conceptual framework developed by the International Organization for Standardization (ISO) to explain how computers and devices communicate over a network. Its primary purpose is to standardize network communication, ensuring that devices from different manufacturers can communicate with each other. The OSI model divides the communication process into seven layers, where each layer has a specific function. This layered approach simplifies network design, troubleshooting, and understanding of how data flows from one device to another. By separating tasks into layers, network engineers can focus on individual layers without worrying about the entire system.

Functions of the OSI Model

- **Standardization –** Provides a universal set of guidelines for communication between devices and networks, making hardware and software interoperable.
- **Modularity –** Divides complex communication tasks into smaller, manageable layers.
- **Troubleshooting –** Helps network engineers identify and fix problems by checking each layer individually.
- **Interoperability –** Ensures devices from different manufacturers or operating systems can work together.
- **Efficiency –** Optimizes communication by defining clear roles for each layer, preventing redundancy and conflicts.

The Seven Layers of the OSI Model

1. Physical Layer

The physical layer is the lowest layer of the OSI model and deals with the actual transmission of raw data (bits 0 and 1) over physical media. It defines the hardware requirements, including cables (twisted pair, coaxial, optical fiber), connectors, network interface cards (NICs), and electrical signals. This layer ensures that bits sent from one device can physically reach another device, either through wired or wireless media.

Key Functions:

- Converts data into electrical, optical, or radio signals.
- Defines how devices are physically connected.
- Handles data rate, voltage levels, and signal timing.
- Examples: Ethernet cables, fiber optic cables, Wi-Fi signals, hubs.

2. Data Link Layer

The data link layer provides error-free transmission of data frames between two devices on the same network. It organizes raw bits from the physical layer into frames, detects and corrects errors, and uses MAC addresses to identify devices on the network. This layer is essential for reliable local communication and prevents collisions in networks like LANs.

Key Functions:

- Framing: Divides data into frames for transmission.
- Error detection and correction: Uses techniques like CRC (Cyclic Redundancy Check).
- Flow control: Prevents a fast sender from overwhelming a slow receiver.
- MAC addressing: Identifies devices within the same network.
- Examples: Switches, bridges, Ethernet cards.

3. Network Layer

The network layer is responsible for routing data packets from the source device to the destination device across multiple networks. It assigns logical addresses (IP addresses) and decides the best path for data to travel. This layer ensures that data can reach devices even if they are located in different cities, countries, or networks.

Key Functions:

- Logical addressing: Assigns IP addresses to devices.
- Routing: Determines the best path for data packets.
- Packet forwarding: Moves packets from source to destination across routers.
- Examples: Routers, IP addressing, ICMP (Internet Control Message Protocol).

4. Transport Layer

The transport layer provides end-to-end communication between devices. It ensures that the data sent from one device is received completely and correctly by another device. This layer breaks large messages into smaller segments for easier transmission and reassembles them at the destination. It also manages error recovery, flow control, and data sequencing.

Key Functions:

- Segmentation and reassembly of data.
- Error detection and correction.
- Ensures reliable delivery using protocols like TCP.

- Provides faster delivery with protocols like UDP (without error checking).
- Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

5. Session Layer

The session layer manages sessions or connections between applications on different devices. A session is a continuous exchange of information. This layer is responsible for establishing, maintaining, and terminating sessions, ensuring that communication between applications is synchronized.

Key Functions:

- Establishing sessions: Starts communication between devices.
- Maintaining sessions: Keeps track of ongoing communication.
- Terminating sessions: Ends the session properly after communication is complete.
- Synchronization: Ensures data consistency during communication.
- Examples: Online banking sessions, video conferencing sessions, and remote login sessions.

6. Presentation Layer

The presentation layer acts as a translator and formatter between the application layer and the lower layers. It converts data into a format that the receiving application can understand. This layer also handles encryption, decryption, and compression, ensuring secure and efficient transmission of data.

Key Functions:

- Data translation: Converts data formats (e.g., text, images, videos).
- Data encryption and decryption: Ensures secure communication.
- Data compression: Reduces data size for faster transmission.
- Examples: JPEG, MP3, ASCII, HTTPS encryption.

7. Application Layer

The application layer is the topmost layer and interacts directly with users. It provides network services and applications, enabling users to perform tasks like web browsing, email communication, file transfers, and remote access. This layer defines how software applications communicate over a network.

Key Functions:

- Provides services to users.
- Supports protocols for email, web, file transfer, and more.
- Ensures user requests are processed and delivered over the network.
- Examples: HTTP (web browsing), FTP (file transfer), SMTP (email), DNS (domain resolution).

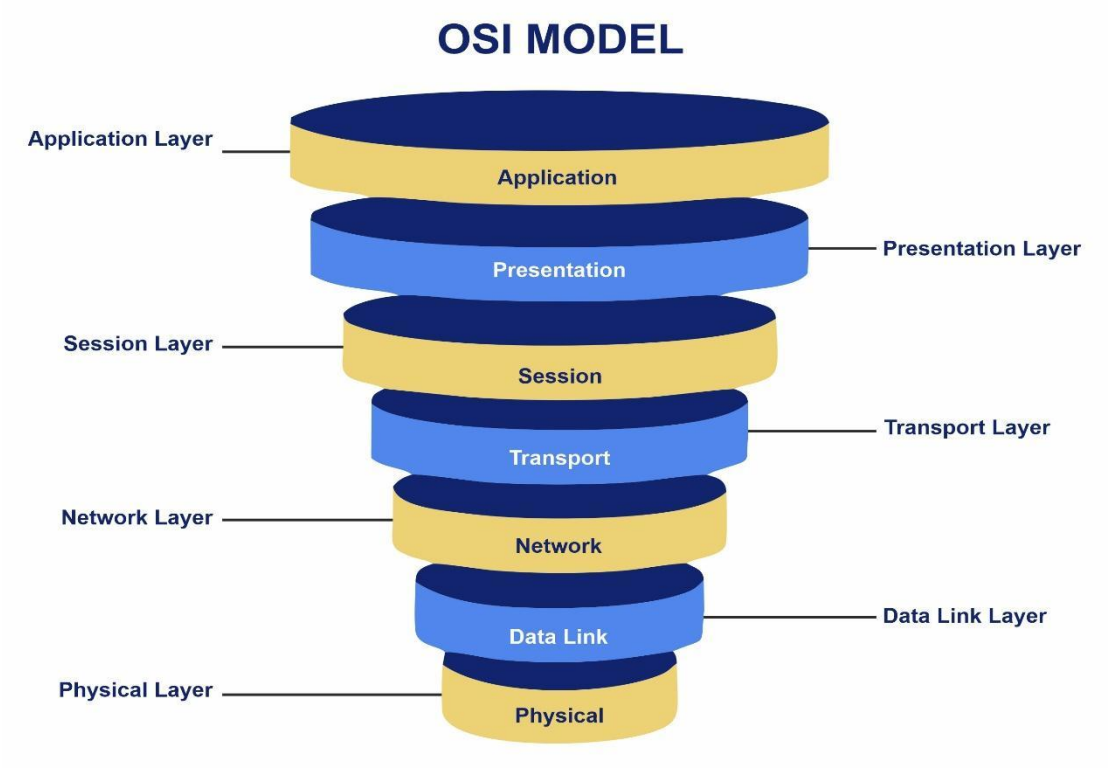


Figure: 2.2: Illustration of an OSI Model

Advantages of the OSI Model

- Provides a standard framework for network communication.
- Simplifies troubleshooting by separating functions layer-wise.
- Ensures interoperability between devices from different manufacturers.
- Helps in designing, developing, and understanding complex networks.

Disadvantages of the OSI Model

- Complex and theoretical; not always fully implemented in real networks.
- Some layers may overlap in functionality, causing redundancy.
- Slower performance in real-world use compared to simplified models like TCP/IP.

Assignment 2.1.

1. List the seven layers of the OSI model.

Explain the role of the Physical Layer in the OSI model.

2.3. TCP/IP 4 Layer Model and Protocol Mapping

The TCP/IP model is a simplified framework used to describe how data is transmitted across networks, especially the Internet. It was developed in the 1970s by the U.S. Department of Defense to provide reliable, end-to-end communication over networks. Unlike the OSI model, which has seven layers, the TCP/IP model has four layers. It is more practical and widely used in real-world networks.

The main purpose of the TCP/IP model is to standardize communication protocols, ensure reliable data transfer, and allow devices from different networks to communicate over the Internet.

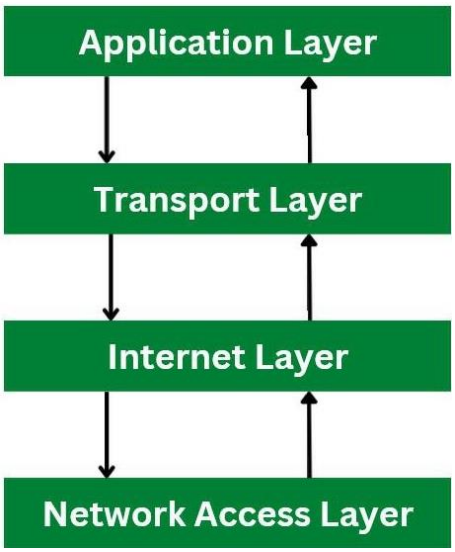


Figure: 2.3: Illustration of a TCP/IP MODEL

i. Network Interface Layer (Link Layer)

The Network Interface Layer is the lowest layer of the TCP/IP model. It handles the physical transmission of data over cables, fiber optics, or wireless media. This layer ensures that bits (0s and 1s) are sent and received correctly between devices on the same network. It also manages hardware addressing using MAC addresses and handles error detection on the local network.

Key Functions:

- Transmits raw data frames between devices.
- Provides physical addressing using MAC addresses.
- Manages access to physical media (cables, Wi-Fi).
- Detects and corrects errors in local transmission.

ii. Internet Layer

The Internet Layer is responsible for logical addressing and routing of data packets across networks. It ensures that data sent from one device reaches the correct device on another network. Each device is assigned a unique IP address, and routers use this layer to forward packets along the best path to the destination.

Key Functions:

- Provides logical addressing with IP addresses.
- Routes packets between networks.
- Fragmentation and reassembly of data packets for efficient delivery.
- Ensures data reaches the correct destination across multiple networks.

iii. Transport Layer

The Transport Layer provides end-to-end communication between devices. It ensures that the data sent from one device is received completely, accurately, and in order at the destination. It breaks large messages into smaller segments, reassembles them, and manages error checking and flow control.

Key Functions:

- Divides data into segments and reassembles them at the receiver.
- Ensures reliable delivery using TCP or faster delivery using UDP.
- Provides error detection and correction.
- Manages flow control to prevent network congestion.
- Supports multiple applications using the same network (multiplexing).

iv. Application Layer

The Application Layer is the topmost layer and provides services directly to users and applications. It enables network-based applications like web browsing, email, file transfers, and remote access. This layer also handles data formatting, encoding, and presentation for applications.

Key Functions:

- Provides network services to end-users.
- Supports protocols like HTTP, FTP, SMTP, DNS, Telnet, and SSH.
- Ensures proper data formatting and encoding.
- Allows applications to communicate over the network seamlessly.

Did You Know?
TCP/IP was developed in the 1970s by the U.S. Department of Defense to allow reliable communication over complex networks.

2.4. TCP vs UDP Protocols

2.4.1. TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol used in the transport layer of the TCP/IP model. It establishes a reliable connection between two devices before data transfer begins. TCP ensures that data is delivered accurately and in order, making it ideal for applications where reliability is crucial.

Key Features of TCP:

- Connection-oriented: A connection is established before data is sent.
- Reliable delivery: Uses acknowledgments (ACKs) to confirm receipt of data.
- Data segmentation: Breaks large messages into smaller packets and reassembles them.
- Error detection and correction: Ensures data integrity during transmission.
- Flow control: Prevents network congestion by managing data transmission rate.

Examples of TCP Applications:

- Web browsing (HTTP/HTTPS)
- Email (SMTP, IMAP, POP3)
- File Transfer (FTP)
- Remote login (SSH, Telnet)

Advantages of TCP:

- Reliable data transmission.
- Ensures data is delivered in the correct order.
- Error detection and correction.

Disadvantages of TCP:

- Slower compared to UDP due to connection setup and error checking.
- More overhead (extra data for reliability).

2.4.2. UDP (User Datagram Protocol)

UDP is a connectionless protocol also used in the transport layer. Unlike TCP, UDP does not establish a connection and does not guarantee reliable delivery. Data packets (called datagrams) are sent independently, which makes UDP faster and more efficient. It is suitable for applications where speed is more important than accuracy.

Key Features of UDP:

- Connectionless: No handshake or connection is established.
- Unreliable delivery: No acknowledgment is sent; some data may be lost.
- Faster and lighter: Minimal overhead compared to TCP.
- No flow control or sequencing: Data packets may arrive out of order.

Examples of UDP Applications:

- Online gaming
- Video streaming and live broadcasts
- VoIP (Voice over IP, e.g., Skype, WhatsApp calls)
- DNS (Domain Name System) queries

Advantages of UDP:

- Faster data transmission.
- Low overhead, efficient for real-time applications.
- Suitable for applications that can tolerate some data loss.

Disadvantages of UDP:

- Data may be lost or arrive out of order.
- No error checking or correction.
- Not suitable for applications requiring reliable communication.

Table 2.1: Comparison between TCP and UDP

Feature	TCP	UDP
Type	Connection-oriented	Connectionless
Reliability	Reliable, ensures delivery	Unreliable, no guarantee of delivery
Data Ordering	Data arrives in order	Data may arrive out of order
Speed	Slower	Faster
Error Checking	Yes, with retransmission	Yes, basic checksum only
Overhead	High	Low
Use Cases	Web browsing, email, and file transfer	Streaming, gaming, VoIP, DNS

Did You Know?

- The OSI model has 7 layers, while the TCP/IP model has only 4 layers, but both explain how data travels over networks.
- TCP ensures reliable delivery of data, while UDP is faster but may lose some data during transmission.

Assignment 2.2

1. Write the four layers of the TCP/IP model.
2. What is the role of the Application Layer in TCP/IP?

2.4.3. Illustration of Port Numbers, Common TCP & UDP Ports

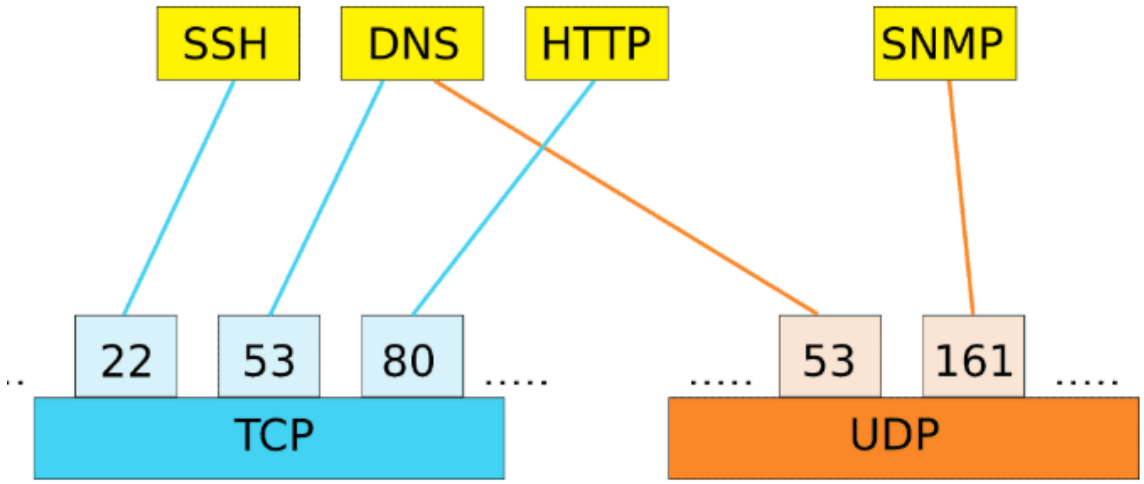


Figure: 2.4: Illustration of Port Numbers, Common TCP & UDP Ports

In TCP/IP networking, port numbers identify specific processes or network services on a host. They are part of the Transport Layer and help in multiplexing communication streams between applications.

- Port numbers range from 0 to 65535.
  - 0–1023: Well-known ports (reserved for common services)
  - 1024–49151: Registered ports
  - 49152–65535: Dynamic/private ports

Common TCP Ports/Common UDP Ports

Port Number	Protocol	Description
20, 21	FTP	File Transfer Protocol (Data, Control)
22	SSH	Secure Shell
23	Telnet	Remote Login (Insecure)
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System (also uses UDP)
80	HTTP	Web traffic (insecure)
110	POP3	Post Office Protocol (email)
143	IMAP	Internet Message Access Protocol
443	HTTPS	Secure HTTP
3389	RDP	Remote Desktop Protocol

Table 2.1: Common TCP Ports/Common UDP Ports

Each port acts as a communication endpoint for a specific process, allowing multiple network services to operate simultaneously on a single machine.

2.5 Common Protocols (HTTP, FTP, DNS, SMTP)

1. HTTP (HyperText Transfer Protocol)

HTTP is the protocol used for transferring web pages and content over the Internet. It allows web browsers (clients) to communicate with web servers and request web pages, images, videos, or other resources. When you type a website address (URL) in your browser, HTTP is the protocol that fetches the web page from the server.

Key Features:

- Connectionless: Each request is independent.
- Text-based: Commands and responses are readable as text.
- Stateless: Server does not remember previous requests from a client.
- Secure Version: HTTPS (HyperText Transfer Protocol Secure) encrypts data to protect it from hackers.
- Example: Accessing www.wikipedia.org or any website in a browser.

2. FTP (File Transfer Protocol)

FTP is used to transfer files between computers over a network. It allows users to upload files to a server or download files from a server. FTP can be used via a web browser, dedicated FTP clients, or command-line tools.

Key Features:

- Requires authentication (username and password).
- Can transfer multiple files and directories.
- Supports both upload (client to server) and download (server to client).
- Secure Version: SFTP (Secure FTP) encrypts the data for secure file transfer.
- Example: Uploading homework files to a school server or downloading software updates.

3. DNS (Domain Name System)

DNS is like the phonebook of the Internet. It translates human-readable domain names (like www.google.com) into IP addresses (like 172.217.12.206) so that computers can locate each other on the Internet. Without DNS, users would need to remember complex IP addresses to visit websites.

Key Features:

- Fast resolution of domain names to IP addresses.
- Distributed system for reliability and speed.
- Supports caching to reduce repeated queries.
- Example: When you type www.facebook.com, DNS translates it to the server's IP address.

4. SMTP (Simple Mail Transfer Protocol)

SMTP is used for sending emails over the Internet. It ensures that emails are sent from a client (like Outlook, Gmail) to a mail server and then to the recipient's mail server.

Key Features:

- Works for sending emails only (not for receiving).
- Uses ports 25, 465 (SSL), or 587 (TLS) for communication.
- Often used with POP3 or IMAP, which are protocols for receiving emails.
- Example: Sending an email from Gmail to your friend's Yahoo account.

5. POP3 (Post Office Protocol 3) and IMAP (Internet Message Access Protocol)

These protocols are used for retrieving emails from a server.

POP3: POP3, short for Post Office Protocol Version 3, is a protocol designed to let users access their email inbox stored on a mail server. It allows downloading of emails and, in many cases, removing them from the server once retrieved. After the POP3 client connects to the server, it can fetch all available messages, which can then be read locally, even without an internet connection.

- When an email is sent, the SMTP protocol is responsible for moving it from the sender's client to their mail server, and then forwarding it to the recipient's mail server.
- Downloads emails from the server to your device.
- Emails are usually deleted from the server after download.
- Suitable when you check emails from a single device.

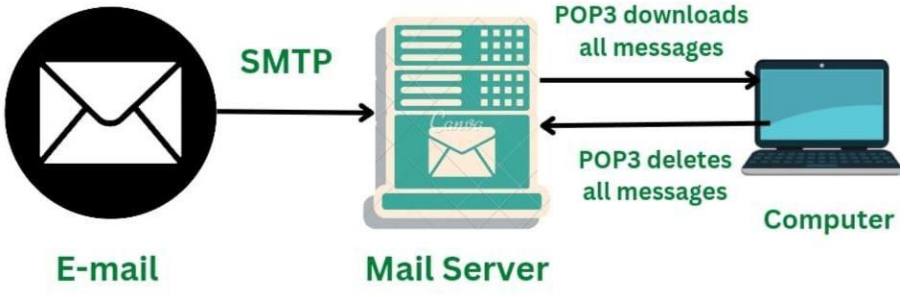


Figure 2.5: POP3

IMAP:

- Keeps emails on the server, allowing access from multiple devices.
- Synchronizes read/unread status across devices.
- Suitable for smartphones, tablets, and computers.
- Example: Accessing your Gmail account on both phone and laptop using IMAP.

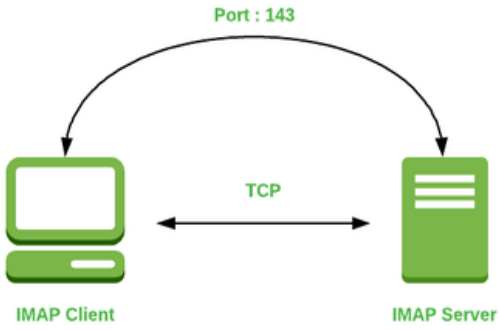


Figure 2.6: IMAP

6. Telnet

Telnet is a protocol used for remote login to another computer or server over a network. It allows users to access and manage devices as if they were physically present.

Key Features:

- Command-line interface.
- Connection-oriented (requires authentication).
- Not secure; data, including passwords, is sent in plain text.
- Secure Version: SSH (Secure Shell) encrypts data for safe remote access.
- Example: Logging into a remote server to manage a website.

7. HTTPS (HyperText Transfer Protocol Secure)

HTTPS is the secure version of HTTP, which encrypts data using SSL/TLS. It ensures that sensitive information like passwords, credit card numbers, or personal details is protected from hackers.

Example: Online banking websites, shopping websites, or email login pages.

Table 2.2: Comparison of Common Protocols

Protocol	Purpose	Port	Secure Version	Example Use
HTTP	Transfer web pages	80	HTTPS	Browsing websites
FTP	File transfer	21	SFTP	Upload/download files
DNS	Resolve domain names	53	N/A	Translating www.google.com to an IP
SMTP	Sending emails	25	SMTPS	Sending Gmail to Yahoo
POP3	Receiving emails	110	POP3S	Download emails to the device
IMAP	Receiving emails, sync across devices	143	IMAPS	Access Gmail on phone & PC
Telnet	Remote login	23	SSH	Managing a server remotely
HTTPS	Secure web browsing	443	N/A	Online banking, shopping

Did You Know?

- SMTP is used for sending emails, while POP3 and IMAP are used for receiving emails.
- Telnet allows remote access to a computer, but it is not secure, so SSH is preferred for safe communication.

Practical Activity 2.1: Comparing OSI and TCP/IP Models

Objective: To understand the similarities and differences between the OSI model and the TCP/IP model, and to map protocols and devices to their respective layers.

Materials Required:

- Computer with internet access
- Chart paper or notebook
- Pen/pencil
- (Optional) Cisco Packet Tracer or any network simulation software

Steps:

Step 1: Prepare a Table:

Draw a table with three columns:

- Column 1: OSI Layer
- Column 2: TCP/IP Layer
- Column 3: Examples of Protocols/Devices

Step 2: Identify Layers:

List all 7 OSI layers in Column 1 (Physical, Data Link, Network, Transport, Session, Presentation, Application).

Step 3: Map TCP/IP Layers:

Map the 4 TCP/IP layers to the OSI layers in Column 2:

- Network Interface → Physical + Data Link
- Internet → Network
- Transport → Transport
- Application → Session + Presentation + Application

Step 4: Add Examples:

In Column 3, write protocols or devices that belong to each layer:

- OSI Physical/Data Link → Ethernet cable, Wi-Fi, switch, hub
- OSI Network → IP, ICMP, router
- OSI Transport → TCP, UDP
- OSI Session/Presentation/Application → HTTP, FTP, SMTP, DNS

Step 5: Discussion:

- Compare the functions of OSI and TCP/IP layers.
- Discuss which layers are merged in TCP/IP and why.
- Note which protocols operate at each layer.

Step 6: Optional Simulation:

- Use Cisco Packet Tracer to simulate sending data between two computers.
- Observe how data flows through the different layers of the network.
- Identify which layer handles addressing, routing, and application communication.

Step 7: Observations to Note:

- OSI is a theoretical model, while TCP/IP is practical and widely used.
- TCP/IP merges several OSI layers for simplicity.

Different protocols operate at different layers in both models.

Practical Activity 2.2: Simulation of Data Packet Flow Across Layers

Objective: To understand how data travels through the different layers of OSI/TCP-IP models from sender to receiver, and to observe how each layer adds its own information to the data packet.

Materials Required:

- Computer with internet access
- Cisco Packet Tracer or any network simulation software
- Notebook and pen

Steps:

Step 1: Set Up the Network:

- Open Cisco Packet Tracer.
- Create a simple network with two computers (PC1 and PC2) connected via a switch or router.
- Ensure the devices are assigned IP addresses.
- Choose a Communication Protocol:
- For example, select HTTP for web browsing or FTP for file transfer.
- This will simulate data transfer from the Application Layer down to the Network Interface Layer.

Step 2: Send Data from PC1 to PC2:
On PC1, create a simple message like "Hello from PC1."
Use the simulation tool to send this message to PC2.

Step 3: Observe Encapsulation:
- Watch how the message is encapsulated at each layer:
- Application Layer: Adds application-specific header (e.g., HTTP header).
- Transport Layer: Adds TCP/UDP header with port numbers.
- Network/Internet Layer: Adds an IP header with source and destination addresses.
- Data Link Layer: Adds MAC addresses for local delivery.
- Physical Layer: Converts data into electrical or optical signals for transmission.

Step 4: Observe Data Flow Through Network Devices:
- Notice how the switch forwards frames using MAC addresses.
- If a router is used, observe how it forwards packets using IP addresses.

Step 5: Decapsulation at Receiver (PC2):
- Observe how PC2 removes the headers layer by layer to retrieve the original message.
- Confirm that PC2 receives "Hello from PC1" correctly.

Step 6: Document Observations:
- Note the role of each layer in sending, routing, and receiving data.
- Identify the protocols and headers added at each layer.

Compare this simulation to the theoretical OSI/TCP-IP model.

Practical Activity 2.3: Identification of Physical, Logical, and Port Addresses
Objective: To identify and understand the difference between physical (MAC) addresses, logical (IP) addresses, and port numbers in a networked environment.
Materials Required:
- Computers or laptops (at least two)
- Network connection (LAN, Wi-Fi, or virtual lab like Packet Tracer)
- Cisco Packet Tracer or Command Prompt/Terminal access

Steps:
Step 1: Identify Physical (MAC) Address:
- On a computer, open Command Prompt (Windows) or Terminal (Linux/Mac).
- Type the command:
  - Windows: ipconfig /all
  - Linux/Mac: ifconfig or ip addr show
- Locate the Physical Address / MAC Address of the network adapter.

- Note down the MAC address (example format: 00-1A-2B-3C-4D-5E).
- MAC addresses are unique hardware identifiers for each network interface card (NIC).

Step 2: Identify Logical (IP) Address:

- In the same command output, find the IPv4 or IPv6 address.
- Example: 192.168.1.5 (IPv4) or fe80::1a2b:3c4d:5e6f (IPv6).
- Logical addresses are assigned to devices to allow communication across networks.

Step 3: Identify Port Numbers:

- Open Command Prompt / Terminal.
- Use the command to display active network connections:
  - Windows: netstat -a
  - Linux/Mac: netstat -tuln
- Identify local port numbers and remote port numbers in use.
- Example: HTTP uses port 80, HTTPS uses port 443, FTP uses port 21.
- Port numbers help the Transport Layer identify the specific application/service on a device.

Step 4: Optional: Simulation in Packet Tracer

- Create a small network with two PCs and a switch.
- Assign IP addresses to both PCs.
- Use the simulation mode to send a ping from PC1 to PC2.
- Observe the source MAC, destination MAC, source IP, destination IP, and ports in the packet details.

Step 5: Record Observations:

- Note the MAC address, IP address, and port number for each device.
- Observe how physical addresses are used locally, IP addresses identify devices on networks, and ports identify services/applications.

Summary

- The OSI model has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- Each OSI layer has a specific role in sending, receiving, and managing data across a network.
- The TCP/IP model has 4 layers: Network Interface, Internet, Transport, and Application.
- TCP/IP combines some OSI layers for simplicity; for example, the Application Layer in TCP/IP includes OSI's Application, Presentation, and Session layers.
- TCP is connection-oriented, ensures reliable delivery, and is used in applications like web browsing and email.
- UDP is connectionless, faster, and used in real-time applications like video streaming, gaming, and VoIP.
- DNS (Domain Name System) converts human-readable domain names into IP addresses for communication over networks.
- SMTP is used for sending emails, while POP3 and IMAP are used for receiving emails.

- HTTP is used for web browsing; HTTPS encrypts data to provide secure communication.
- Telnet allows remote login to devices, while SSH is a secure alternative.
- Routers operate at the Internet layer and forward packets between networks using IP addresses.
- Network Interface Layer deals with physical and data link functions, enabling devices to connect via Ethernet, Wi-Fi, etc.

ASSESSMENT

A. Multiple Choice Questions

1. Which layer of the OSI model is responsible for reliable data delivery?
   a) Physical
   b) Transport
   c) Network
   d) Application

2. TCP is a _____ protocol.
   a) Connectionless
   b) Connection-oriented
   c) Broadcast
   d) None of the above

3. Which protocol translates domain names into IP addresses?
   a) FTP
   b) DNS
   c) HTTP
   d) SMTP
4. Which TCP/IP layer corresponds to the OSI's Session, Presentation, and Application layers?
   a) Internet Layer
   b) Transport Layer
   c) Application Layer
   d) Network Interface Layer

5. Which port is used by HTTP by default?
   a) 21
   b) 25
   c) 80
   d) 443

6. UDP is preferred for _____.
   a) Web browsing
   b) File transfer
   c) Video streaming
   d) Email delivery

7. The OSI model has how many layers?
   a) 4
   b) 5

c) 6
d) 7

8. Which protocol is used for sending emails?
   a) POP3
   b) SMTP
   c) IMAP
   d) FTP

9. The Physical Layer of OSI corresponds to which TCP/IP layer?
   a) Internet Layer
   b) Network Interface Layer
   c) Transport Layer
   d) Application Layer

10. SSH is a secure alternative to which protocol?
    a) FTP
    b) Telnet
    c) HTTP
    d) DNS

B. Fill-in-the-blanks

1. TCP/IP model has _____ layers.
2. UDP is a _____ protocol.
3. DNS translates _____ into IP addresses.
4. The _____ layer of OSI model provides reliable end-to-end delivery.
5. HTTP uses port number _____ by default.
6. IMAP keeps emails on the _____.
7. Ethernet is an example of a _____ layer protocol.
8. SSL/TLS is used to secure _____.
9. IP addresses are _____ addresses.
10. Routers operate at the _____ layer of TCP/IP model.

C. True/False questions

1. TCP is a connectionless protocol.
2. DNS is used to resolve domain names to IP addresses.
3. UDP ensures reliable delivery of data.
4. The application layer of TCP/IP combines OSI's Session, Presentation, and Application layers.
5. FTP is used for file transfer over the network.
6. SSH is a secure version of Telnet.
7. Physical addresses are also called IP addresses.

8. The TCP/IP model was developed before the OSI model.
9. SMTP is used to send emails.
10. Routers use MAC addresses to forward packets between networks.

D. Short Questions Answers

1. What is the main difference between TCP and UDP?
2. Name two protocols used for sending and receiving emails.
3. What is the role of DNS in a network?
4. How many layers are there in the OSI model?
5. Which TCP/IP layer handles logical addressing?
6. Give an example of a protocol working at the Application Layer.
7. What is the purpose of port numbers in a network?
8. What is the function of the Network Interface Layer?
9. Name one secure protocol used for web browsing.
10. Explain the concept of encapsulation in networking.

Answer Key

A. MCQ Answers

1. Transport, 2. Connection-oriented, 3. DNS, 4. Application Layer, 5. 80, 6. Video streaming, 7. 7, 8. SMTP, 9. Network Interface Layer, 10. Telnet

B. Fill in the Blanks

1. 4, 2. Connectionless, 3. Domain names, 4. Transport, 5. 80, 6. Server, 7. Network Interface, 8. HTTP/HTTPS, 9. Logical, 10. Internet

C. True/False

1. False, 2. True, 3. False, 4. True, 5. True, 6. True, 7. False, 8. True, 9. True, 10. False

Chapter-3

IP Addressing and Subnetting

In a busy city, computers were sending messages to each other, but many messages were getting lost. People didn't know where to send them because some computers didn't have proper addresses. A clever student, Arjun, suggested giving every computer a unique number called an IP address. This way, each message could find its correct destination. Later, as more computers joined, Arjun divided them into smaller groups called subnets to make sending messages faster and easier. The computers were happy—they could now communicate without confusion. Arjun smiled and said, "Just like houses need addresses for mail, computers need IP addresses to send and receive data safely!"

3.1. IP Addressing Overview

IP Addressing is a system of assigning unique identifiers to devices on a network so they can communicate with each other. IP stands for Internet Protocol, which is a set of rules that allows devices to send and receive data over a network.

Each device connected to a network (like computers, routers, or smartphones) must have a unique IP address to ensure proper delivery of data.

Structure of an IP Address

- An IP address is a logical address, not tied to hardware, unlike a MAC address.
- IPv4 addresses are 32-bit numbers divided into four octets (8 bits each).
- Written in dotted decimal notation: example: 192.168.1.1
- Each octet ranges from 0 to 255 because 8 bits can represent 256 values.

Binary Representation Example:

192.168.1.1 → 11000000.10101000.00000001.00000001

Components of an IP Address

1. Network ID

- Identifies the specific network a device belongs to.
- Used by routers to forward packets to the correct network.

2. Host ID

- Identifies a specific device within that network.
- Ensures each device has a unique identifier in its network.

3. Subnet Mask

- Helps separate the network ID and host ID in an IP address.
- Example: 255.255.255.0 → first 24 bits are network ID, last 8 bits are host ID.

3.2. Types of IP Addresses

1. IPv4 Addressing

IPv4 (Internet Protocol Version 4) is the most widely used IP addressing system in the world. It is a 32-bit logical address that uniquely identifies devices on a network. IPv4 addresses are written in dotted decimal notation, for example, 192.168.1.1, and are divided into four octets of 8 bits each. Each IP address consists of a Network ID, which identifies the network, and a Host ID, which identifies the specific device within that network. IPv4 addresses are categorized into classes A, B, C, D, and E, where Classes A, B, and C are used for unicast communication, Class D for multicast, and Class E is reserved for experimental use. IPv4 provides about 4.3 billion unique addresses and supports both private and public addressing. While it is simple, widely supported, and easy to configure, its address space is limited, and NAT (Network Address Translation) is often required to conserve addresses.

2. IPv6 Addressing

IPv6 (Internet Protocol Version 6) was developed to overcome the limitations of IPv4, mainly the shortage of addresses due to the rapid growth of devices connected to the Internet. IPv6 is a 128-bit logical address, written in hexadecimal notation separated by colons, for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 offers an enormous address space, around 3.4×10^{38} addresses, which is enough for global connectivity and the Internet of Things (IoT). It supports unicast, multicast, and anycast addressing, eliminates the need for NAT, and provides built-in security with IPsec. IPv6 also allows automatic address configuration using SLAAC or DHCPv6, making network management easier. However, full adoption requires IPv6-compatible hardware and software, and migration from IPv4 can be complex in existing networks.

Did You Knows?

- The total number of IPv4 addresses is around 4.3 billion, but most of them are already allocated.
- IPv6 can support 340 undecillion addresses, enough to give trillions of IPs to every person on Earth.

3.3 IP Address Classes (IPv4) Addresses

- Class A: Large networks, first bit 0, range 0–127.
- Class B: Medium networks, first two bits 10, range 128–191.
- Class C: Small networks, first three bits 110, range 192–223.
- Class D: Multicast, first four bits 1110, range 224–239.
- Class E: Reserved for experimental use, first four bits 1111, range 240–255.

Class	Range	Default Subnet Mask	Usage
A	1.0.0.0 – 126.0.0.0	255.0.0.0	Large networks
B	128.0.0.0 – 191.255.0.0	255.255.0.0	Medium-sized networks
C	192.0.0.0 – 223.255.255.0	255.255.255.0	Small networks
D	224.0.0.0 – 239.255.255.255	N/A	Multicasting
E	240.0.0.0 – 255.255.255.255	N/A	Experimental/Research

Table 2.3: IP Address Classes

Note: 127.0.0.0 is reserved for loopback testing (e.g., 127.0.0.1)

3.4. Special Types of IPv4 Addresses

1. Private IP Addresses

- Used within local networks, not routable on the Internet.
- Examples:
  - Class A: 10.0.0.0 – 10.255.255.255
  - Class B: 172.16.0.0 – 172.31.255.255
  - Class C: 192.168.0.0 – 192.168.255.255

2. Public IP Addresses

- Assigned by ISPs and can be accessed over the Internet.

3. Loopback Address

- 127.0.0.1, used to test the network interface of a device.

4. Broadcast Address

- The address used to send data to all hosts in a network.
- Last host in a network, e.g., 192.168.1.255 for network 192.168.1.0/24.

Key Terms Related to IP Addressing

- Subnet Mask: Determines the boundary between network ID and host ID.
- Default Gateway: Router IP that connects local networks to external networks.
- CIDR (Classless Inter-Domain Routing): A Method to allocate IP addresses efficiently using prefixes like /24.

Importance of IP Addressing

- Ensures unique identification of devices.
- Enables data routing across networks.
- Helps organize networks into manageable subnets.
- Supports both private and public communication.

3.5. Private vs Public IPs

Private IP addresses are used within a local network, such as in homes, offices, or schools, to allow devices to communicate internally. These addresses are not routable on the Internet, meaning they cannot be accessed directly from outside the local network. Private IPs help conserve public IP addresses and enhance security by keeping internal devices hidden from external networks. Examples of private IP ranges include 10.0.0.0 – 10.255.255.255 for Class A, 172.16.0.0 – 172.31.255.255 for Class B, and 192.168.0.0 – 192.168.255.255 for Class C. Devices using private IP addresses often connect to the Internet via a router or firewall that uses Network Address Translation (NAT) to map private addresses to a public IP.

Public IP addresses, on the other hand, are assigned by Internet Service Providers (ISPs) and are used for devices that need to communicate over the Internet. Each public IP address is globally unique, allowing a device to be identified anywhere in the world. Public IPs are essential for hosting websites, servers, or online services that must be accessible by users globally. An example of a public IP address could be 203.0.113.5. While public IPs enable worldwide connectivity, they expose devices to potential Internet threats, so security measures like firewalls and encryption are important when using them.

Did You Know?

- A device can have both a private and a public IP address at the same time.

Assignment 3.1.

1. List the five classes of IPv4 addresses.
2. What is the difference between a public IP and a private IP?

3.3. Subnet Mask and CIDR Notation

Subnet Mask: A subnet mask is a 32-bit number used in IPv4 addressing to divide an IP address into network and host portions. It tells devices which part of the IP address identifies the network and which part identifies individual devices (hosts) within that network. Subnet masks are typically written in dotted decimal notation, just like IP addresses. For example, 255.255.255.0 is a common subnet mask for a Class C network, where the first 24 bits (255.255.255) represent the network portion, and the last 8 bits (0) represent the host portion. By applying a subnet mask, routers and devices can efficiently determine whether a device is on the same network or if the data should be sent through a gateway to another network.

CIDR notation: CIDR (Classless Inter-Domain Routing) notation is a more flexible way of representing IP addresses and their associated subnet masks. Instead of using the traditional class-based system (A, B, C), CIDR specifies the number of bits used for the network portion

directly after a slash /. For example, 192.168.1.0/24 indicates that the first 24 bits of the IP address are the network part, and the remaining 8 bits are for host addresses. CIDR allows networks to be divided into subnets of any size, rather than being restricted to fixed class sizes, making IP address allocation much more efficient. It also helps reduce wastage of IP addresses and simplifies routing tables on the Internet.

3.4. Basics of Subnetting

Subnetting is the process of dividing a large network into smaller, more manageable networks called subnets. This allows network administrators to organize devices efficiently, improve performance, and increase security. Instead of using a single large network where all devices share the same network ID, subnetting creates multiple networks, each with its own network ID and range of host addresses.

The main purpose of subnetting is to reduce network congestion and make better use of IP addresses. Without subnetting, a large network might waste IP addresses or experience slow data transmission due to too many devices sharing the same network. By creating smaller subnets, devices in each subnet can communicate efficiently, and routers can manage traffic more effectively.

Working of Subnetting:

- A subnet mask is used to separate the network portion and the host portion of an IP address.
- By borrowing bits from the host portion, a network can be divided into multiple subnets.
- Each subnet has a unique network ID, a range of host addresses, and a broadcast address for sending data to all hosts in that subnet.
- Example:
  - Original Network: 192.168.1.0/24 → 256 addresses (0–255)
- If we divide this into 4 subnets:
  - Subnet 1: 192.168.1.0/26 → Hosts 1–62
  - Subnet 2: 192.168.1.64/26 → Hosts 65–126
  - Subnet 3: 192.168.1.128/26 → Hosts 129–190
  - Subnet 4: 192.168.1.192/26 → Hosts 193–254

Key Terms in Subnetting:

- Network ID: Identifies the subnet.
- Host ID: Identifies a device within the subnet.
- Broadcast Address: Used to send data to all devices in the subnet.
- Subnet Mask: Determines the division between network and host parts.
- CIDR Notation: Shows how many bits are used for the network portion, e.g., /26.

Advantages of Subnetting:

- Efficient use of IP addresses.
- Reduces network congestion.
- Improves security by isolating subnets.
- Simplifies network management and troubleshooting.

Disadvantages:

- Requires planning and careful calculation.
- Complex for very large networks if done manually.

3.5. Subnetting for Class Networks

3.5.1. Subnetting for Class A Networks

A Class A IP address has a default subnet mask of 255.0.0.0 or /8, meaning the first 8 bits are used for the network ID, and the remaining 24 bits are for host IDs. Class A networks are designed for very large networks, capable of supporting over 16 million hosts per network. Subnetting allows these large networks to be divided into smaller, more manageable subnets by borrowing bits from the host portion.

For example, if we take a Class A network 10.0.0.0/8 and want to create 16 subnets, we need to borrow 4 bits from the host portion (because $2^4 = 16$). This changes the subnet mask to 255.240.0.0 or /12. After subnetting, each subnet will have 1,048,574 usable host addresses ($2^{20} - 2$, since 20 bits remain for host IDs). The network IDs for the first few subnets would be:

- Subnet 1: 10.0.0.0/12
- Subnet 2: 10.16.0.0/12
- Subnet 3: 10.32.0.0/12
- Subnet 4: 10.48.0.0/12

Subnetting Class A networks is essential for very large organizations, such as multinational companies or large service providers, because it allows better management, traffic control, and efficient use of IP addresses across multiple departments or locations.

3.5.2. Subnetting for Class B Networks

A Class B IP address has a default subnet mask of 255.255.0.0 or /16, meaning the first 16 bits are for the network ID, and the remaining 16 bits are for host IDs. Subnetting allows you to divide this large network into smaller subnets by borrowing bits from the host portion.

For example, if we want to create 4 subnets from a Class B network 172.16.0.0/16, we need 2 bits (since $2^2 = 4$) from the host portion for subnetting. This changes the subnet mask to 255.255.192.0 or /18. Each subnet will now have 16,382 usable host addresses ($2^{14} - 2$, because 14 bits remain for hosts). The network IDs for the 4 subnets would be:

- Subnet 1: 172.16.0.0/18
- Subnet 2: 172.16.64.0/18
- Subnet 3: 172.16.128.0/18
- Subnet 4: 172.16.192.0/18

By subnetting Class B networks, organizations can efficiently use IP addresses and segment their network to reduce congestion and improve security.

3.5.3. Subnetting for Class C Networks

A Class C IP address has a default subnet mask of 255.255.255.0 or /24, meaning the first 24 bits are for the network ID, and the remaining 8 bits are for host IDs. Class C networks are smaller, typically supporting up to 254 hosts per network. Subnetting divides the host portion into subnets.

For example, if we want to create 4 subnets from a Class C network 192.168.1.0/24, we need 2 bits (since $2^2 = 4$) from the host portion. This changes the subnet mask to 255.255.255.192 or /26. Each subnet will now have 62 usable host addresses ($2^6 - 2$). The subnets would be:

- Subnet 1: 192.168.1.0/26 → Hosts 1–62
- Subnet 2: 192.168.1.64/26 → Hosts 65–126
- Subnet 3: 192.168.1.128/26 → Hosts 129–190
- Subnet 4: 192.168.1.192/26 → Hosts 193–254

Subnetting Class C networks is useful for small offices or departments, allowing network administrators to organize devices logically and control traffic within each subnet.

Did You Know?

- Subnetting borrows bits from the host portion to create more subnets.
- Class B networks have more host addresses and are suitable for medium to large networks, while Class C networks are suitable for small networks.
- Subnetting helps efficiently use IP addresses, reduce congestion, and improve network security.

3.6. Introduction to IPv6 (Internet Protocol Version 6)

IPv6 is the latest version of the Internet Protocol, developed to replace IPv4 due to its limited address space. While IPv4 uses 32-bit addresses and can provide about 4.3 billion unique addresses, IPv6 uses 128-bit addresses, which allows for an almost unlimited number of devices to be connected to the Internet. This makes IPv6 essential for the growth of the Internet, particularly with the rise of smartphones, IoT (Internet of Things) devices, and large-scale networks.

IPv6 addresses are written in hexadecimal notation and separated by colons. An example of an IPv6 address is:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

To simplify, leading zeros in each block can be removed, and consecutive blocks of zeros can be compressed using::.

For example: 2001:db8:85a3::8a2e:370:7334

Features of IPv6

1. Large Address Space: Provides 2^{328} addresses, enough for every device in the world to have a unique IP address.

2. Simplified Header: IPv6 has a simpler packet header than IPv4, which improves routing efficiency.

3. No NAT Needed: Unlike IPv4, IPv6 eliminates the need for Network Address Translation (NAT) because there are enough addresses for all devices to have public IPs.

4. Built-in Security: IPv6 was designed with IPsec (Internet Protocol Security) support, ensuring data integrity and encryption.

5. Support for Auto-Configuration: Devices can automatically generate their IPv6 address using SLAAC (Stateless Address Auto-Configuration), simplifying network management.

6. Better Support for Mobile and IoT Devices: IPv6 is optimized for modern networks, including smartphones, smart devices, and sensors.

Types of IPv6 Addresses

1. **Unicast –** Identifies a single device.
2. **Multicast –** Identifies a group of devices; data is sent to all members of the group.
3. **Anycast –** Identifies multiple devices, but data is delivered to the nearest device.

Advantages of IPv6

- Vast address space to support future Internet growth.
- Simplified routing and improved network efficiency.
- Enhanced security with built-in IPsec.
- No need for NAT, enabling end-to-end connectivity.
- Better support for mobile networks and IoT devices.

Disadvantages of IPv6

- Requires IPv6-compatible hardware and software.
- Full transition from IPv4 is complex and gradual.
- Some older applications and devices may not support IPv6 yet.

Did You Know?

- In IPv4, addresses are written in decimal format, while in IPv6, they are written in hexadecimal.
- The concept of CIDR (Classless Inter-Domain Routing) replaced traditional classes to improve flexibility.
- IP addresses are like the “digital home address” of every device on the internet.

Assignment 3.2

1. Write a short note on IPv6 features.
2. Write the private IP ranges for Class A, B, and C.

3.7. Static and Dynamic IP

Static IP Address

A static IP address is an IP address that is manually assigned to a device and does not change over time. Once configured, the device always uses the same IP address to communicate on the network. Static IPs are commonly used for servers, printers, or network devices that need a constant address for reliable access. For example, a web server hosting a website needs a static IP so users can always reach the site at the same address.

Advantages of Static IP:

- Ensures consistent network identification for devices.
- Useful for hosting websites, servers, and remote access.
- Easier to manage in small networks where IPs rarely change.

Disadvantages of Static IP:

- Requires manual configuration, which can be time-consuming.
- Prone to errors if multiple devices are assigned the same IP address.
- Not flexible for large networks where devices frequently join and leave.

Dynamic IP Address

A dynamic IP address is an IP address that is automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server whenever a device connects to the network. Dynamic IPs can change over time or when the device reconnects. Most home networks, offices, and Internet users use dynamic IPs because they are easier to manage and reduce the need for manual configuration.

Advantages of Dynamic IP:

- Easy to manage, especially in large networks.
- Reduces configuration errors and IP conflicts.
- Efficient use of limited IP addresses by reassigning them as needed.

Disadvantages of Dynamic IP:

- The device's IP address may change, which can be inconvenient for hosting services or remote access.
- Less control over IP addressing for network administrators.

Practical Activity 3.1: IP Address Classification Exercise

Objective: To identify the class, type (public/private), and network/host portions of given IP addresses.

Materials Required:

- Computers or laptops with network simulation software (optional)
- Paper and pen for calculations

Activity Steps:

Step 1: List IP Addresses

- Prepare a set of IPv4 addresses for students to classify. Example list:
  - 10.25.36.5
  - 172.16.45.10
  - 192.168.1.1
  - 8.8.8.8
  - 224.0.0.5

Step 2: Identify the Class of Each IP Address

- Determine the first octet of the IP address.
- Use the range to identify the class:
  - Class A: 1–126

- Class B: 128–191
- Class C: 192–223
- Class D: 224–239 (Multicast)
- Class E: 240–255 (Experimental)

Step 3: Determine Public or Private IP

- Check if the IP falls within private IP ranges:
- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255
- If it falls outside these ranges, it is a public IP.

Step 4: Identify Network and Host Portions

- Use the default subnet mask for the class:
- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0
- Split the IP address into network ID and host ID.

Step 5: Record Observations

Create a table like this for each IP address:

IP Address	Class	Public/Private	Network ID	Host ID
10.25.36.5	A	Private	10.0.0.0	25.36.5
172.16.45.10	B	Private	172.16.0.0	45.10
192.168.1.1	C	Private	192.168.1.0	1
8.8.8.8	A	Public	8.0.0.0	8.8.8
224.0.0.5	D	Public	N/A	N/A

Practical Activity 3.2: Subnetting Practice with Class B and Class C Networks

Objective: To practice subnetting Class B and Class C networks, calculate the number of subnets, hosts per subnet, and determine network and broadcast addresses.

Materials Required:

- Computer or notebook
- Pen and paper for calculations
- Optional: Network simulation software (Cisco Packet Tracer)

Activity Steps:

Step 1: List the IP Addresses for Practice

- Class B Example: 172.16.0.0/16
- Class C Example: 192.168.1.0/24

Step 2: Decide the Number of Subnets Needed

- Example for Class B: Create 8 subnets
- Example for Class C: Create 4 subnets

Step 3: Calculate the Number of Borrowed Bits

- Formula: 2^n ≥ Number of required subnets
- For Class B (8 subnets): 2^3 = 8 → Borrow 3 bits from host portion
- For Class C (4 subnets): 2^2 = 4 → Borrow 2 bits from host portion

Step 4: Determine the New Subnet Mask

- Class B: Default mask /16 → Borrow 3 bits → New mask /19 → 255.255.224.0

- Class C: Default mask /24 → Borrow 2 bits → New mask /26 → 255.255.255.192

Step 5: Calculate the Number of Hosts per Subnet
- Formula: 2^h − 2 (h = number of host bits remaining)
- Class B: 16 host bits − 3 borrowed = 13 host bits → 2^13 − 2 = 8190 hosts
- Class C: 8 host bits − 2 borrowed = 6 host bits → 2^6 − 2 = 62 hosts

Step 6: Determine Network and Broadcast Addresses for Each Subnet
Class B Example: 172.16.0.0/19

Subnet	Network ID	Broadcast Address	Host Range
1	172.16.0.0	172.16.31.255	172.16.0.1 – 172.16.31.254
2	172.16.32.0	172.16.63.255	172.16.32.1 – 172.16.63.254
3	172.16.64.0	172.16.95.255	172.16.64.1 – 172.16.95.254
4	172.16.96.0	172.16.127.255	172.16.96.1 – 172.16.127.254

Class C Example: 192.168.1.0/26

Subnet	Network ID	Broadcast Address	Host Range
1	192.168.1.0	192.168.1.63	192.168.1.1 – 192.168.1.62
2	192.168.1.64	192.168.1.127	192.168.1.65 – 192.168.1.126
3	192.168.1.128	192.168.1.191	192.168.1.129 – 192.168.1.190
4	192.168.1.192	192.168.1.255	192.168.1.193 – 192.168.1.254

Practical Activity 3.3: Exploring WHOIS.net and WhatIsMyIP Portals

Objective: To understand IP address information, domain registration details, and the tools available to check public IP addresses.
Materials Required:
- Computer or laptop with internet access
- Web browser (Chrome, Firefox, etc.)

Activity Steps:
Part A: Using WHOIS.net
Step 1: Open your web browser and visit https://www.whois.net
Step 2: In the search bar, enter a domain name (e.g., google.com, wikipedia.org) and click Search.
Step 3: Observe the information provided by WHOIS:
- Domain Name: The registered name of the website.
- Registrar: The organization that manages the domain registration.
- Registration Dates: Creation date, expiry date, and last updated date.
- Contact Information: Owner/administrative contact details (may be hidden due to privacy policies).
- Name Servers: The servers responsible for DNS resolution of the domain.

Step 4: Record the details in a table for analysis:

Domain Name	Registrar	Creation Date	Expiry Date	Name Servers
google.com	MarkMonitor	1997-09-15	2028-09-14	ns1.google.com, ns2.google.com
wikipedia.org	Public Interest Registry	2001-01-13	2025-01-13	ns0.wikimedia.org, ns1.wikimedia.org

Step 5: Discuss how WHOIS information is useful for network administrators, cybersecurity, and domain management.

Part B: Using WhatIsMyIP Portal

Step 1: Open your web browser and visit https://www.whatismyip.com or https://www.whatismyipaddress.com

Step 2: Observe the information displayed automatically:

- Public IP Address of your device.
- IP Location: Country, region, city (approximate).
- ISP (Internet Service Provider).
- IP Type: IPv4 or IPv6.

Step 3: Record the information for your device:

IP Address	IP Type	Location	ISP
203.0.113.25	IPv4	Mumbai, India	Jio Digital

Step 4: Discuss the significance of public IP addresses and how they are different from private IP addresses.

Summary

- An IP address is a unique identifier assigned to each device on a network to enable communication.
- IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses for a larger address space.
- IPv4 addresses are written in dotted decimal format (e.g., 192.168.1.1).
- IPv6 addresses are written in hexadecimal separated by colons (e.g., 2001:0db8::1).
- IP addresses can be public (accessible on the Internet) or private (used within local networks).
- Static IP is manually assigned and does not change; Dynamic IP is automatically assigned by a DHCP server.
- Subnetting divides a large network into smaller subnets to improve efficiency and security.
- A subnet mask separates the network and host portions of an IP address.
- CIDR (Classless Inter-Domain Routing) notation represents the number of bits used for the network portion (e.g., /24).
- Subnetting for Class A, B, and C involves borrowing bits from the host portion to create subnets.
- Key subnetting concepts include network ID, host ID, and broadcast address.
- WHOIS.net can be used to find domain registration details.
- The WhatIsMyIP portal helps identify the public IP address, ISP, and approximate location of a device.
- Subnetting and IP address classification help in efficient network management, security, and planning.

ASSESSMENT

A. Multiple Choice Questions

1. An IPv4 address is of how many bits?

a) 16
b) 32
c) 64
d) 128

2. Which class of IP address has the range 192–223 in the first octet?
a) Class A
b) Class B
c) Class C
d) Class D

3. The default subnet mask of Class B is:
a) 255.0.0.0
b) 255.255.0.0
c) 255.255.255.0
d) 255.255.255.255

4. IPv6 addresses are written in:
a) Binary form
b) Decimal form
c) Hexadecimal form
d) Octal form

5. A private Class C IP address range is:
a) 10.0.0.0 – 10.255.255.255
b) 172.16.0.0 – 172.31.255.255
c) 192.168.0.0 – 192.168.255.255
d) 224.0.0.0 – 239.255.255.255

6. Which protocol is used for assigning dynamic IP addresses?
a) DNS
b) DHCP
c) FTP
d) SMTP

7. The notation /24 in CIDR represents which subnet mask?
a) 255.0.0.0
b) 255.255.0.0
c) 255.255.255.0
d) 255.255.255.255

8. The address used to send data to all devices in a network is called:
a) Network address
b) Host address
c) Broadcast address
d) Gateway address

9. IPv6 provides how many bits of address space?
a) 32
b) 64
c) 128
d) 256

10. A static IP address is:
a) Assigned automatically
b) Changes frequently
c) Fixed and manually configured

d) Temporary

B. Fill-in-the-blanks

1. IPv4 uses a _____-bit address format.
2. IPv6 addresses are written in _____ notation.
3. The default subnet mask of Class C is _____.
4. _____ IP addresses are used within local networks only.
5. DHCP stands for _____.
6. A _____ IP address does not change and is manually assigned.
7. In CIDR notation, /16 means _____ bits are used for the network part.
8. The range of Class A IP addresses is _____ to _____.
9. The process of dividing a network into smaller parts is called _____.
10. A device's public IP address can be checked using _____ portal.

C. True/False questions

1. IPv4 addresses are 64-bit long.
2. IPv6 provides a larger address space than IPv4.
3. Public IP addresses are accessible on the Internet.
4. The default mask of Class B is 255.255.0.0.
5. CIDR is used for efficient IP address allocation.
6. Private IP addresses can be accessed directly from the Internet.
7. DHCP automatically assigns IP addresses to devices.
8. A subnet mask separates the network portion from the host portion of an IP address.
9. The broadcast address is used to communicate with a single host.
10. WHOIS.net provides information about domain registration.

D. Short Questions

1. Define an IP address.
2. Differentiate between IPv4 and IPv6.
3. Write two advantages of using subnetting.
4. What is the diifference between public and private IP addresses?
5. Explain the purpose of a subnet mask.
6. What does /24 represent in CIDR notation?
7. State the IP address range of Class B.
8. What is a static IP address?

9. Why is IPv6 needed when we already have IPv4?
10. What is the role of DHCP in networking?

Answer Key

A. Multiple Choice Questions

1. b), 2. c), 3. b), 4. c), 5. c), 6. b), 7. c), 8. c), 9. c), 10. c)

B. Fill-in-the-blanks

1. 32, 2. Hexadecimal, 3. 255.255.255.0, 4. Private, 5. Dynamic Host Configuration Protocol, 6. Static, 7. 16, 8. 1 – 126, 9. Subnetting, 10. WhatIsMyIP

C. True/False questions

1. False, 2. True, 3. True, 4. True, 5. True, 6. False, 7. True, 8. True, 9. False, 10. True

Chapter-4

TCP/IP Utilities and Troubleshooting

In a small school, the students noticed that the internet was not working properly. Pages were loading slowly, and some computers couldn't connect at all. Mr. Rao, the computer teacher, became the "network detective." He used the ping command to check if computers were reachable and ipconfig to see the IP addresses. He traced the route of data using tracert and checked active connections with netstat. To solve a website issue, he used nslookup to find the server's address. After following these steps, Mr. Rao discovered an IP conflict and corrected it. The network was back to normal. Riya, a student, said, "Wow! It's like solving a mystery using special tools!" From that day, everyone learned how important TCP/IP utilities are for finding and fixing network problems.

4.1. TCP/IP Protocol Stack Overview

The TCP/IP protocol stack is a set of communication layers that define how data is transmitted over the Internet and other networks. It is the foundation of modern networking and is based on the idea of breaking down communication into smaller, manageable layers. Each layer has its own function and works together with other layers to ensure reliable data transfer.

The stack is made up of four layers:

1. Application Layer

This is the top layer where users interact with the network. It provides services and applications that allow communication between devices. Examples include HTTP (web browsing), SMTP (email), FTP (file transfer), and DNS (domain name resolution).

Function: Provides network services directly to users and applications.

Example: When you open a website, your browser uses the application layer protocols to request and display the content.

2. Transport Layer

This layer is responsible for ensuring that data is delivered accurately and reliably from one computer to another. It uses two main protocols:

- TCP (Transmission Control Protocol): Provides reliable, connection-oriented communication with error checking.
- UDP (User Datagram Protocol): Provides faster, connectionless communication without error correction.

Function: Breaks large data into smaller segments, ensures correct delivery, and reassembles the data at the destination.

3. Internet Layer

This layer is responsible for logical addressing and routing. It decides the best path for the data to travel across different networks.

Main protocol: IP (Internet Protocol).

It also uses supporting protocols like ICMP (Internet Control Message Protocol) for error reporting.

Function: Assigns IP addresses, routes data packets, and ensures they reach the correct destination network.

4. Network Interface (or Link) Layer

This is the lowest layer of the stack. It deals with the physical connection between devices, such as cables, switches, Wi-Fi, or Ethernet.

Function: Defines how data is actually transmitted over the hardware.

It uses MAC (Media Access Control) addresses for device-to-device communication in a local network.

4.2. Port Numbers, Protocol Ports (HTTP-80, FTP-21, etc.)

4.2.1. Port Numbers

In networking, a port number is a numerical identifier that helps direct data to the correct application or process on a computer. While an IP address identifies the device on a network, the port number identifies the specific service or application running on that device. Together, they form a socket (IP address + Port number) that uniquely identifies a communication endpoint.

Need for Port Numbers

- Imagine a computer like a large office building:
- The IP address is the building's street address.
- The port number is the specific room number where the message should be delivered.
- Without port numbers, the computer would not know which program should handle the incoming data.

Ranges of Port Numbers

The Internet Assigned Numbers Authority (IANA) has divided port numbers into three ranges:

1. Well-Known Ports (0–1023):

- Reserved for standard services and applications.
- Examples:
  - HTTP: Port 80
  - HTTPS: Port 443
  - FTP: Port 21
  - SMTP: Port 25
  - DNS: Port 53

2. Registered Ports (1024–49151):

- Assigned to user applications and software processes.
- Examples:
  - Microsoft SQL Server: 1433
  - MySQL: 3306

3. Dynamic or Private Ports (49152–65535):

- Used temporarily by applications for communication.
- Assigned dynamically by the operating system when needed.

Common Examples of Port Numbers

- Web Browsing: HTTP (80), HTTPS (443)
- Email: SMTP (25), IMAP (143), POP3 (110)
- File Transfer: FTP (21), SFTP (22)
- Remote Access: Telnet (23), SSH (22)
- Domain Name Resolution: DNS (53)

Working of Port Numbers

1. When you open a website, your browser (client) sends a request to the server's IP address on port 80 (for HTTP) or 443 (for HTTPS).
2. The server listens on that port, processes the request, and sends back the response.
3. On your computer, the browser uses a temporary dynamic port number to receive the reply.

Advantages of Port Numbers

- Allow multiple applications to run and communicate on the same device simultaneously.

- Provide a standardized way to identify services.
- Enable efficient routing of data to the correct process.

Disadvantages of Port Numbers

- Some well-known ports are common targets for hackers (e.g., port 23 for Telnet, port 21 for FTP).
- Misconfigured or open ports can create security vulnerabilities.
- Overuse of dynamic ports can sometimes lead to conflicts.

4.2.2. Protocol Ports

In computer networking, protocol ports are special numerical identifiers used to connect applications and services on different devices. While the IP address identifies which device the data is going to, the port number identifies which service or application on that device should handle the data.

For example:

- When you browse a website, your computer connects to the server's IP address on port 80 (for HTTP).
- If the website uses encryption, it connects on port 443 (for HTTPS).

Thus, protocol ports are like "doors" through which specific services communicate.

Common Protocols and Their Ports

1. HTTP (Port 80)

- Stands for HyperText Transfer Protocol.
- Used for transferring web pages over the Internet.
- Example: Opening a website like http://example.com.

2. HTTPS (Port 443)

- Secure version of HTTP with encryption (SSL/TLS).
- Ensures safe browsing, banking, and online shopping.
- Example: https://example.com.

3. FTP (Port 21)

- Stands for File Transfer Protocol.
- Used to upload and download files between the client and the server.
- Example: Transferring website files to a hosting server.

4. SSH (Port 22)

- Stands for Secure Shell protocol.
- Provides secure remote login and command execution.
- Example: A system administrator managing a server remotely.

5. Telnet (Port 23)

- Used for remote login, but not secure (data sent in plain text).
- Mostly replaced by SSH today.

Assignment 4.1.

1. What is the TCP/IP protocol stack?
2. Explain the importance of port numbers in networking.
3. Write the port number for HTTP, FTP, and SMTP.

4.3. Troubleshooting Tools

When network issues occur, certain tools help us diagnose and fix problems. These tools are available in operating systems like Windows, Linux, and macOS, and they allow users to test connectivity, check configurations, and analyze network performance.

1. PING (Packet Internet Groper)

- **Purpose:** Tests whether a device (computer, server, or website) is reachable on the network.
- **Working:** It sends small packets called ICMP Echo Requests to a target device, and the target replies with ICMP Echo Replies.
- **Usage Example:** ping www.google.com
- **Output Information:**
  - Whether the host is reachable.
  - Time taken (latency) in milliseconds.
  - Packet loss percentage.
- **Use Case:**
  - Checking if the internet is working.
  - Verifying if a server or another computer is active.

2. IPCONFIG (Internet Protocol Configuration)

- **Purpose:** Displays and manages the network settings of a computer.
- **Working:** It shows IP address, subnet mask, default gateway, and DNS server information.
- **Usage Example:**

  ipconfig

  ipconfig /all

  ipconfig /release

  ipconfig /renew

Output Information:

- IPv4 / IPv6 address.
- MAC address (physical address).
- Gateway and DNS details.

Use Case:

- Finding your computer's IP address.
- Renewing IP when there is a connection issue.

3. TRACERT (Trace Route)

- **Purpose:** Shows the route taken by data packets from your computer to a destination.
- **Working:** It lists all intermediate devices (routers) that the data passes through before reaching the target.
- **Usage Example:** tracert www.google.com

Output Information:

- Hop-by-hop details of the journey.
- IP address of each router.
- Time taken to reach each hop.

Use Case:

- Finding where a network delay occurs.
- Identifying if a server is down or unreachable.

4. NETSTAT (Network Statistics)

- **Purpose:** Displays active network connections, ports, and protocol statistics.
- **Working:** It shows which applications are using the network and on which ports.
- **Usage Example:**

  netstat

  netstat -an

Output Information:

- Active TCP/UDP connections.
- Local and foreign IP addresses.
- Port numbers are being used.

Use Case:

- Checking if a port is open.
- Detecting unauthorized or suspicious connections.

5. NSLOOKUP (Name Server Lookup)

- **Purpose:** Tests and troubleshoots DNS (Domain Name System) resolution.
- **Working:** Converts a domain name into its corresponding IP address.
- **Usage Example:** nslookup www.google.com

Output Information:

- IP address of the domain.
- DNS server being used.

Use Case:

- Verifying if DNS is resolving correctly.
- Troubleshooting when websites don't open.

Assignment 4.2.

1. What is the purpose of the ping command?
2. Explain the use of the nslookup tool.

Practical Activity 4.1: Network Diagnostics Using Command-Line Tools

Objective: To learn how to use basic command-line tools (PING, IPCONFIG, TRACERT, NETSTAT, and NSLOOKUP) for diagnosing network connectivity and configuration issues.

Materials Required:

- A computer or laptop with an Internet connection.
- Windows/Linux operating system (Command Prompt or Terminal).

Steps:

Step 1: Check IP Configuration

- Open Command Prompt.
- Type the command:
  - ipconfig
- Note down the IP Address, Subnet Mask, and Default Gateway.
- Observe the output to verify if the system has a valid IP address.

Step 2: Test Connectivity with PING

- In the Command Prompt, type: ping 127.0.0.1 (This checks if the computer's network card is working.)
- Then type: ping www.google.com (This checks internet connectivity.)
- Observe the response time and packet loss.

Step 3: Trace the Route of Data Packets (TRACERT)

- Type the command: tracert www.google.com
- Observe how many "hops" the data takes to reach Google's server.
- Identify the routers or gateways the data passes through.

Step 4: View Active Connections (NETSTAT)

- Type the command: netstat
- Observe all active TCP/UDP connections.
- Identify which applications are using network ports.

Step 5: Check DNS Resolution (NSLOOKUP)

- Type the command: nslookup www.yahoo.com
- Observe the IP address returned by the DNS server.

Verify which DNS server is being used.

Practical Activity 4.2: Simulating and Resolving IP Conflicts

Objective: To understand what an IP conflict is, simulate it in a controlled environment, and learn how to resolve it.

Materials Required:

- Two computers or virtual machines (VMs) on the same network.
- Router or switch (for network connection).
- Windows or Linux operating system.
- Access to network settings.

Steps:

Step 1: Assign the Same IP Address

- On Computer 1, go to Network Settings → IPv4 properties.
- Set a static IP address, e.g., 192.168.1.100.
- On Computer 2, assign the same IP address: 192.168.1.100.

Step 2: Observe the IP Conflict

- Both computers are now using the same IP address.
- Check for warnings:
  - Windows will show a message: "Another device on the network has the same IP address."
  - Linux may show a network warning in system logs.
- Try pinging the IP from either computer and notice packet loss or errors.

Step 3: Diagnose the Conflict

- Open Command Prompt/Terminal.
- Use the ipconfig (Windows) or ifconfig (Linux) command to verify the IP addresses.
- Use ping 192.168.1.100 from another device to see conflicting responses.

Step 4: Resolve the IP Conflict

Option 1 – Change IP Address Manually

- On Computer 2, go to network settings and assign a different IP address, e.g., 192.168.1.101.
- Verify with ipconfig / ifconfig that the new IP is active.

Option 2 – Use DHCP for Automatic IP Assignment

- Set both computers to obtain IP automatically from the DHCP server/router.
- Verify that the router assigns unique IP addresses.

Step 5: Verify Network Connectivity

- Ping between the two computers using their new IP addresses.

Confirm that there are no IP conflicts and that both devices communicate successfully.

Practical Activity 4.3: Port Scanning Demo with Nmap

Objective: To understand how port scanning works and learn to identify open ports and services on a device using the Nmap tool.

Materials Required:

- A computer or laptop with Nmap installed (available for Windows, Linux, macOS).
- A target device on the same network (e.g., another computer or VM).
- Internet access (optional if scanning external IPs).

Safety Note:

- Only scan devices you own or have permission to scan.
- Unauthorized scanning of external networks is illegal and can cause security issues.

Steps:

Step 1: Install Nmap

- Download and install Nmap from https://nmap.org
- Verify installation by opening Command Prompt/Terminal and typing: nmap --version

Step 2: Identify the Target IP

- On the target device, find its IP address:
  - Windows: ipconfig
  - Linux: ifconfig or ip addr
  - Note the IP, e.g., 192.168.1.101.

Step 3: Basic Port Scan

- Open Command Prompt/Terminal on your scanning computer.
- Type the command: nmap 192.168.1.101
- **Observe the output:**
  - List of open ports.
  - Services running on those ports (e.g., SSH, HTTP, FTP).

Step 4: Scan Specific Ports

- To scan a specific range of ports, type: nmap -p 20-100 192.168.1.101
- Observe which ports are open in that range.

Step 5: Service and OS Detection

- To detect the services and operating system of the target, type: nmap -sV -O 192.168.1.101
- Observe the service version and OS information reported.

Step 6: Analyze Results

- Identify open ports and running services.
- Discuss which services are safe to keep open and which may pose a security risk.

Summary

- TCP/IP protocol stack consists of Application, Transport, Internet, and Network Interface layers.
- Each layer has a specific function: Application handles user services, Transport ensures reliable data transfer, Internet manages logical addressing and routing, Network Interface deals with physical data transmission.
- Port numbers identify specific applications or services on a device, while IP addresses identify the device.
- Common protocol ports include: HTTP → 80, HTTPS → 443, FTP → 21, SSH → 22, Telnet → 23, SMTP → 25, DNS → 53, RDP → 3389.
- IP conflicts occur when two devices share the same IP address, disrupting network communication.
- IP conflicts can be resolved by assigning unique static IPs or using DHCP for automatic IP allocation.

ASSESSMENT

A. Multiple Choice Questions

1. Which layer of the TCP/IP stack handles user applications?
   a) Transport
   b) Internet
   c) Application
   d) Network Interface

2. Which command is used to test connectivity between devices?
   a) tracert
   b) ping
   c) netstat
   d) nslookup

3. What is the default port number for HTTP?
   a) 21
   b) 80
   c) 22
   d) 443

4. Which tool displays the path packets take to reach a destination?
   a) ipconfig
   b) tracert
   c) ping
   d) netstat

5. Which port is used for secure remote login via SSH?
   a) 23
   b) 21
   c) 22
   d) 25

6. Which command shows active TCP/UDP connections on a computer?
   a) nslookup
   b) netstat
   c) ping
   d) tracert

7. What happens if two devices have the same IP address on a network?
   a) Faster connectivity
   b) IP conflict
   c) Automatic update
   d) Encryption

8. Nmap is primarily used for:
   a) Assigning IP addresses
   b) Port scanning and security auditing
   c) Testing DNS resolution
   d) Checking subnet masks

9. Which command helps in checking DNS resolution?
   a) ping
   b) nslookup
   c) tracert
   d) netstat

10. HTTPS uses which port number by default?
    a) 80
    b) 21
    c) 22
    d) 443

B. Fill-in-the-blanks

1. The _____ layer of TCP/IP handles user services and applications.
2. _____ is used to test connectivity between two network devices.
3. The default port number for FTP is _____.
4. _____ displays the IP configuration of a computer.
5. _____ is used to trace the route taken by packets to a destination.
6. Two devices using the same IP address result in an _____.
7. _____ is used to view active connections and open ports on a computer.
8. Port number 22 is used by _____ for secure remote access.
9. _____ is used to check DNS resolution for a domain name.
10. Nmap is a tool used for _____ and network security auditing.

C. True/False questions

1. TCP/IP has four layers: Application, Transport, Internet, and Network Interface.
2. The PING command cannot check if a website is reachable.
3. Port number 80 is used for HTTPS.
4. TRACERT shows the path of data packets from source to destination.
5. NETSTAT can display active connections and open ports.
6. An IP conflict occurs when two devices share the same IP address.
7. NSLOOKUP is used to assign IP addresses automatically.
8. SSH uses port number 22 for secure remote login.
9. Nmap can be used to scan ports on authorized devices only.
10. DHCP assigns unique IP addresses to devices to avoid conflicts.

D. Short Questions Answers

1. What is the TCP/IP protocol stack?
2. Name two purposes of port numbers.
3. What is the default port number for SMTP?
4. Explain the function of the PING command.
5. What information does IPCONFIG provide?
6. What is the purpose of the TRACERT command?
7. How can an IP conflict occur?

8. What is the use of NETSTAT in networking?
9. How does NSLOOKUP help in troubleshooting?
10. What is Nmap used for in network security?

Answer Key

A. Multiple Choice Questions

1. c), 2. b), 3. b), 4. b), 5. c), 6. b), 7. b), 8. b), 9. b), 10. d)

B. Fill-in-the-blanks

1. Application, 2. PING, 3. 21, 4. IPCONFIG, 5. TRACERT, 6. IP conflict, 7. NETSTAT, 8. SSH, 9. NSLOOKUP, 10. port scanning

C. True/False questions

1. True, 2. False, 3. False, 4. True, 5. True, 6. True, 7. False, 8. True, 9. True, 10. True

Chapter-5

Exploring Windows Operating System

At Greenwood School, the computer lab was slow and confusing for students. Files were hard to find, and students often forgot their passwords. Ms. Kapoor, the computer teacher, decided to give the lab a Windows makeover. She installed Windows on all computers and showed students how to use the Control Panel to adjust settings. She also taught them how to manage user accounts and use Task Manager to monitor programs. One day, Rohan needed to access a computer remotely from home. Using Remote Desktop, he logged in and completed his assignments without problems. The students were amazed. "Everything is so easy now!" said Riya. Thanks to Windows, the lab became organized, secure, and fun for learning.

5.1. Basics of Windows OS and Control Panel

5.1.1. Basics of Windows OS

An Operating System (OS) is system software that acts as an interface between the user and the computer hardware. It manages system resources and allows users to interact with the machine easily.

- **Windows OS**

The Windows Operating System (OS) is one of the most widely used operating systems in the world, developed by Microsoft. An operating system is software that acts as a bridge between the user and the computer hardware. Without an OS, a computer cannot work properly because the OS manages all activities such as running applications, storing files, and controlling devices like the keyboard, mouse, and printer.

Windows OS was first introduced in 1985 as a graphical interface on top of MS-DOS. Over the years, it has evolved into a powerful and user-friendly operating system used in homes,

schools, and businesses. It is called “Windows” because it allows users to open different tasks in separate windows on the screen.

Windows helps you to use your computer by showing everything on the screen in a simple and easy way using icons, folders, buttons, and menus.

Think of Windows as the manager of your computer. It helps you:

- Open and use apps like Paint, Word, or games
- Save your files and folders
- Connect to the internet
- Play music and videos
- Use a mouse and keyboard easily

It’s called Windows because it shows different programs and files in boxes called "windows" on the screen. Example: When you turn on your computer and see the desktop with icons, and click on the Start button to open things—that’s all part of Windows!

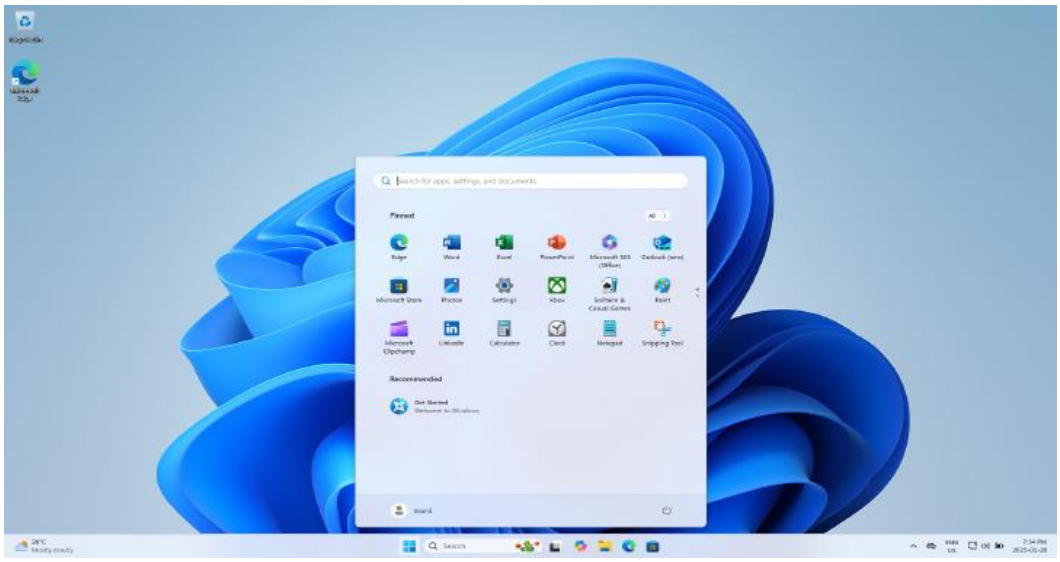


Figure: 5.1 Windows Operating System (OS)

Features of Windows OS

Some important features of Windows OS are:

- **Graphical User Interface (GUI):** Instead of typing commands, users can interact with icons, buttons, and menus.
- **Multitasking:** Windows can run more than one application at the same time (for example, browsing the internet while listening to music).
- **File Management:** Windows provides tools like File Explorer to create, store, organize, and search files and folders.
- **Device Management:** It automatically detects and manages hardware like USB drives, printers, and cameras.
- **Security:** Windows includes features like User Accounts, Passwords, Windows Defender, and Firewalls to protect data and devices.

- **Networking:** It supports easy connection to the Internet and Local Area Networks (LANs).
- **Updates and Support:** Microsoft provides regular updates to improve performance and security.

Today, modern versions like Windows 10 and Windows 11 have advanced features such as Cortana (voice assistant), touch support, cloud integration (OneDrive), and stronger security measures.

Advantages of Windows OS

- **User-Friendly Interface:** Windows offers a simple and attractive Graphical User Interface (GUI) with icons, menus, and buttons, making it easy even for beginners.
- **Wide Compatibility:** Supports a wide range of hardware devices like printers, scanners, and webcams, as well as most software applications and games.
- **Multitasking Support:** Allows running multiple applications at the same time without much difficulty (e.g., browsing, working on Word, and listening to music).
- **Large User Base:** Windows is the most popular desktop OS worldwide, so it has a strong support community, tutorials, and resources for troubleshooting.
- **Regular Updates:** Microsoft provides frequent security patches and updates to improve system stability and protect against viruses and malware.
- **Networking Features:** Easy to connect to the internet, local networks, and file sharing, which is helpful in schools, offices, and homes.

Disadvantages of Windows OS

- **Cost:** Unlike some operating systems (e.g., Linux), Windows is not free. Users must buy a license.
- **Vulnerability to Viruses:** Because of its popularity, Windows is a common target for hackers, so it needs strong antivirus protection.
- **High System Requirements:** New versions of Windows require powerful hardware, which may not run smoothly on older computers.
- **Frequent Updates:** Although updates improve security, they sometimes interrupt work or require restarts.
- **Less Control for Advanced Users:** Windows is designed for ease of use, so advanced users may find it less customizable compared to Linux.

Did You Know?

- Windows OS was first introduced by Microsoft in 1985 as a graphical extension of MS-DOS.
- The Start Menu was introduced in Windows 95 and has been a key navigation element ever since.

5.1.2. Control Panel in Windows

The Control Panel is an important feature of the Windows Operating System that allows users to manage and configure their computer's settings. It acts like the "command center" of the computer, where you can control how the system looks, works, and connects to other devices.

When you open the Control Panel, you will find different categories and icons that represent various settings. Instead of using commands, you can simply click on icons and menus to make changes.

Functions of the Control Panel

- **System and Security:** Helps manage system performance, firewall, updates, and backup settings. Example: Turning Windows Defender Firewall on or off.
- **Network and Internet:** Allows users to connect to Wi-Fi, set up wired connections, or manage internet options. Example: Checking network status or setting up a new connection.
- **Hardware and Sound:** Used to configure devices like printers, scanners, speakers, and displays. Example: Adding a new printer or adjusting speaker volume.
- **Programs:** Let users install or uninstall software, view installed updates, and manage default programs. Example: Removing unwanted applications.
- **User Accounts:** Used to create, manage, or delete user accounts and set passwords. Example: Adding a guest account.
- **Appearance and Personalization:** Allows changes to desktop background, themes, taskbar, and display settings. Example: Changing wallpaper or adjusting screen resolution.
- **Clock, Language, and Region:** Used to set the date and time, change time zones, and add new languages. Example: Setting the system clock to the correct time zone.
- **Ease of Access:** Provides accessibility options for users with disabilities. Example: Turning on Narrator or Magnifier.

Steps to Access the Control Panel in Windows

The Control Panel can be opened in different ways, depending on the version of Windows (7, 8, 10, or 11). Here are the most common methods:

- **Using the Start Menu**
  - Click the Start button.
  - Type Control Panel in the search box.
  - Click on the Control Panel from the results.

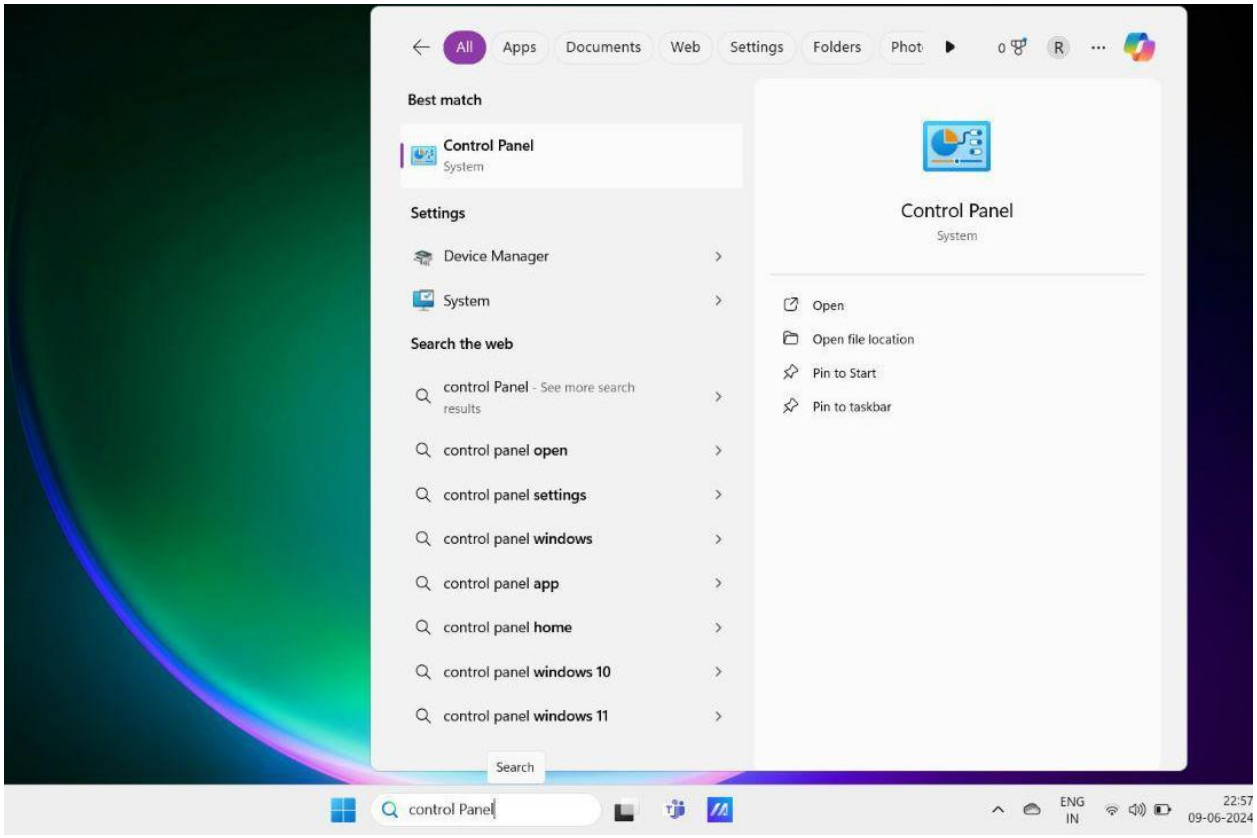


Figure 5.2. Start of Control Panel

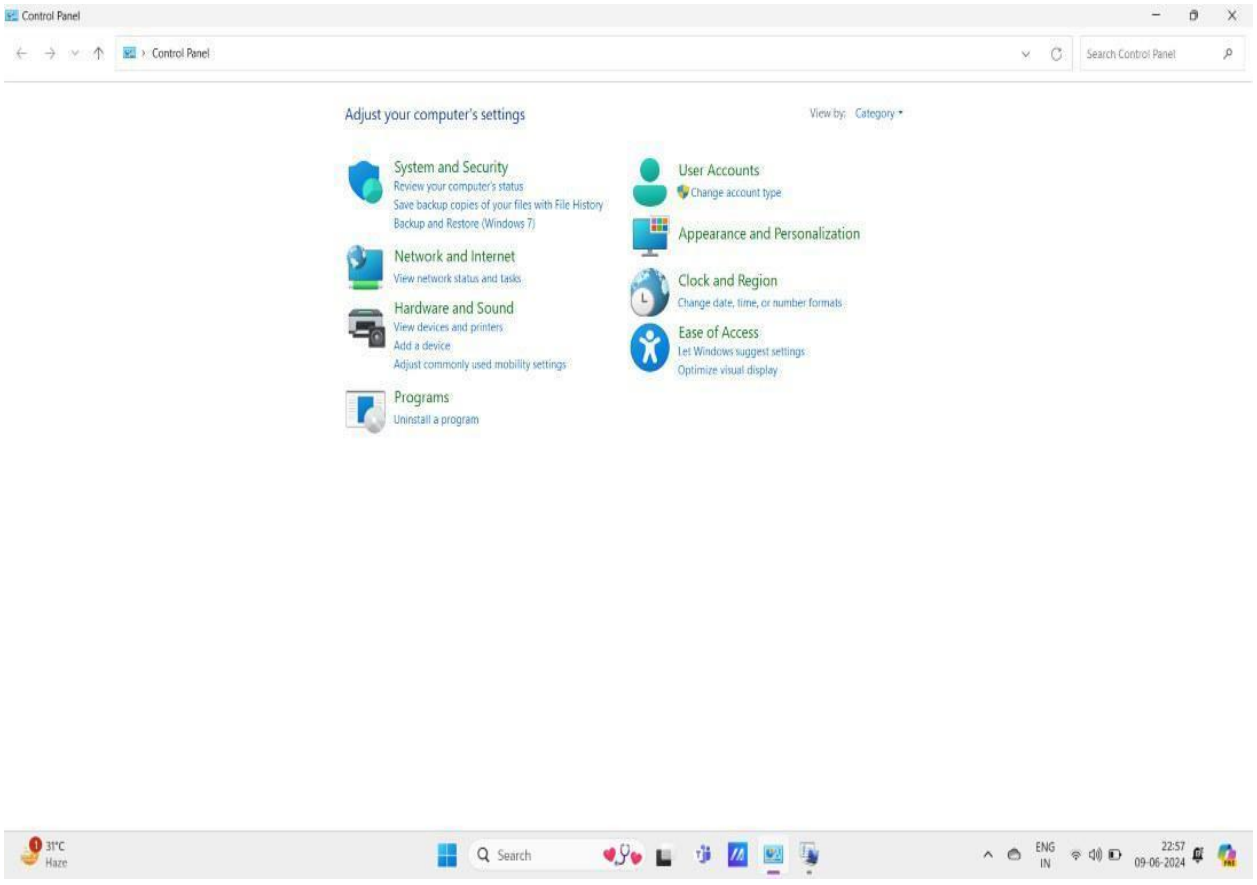


Figure 5.3. Control Panel

- **Using Run Command**
  - Press Windows Key + R together.
  - In the Run box, type control and press Enter.
  - The Control Panel window will open.
- **Using Command Prompt/PowerShell**
  - Open Command Prompt or PowerShell.
  - Type control and press Enter.
  - This will launch the Control Panel.
- **From Settings (Windows 10/11)**
  - Open the Settings app (Windows Key + I).
  - In the search bar, type Control Panel.
  - Click on it when it appears in the list.

Advantages of the Control Panel

- An easy and organized way to manage system settings.
- No need to remember commands—just click on icons.
- Provides quick access to important security, personalization, and hardware options.

Disadvantages of the Control Panel

- New users may feel confused because there are many options.
- Some advanced settings are hidden or difficult to find.
- In Windows 10 and 11, many settings are now shifting to the Settings app, so users need to use both.

Did You Know?

- Control Panel has been gradually replaced by the Settings app in modern Windows versions, but it still exists for advanced configuration.

Assignment 5.1.

1. List three key features of the Windows OS.
2. Write a short note on the Control Panel.

5.2. User and Role Management in Windows

In any computer system, especially in Windows, user and role management are important for controlling who can use the computer and what tasks they are allowed to perform. It helps in maintaining security, privacy, and proper usage of the system.

User Management

- A user is anyone who has a login account on the computer.
- Each user account has its own files, folders, and settings (like desktop background, browser history, documents, etc.).
- Windows allows creating multiple user accounts on the same computer.

Types of User Accounts in Windows:

- **Administrator Account**
  - Has full control over the computer.
  - Can install/uninstall software, create/delete users, and change system settings.
  - Example: The person who owns the PC usually has this role.
- **Standard User Account**
  - Can use installed applications, browse the internet, and save files.
  - Cannot make big changes to the system (like installing/uninstalling programs).
  - Safer for daily use because it prevents accidental system damage.
- **Guest Account (older Windows versions)**
  - Limited access, usually for temporary users.
  - Cannot install programs or change settings.
  - Example: Allowing a friend to use your computer just to browse or type a document.

Role Management

- A role defines the level of permission or access a user has.
- Windows assigns roles based on the type of account (Administrator, Standard, Guest).
- Roles are important in both personal computers and networks.
- Examples of Roles:
  - *Administrator Role:* Can manage users, control security settings, and configure the whole system.
  - *User Role:* Can only perform normal daily tasks like browsing, editing documents, or using apps.
  - *Network Role (in organizations):* Users may have roles like "Student," "Teacher," or "Staff," with specific permissions.

Advantages of User and Role Management

- Protects the system from unauthorized access.
- Ensures privacy—each user's files are separate.
- Helps in controlling what tasks different people can perform.
- Prevents accidental system changes by restricting permissions.

Disadvantages

- If passwords are forgotten, users may lose access.
- Administrator accounts can be misused if given to the wrong person.
- Managing too many users in large organizations can become complex.

5.3. Remote Desktop and Task Manager

5.3.1. Remote Desktop

Remote Desktop is a feature in Windows that allows you to connect to another computer from a different location and use it as if you were sitting right in front of it. It is widely used in offices, schools, and organizations for remote work and troubleshooting.

How it Works:

- A computer (called the host) enables Remote Desktop.
- Another computer (called the client) connects to the host using the Remote Desktop Connection app.
- Once connected, the user can access files, run programs, and control the remote computer.

Steps to Use Remote Desktop:

- On the host computer, enable Remote Desktop from System Settings.
- Note down the host's IP address or computer name.
- On the client computer, open Remote Desktop Connection (search in Start Menu).
- Enter the host's IP or computer name and log in with username/password.
- The remote computer screen will now appear, ready for use.

Advantages of Remote Desktop:

- Allows working from anywhere without carrying a physical computer.
- Helps IT staff to troubleshoot problems remotely.
- Saves time and improves productivity.

Disadvantages of Remote Desktop:

- Needs internet/network connection.
- Security risk if passwords are weak or the connection is not encrypted.
- Performance may be slow if the network speed is low.

Assignment 5.2.

1. Write any three functions that can be performed using the Task Manager.
2. Mention two advantages of using Remote Desktop.

5.3.2. Task Manager

The Task Manager is a powerful tool in Windows that shows information about the computer's performance, running programs, and processes. It helps in monitoring system activities and troubleshooting problems.

Steps to Open Task Manager:

- Press Ctrl + Shift + Esc
- OR Ctrl + Alt + Delete → Task Manager

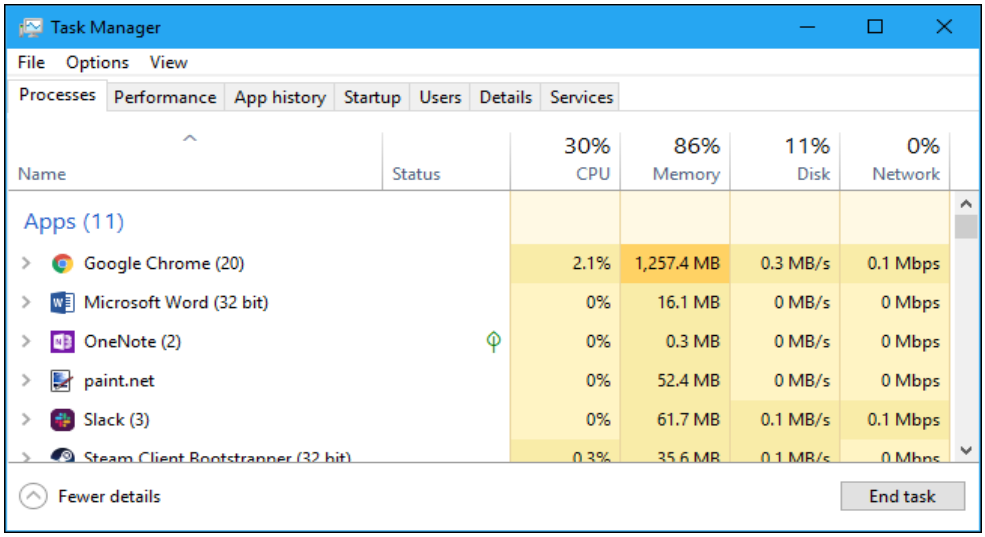


Figure 5.4. Task Manager

Key Tabs in Task Manager:

1. **Processes**
   - Shows all running applications and background processes.
   - You can end (close) unresponsive programs here.
2. **Performance**
   - Displays real-time graphs of CPU, Memory (RAM), Disk, and Network usage.
   - Useful to check if the system is overloaded.
3. **App History (in newer Windows)**
   - Shows resource usage (CPU time, network data) of apps over time.
4. **Startup**
   - Lists programs that automatically start when Windows boots.
   - You can enable/disable them to improve startup speed.
5. **Users**
   - Shows which users are currently logged in and what resources they are using.
6. **Details**
   - Provides technical information about each process (PID, status, etc.).
7. **Services**
   - Displays system services and their status (running, stopped, etc.).

Advantages of Task Manager:

- Helps in closing unresponsive programs.
- Monitors performance and detects heavy resource usage.
- Controls startup programs to speed up boot time.

Disadvantages of Task Manager:

- Beginners may get confused by too much technical information.
- Accidentally ending critical system processes may cause instability.

Did You Know?

- Remote Desktop uses the RDP (Remote Desktop Protocol) to allow secure access over the network.
- Virtual Machines allow running multiple operating systems on a single physical computer for testing and training purposes.

Practical Activity 5.1: Installing Windows OS in a Virtual Environment

Objective: To simulate the installation of the Windows Operating System using a virtual machine without affecting the main computer.

Materials Required:

- A computer with sufficient RAM (minimum 4 GB recommended)
- Virtualization software (e.g., Oracle VirtualBox or VMware Workstation Player)
- Windows OS ISO file (setup image)

Steps:

- **Download and Install Virtualization Software**
  - Download and install VirtualBox (or VMware) on your computer.
- **Open VirtualBox and Create a New Virtual Machine (VM)**
  - Click New.
  - Enter the name (e.g., "Windows 10 VM").
  - Choose Type: Microsoft Windows and Version (Windows 7/8/10, depending on ISO).
- **Allocate Memory (RAM)**
  - Assign memory to the VM (e.g., 2048 MB or more, depending on your system).
- **Create a Virtual Hard Disk**
  - Choose Create a virtual hard disk now.
  - Set disk size (e.g., 20 GB or more).
  - Select VDI (VirtualBox Disk Image) and Dynamically allocated.
- **Attach Windows ISO File**
  - Go to VM settings → Storage.
  - Select the empty disk icon → Choose a disk file.
  - Browse and attach the Windows ISO file.
- **Start the Virtual Machine**
  - Click Start to boot from the ISO.
  - The Windows Setup screen will appear.
- **Windows Installation Steps (Simulated):**
  - Choose language, time, and keyboard settings → Click Next.
  - Click Install Now.
  - Accept license agreement.
  - Choose Custom Installation.
  - Select the virtual hard disk created earlier and click Next.
- **File Copying and Installation**
  - Windows will copy and install files.
  - The VM will restart automatically.

- **User Setup**
  - Enter username and password.
  - Choose privacy/security options.
- **First Desktop View**
  - After completion, the Windows desktop will appear in the virtual environment.
- **Observation/Result:** Students will be able to see the complete installation process of Windows OS in a safe virtual machine without affecting the host computer.
- **Precautions:**
  - Do not assign too much RAM or disk space; it may slow down the host system.
  - Always use a licensed or educational ISO image.

Practical Activity 5.2: Configure Users, Security Settings, and Manage Basic Admin Tasks

Materials Required:

- A computer running Windows OS
- Administrator privileges on the system

Step-wise Procedure:

Step 1: Open the Control Panel
- Click Start → Control Panel or press Windows + R, type control, and press Enter.

Step 2: Access User Accounts
- In Control Panel, click User Accounts → Manage another account.

Step 3: Create a New User Account
- Click Add a new user (Windows 7/8) or Add someone else to this PC (Windows 10/11).
- Enter a username and password.
- Choose account type: Administrator or Standard User.

Step 4: Change the Account Type of Existing Users
- Select an account → Click Change the account type → choose Administrator or Standard.

Step 5: Set or Change Passwords
- Select the user → Click Create/change password → enter and confirm the new password.

Step 6: Configure Security Settings
- Go to Control Panel → System and Security → Windows Defender Firewall.
- Turn Firewall On or Off as required.
- Check antivirus status: Windows Security → Virus & threat protection.

Step 7: Manage Basic Admin Tasks
- Install/Uninstall software: Control Panel → Programs → Programs and Features.
- View system info/change settings: Control Panel → System and Security → System.
- Set folder permissions: Right-click folder → Properties → Security → Edit permissions.

Step 8: Log Out and Test User Accounts
- Log in with the newly created accounts to verify access and permissions.

Observation/Result:

- New user accounts were successfully created and tested.
- Security settings and folder permissions were configured correctly.
- Basic administrative tasks were performed successfully.

Precautions:
- Keep at least one Administrator account active.
- Use strong passwords for security.
- Avoid modifying system files unnecessarily.

Practical Activity 5.3: Access System Tools and Control Panel Utilities
Materials Required:
- A computer running Windows OS
- Administrator or standard user account

Step-wise Procedure:
Step 1: Open the Control Panel
Click Start → Control Panel or press Windows + R, type control, and press Enter.
Step 2: Explore System and Security
- Click System and Security.
- Access System to view computer information (OS version, RAM, processor).
- Open Windows Defender Firewall to view firewall settings.
- Open Power Options to check/change power plans.

Step 3: Explore the Network and the Internet
- Click Network and Sharing Center to view network connections and settings.
- Open Internet Options to check browser settings, security, and privacy.

Step 4: Explore Hardware and Sound
- Click Device Manager to view all connected hardware and drivers.
- Open Sound and Display settings to adjust audio and screen configurations.

Step 5: Explore Programs
- Open Programs and Features to install/uninstall software.
- Check Default Programs to set default apps for web browsing, media, etc.

Step 6: Explore User Accounts
- Access User Accounts → Manage another account to view or change account types.
- Change password or account settings if required.

Step 7: Access System Tools from the Start Menu
- Open Start → Windows Accessories → System Tools.
- Explore tools like:
  - Disk Cleanup – removes unnecessary files.
  - Task Scheduler – schedules tasks to run automatically.
  - Event Viewer – checks system logs and errors.
  - Resource Monitor – monitors CPU, memory, disk, and network usage.

Step 8: Access Task Manager
- Press Ctrl + Shift + Esc or Ctrl + Alt + Delete → Task Manager.
- Explore the Processes, Performance, Startup, and Users tabs to monitor system activity.

Observation/Result:
- Students were able to access various Control Panel utilities and system tools.
- System performance, user accounts, network settings, and hardware information were successfully explored.
- Tools like Task Manager, Disk Cleanup, and Event Viewer were accessed and understood.

Precautions:
- Do not change system files or critical settings without guidance.
- Use administrator privileges carefully to avoid system issues.

Only explore tools; avoid making permanent changes unless instructed.

Summary

- Windows OS is a graphical operating system that manages hardware and software resources.
- The Start Menu, Taskbar, and Desktop are key elements for user interaction.
- Control Panel allows access to system settings, hardware, software, and user accounts.
- Users can create and manage multiple accounts with different roles and permissions.
- Administrator accounts have full system control, while standard users have limited access.
- User accounts can have passwords, and security settings can be configured for protection.
- Remote Desktop allows users to access and control another computer remotely.
- Task Manager monitors system performance, running processes, startup programs, and users.
- Windows installation can be simulated in virtual environments using tools like VirtualBox or VMware.
- System tools like Disk Cleanup, Event Viewer, Resource Monitor, and Task Scheduler help maintain and monitor the system efficiently.
- Managing users, security settings, and basic admin tasks ensures proper system organization and safety.
- Control Panel utilities allow configuration of network, hardware, power, programs, and privacy settings.
- Practicing these tools and settings in a lab environment helps students understand Windows OS functionality.

ASSESSMENT

A. Multiple Choice Questions

1. Which of the following is the main interface for user interaction in Windows OS?
   a) BIOS
   b) Desktop
   c) CMD
   d) Registry

2. Which Control Panel category is used to manage hardware devices?
   a) System and Security
   b) Network and Internet
   c) Hardware and Sound
   d) Programs

3. Which account type has full control over the system?
   a) Standard User
   b) Guest User
   c) Administrator
   d) Limited User

4. Which Windows tool is used to monitor CPU, memory, and disk usage?
   a) Disk Cleanup
   b) Task Manager

c) Event Viewer
d) Control Panel

5. Which key combination opens Task Manager directly?
   a) Ctrl + C
   b) Ctrl + Shift + Esc
   c) Alt + F4
   d) Ctrl + Alt + Del

6. Which tool allows connecting to and controlling another computer remotely?
   a) Task Manager
   b) Device Manager
   c) Remote Desktop
   d) Windows Firewall

7. Disk Cleanup is used to:
   a) Uninstall programs
   b) Remove unnecessary files
   c) Check RAM usage
   d) Schedule tasks

8. Which of the following is not part of the System Tools?
   a) Disk Cleanup
   b) Resource Monitor
   c) Microsoft Word
   d) Event Viewer

9. VirtualBox is used to:
   a) Monitor hardware
   b) Simulate virtual machines
   c) Manage user accounts
   d) Configure network settings

10. Which of the following can be managed via Control Panel?
    a) User Accounts
    b) Installed Programs
    c) Network Connections
    d) All of the above

B. Fill-in-the-blanks

1. The main interface of Windows OS is called the _____.
2. _____ accounts have full system privileges.
3. _____ is used to monitor running processes and system performance.
4. Remote Desktop allows users to access a computer _____.
5. The Control Panel is used to configure system _____.
6. Disk Cleanup helps in removing _____ files from the system.
7. _____ Manager is used to check hardware device status.
8. VirtualBox and VMware are tools for creating _____ machines.
9. Task Manager can be opened using the keyboard shortcut _____.
10. User Accounts can be accessed through the _____.

C. True/False questions

1. Standard users have full control over system settings.
2. Task Manager can show CPU, memory, disk, and network usage.
3. Remote Desktop allows remote access to other computers.
4. Disk Cleanup is used to install new programs.
5. The Control Panel cannot be used to manage user accounts.
6. Administrator accounts can change system security settings.
7. Virtual machines allow Windows to run inside another operating system.
8. Event Viewer is used to uninstall programs.
9. Device Manager helps manage hardware devices connected to the computer.
10. Guest accounts have full administrative privileges.

D. Short Question Answers

1. What is the main interface of Windows OS called?
2. Name the two main types of user accounts in Windows.
3. What is the purpose of Task Manager?
4. How can you open Task Manager using the keyboard?
5. What is Remote Desktop used for?
6. Name any three system tools in Windows.
7. How can you access the Control Panel in Windows?
8. What is the function of Disk Cleanup?
9. What is the difference between Administrator and Standard User?
10. What are Virtual Machines, and why are they used?

Answer Key

A. Multiple Choice Questions

1. b), 2. c), 3. c), 4. b), 5. b), 6. c), 7. b), 8. c), 9. b), 10. d)

B. Fill-in-the-blanks

1. Desktop, 2. Administrator, 3. Task Manager, 4. Remotely, 5. Settings, 6. Unnecessary, 7. Device, 8. Virtual, 9. Ctrl + Shift + Esc, 10. Control Panel

C. True/False questions

1. False, 2. True, 3. True, 4. False, 5. False, 6. True, 7. True, 8. False, 9. True, 10. False

Chapter-6

Exploring Linux Operating System

At Riverside School, the computer lab had old computers that often crashed. The students wanted a system that was fast, secure, and reliable. Mr. Verma, the computer teacher, introduced them to Linux. He installed Ubuntu on one computer and CentOS on another to show the differences. He explained how the file system worked, how to use basic commands like ls, cd, cp, and chmod, and how sudo helps perform administrative tasks. The students practiced creating files, changing permissions, and exploring directories. Seema said, "It's amazing how we can control everything and even fix problems ourselves!" By the end of the week, the lab ran smoothly, and students learned that Linux was powerful, secure, and perfect for both learning and real-world applications.

6.1. Overview of Linux OS

Linux OS

Linux is also a type of Operating System (OS) like Windows, but it works a bit differently. It helps the computer run apps, manage files, and connect to the internet.

What makes Linux special is that:

- It is free to use, and anyone can change or improve it.
- It is used mostly in servers, school labs, tech companies, and even in mobile phones (like Android).
- It is very safe and secure from viruses.

Linux often uses a command line (text-based screen) to give instructions, but many versions also have desktops with icons and menus, just like Windows. Example: If you have ever seen someone using Ubuntu, Kali Linux, or Linux Mint, they are using a version of the Linux OS.

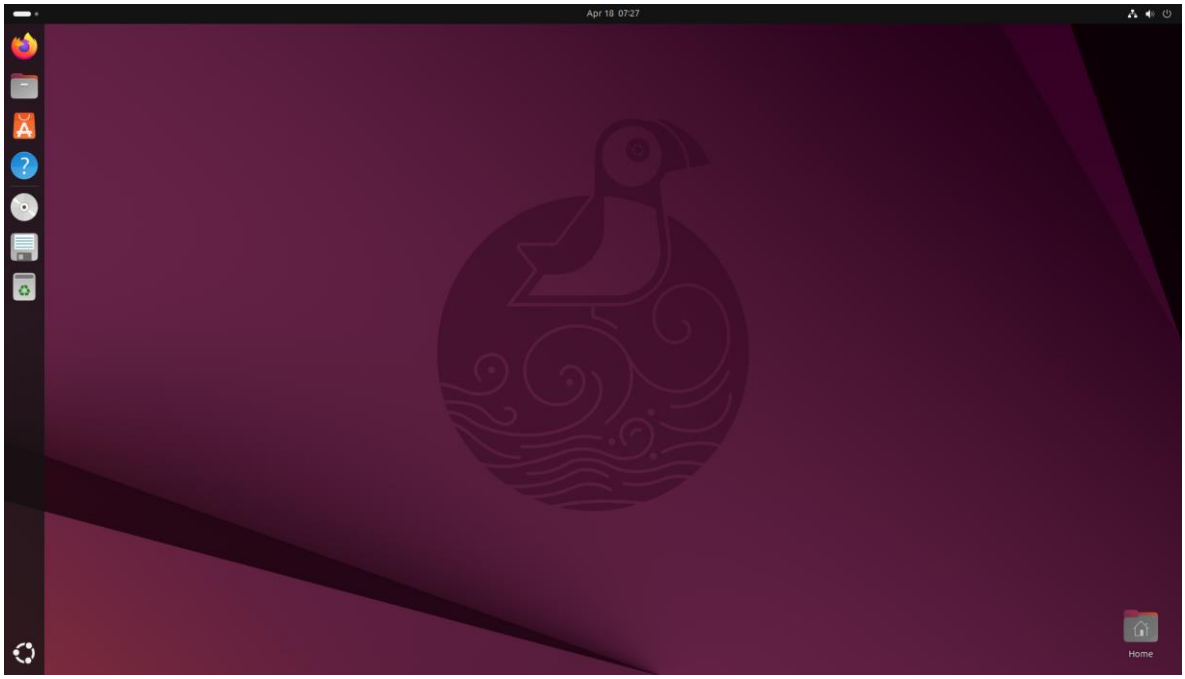


Figure:6.1 Linux operating system

Linux is also known for its command-line interface (CLI), which allows users to interact with the system using text commands. In addition, many Linux distributions provide a graphical user interface (GUI), making it easier for beginners to use. Popular Linux distributions include Ubuntu, Fedora, Debian, CentOS, and Linux Mint.

Linux supports a wide range of software applications and networking protocols. It is highly secure, with built-in permission systems to control access to files and resources. It is also highly customizable, allowing users to modify the system to suit their needs.

Advantages of Linux:

- Free and open-source
- Highly secure and stable
- Can run on older hardware
- Supports multitasking and multi-user environment
- Highly customizable
- Wide range of distributions and applications

Disadvantages of Linux:

- A steeper learning curve for beginners compared to Windows
- Some commercial software may not be available
- Hardware compatibility can sometimes be an issue

Real-Life Examples:

- Linux is used on most web servers and cloud platforms.
- Android smartphones are built on the Linux kernel.
- Supercomputers and embedded systems often run Linux due to its performance and reliability.

Ubuntu

Ubuntu is one of the most popular Linux distributions (distros), developed and maintained by Canonical Ltd. It is based on Debian Linux and is designed to be user-friendly, making it ideal for beginners. Ubuntu comes with a Graphical User Interface (GUI) by default, but advanced users can also use the Command-Line Interface (CLI) for powerful system management.

Ubuntu is widely used for desktop computers, servers, cloud computing, and IoT devices. It provides a wide range of software packages through its repositories, making it easy to install and update applications. Ubuntu also receives regular updates, including security patches, ensuring system stability and protection against vulnerabilities.

Figure 6.2. Ubuntu

Advantages of Ubuntu:

- Easy to install and use
- Large community support and documentation
- Regular updates and security patches
- Free and open-source
- Suitable for both beginners and advanced users

Disadvantages of Ubuntu:

- Some proprietary software may not be available by default
- Less suitable for older hardware compared to lightweight Linux distros

CentOS

CentOS (Community ENTerprise Operating System) is a Linux distribution derived from Red Hat Enterprise Linux (RHEL). It is designed for servers and enterprise environments due to its stability and long-term support. Unlike Ubuntu, CentOS focuses more on performance, reliability, and security rather than user-friendliness.

CentOS is widely used in web servers, database servers, and cloud environments. It comes with fewer pre-installed applications for desktop use, as it is optimized for server tasks. Being community-driven, CentOS is free to use and receives updates aligned with RHEL, ensuring enterprise-grade reliability.

Figure 6.3 CentOS

Advantages of CentOS:

- Highly stable and secure
- Free and open-source
- Long-term support for server environments
- Ideal for enterprise and server applications

Disadvantages of CentOS:

- Less user-friendly for beginners
- Limited GUI support; mostly managed via command line
- Slower to receive updates compared to Ubuntu

6.2. File System Structure and Permissions

6.2.1 Linux File System Structure

The Linux operating system organizes files in a hierarchical tree structure, starting from the root directory, denoted by /. Every file and directory in Linux exists under this root. Unlike Windows, which uses drive letters like C: or D:, Linux treats all storage devices as part of a single directory tree.

Some important directories in Linux include:

- / (Root Directory): The top-most directory of the file system. All other files and directories branch from here.
- /home – where users keep their files (like Documents or Pictures).
- /bin – has programs and commands that the system uses.
- /etc – stores settings and system files.
- /dev – has files for devices like your mouse or keyboard.
- /tmp – a place for temporary files that are deleted automatically.
- /var: Stores variable data like logs, mail, and databases.
- /mnt or /media: Mount points for external drives, USBs, and other file systems.

Linux also supports mounting additional drives and partitions at any directory, which makes the file system flexible.

Did You Know?

- In Linux, everything is treated as a file—even folders and connected devices!
- Linux was created in 1991 by Linus Torvalds as a hobby project.
- The mascot of Linux is a penguin named Tux.
- More than 90% of the world's supercomputers run on Linux.

6.2.2. Linux File Permissions

Linux is a multi-user system, so it uses file permissions to control access to files and directories. Each file or directory has three types of permissions for three categories of users:

1. Types of Permissions:

- Read (r): Permission to view the contents of a file or list the contents of a directory.
- Write (w): Permission to modify or delete a file, or add/remove files in a directory.
- Execute (x): Permission to run a file as a program or script, or access a directory.

2. Categories of Users:

- Owner (user): The person who created the file.
- Group: A set of users assigned to the same group.
- Others: All other users on the system.

Example: -rwxr-xr-- 1 sneha staff 1024 Sep 23 2025 file.txt

- -rwxr-xr-- : Permissions
  - rwx → Owner (sneha) can read, write, and execute
  - r-x → Group (staff) can read and execute
  - r-- → Others can only read

- 1 → Number of links
- sneha → Owner
- staff → Group
- 1024 → File size in bytes
- file.txt → File name

Changing Permissions:

- chmod: Change file permissions. Example: chmod 755 file.txt
- chown: Change file owner. Example: chown monika file.txt
- chgrp: Change file group. Example: chgrp staff file.txt

Advantages of Linux File Permissions:

- Ensures security and privacy in multi-user environments.
- Prevents unauthorized access or modification of files.
- Flexible control over who can read, write, or execute files.

Disadvantages of Linux File Permissions:

- Can be confusing for beginners to manage multiple permissions.
- Incorrect settings may prevent access to critical files.

Assignment 6.1.

1. Write the use of the following commands: ls, cd, cp, chmod.
2. Write the steps to install Linux in a virtual machine.

6.3. Installation of Linux OS

Installing Linux involves preparing the system, selecting the Linux distribution, and following setup steps to get a functional operating system. Popular distributions for beginners include Ubuntu, Linux Mint, and Fedora, while CentOS and Debian are preferred for servers.

Linux can be installed on a physical machine or a virtual environment using tools like VirtualBox or VMware. Virtual installation is ideal for learning, testing, and practicing without affecting the host computer.

Steps for Installing Linux OS (General Process)

Step 1: Prepare Installation Media

- Download the ISO file of the Linux distribution from its official website.
- Create a bootable USB using tools like Rufus, Etcher, or UNetbootin, or attach the ISO to a virtual machine.

Step 2: Boot from Installation Media

- Insert the USB in the computer and restart.

- Access the Boot Menu (usually pressing F12, Esc, or Del) and select the USB drive.
- For virtual machines, attach the ISO to the virtual CD/DVD drive and start the VM.

Step 3: Start the Installation Process

- Most distributions provide a Live Mode to try the OS without installing.
- Click Install Linux to start the installation wizard.

Step 4: Configure Language, Keyboard, and Time Zone

- Select your preferred language, keyboard layout, and time zone.

Step 5: Partitioning and Disk Setup

- Choose the installation type:
- Erase the disk and install Linux (for fresh installations)
- Manual partitioning (for dual-boot or advanced users)
- Linux typically uses partitions like / (root), /home (user data), and swap (virtual memory).

Step 6: Create User Account

- Enter a username, password, and hostname for the computer.
- Decide whether to enable automatic login or require a password at startup.

Step 7: Installation and System Configuration

- The installer copies files to the disk and configures the system.
- Wait for the installation to complete; this may take several minutes.

Step 8: Restart and Remove Installation Media

- After installation, reboot the system.
- Remove the USB or detach the ISO in a virtual machine.
- The system will boot into the new Linux OS.

Step 9: Post-Installation Setup

- Update the system using the package manager:
- Ubuntu/Debian: sudo apt update && sudo apt upgrade
- CentOS/Fedora: sudo yum update or sudo dnf update
- Install additional software and drivers if required.
- Customize desktop environment, themes, and settings.

Advantages of Linux Installation

- Free and open-source; no licensing cost.
- Provides a secure and stable operating system.
- It can be installed on old hardware or virtual environments.
- Multiple distributions for different needs: desktop, server, cloud.

Disadvantages of Linux Installation

- It may be challenging for beginners without prior experience.

- Hardware drivers may not be available for some devices.
- Partitioning and dual-boot setup can be risky if not done correctly.

Real-Life Example:

Students can install Ubuntu in VirtualBox to practice Linux commands and explore the GUI without affecting their main operating system.

Did You Know?

- Android, the most popular mobile operating system, is based on the Linux kernel.
- Linux powers most of the world's web servers, including Google, Facebook, and Amazon.

6.4. Basic Linux Commands and sudo usage

6.4.1. Basic Linux Commands

Linux uses a Command-Line Interface (CLI) where users can interact with the system by typing commands. Even though most Linux distributions provide a GUI, knowing CLI commands is essential for administration, troubleshooting, and server management. Here are some fundamental commands:

File and Directory Management

- pwd – Prints the current working directory.
- ls – Lists files and directories in the current location.
- cd <directory> – Changes to the specified directory.
- mkdir <directory> – Creates a new directory.
- rmdir <directory> – Removes an empty directory.
- rm <file> – Deletes a file.
- cp <source> <destination> – Copies files or directories.
- mv <source> <destination> – Moves or renames files/directories.

Viewing File Contents

- cat <file> – Displays the content of a file.
- less <file> – Views file content page by page.
- head <file> – Shows the first 10 lines of a file.
- tail <file> – Shows the last 10 lines of a file.

System Information

- uname -a – Displays system information.
- df -h – Shows disk space usage in human-readable format.
- free -h – Displays memory usage.
- top – Displays running processes and system performance.

User Management

- whoami – Shows the currently logged-in user.
- id – Shows user ID and group information.

Searching and Finding Files

- find <directory> -name <filename> – Searches for files by name.
- grep <pattern> <file> – Searches for a pattern in a file.

Package Management

- Ubuntu/Debian: sudo apt install <package> – Installs a package.
- CentOS/Fedora: sudo yum install <package> or sudo dnf install <package>

Did You Know?

- Many hacking and cybersecurity tools, like Kali Linux, are based on Linux.
- NASA uses Linux for space missions because of its reliability and flexibility.

6.4.2. sudo Usage

- sudo stands for SuperUser DO.
- It allows a normal user to execute commands with administrative (root) privileges.
- Required for commands that modify system settings, install software, or manage users.

Example Commands with sudo:

- sudo apt update – Updates package lists (Ubuntu/Debian).
- sudo apt upgrade – Upgrades installed packages.
- sudo useradd monika – Creates a new user named "monika".
- sudo reboot – Restarts the system.

Important Points about sudo:

- Requires the user to enter their password.
- Prevents accidental system-wide changes by limiting administrative access.
- Logs all commands executed with sudo for security auditing.

Advantages of sudo:

- Provides controlled administrative access without logging in as root.
- Improves system security by limiting full root access.
- Tracks administrative actions for accountability.

Disadvantages of sudo:

- Misuse of sudo commands can damage the system.
- Beginners may accidentally execute dangerous commands with elevated privileges.

Real-Life Example:

When installing software on Ubuntu, typing apt install alone will fail. Using sudo apt install gives the necessary permission to complete the task.

Assignment 6.2.

1. What is the role of the sudo command in Linux?
2. Differentiate between Ubuntu and CentOS.

Practical Activity 6.1: Installing Linux Using Virtual Machine

Objective: To install a Linux operating system (e.g., Ubuntu) in a virtual environment using VirtualBox or VMware.

Materials Required:

- Computer with at least 4 GB RAM
- VirtualBox or VMware Workstation Player installed
- Linux ISO file (e.g., Ubuntu Desktop)
- USB or internet connection (for downloading ISO and updates)

Procedure:

Step 1: Launch Virtual Machine Software
- Open VirtualBox or VMware on your computer.

Step 2: Create a New Virtual Machine
- Click New to create a new VM.
- Enter a name (e.g., Ubuntu VM), type as Linux, and version as the specific distribution (e.g., Ubuntu 64-bit).

Step 3: Allocate Memory (RAM)
- Assign RAM (at least 2 GB recommended for Ubuntu).

Step 4: Create a Virtual Hard Disk
- Select Create a virtual hard disk now.
- Choose VDI (VirtualBox Disk Image) or the default option.
- Set dynamically allocated or fixed size (at least 20 GB recommended).

Step 5: Attach ISO File
- Go to Settings → Storage → Optical Drive and attach the downloaded Linux ISO file.

Step 6: Start the Virtual Machine
- Click Start. The VM will boot from the ISO file.

Step 7: Begin Linux Installation
- Choose Install Linux in the boot menu.
- Select language, keyboard layout, and time zone.

Step 8: Disk Partitioning
- Select Erase disk and install Linux (for beginners).
- For advanced users, choose Manual partitioning for custom setup.

Step 9: Create User Account
- Enter a username, password, and computer name/hostname.
- Optionally enable automatic login.

Step 10: Installation Process
- Click Install Now. Wait for files to be copied and the system configured.

Step 11: Restart the Virtual Machine
- After installation, remove the ISO from the virtual drive.
- Click Restart Now to boot into the new Linux system.

Step 12: Post-Installation Setup

- Update the system using the terminal:
  - sudo apt update
  - sudo apt upgrade
- Install additional applications if required.

Observation:

- The Linux OS should boot successfully in the virtual machine.
- You can log in with the created user account and explore the desktop and terminal.

Conclusion:

- The student successfully installed Linux on a virtual machine without affecting the host operating system.
- The VM allows experimenting with Linux commands, software, and system settings safely.

Practical Activity 6.2: Practicing Linux Terminal Commands

Objective: To practice basic Linux terminal commands such as ls, cd, cp, mv, chmod, and sudo.

Materials Required:

- Computer with Linux installed (real or virtual machine, like Ubuntu)
- Terminal access

Procedure:

Step 1: Open the Terminal

- Press Ctrl + Alt + T or open the terminal from the applications menu.

Step 2: Check Current Directory

- Use the command: pwd
- Note the current working directory.

Step 3: List Files and Directories

- List all files in the current directory: ls
- List files with details: ls -l

Step 4: Change Directory

- Navigate to another directory: cd <directory_name>
- Move back to the home directory: cd ~

Step 5: Create and Copy Files/Directories

- Create a new directory: mkdir TestDir
- Create a new file inside the directory: touch TestDir/file1.txt
- Copy a file: cp TestDir/file1.txt TestDir/file2.txt
- Move/rename a file: mv TestDir/file2.txt TestDir/file3.txt

Step 6: Change File Permissions

- Check file permissions: ls -l TestDir
- Give execute permission to a file: chmod +x TestDir/file1.txt
- Remove write permission from others: chmod o-w TestDir/file1.txt

Step 7: Using sudo for Administrative Tasks

- Update system package list (requires sudo): sudo apt update
- Upgrade packages: sudo apt upgrade

Note: Enter your user password when prompted.

Step 8: Delete Files and Directories

- Delete a file: rm TestDir/file3.txt
- Delete a directory: rm -r TestDir

Observation:

- Students should see the results of each command reflected immediately in the terminal.
- Permissions, file creation, copying, and movement should function as expected.

Conclusion:

- The student successfully practiced basic Linux commands and learned to manage files, directories, and permissions.
- Using sudo allows performing administrative tasks safely.

Practical Activity 6.3: Simulating Admin Tasks with Root Privileges

Objective: To practice performing administrative tasks in Linux using root privileges and the sudo command.

Materials Required:

- Computer with Linux installed (real or virtual machine-like Ubuntu)
- Terminal access

Procedure:

Step 1: Open the Terminal

- Press Ctrl + Alt + T or open the terminal from the applications menu.

Step 2: Switch to Root User (Optional)

- Switch to root using: sudo -i
- Enter your user password when prompted.

Step 3: Update and Upgrade System

- Update the package list: sudo apt update
- Upgrade installed packages: sudo apt upgrade

Step 4: Create a New User with Administrative Privileges

- Add a new user: sudo adduser student1
- Add the user to the sudo group: sudo usermod -aG sudo student1

Step 5: Manage File Permissions

- Create a directory accessible only to root:
  - sudo mkdir /root/TestAdmin
- Change ownership and permissions:
  - sudo chown root: root /root/TestAdmin
  - sudo chmod 700 /root/TestAdmin

Step 6: Install Software Using Sudo

- Install a package (example: tree for viewing directory structure): sudo apt install tree

Step 7: Start/Stop a Service

- Check the status of a service (example: ssh): sudo systemctl status ssh
- Stop the service: sudo systemctl stop ssh
- Start the service: sudo systemctl start ssh

Step 8: Reboot and Shutdown the System

- Reboot the system: sudo reboot
- Shutdown the system: sudo shutdown now

Observation:

- Students should notice that commands requiring root privileges fail without sudo.
- Using sudo or root access allows performing administrative tasks like user management, software installation, and service control.

Conclusion:

- The student successfully simulated administrative tasks using root privileges in Linux.
- Proper use of sudo ensures system security while allowing authorized administrative operations.

Summary

- Linux is an open-source operating system widely used for servers, desktops, and embedded systems.
- It is known for its stability, security, and flexibility compared to many other operating systems.

- Popular Linux distributions include Ubuntu, which is user-friendly, and CentOS, which is enterprise-focused.
- The Linux file system is organized hierarchically, starting from the root ("/") directory.
- Important directories include /home for user files, /etc for configuration, /bin for essential commands, and /var for logs.
- Permissions in Linux define who can read, write, or execute files and are controlled for users, groups, and others.
- Linux installation can be done on physical machines or virtual machines, making it easy to test without affecting the host system.
- Basic Linux commands such as ls, cd, cp, and chmod are essential for file and directory management.
- The sudo command allows users to perform administrative tasks with root privileges securely.
- Linux is widely used in servers, cloud environments, and supercomputers due to its performance and scalability.

ASSESSMENT

A. Multiple Choice Questions

1. Linux was first developed by:
   a) Bill Gates
   b) Linus Torvalds
   c) Steve Jobs
   d) Dennis Ritchie

2. The root directory in Linux is denoted by:
   a) \
   b) /
   c) C:
   d) //

3. Which command is used to list files in a directory?
   a) pwd
   b) ls
   c) cd
   d) mkdir

4. Which of the following commands changes file permissions?
   a) chmod
   b) chown
   c) ls
   d) mv

5. The default package manager for Ubuntu/Debian is:
   a) yum
   b) apt
   c) rpm
   d) dnf

6. Which command is used to switch to the root user?
   a) su

b) pwd
c) mkdir
d) ls

7. Which directory stores a user personal files in Linux?
   a) /etc
   b) /bin
   c) /home
   d) /dev

8. What is the use of the sudo command?
   a) List files
   b) Execute commands with administrative privileges
   c) Change directories
   d) Delete files

9. Ubuntu is based on which Linux distribution?
   a) Red Hat
   b) Debian
   c) Fedora
   d) CentOS

10. Which command is used to display the current directory?
    a) ls
    b) pwd
    c) cd
    d) mkdir

B. Fill-in-the-blanks

1. The Linux kernel was created by _____.
2. The root directory is represented by the symbol _____.
3. Command to create a new directory is _____.
4. Command to remove a file is _____.
5. Ubuntu uses the _____ package manager.
6. To view file permissions in Linux, the command _____ is used.
7. To switch to superuser or root, the command _____ is used.
8. Linux is a _____-user and _____-tasking operating system.
9. Command to copy a file is _____.
10. The directory that contains system configuration files is _____.

C. True/False questions

1. Linux is an open-source operating system.
2. Windows uses the root directory /.
3. The command cd is used to change directories in Linux.
4. The sudo command allows normal users to run commands as root.

5. CentOS is based on Debian.
6. The /home directory stores system binaries.
7. The command chmod is used to change file permissions.
8. Linux can only be used on servers.
9. The ls command lists files and directories.
10. apt is used to manage packages in Ubuntu.

D. Short Questions

1. Who created Linux and in which year?
2. What is the root directory in Linux?
3. Name any three basic Linux commands for file management.
4. What is the use of the sudo command?
5. Name two popular Linux distributions.
6. Which directory contains user files in Linux?
7. How do you view the permissions of a file in Linux?
8. What is the difference between the cp and mv commands?
9. Explain the multi-user and multitasking features of Linux.
10. How can a user switch to root in Linux?

Answer Key

A. Multiple Choice Questions

1. b), 2. b), 3. b), 4. a), 5. b), 6. a), 7. c), 8. b), 9. b), 10. b)

B. Fill-in-the-blanks

1. Linus Torvalds, 2. /, 3. Mkdir, 4. rm, 5. apt, 6. ls -l, 7. sudo or su, 8. multi-user, multi-tasking, 9. cp, 10. /etc

C. True/False questions

1. True, 2. False, 3. True, 4. True, 5. False, 6. False, 7. True, 8. False, 9. True, 10. True

PSS Central Institute of Vocational Education

[A constituent unit of NCERT, under the Ministry of Education, Government of India)

Shyamla Hills, Bhopal - 462 002, Madhya Pradesh, India

www.psscive.ac.in