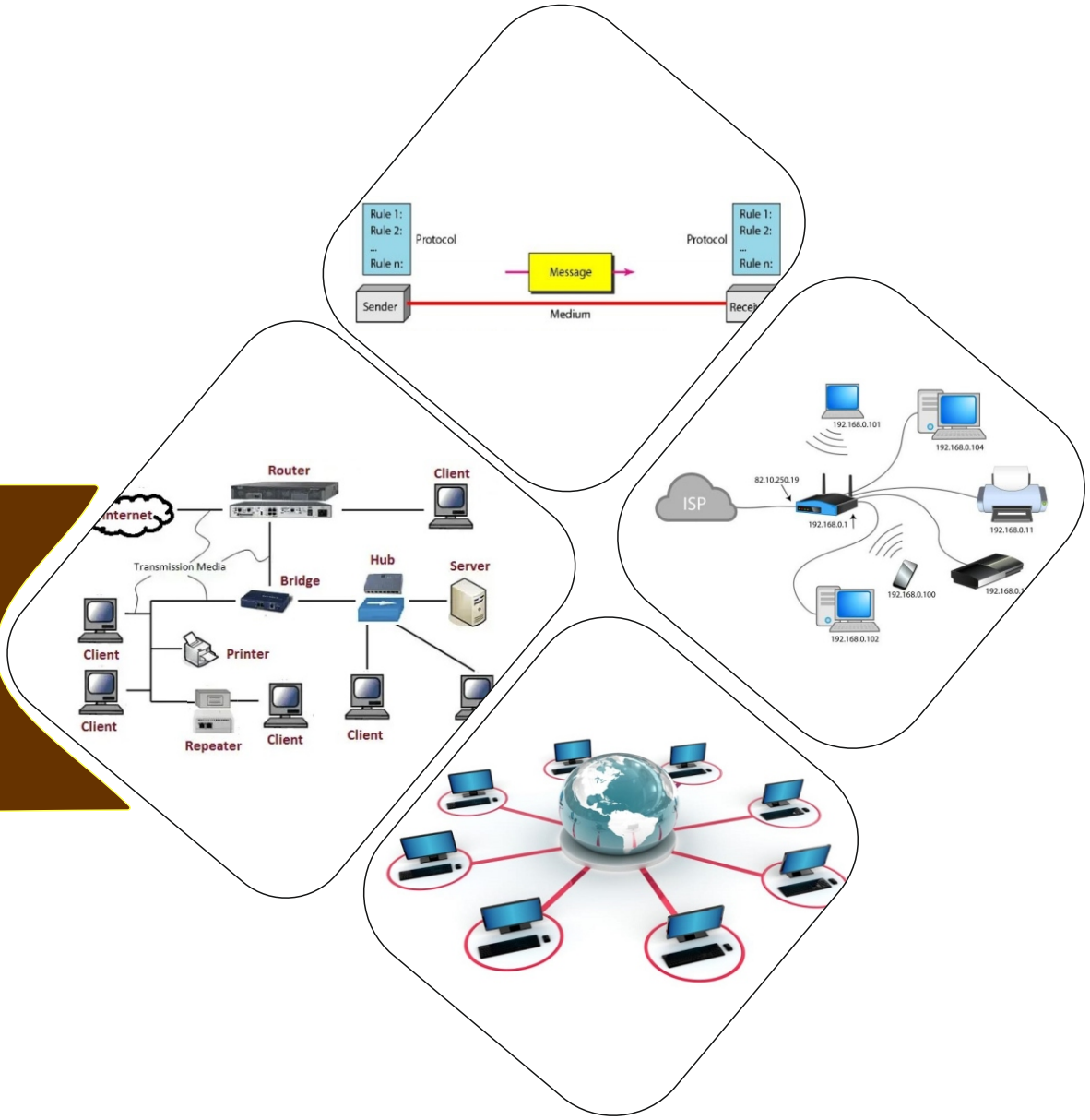
SCHEME :K

Name :_____
Roll No.:_____ Year : 20 ___ 20 __
Exam Seat No. :_____

LABORATORY MANUAL FOR

COMPUTER NETWORK & DATA COMMUNICATION (316338)



ELECTRONICS ENGINEERING GROUP

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI
(Autonomous)(ISO21001:2018)(ISO/IEC27001:2013)

Vision

To ensure that the Diploma level Technical Education constantly matches the latest requirements of Technology and industry and includes the all-round personal development of students including social concerns and to become globally competitive, technology led organization.

Mission

To provide high quality technical and managerial manpower, information and consultancy services to the industry and community to enable the industry and community to face the challenging technological & environmental challenges.

Quality Policy

We, at MSBTE are committed to offer the best in class academic services to the students and institutes to enhance the delight of industry and society. This will be achieved through continual improvement in management practices adopted in the process of curriculum design, development, implementation, evaluation and monitoring system along with adequate faculty development programmes.

Core Values

MSBTE believes in the following:

- Skill development in line with industry requirements
- Industry readiness and improved employability of Diploma holders
- Synergistic relationship with industry
- Collective and Cooperative development of all stake holders
- Technological interventions in societal development
- Access to uniform quality technical education

A Laboratory Manual

for

Computer Network and Data Communication

(316338)

Semester-VI

DE/ EJ/ ET/ EX/ IE/ TE

Maharashtra State Board of Technical Education, Mumbai

(Autonomous) (ISO 21001:2018) (ISO/IEC 27001:2013)

Maharashtra State Board of Technical Education, Mumbai
(Autonomous) (ISO 21001:2018) (ISO/IEC 27001:2013)
4th Floor, Government Polytechnic Building 49, Kherwadi, Bandra (East), Mumbai – 400051

Maharashtra State Board of Technical Education

Certificate

This is to certify that Mr./Ms. ……..…… Roll No …… of the Sixth Semester of Diploma in ……..……..…… of the Institute ……..……..…… (Code ……..) has attained pre-defined practical outcomes (PROs) satisfactorily in course **Computer Network and Data Communication (316338)** for the academic year 20… - 20…. as prescribed in the curriculum.

Place ……. Enrollment No……

Date: …..... Exam Seat No. ……..…..

Course Teacher **Head of the Department** **Principal**

Seal of Institute

Preface

The primary focus of any engineering laboratory/field work in the technical education system is to develop the much needed industry relevant competencies and skills. With this in view, MSBTE embarked on this innovative 'K' Scheme curricula for engineering diploma programmes with outcome- based education as the focus and accordingly, a relatively large amount of time is allotted for the practical work. This displays the great importance of laboratory work, making each teacher, instructor and student realize that every minute of the laboratory time needs to be effectively utilized to develop these outcomes, rather than doing other mundane activities. Therefore, for the successful implementation of this outcome-based curriculum, every practical has been designed to serve as a ***'vehicle'*** to develop this industry identified competency in every student. The practical skills are difficult to develop through 'chalk and duster' activity in the classroom situation. Accordingly, the 'K' scheme laboratory manual development team designed the practicals to ***focus*** on the ***outcomes***, rather than the traditional age old practice of conducting practicals to 'verify the theory' (which may become a byproduct along the way).

This laboratory manual is designed to help all stakeholders, especially the students, teachers and instructors to develop in the student the predetermined outcomes. It is expected from each student that at least a day in advance, they have to thoroughly read through the concerned practical procedure that they will do the next day and understand the minimum theoretical background associated with the practical. Every practical in this manual begins by identifying the competency, industry relevant skills, course outcomes and practical outcomes which serve as a key focal point for doing the practical. The students will then become aware about the skills they will achieve through the procedure shown there and necessary precautions to be taken, which will help them to apply in solving real-world problems in their professional life.

This manual also provides guidelines to teachers and instructors to effectively facilitate student-centered lab activities through each practical exercise by arranging and managing necessary resources in order that the students follow the procedures and precautions systematically ensuring the achievement of outcomes in the students.

Computer Network and Data Communication focus on the exchange of data and information between computers and devices over various types of networks. It forms the backbone of modern communication systems, enabling seamless connectivity for applications such as online education, e-banking, e-governance, cloud computing, and social networking. Diploma Engineers should be capable of designing, selecting, configuring, troubleshooting, and maintaining different types of computer networks used in industries and organizations.

This manual provides essential theoretical concepts and practical techniques related to computer networks and data communication, empowering students to analyze, manage, and troubleshoot real-world networking systems effectively.

Programme Outcomes (POs) to be achieved through Practical of this Course

Following programme outcomes are expected to be achieved through the practical of this course.

PO1: Basic and Discipline specific knowledge: Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the broad based Electronics engineering problems.

PO2: Problem analysis: Identify and analyze broad based Electronics engineering problems using codified standard methods.

PO3: Design/ development of solutions: Design solutions for broad based technical problems and assist with the design of Electronics system's components or processes to meet specified needs.

PO4: Engineering Tools, Experimentation and Testing: Apply modern Electronics engineering tools and appropriate technique to conduct standard tests and measurements.

PO5: Engineering practices for society, sustainability and environment: Apply appropriate Electronics technology in context of society, sustainability, environment and ethical practices.

PO6: Project Management: Use Electronics engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about broad based engineering activities.

PO7: Life-long learning: Ability to analyze individual needs and engage in updating in the context of Electronics technological changes.

List of Industry Relevant Skills

This course aims to help the student to attain the following industry – identified outcomes by undertaking the laboratory work suggested in this practical manual, 'Maintain and troubleshoot network devices'.

1. Identify and explain the components, devices, topologies, and classifications of computer networks used in data communication systems.
2. Identify, configure, and test various network models, transmission media, and switching techniques for efficient data communication.
3. Implement and verify flow control and error control techniques such as Stop-and-Wait, ARQ, CRC, and Hamming code for reliable data transmission.
4. Identify and configure IPv4 and IPv6 addressing schemes according to network requirements.
5. Configure and verify Application Layer services such as DNS, Email (SMTP/POP/IMAP), FTP and Telnet for efficient network communication.

Guidelines to Teachers

1. Teacher should provide the guideline with demonstration of practical to the students with all features.
2. Teacher shall explain prior concepts to the students before starting of each practical.
3. Involve students in the performance of each practical.
4. Teacher should ensure that the respective skills and competencies are developed in the students after the completion of the practical exercise.
5. Teachers should give opportunities to students for hands-on experience after the demonstration.
6. Teacher is expected to share the skills and competencies to be developed in the students.
7. Teacher may provide additional knowledge and skills to the students even though not covered in the manual but are expected from the students by the industry.
8. Finally give practical assignments and assess the performance of students based on task assigned to check whether it is as per the instructions.
9. Teacher is expected to refer complete curriculum document and follow guidelines for implementation.
10. At the beginning of the practical, which is based on the simulation, teacher should make the students acquainted with simulation software environment.
11. Teacher should utilize projector to demonstrate the procedure for software installation / application to the group of students.

Instructions for Students

1. Listen carefully to the lecture given by the teacher about course, curriculum, learning structure, skills to be developed.
2. Organize the work in the group and make a record of all observations.
3. Do the calculations and plot the graph wherever it is required in the practical.
4. Students shall develop maintenance skills as expected by industries.
5. Student shall attempt to develop related hand-on skills and gain confidence.
6. Student shall develop the habits of evolving more ideas, innovations, skills etc. those included in scope of manual.
7. Student should develop the habit to submit the practical on date and time.
8. Student should prepare well while submitting a write-up of exercise.
9. Attach / paste separate papers wherever necessary.

Practical Course Outcome Matrix

Course Outcomes (COs)

CO1	Implement relevant Network Topology
CO2	Select relevant network model and Transmission Media for data communication system
CO3	Troubleshoot transmission errors and flow control of the data in Data Link Layer
CO4	Maintain Network layer and Transport layer
CO5	Interprete functions of Application layer and Protocols associated with it

Sr. No.	Title of the Experiment	CO1	CO2	CO3	CO4	CO5
1	*Installation and introduction of Cisco Packet Tracer	✓				
2	Installation and introduction GNS3 software simulator tools	✓				
3	Identify the topology used in the computer lab	✓				
4	*Simulation of Mesh topology	✓				
5	*Simulation of Star topology	✓				
6	Simulation of Tree topology	✓				
7	*Share resources in a computer network	✓				
8	Configuring VPN (Virtual Private Network) using simulator	✓				
9	Installation of Repeater and Bridge	✓				
10	*Troubleshoot computer network using given commands		✓			
11	*Troubleshoot computer network using given commands		✓			
12	*Prepare a standard network straight cable by using crimping tool		✓			
13	*Create cross-over network straight cable by using crimping tool		✓			
14	*Use PDU tool to analyse layers of OSI Model		✓			
15	Implementation of the Hamming code using C programming language to detect error			✓		
16	*Implementation of Hamming code using C programming language to correct error			✓		

17	Implement C Program for CRC			✓		
18	*Use PPP Protocol to establish a direct connection between two PCs			✓		
19	Measure types of transmission delays using CISCO Packet Tracer				✓	
20	Installation of Modem and Router				✓	
21	Implement IPv6 addressing scheme on a network				✓	
22	*Implement IP addresses for intranet in Class A, Class B, Class C				✓	
23	Configuration and Testing of basic Firewall					✓
24	*Use the FTP protocol to transfer files from one system to another system.					✓
25	*Use of Packet tracer as packet sniffer					✓
26	*Implementation of SMTP protocol using CISCO packet tracer					✓
27	Filter ARP and ICMP packets Traffic using network simulation software					✓
28	Configuration of POP3 protocol using CISCO Packet Tracer					✓
29	Configuration of a Web Server (HTTP/HTTPS) using CISCO Packet tracer					✓
30	*Configuration DNS Server using CISCO Packet Tracer					✓

Content Page

List of Practical and Formative Assessment Sheet

Sr. No.	Title of the practical	Page No.	Date of Performance	Date of Submission	Assessment Marks (25)	Dated Sign of Teacher	Remark (if any)
17	Implement C Program for CRC	139					
18	*Use PPP Protocol to establish a direct connection between two PCs	149					
19	Measure types of transmission delays using CISCO Packet Tracer	159					
20	Installation of Modem and Router	171					
21	Implement IPv6 addressing scheme on a network	183					
22	*Implement IP addresses for intranet in Class A, Class B, Class C	193					
23	Configuration & Testing of basic Firewall	205					
24	*Use the FTP protocol to transfer files from one system to another system.	219					
25	*Use of Packet tracer as packet sniffer	231					
26	*Implementation of SMTP protocol using CISCO packet tracer	243					
27	Filter ARP and ICMP packets Traffic using network simulation software	255					
28	Configuration of POP3 protocol using CISCO Packet Tracer	267					
29	Configuration of a Web Server (HTTP/HTTPS) using CISCO Packet tracer	279					
30	*Configuration DNS Server using CISCO Packet Tracer	291					
				TOTAL			

Note: Out of above suggestive LLOs-

- '*' Marked Practical (LLOs) are mandatory.
- Minimum 80% of above list of lab practical are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

Practical No.1: *Installation and Introduction of Cisco Packet Tracer

I. Practical Significance

This practical enables student to install and use Cisco Packet Tracer for creating and analyzing network topologies. It helps in understanding network configuration, troubleshooting, and maintenance, bridging theory with real-world networking applications.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcomes

LLO 1.1 Install packet tracer tools and workspaces.

LLO 1.2 Place and connect network devices (PCs, switches and routers).

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco Systems. It allows users to design, configure, and troubleshoot network topologies without requiring physical hardware. It supports routers, switches, PCs, servers, wireless devices, and IoT components. Packet Tracer helps in visualizing packet flow and learning networking concepts like IP addressing, routing, and switching.

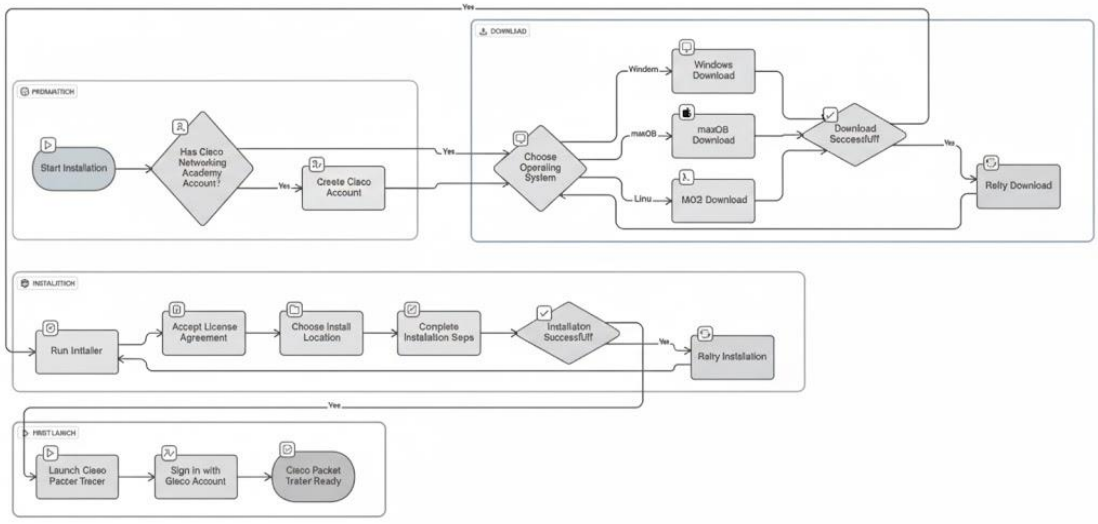


Fig. 1.1: Cisco Packet Tracer Installation Process

Key Features

- Virtual simulation of Cisco devices.
- Supports configuration using CLI (Command Line Interface).
- Offers real-time and simulation modes.
- Enables IoT and programming integration (IoT mode, Python).
- Supports multi-user collaboration.

IP Address

An IP Address (Internet Protocol Address) is a unique numerical identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication. It acts like a digital address that allows devices to locate and communicate with each other over a network.

Purpose of an IP Address

- To identify a device on the network.
- To locate where that device is within the network.
- To enable communication between devices over the Internet or LAN.

Ping Command

Ping (Packet Internet groper): The ping command is the basic troubleshooting tool for TCP/IP. It is a command used to verify the network connectivity of a computer. It uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply. This command is used to test a machine‘s connectivity to another system and to verify that the target system is active. Usually, this command is the first step to any troubleshooting if a connectivity problem is occurring between two computers. The Ping utility executes an end-to-end connectivity test to other devices and obtains the round-trip time between source and destination device. Ping uses the ICMP Echo and Echo Reply packets to test connectivity. Excessive usage may appear to be a denial of service (DoS) attack.

Syntax: ping <ip address>

Example

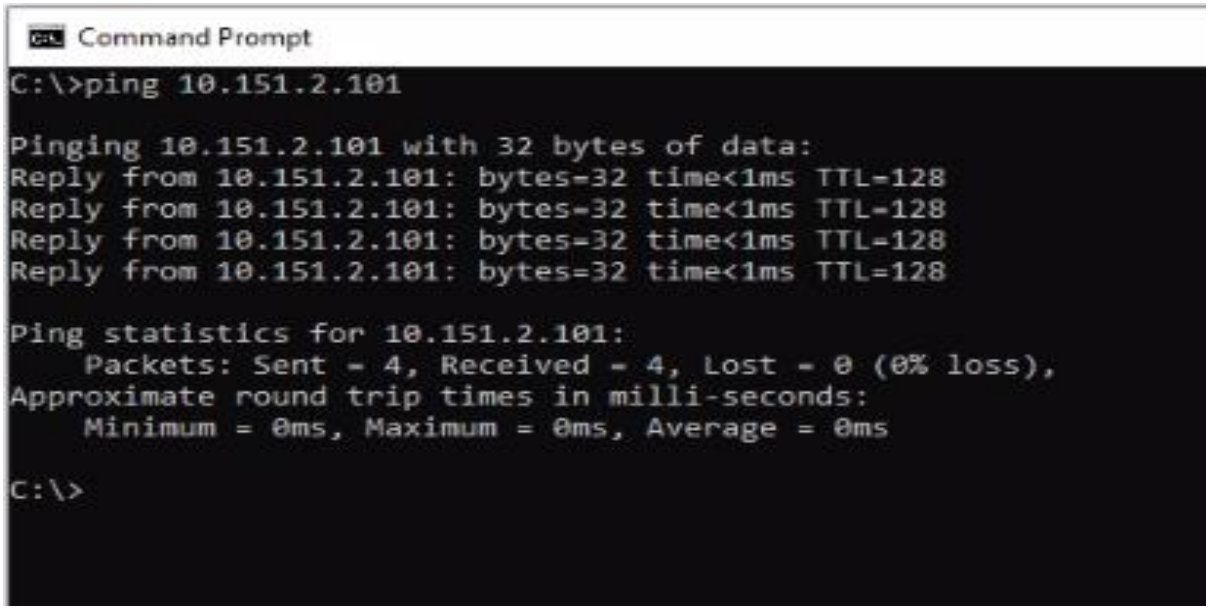


Fig. 1.2: Output of ping command

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

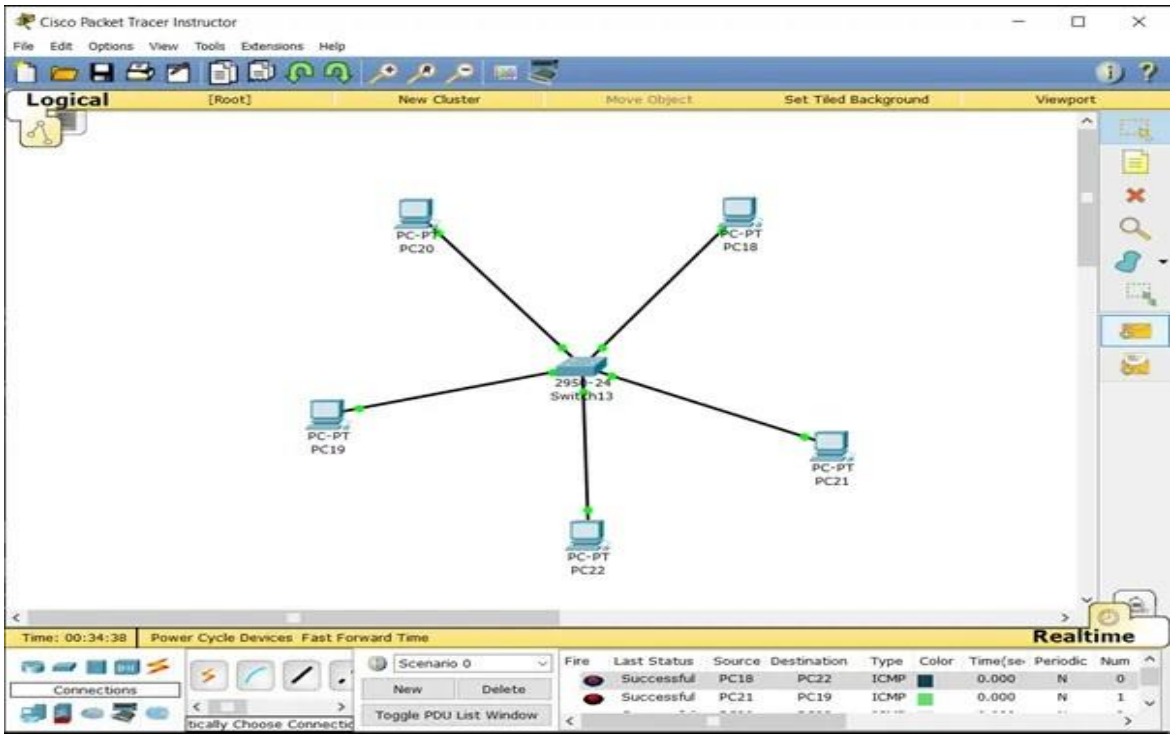


Fig. 1.3: Simulation of Star Topology

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 1.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that the system meets the minimum requirements before installation.
2. Download Cisco Packet Tracer only from the official Cisco Networking Academy website to avoid security risks.

X. Suggested Procedure

1. Prerequisites

Before installation, make sure computer system have:

- A computer running Windows 10/11or Linux (Ubuntu) or macOS.
- At least 2 GB RAM and 1 GB free disk space.
- A Cisco Networking Academy account (free registration required).

2. Create a Cisco NetAcad Account (if you don't have one)

- Go to https://www.netacad.com/
- Click on Login button.
- Click Sign Up button.
- Create a new Cisco Networking Academy account.
- Fill in your details (Name, Email, Password, etc.).
- Verify your email and log in to your account.

3. Download Cisco Packet Tracer

- After login into Cisco Networking Academy, open: https://www.netacad.com/portal/resources/packet-tracer
- Select the Operating System: Windows (64-bit / 32-bit)
- Click Download Packet Tracer to get the installer file.

4. Install on Windows 10/11

- Locate the downloaded file (e.g., PacketTracer8.2.2-setup.exe).

- Double-click to run the installer.
- When prompted, click yes to allow installation.
- Click Next.
- Accept the License Agreement.
- Choose the Destination Folder (default is fine).
- Click Install.
- Wait for installation to complete.
- Click Finish when done.

5. Launch Cisco Packet Tracer

- Go to Start Menu → Cisco Packet Tracer.
- On first launch, you'll be asked to log in using your Netcad credentials.
- After successful login, the Packet Tracer workspace will open.

6. Create a Simple Test Network

- Drag and drop two PCs from the "End Devices" section into the workspace.
- Drag and drop a switch (e.g., 2960) into the workspace.
- Select the Connection tool (Lightning icon) → choose Copper Straight-Through Cable.
- Connect:
  PC0 → FastEthernet0 to Switch → FastEthernet0/1
  PC1 → FastEthernet0 to Switch → FastEthernet0/2

7. Assign IP Addresses

- Click on PC0 → Desktop → IP Configuration
  Set IP: 192.168.1.1
  Subnet Mask: 255.255.255.0
- Click on PC1 → Desktop → IP Configuration
  Set IP: 192.168.1.2
  Subnet Mask: 255.255.255.0

8. Test Network Connectivity

- Click PC0 → Desktop → Command Prompt
- Type: ping 192.168.1.2
- Press Enter
- Expected Output: Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

9. Save the Project

- Click File → Save project As
- Save the file with proper filename and extension, for example: Test_Network.pkt.

10. Simulation

- Switch to Simulation Mode (bottom right corner).
- Send a ping packet again and observe the packet movement animation between the devices.

XI. Resources used during performance

Table 1.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.
6.
7.

XIII. Observation Table

NA

XIV. Results

……..…

……...……...…

XV. Interpretation of results

……..…….

……...……...…

XVI. Conclusions and Recommendations

……..……

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of Cisco Packet Tracer.
2. List steps to install Cisco Packet Tracer.
3. List the components available in the Packet Tracer workspace.
4. Explain the procedure to test connectivity between two PCs.

[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.netacad.com/cisco-packet-tracer	Cisco Packet Tracer Software Simulator
2	https://www.youtube.com/watch?v=cgLfAWO0IkI	Cisco Packet Tracer Installation process

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Successful installation of Packet Tracer	10%
2	Identification of Packet Tracer Simulator components	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Create a simple network topology	10%
2	Demonstrate device configuration and connections	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.2: Installation and Introduction of GNS3 Software Simulator Tools

I. Practical Significance

This practical enables student to install and use GNS3 Software Simulator for designing, configuring, and analyzing complex network topologies in a virtual environment. Through GNS3, learners gain hands-on experience with enterprise-grade network devices such as routers, switches, modems, and repeaters, allowing them to simulate real-world networking scenarios without the need for physical hardware.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcomes

LLO 2.1 Install GNS3 software simulator tools.

LLO 2.2 Place and connect network devices (PCs, switches and routers).

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

GNS3 (Graphical Network Simulator 3) is an open-source network simulation tool that allows users to emulate real network hardware such as Cisco routers, switches, and firewalls. It provides a virtual environment for testing and verifying network configurations before real-world deployment.GNS3 supports integration with Virtual Box, VMware, and Dockers to simulate hybrid and cloud-based networks. It is widely used for CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional), and network engineering training.

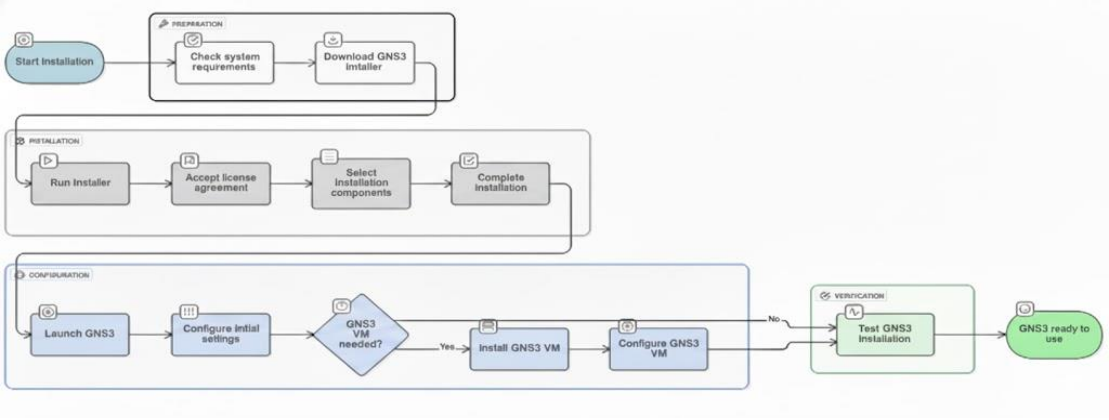


Fig. 2.1: GNS3 Installation Process

Key difference between Cisco Packet Tracer and GNS3

Sr. No.	Feature	Cisco Packet Tracer	GNS3
1	Purpose	Learning and practice for beginners.	Real-world network testing and advanced labs.
2	Device Support	Supports only Cisco devices such as routers, switches, PCs, servers, IoT devices.	Supports multi-vendor devices –Cisco, Juniper, Fortinet, Palo Alto, etc.
3	Real IOS Support	Does not support real Cisco IOS images	Supports real IOS, IOU images for accurate emulation.
4	Hardware Integration	Limited; cannot connect easily with real hardware or external devices.	Can be integrated with real routers, switches, and physical network interfaces.
5	Automation / Scripting	Limited scripting or automation support.	Supports Python, API integration, Ansible, and other automation tools.
6	Integration with Other Tools	Does not integrate with third-party tools or VMs.	Integrates with Wireshark, VirtualBox, VMware, Docker, and cloud services.
7	Licensing	Free but requires Cisco Networking Academy login.	Completely free and open-source.
8	Scalability	Suitable for small to medium network topologies.	Supports very large and complex enterprise-level topologies.

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

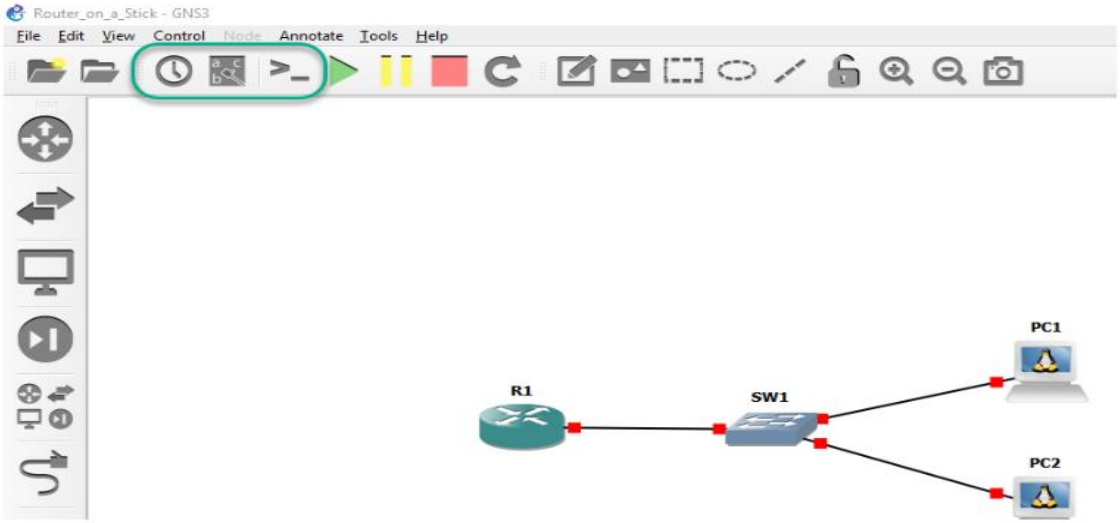


Fig. 2.2: Simulation using GNS3

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 2.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that the system meets the minimum requirements before installation.
2. Download GNS3 only from the official website to avoid installation errors and security issues.

X. Suggested Procedure

1. Prerequisites

Before installation, make sure computer system have:

- A computer running Windows 10/11 or Linux (Ubuntu), or macOS.
- Minimum 4 GB RAM (8 GB recommended) and 2 GB free disk space.
- Administrative privileges on your computer.

2. Create a GNS3 Account (if you don't have one)

- Go to https://gns3.com

- Click Sign Up in the top-right corner.
- Left click on Create Account (button).
- Fill in the registration form with your details (email, password, etc.).
- Verify your email and Log in to your GNS3 account.

3. Download GNS3

- After logging in, visit the official download page: https://gns3.com/software/download
- Select the Operating System: Windows (64-bit / 32-bit)
- Left click on "Download (button).
- Save the installer file to your computer.

4. Install GNS3 on Windows 10 or 11

- Locate the downloaded installer file.
- Right-click the file → Run as Administrator.
- When prompted by User Account Control, click yes.
- Click Next to begin installation.
- Accept the License Agreement and click next.
- Choose the default installation location or select a custom folder.
- When asked to install Wireshark, WinPcap/Npcap, or Solar Winds Response Time Viewer, click Yes (recommended).
- Wait for all components to install.
- Click Finish to complete installation.

5. Launch GNS3

- Go to Start Menu → GNS3 → GNS3 (GUI).
- On first launch, the Setup Wizard will appear.
- Choose: Run appliances on my local computer (for beginners).

6. Create a Simple Test Network

- In the Devices Toolbar, drag and drop two VPCS (Virtual PCs**)** and one Ethernet Switch into the workspace.
- Use the Connection Tool (Cable Icon) to connect.
  PC0 → FastEthernet0 to Switch → FastEthernet0/1
  PC1 → FastEthernet0 to Switch → FastEthernet0/2

7. Assign IP Addresses

- Right-click on PC1 → Console
- Type the following commands
- ip 192.168.1.1/24
- Press Enter
- Right-click on PC2 → Console
- ip 192.168.1.2/24
- Press Enter

8. Test Network Connectivity

- In the PC1 Console, type:
- Type: ping 192.168.1.2
- Press Enter
- System output ‘84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=1.2 ms’

9. **Save the Project**
    - Click File → Save Project As
    - Save the file with proper filename and extension, for example: Test_Network.gns3.
10. **Simulation**
    - Switch Click Start/Resume all devices (green play button).
    - Observe packet flow in the console.
    - Stop all devices when testing is complete.

XI. Resources used during performance

Table 2.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.

XIII. Observation Table

NA

XIV. Results

……..…

……...……...……

XV. Interpretation of results

……..……

……...……...……

XVI. Conclusions and Recommendations

……..……

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of GNS3 software in network simulation.
2. List the steps to install GNS3.
3. Differentiate between GNS3 and Cisco Packet Tracer.
4. Explain the components of the GNS3 interface.

[Space for Answers] (If required attach separate page)

……..…

……..…

……..…

……..…

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.gns3.com	GNS3 Software Simulator
2	https://www.youtube.com/watch?v=lCOUvksX8Xo	GNS3 Installation process

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Successful installation of GNS3	10%
2	Identification of GNS3 Simulator components	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Create a simple network topology	10%
2	Demonstrate device configuration and connections	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.3: Identify the Topology Used in the Computer Lab

I. Practical Significance

This practical enables student to physically identify, trace, and connect network components such as computers, switches, and routers to determine the topology used in the computer lab. Through hands-on observation, learners practice handling cables and devices, mapping network layouts, and verifying connectivity between components. It also develops the ability to use basic networking tools and techniques to test links and confirm the logical structure of the network, thereby strengthening practical skills in network installation, configuration, and troubleshooting.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 2.1 Analyse the type of network topology used in your lab.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A network topology refers to the arrangement or layout of various elements (links, nodes, and devices) in a computer network. It defines how computers, switches, routers, and other devices are physically and logically interconnected to enable communication and data exchange. Understanding network topology is fundamental for designing efficient networks, troubleshooting connectivity issues, and ensuring scalability and fault tolerance.

Types of Network Topologies

1. **Star Topology**
   - All devices are connected to a central device, usually a switch or hub.
   - The central device manages data transmission.
   - **Advantages:** Easy to manage, isolate faults, and add/remove devices without disrupting the network.
   - **Disadvantages:** Central device failure causes the whole network to fail.
2. **Bus Topology**
   - All devices are connected to a single central cable (backbone).
   - Data travels along the backbone to the intended device.
   - **Advantages:** Simple design, requires less cabling.

- **Disadvantages:** Backbone failure disrupts the network; troubleshooting is difficult in large networks.

3. **Ring Topology**
   - Devices are connected in a circular fashion. Data travels in one or both directions.
   - **Advantages:** Predictable data transmission; minimal collisions.
   - **Disadvantages:** Single device failure can disrupt communication.
4. **Mesh Topology**
   - Every device is connected to all other devices.
   - **Advantages:** Highly fault-tolerant; provides redundancy.
   - **Disadvantages:** Complex and requires more cabling.
5. **Hybrid Topology**
   - Combines two or more topologies to utilize the benefits of each.

Switch

A switch is a networking device that connects multiple devices (computers, printers, servers) within a local area network (LAN) and enables them to communicate efficiently. It operates primarily at the Data Link Layer (Layer 2) of the OSI model, though some switches also operate at Layer 3 (for routing functions).

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

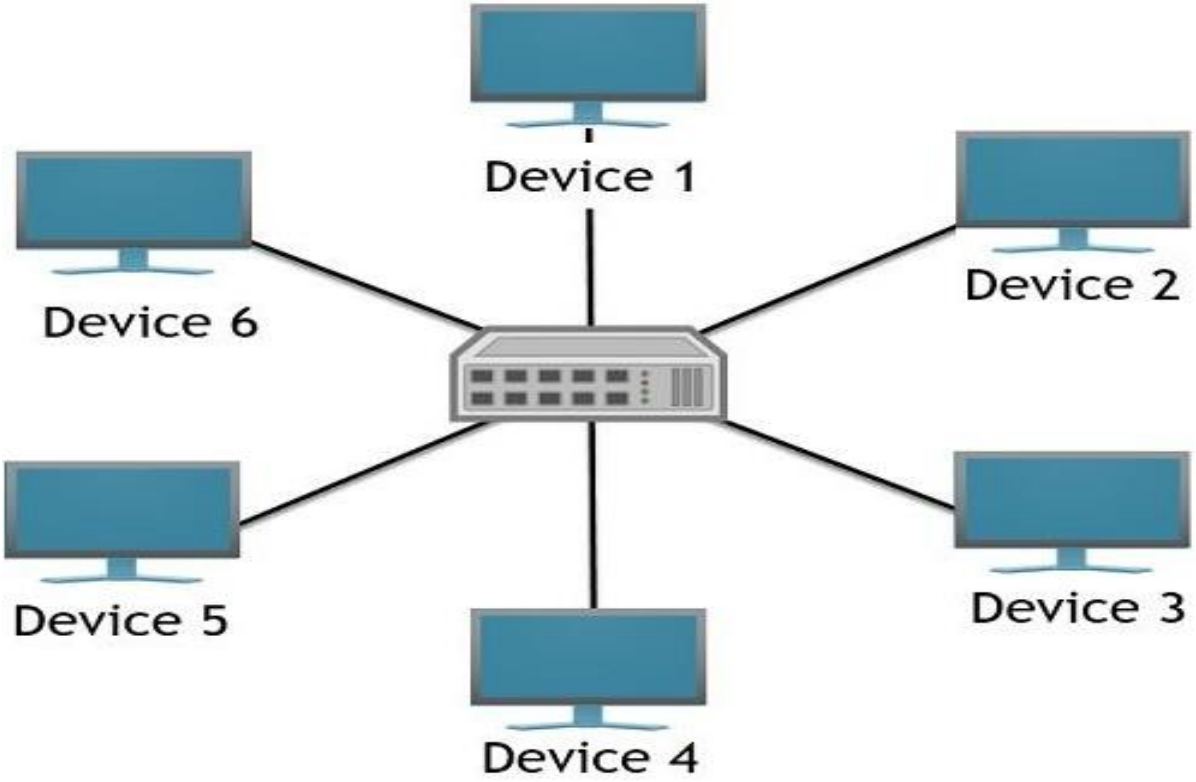


Fig. 3.1: Star Topology

(Courtesy: https://circuitglobe.com/difference-between-star-and-ring-topology.html#google_vignette)

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 3.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	10
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01
5	Network Cable (UTP Cable)	Category 5e or 6 Unshielded Twisted Pair (UTP) cable, 4 twisted pairs (8 copper wires); used for Ethernet LAN connections; supports up to 1 Gbps (Cat5e) or 10 Gbps (Cat6)	As required

IX. Precautions to be followed

1. Ensure all cables are connected properly and securely.
2. Do not connect or disconnect cables when devices are powered on.

X. Suggested Procedure

1. Prerequisites

- A computer lab with functional computers, switches, and routers**.**
- Basic knowledge of network devices and IP addressing.

2. Observe the Physical Layout

- Visit the computer lab and carefully look at how the computers are physically connected.
- Identify the location of networking devices such as switches, hubs, routers, and servers.
- Note whether all computers connect to a single central device or share a common cable.

3. Trace the Network Cables

- Follow the Ethernet cables connected to each computer to see where they lead.
- If each computer's cable connects to a central device (like a switch or hub), this indicates a Star Topology**.**
- If all computers are connected along a single main cable (bus line), it indicates a Bus Topology**.**
- If devices are connected circularly, forming a closed loop, it indicates a Ring Topology.

4. Identify Central Devices

- Locate any central network device (switch, hub, or router).
- A switch or hub typically has multiple Ethernet ports, each connected to a computer.
- If this device exists, note how many systems are connected to it — this helps confirm the topology type.

5. Draw a Network Diagram

- Based on the observations**,** draw a neat and labelled diagram showing all devices and connections.
- Represent PCs and switches, clearly with connecting lines.
- Ensure the diagram reflects the actual physical connections in the lab.

6. Determine Topology

- Compare the identified layout with standard network topologies such as Star, Bus, Ring, Mesh, or Hybrid**.**
- Identify the topology used in the lab.

7. Conclude the Topology

- Based on the observations and comparison, conclude which topology is implemented in the computer lab.
- For example: The computer lab uses a Star Topology, where all computers are connected to a central switch, allowing efficient communication and easy fault isolation.

XI. Resources used during performance

Table 3.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.
6.

XIII. Observation Table

Sr. No.	Action Performed	Expected Output	Actual Output(Successful/ As Expected)	Status (Pass/ Fail)
1	Type of Connection	Wired LAN		
2	Networking Devices Used	Switch, Router, Hub		
3	Central Device	Network Switch		
4	Network Layout	All computers connected to a central		
5	Identified Topology	Type of topology		

XIV. Results

……..

……...……...…

XV. Interpretation of results

…….

……...……..

XVI. Conclusions and Recommendations

……

…..……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give importance of network topology.
2. List and explain different types of network topologies.
3. Draw a neat diagram of the identified network topology and label all connected devices.
4. State one advantage and one disadvantage of star topology.

[Space for Answers] (If required attach separate page)

……..…

……..…

……..…

……..…

……..…

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=uDulBxDb7GM	Topologies in Computer Networks

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Identification of topology	10%
2	Observation and documentation	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Drawing of network diagram	10%
2	Explanation of working topology	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.4: *Simulation of Mesh topology

I. Practical Significance

This practical enables student to configure mesh topology using cisco packet tracer simulator. By creating multiple interconnections between network nodes, learners explore how data can be transmitted through various paths, ensuring high reliability and fault tolerance. Through simulation, they gain hands-on experience in configuring and testing mesh networks, thereby enhancing their skills in network design, performance optimization, and troubleshooting of complex and large-scale communication systems.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 4.1 Connect computers in Mesh topology and test the performance.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

Mesh topology is a type of network topology in which each device (node) in the network is individually connected to every other device. This means that there are dedicated point-to-point links between every pair of nodes. In a mesh topology, data can be transmitted through several paths. Each device can send data directly to the destination device or route it through intermediate nodes. This means that even if one connection fails, the data automatically finds an alternate route to reach its destination.

Types of Mesh Topology

1. **Full Mesh Topology:**
   - Every device is connected directly to every other device in the network.
   - Number of links required for *n* devices = $n(n-1)/2$.
     (Example: For 4 devices → $4\times3/2 = 6$ links)
2. **Partial Mesh Topology:**
   - Only some devices are connected to all others.
   - The remaining devices are connected to one or two main nodes.
   - Commonly used in large networks.

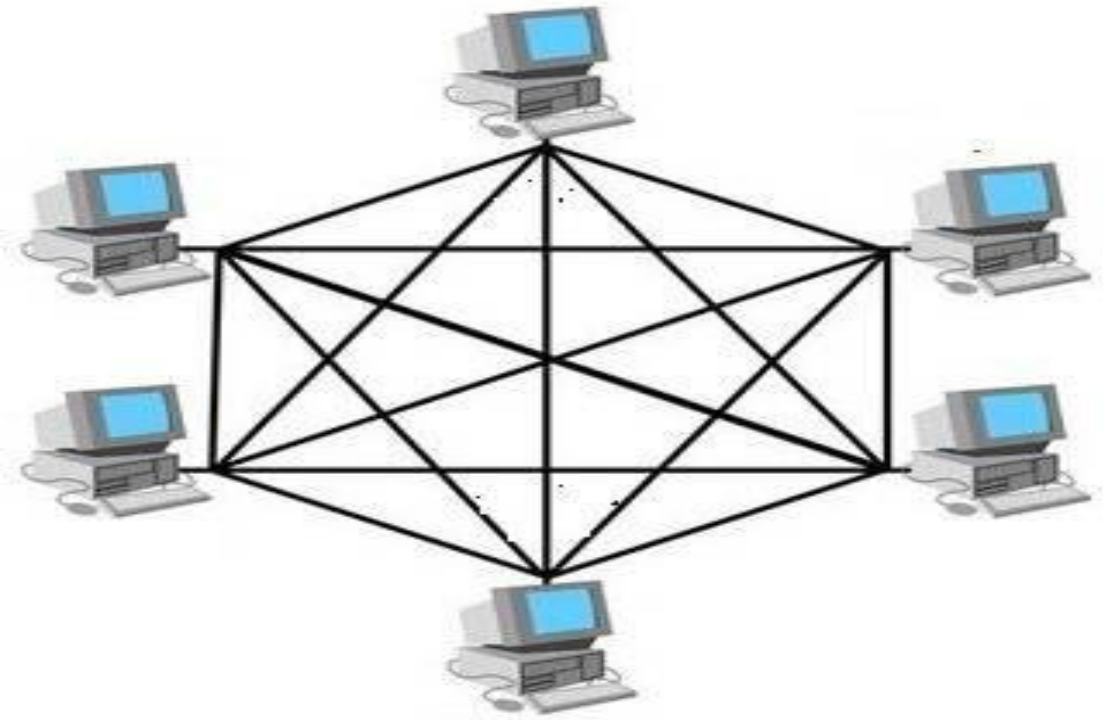


Fig. 4.1: Mesh Topology

(Courtesy: https://www.shiksha.com/online-courses/articles/what-is-mesh-topology-blogId-156361)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

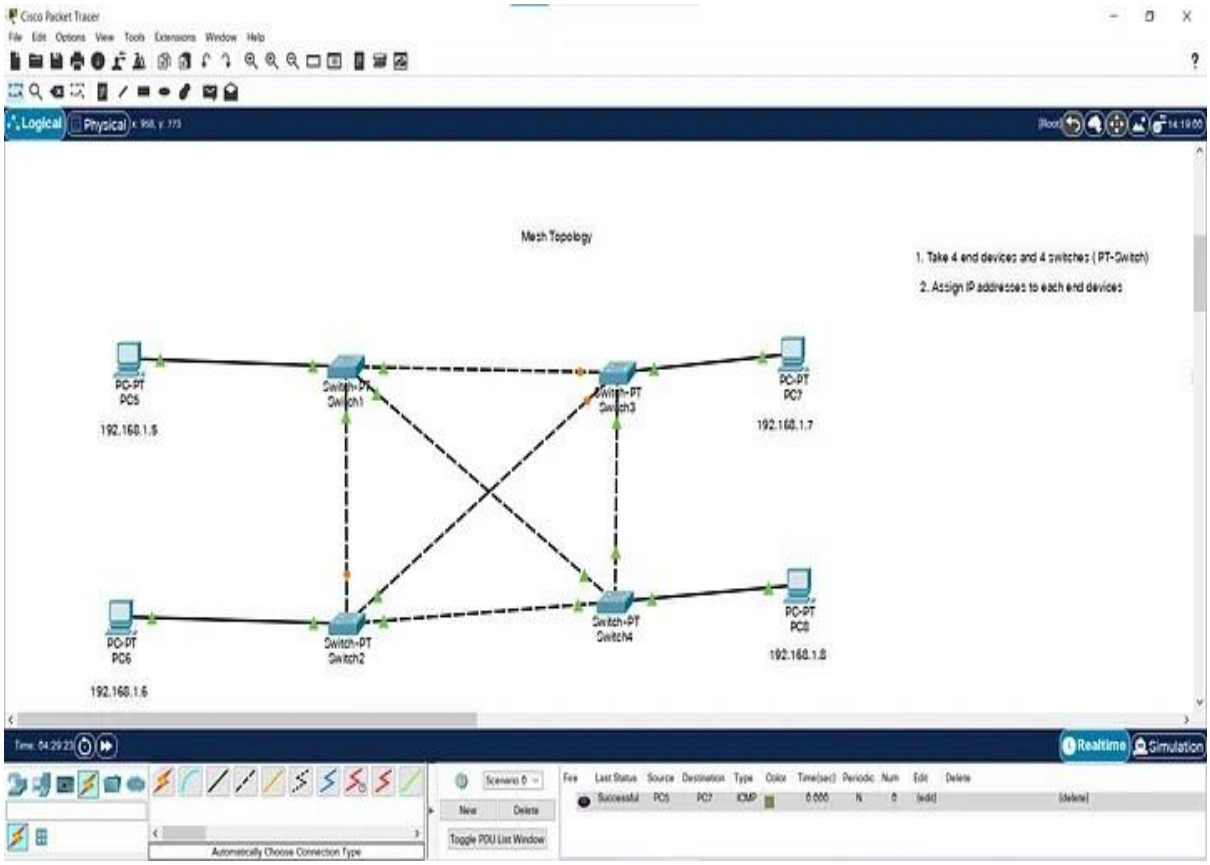


Fig. 4.2: Simulation of Mesh topology Using Cisco Packet Tracer

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 4.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all network devices are properly connected and assigned unique IP addresses during simulation.
2. Verify that each node has a unique IP address to avoid address conflicts.
3. Check all cables connections carefully to ensure proper linking between nodes in the mesh topology in simulation.

X. Suggested Procedure

1. Start Cisco Packet Tracer

- Launch Cisco Packet Tracer software on your computer.
- Wait for the main workspace window to appear.
- Ensure the toolbars and device selection area are visible for adding network components.

2. Create the Network Topology

- From the End Devices section, drag and drop four PCs (e.g., PC0, PC1, PC2, and PC3) into the workspace.
- From the Connections section, choose Copper Cross-Over Cable (used for PC-to-PC connections).
- Connect each PC to every other PC so that all nodes are directly linked to one another.
  PC0 ↔ PC1
  PC0 ↔ PC2
  PC0 ↔ PC3
  PC1 ↔ PC2
  PC1 ↔ PC3
  PC2 ↔ PC3

3. Assign IP Addresses

- Assign unique IP addresses to each PC within the same network (subnet).
- Example
  PC0: IP – 192.168.1.2 Subnet Mask – 255.255.255.0
  PC1: IP – 192.168.1.3 Subnet Mask – 255.255.255.0
  PC2: IP – 192.168.1.4 Subnet Mask – 255.255.255.0
  PC3: IP – 192.168.1.5 Subnet Mask – 255.255.255.0

4. Configure IP Settings on Each PC

- Click on a PC (for example, PC0).
- Select the Desktop tab → IP Configuration option.
- Enter the assigned IP Address and Subnet Mask.
- Repeat the same steps for all other PCs using their respective IP addresses.
- Close the configuration window once done.

5. Verify Network Connectivity

- To check whether all connections are working correctly.
- Go to Desktop → Command Prompt on PC0**.**
- Type the command
  ping 192.168.1.3
  ping 192.168.1.4
  ping 192.168.1.5
- Observe the reply messages from other PCs.
- Successful replies indicate that communication between devices is established.
- Repeat the ping test from other PCs if needed to confirm full connectivity across the network.

6. Observe Communication Using PDU Tool

- From the Toolbar**,** select the add Simple PDU Tool (represented by an envelope icon)**.**
- Click on the source PC and then on the destination PC to simulate data transfer.
- Observe the packet movement through different links in simulation mode**.**

7. Save the Project

- Once the simulation works successfully, go to File → Save As**.**
- Save the file with proper filename and extension, (e.g., mesh.pkt).

XI. Resources used during performance

Table 4.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5**.**
6.
7.
8.
9.

XIII. Observation Table

Table 4.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Connected all PCs using copper cross-over cables	Green link lights on switch and PC interfaces		
2	Verified connectivity between PC0 and PC2	Reply from 192.168.1.4: bytes=32 time 1ms TTL=128		
3	Observed data flow using PDU tool	Data packets travel through multiple		

XIV. Results

……

……..……..…

XV. Interpretation of results

……

……..…….

XVI. Conclusions and Recommendations

……..……

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give importance of mesh topology.
2. Differentiate between full mesh and partial mesh topology.
3. Draw a neat, well-labelled diagram of a mesh topology using four PCs and explain the interconnections.
4. List applications of mesh topology.

[Space for Answers] (If required attach separate page)

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.netacad.com/cisco-packet-tracer	Cisco Packet Tracer Software Simulator
2	https://www.youtube.com/watch?v=UX-c5Cb3LN4	Simulating Mesh Topology

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Identification and Selection of Tools/Devices	10%
2	Selection of proper devices and cables in Cisco Packet Tracer	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful simulation of mesh topology	10%
2	Proper connectivity verification using ping command	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.5: *Simulation of Star topology

I. Practical Significance

This practical enables student to configure star topology using the cisco packet tracer simulator. In this topology, multiple end devices are connected to a central device like a switch or hub, which acts as the main communication point for all data transmission. This simulation demonstrates how data travels from one node to another through the central device, ensuring organized and efficient communication management. This practical enhances students' skills in network design, configuration, performance analysis, and troubleshooting within small- to medium-scale communication systems.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 5.1 Connect computers in Star topology and test the performance.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

Star topology is a type of network topology in which all devices are connected to a central device such as a switch or hub. Each device has a dedicated connection to the central node. The central node acts as a controller for all network communication. If any individual node or cable fails, the rest of the network remains unaffected, but failure of the central device will bring down the entire network.

Types of Star Topology

1. **Active Star Topology:**
   - An active star topology uses an active device, such as a switch or any intelligent networking device, as the central node.
   - This central device regenerates, amplifies, and manages the signals before forwarding them to the destination nodes. It ensures that data transmission is strong, efficient, and error-free, even across longer distances.
   - Active stars are generally used in modern LAN (Local Area Network) environments because they enhance network performance and reliability by reducing data loss and improving communication speed.

2. **Passive Star Topology:**
   - A passive star topology uses a hub as the central device. Unlike an active star, the hub does not amplify or regenerate signals; it simply distributes the incoming data signals to all connected devices.
   - Passive stars are simpler and less expensive but are more prone to signal degradation in large networks.
   - Commonly used in small networks.

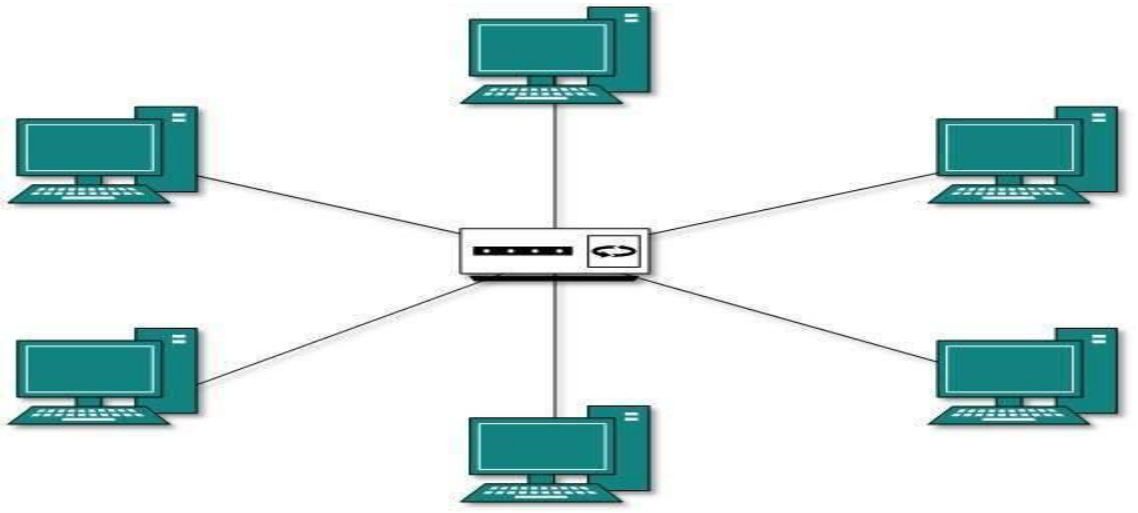


Fig. 5.1: Star Topology

(Courtesy: https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

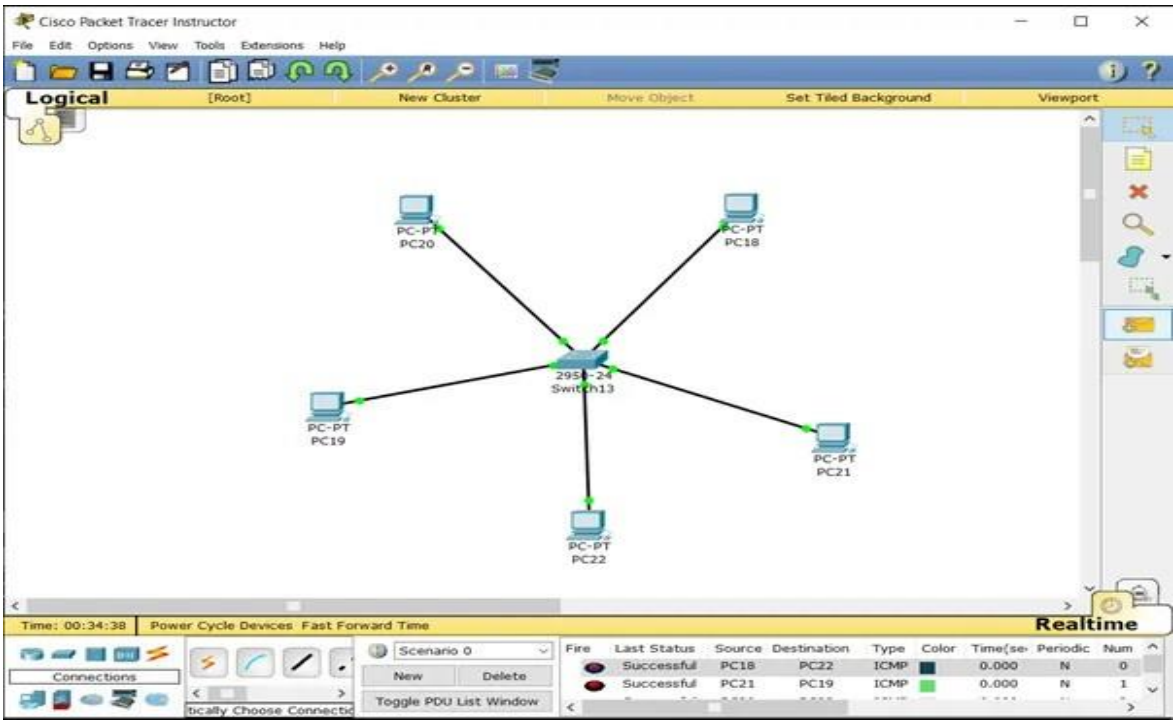


Fig. 5.2: Simulation of star topology Using Cisco Packet Tracer

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 5.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all network devices are properly connected and assigned unique IP addresses before starting the simulation.
2. Verify that each node has a unique IP address to avoid address conflicts.
3. Check all cable connections carefully to ensure proper linking between nodes in the star topology.

X. Suggested Procedure

1. Start Cisco Packet Tracer

- Launch Cisco Packet Tracer software on your computer.
- Wait for the main workspace window to appear.
- Ensure the toolbars and device selection area are visible for adding network components.

2. Create the Network Topology

- From the End Devices section, drag and drop four PCs (e.g., PC0**,** PC1**,** PC2**,** and PC3) into the workspace.
- From the Network Devices section, drag and drop one Switch (e.g., Switch0) into the workspace.
- From the Connections section, choose Copper Straight-Through Cable (used for connecting PCs to switches).
- Connect each PC to the central switch as shown below.
  PC0 ↔ Switch0
  PC1 ↔ Switch0
  PC2 ↔ Switch0
  PC3 ↔ Switch0

3. Assign IP Addresses

- Assign unique IP addresses to each PC within the same network (subnet).
- Example
  PC0: IP – 192.168.1.2 Subnet Mask – 255.255.255.0
  PC1: IP – 192.168.1.3 Subnet Mask – 255.255.255.0
  PC2: IP – 192.168.1.4 Subnet Mask – 255.255.255.0
  PC3: IP – 192.168.1.5 Subnet Mask – 255.255.255.0

4. Configure IP Settings on Each PC

- Click on a PC (for example, PC0).
- Select the Desktop tab → IP Configuration option.
- Enter the assigned IP Address and Subnet Mask**.**
- Repeat the same steps for all other PCs using their respective IP addresses.
- Close the configuration window once done

5. Verify Network Connectivity

- To check whether all connections are working correctly.
- Go to Desktop → Command Prompt on PC0**.**
- Type the command
  ping 192.168.1.3
  ping 192.168.1.4
  ping 192.168.1.5
- Observe the reply messages from other PCs.
- Successful replies indicate that communication between devices is established.
- Repeat the ping test from other PCs if needed to confirm full connectivity across the network.

6. Observe Communication Using PDU Tool

- From the toolbar**,** select the add simple PDU Tool (represented by an envelope icon)**.**
- Click on the source PC and then on the destination PC to simulate data transfer.
- Observe the packet movement through different links in simulation mode.

7. Save the Project

- Once the simulation works successfully, go to file → Save As**.**
- Save the file with proper filename and extension, (e.g., star.pkt).

XI. Resources used during performance

Table 5.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5**.**
6.
7.
8.
9.

XIII. Observation Table

Table 5.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Connected all PCs (PC0–PC3) to Switch using Copper Straight-Through cables	Green link lights on switch and PC interfaces		
2	Verified connectivity between PC0 and PC1	Reply from 192.168.1.3: bytes=32 time 1ms		
3	Verify network communication	All PCs communicate		

XIV. Results

……

……...……

XV. Interpretation of results

……

……...……

XVI. Conclusions and Recommendations

……

…..……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give importance of star topology.
2. State the role of the central device in star topology.
3. Draw a neat, well-labelled diagram of a star topology using six PCs and explain the interconnections.

[Space for Answers] (If required attach separate page)

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.netacad.com/cisco-packet-tracer	Cisco Packet Tracer Software Simulator
2	https://www.youtube.com/watch?v=2pwk_Q3bUkE	Simulating Star Topology

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Identification and selection of tools/devices	10%
2	Selection of proper devices and cables in Cisco Packet Tracer	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful simulation of star topology	10%
2	Proper connectivity verification using ping command	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.6: Simulation of Tree topology

I. Practical Significance

This practical enables student to configure tree topology using the cisco packet tracer simulator. In this topology, multiple star networks are connected in a hierarchical structure with a main switch or hub acting as the root node, and secondary switches branching out to connect end devices. Demonstrates how data travels between different levels of the network, ensuring structured and efficient communication management. This practical enhances students' skills in network design, configuration, performance analysis, and troubleshooting within medium- to large-scale communication systems.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 6.1 Connect computers in Tree topology and test the performance.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A tree topology, also known as a hierarchical topology, is a network structure that combines the features of both star and bus topologies. It is organized in a hierarchical or parent-child structure, where multiple star-configured networks are connected to a main backbone cable. This topology is commonly used in large organizations, schools, and universities where the network is divided into different departments or sections.

Types of Tree Topology

1. **Centralized Tree Topology:**
   - In a centralized tree topology, all secondary hubs or switches are connected to a single main (root) hub or switch, which acts as the central controlling device**.**
   - This central device manages data communication between all the branches and end devices in the network.
2. **Distributed Tree Topology:**
   - In a distributed tree topology, there is no single central device that controls the entire network. Instead, multiple interconnected switches or hubs manage data communication across different sections.
   - Each branch of the network can operate independently to some extent.

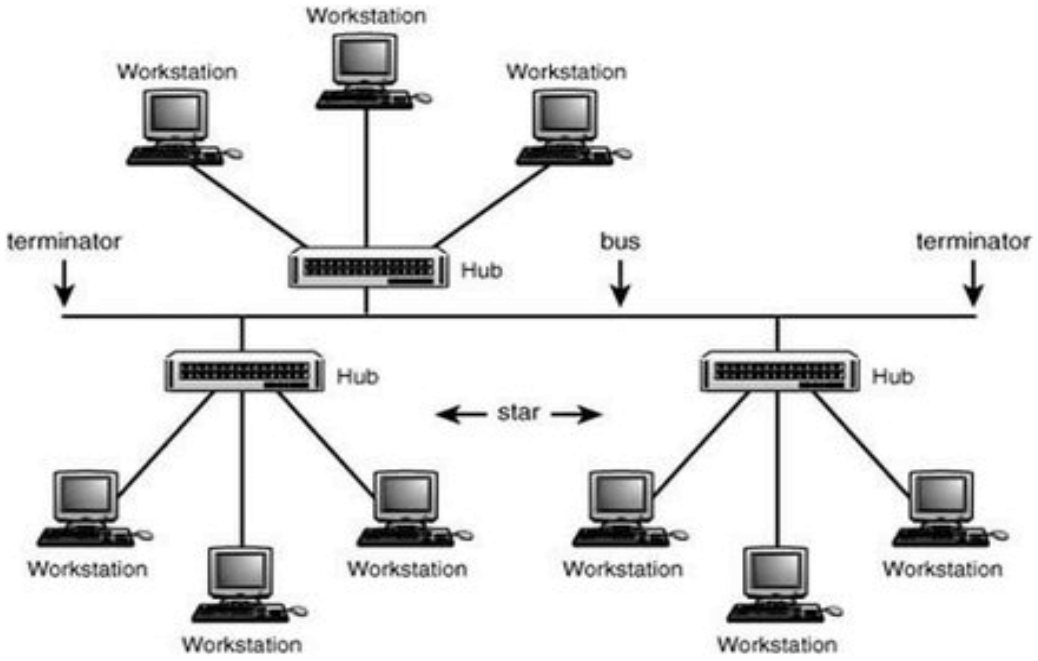


Fig. 6.1: Tree Topology
(Courtesy: https://www.zenarmor.com/docs/network-basics/what-is-tree-topology)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

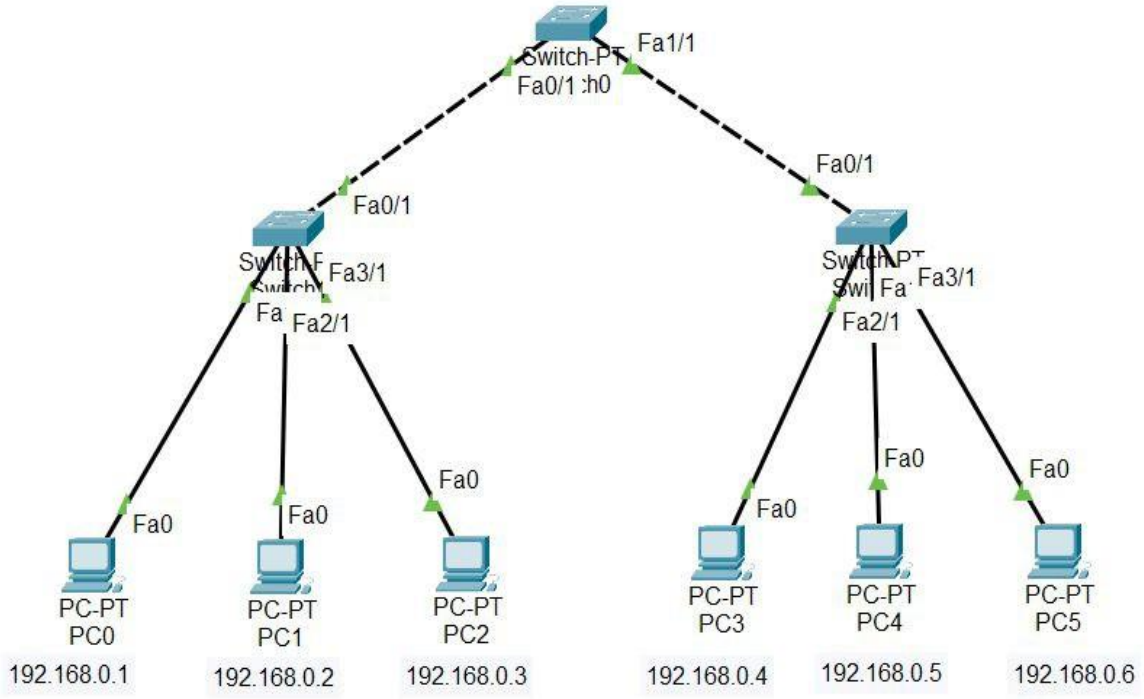


Fig. 6.2: Simulation of tree topology Using Cisco Packet Tracer

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 6.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all network devices are properly connected and assigned unique IP addresses before starting the simulation.
2. Verify that each node has a unique IP address to avoid address conflicts.
3. Check all cable connections carefully to ensure proper linking between nodes in the tree topology.

X. Suggested Procedure

1. Start Cisco Packet Tracer

- Launch Cisco Packet Tracer software on your computer.
- Wait for the main workspace window to appear.
- Ensure the toolbars and device selection area are visible for adding network components.

2. Create the Network Topology

- From the End Devices section, drag and drop six PCs (e.g., PC0 to PC5) into the workspace.
- From the Network Devices section, drag and drop three switches — one Main Switch (Switch Main) and two Sub-Switches (Switch1 and Switch2).
- From the Connections section, choose Copper Straight-Through Cable (used for connecting PCs to switches).
- Switch Connections:
  Switch Main ↔ Switch1
  Switch Main ↔ Switch2
- PC Connections:
  Switch1 ↔ PC0
  Switch1 ↔ PC1
  Switch1 ↔ PC2
  Switch1 ↔ PC3
  Switch1 ↔ PC4
  Switch1 ↔ PC5

3. Assign IP Addresses

- Assign unique IP addresses to each PC within the same network (subnet).
- Example
  PC0: IP – 192.168.0.1 Subnet Mask – 255.255.255.0
  PC1: IP – 192.168.0.2 Subnet Mask – 255.255.255.0
  PC2: IP – 192.168.0.3 Subnet Mask – 255.255.255.0
  PC3: IP – 192.168.0.4 Subnet Mask – 255.255.255.0
  PC4: IP – 192.168.0.5 Subnet Mask – 255.255.255.0
  PC5: IP – 192.168.0.6 Subnet Mask – 255.255.255.0

4. Configure IP Settings on Each PC

- Click on a PC (for example, PC0).
- Select the Desktop tab → IP Configuration option.
- Enter the assigned IP Address and Subnet Mask**.**
- Repeat the same steps for all other PCs using their respective IP addresses.
- Close the configuration window once done

5. Verify Network Connectivity

- To check whether all connections are working correctly.
- Go to Desktop → Command Prompt on PC0**.**
- Type the command
  ping 192.168.0.2

ping 192.168.0.3
ping 192.168.0.4
ping 192.168.0.5
ping 192.168.0.6

- Observe the reply messages from other PCs.
- Successful replies indicate that communication between devices is established.
- Repeat the ping test from other PCs if needed to confirm full connectivity across the network.

6. Observe Communication Using PDU Tool

- From the toolbar**,** select the add simple PDU Tool (represented by an envelope icon)**.**
- Click on the source PC and then on the destination PC to simulate data transfer.
- Observe the packet movement through different links in simulation mode.

7. Save the Project

- Once the simulation works successfully, go to file → Save As**.**
- Save the file with proper filename and extension, (e.g., tree.pkt).

XI. Resources used during performance

Table 6.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

4.

5**.**

6.

7.

XIII. Observation Table

Table 6.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Connected all PCs (PC0–PC3) to Switch using Copper Straight-Through cables	Green link lights on switch and PC interfaces		
2	Verified connectivity between PC0 and PC1	Reply from 192.168.1.3: bytes=32 time 1ms		
3	Verify network communication	All PCs communicate		

XIV. Results

……

……...……

XV. Interpretation of results

……

……...……

XVI. Conclusions and Recommendations

……..……

…..……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give importance of tree topology.
2. State how tree topology combines star and bus structures.
3. Draw a tree topology using six PCs connected through two switches and one main switch in cisco packet tracer.
4. List any two advantages and two disadvantages of tree topology.

[Space for Answers] (If required attach separate page)

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.netacad.com/cisco-packet-tracer	Cisco Packet Tracer Software Simulator
2	https://www.youtube.com/watch?v=eDryQkdQ3hk	Simulating Tree Topology

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Identification and selection of tools/devices	10%
2	Selection of proper devices and cables in Cisco Packet Tracer	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful simulation of tree topology	10%
2	Proper connectivity verification using ping command	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.7:* Share resources in a computer network

I. Practical Significance

This practical enables student to develop skills for sharing resources such as files, folders, and printers within a computer network. This include setting up network sharing options, assigning permissions, and managing user access between connected systems. Through this activity, students demonstrate hands-on skills in resource sharing, communication setup, and efficient utilization of network hardware and software components.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 7.1 Install/configure/Test Peer to Peer LAN and sharing of resources.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A Peer-to-Peer (P2P) Local Area Network (LAN) is a type of network where two or more computers are directly connected to each other without using a central server. Each computer in the network can act as both a client and a server, allowing users to share files, folders, and devices such as printers or internet connections. In this setup, all computers are part of the same workgroup, and each computer is assigned a unique name and IP address. The configuration process involves connecting the computers through network cables or Wi-Fi, enabling network discovery, and turning on file and printer sharing options. Once configured, users can share resources like data files or printers and access them from other systems in the same network. The connection can be verified using the ping command to check communication between systems.

Commonly Shared Resources in a Computer Network

1. **Files and Folders**: Shared among users to exchange data and collaborate.
2. **Printers**: One printer can serve multiple computers in a network.
3. **Internet Connection**: Shared through routers or switches.
4. **Storage Devices**: Shared drives or network storage for saving common data.
5. **Software Applications** – Shared licensed software used by multiple users.
6. **Peripheral Devices**: Devices like scanners and projectors shared among computers.

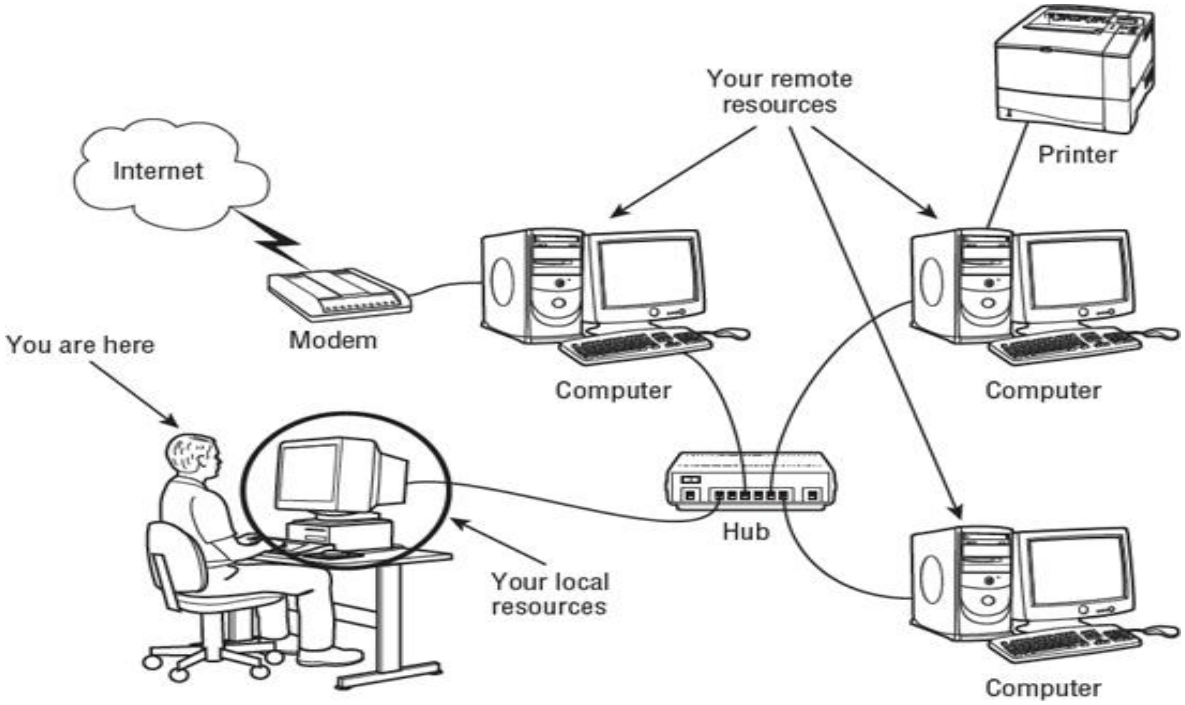


Fig. 7.1: Local and remote resources
(Courtesy: https://programming.wmlcloud.com/desktop/9720.aspx)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

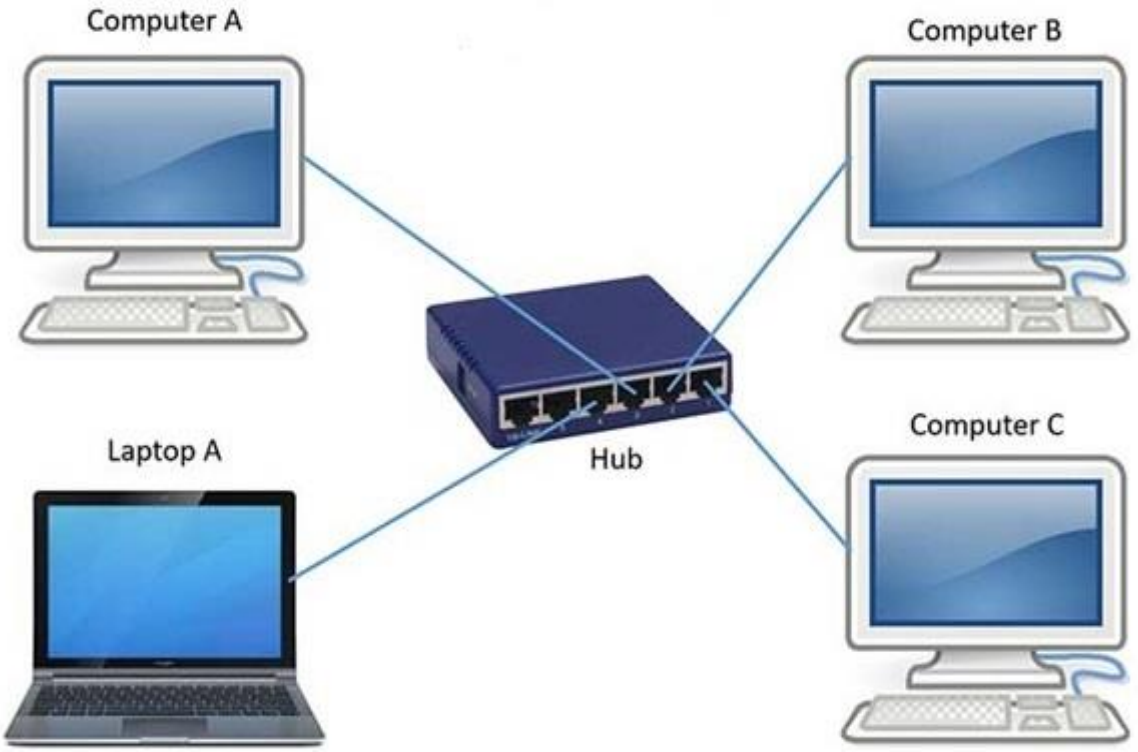


Fig. 7.2: Peer to Peer Network
(Courtesy: https://onlinecomputertips.com/support-categories/networking/673-peer-to-peer-vs-client-server-networks/)

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 7.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01
5	Printer	Printer (Laser/Inkjet)	01

IX. Precautions to be followed

1. Ensure all computers are connected properly and in the same workgroup**.**
2. Share only necessary folders, files, or devices to maintain security.
3. Verify network connectivity before accessing shared resources.

X. Suggested Procedure

1. Prerequisites

- Two or more computers/laptops with LAN ports.
- Ethernet cables (Cat5e or Cat6).
- Network switch or LAN crossover cable (if only two PCs are used).
- Ensure all computers are powered ON and running Windows OS

2. Connect the Computers

- Connect all computers to a common switch using Ethernet cables.
- Confirm that the LAN indicator lights on each PC and switch are blinking**.**

3. Configure IP Addresses

- On each computer.
- Go to Control Panel → Network and Internet→ Network and Sharing Centre → Change Adapter Settings.
- Right-click on Ethernet → Properties.
- Select Internet Protocol Version 4 (TCP/IPv4) → click Properties.
- Assign unique IP addresses within the same network (subnet)
  PC1: IP – 192.168.0.1 Subnet Mask – 255.255.255.0
  PC2: IP – 192.168.0.2 Subnet Mask – 255.255.255.0
- Click OK to save settings.

4. Check Network Connectivity

- On PC1, open Command Prompt and type: ping 192.168.0.2
- Press Enter.
- If Reply from 192.168.0.2 messages appear, connectivity is established.
- Repeat the same test from PC2 to verify bidirectional communication.

5. Enable File and Printer Sharing

- On each computer.
- Open Control Panel → Network and Sharing Centre.
- Click on Change advanced sharing settings**.**
- Turn on:
  Network discovery
  File and printer sharing
- Save the changes.

6. Share a Folder or Drive

- On PC1**,** select a folder or drive to share**.**
- Right-click the folder → Properties.
- Go to Sharing tab → Advanced Sharing**.**
- Check Share this folder**.**
- Assign a share name (e.g., Shared Docs**)**.
- Click Apply → OK.

7. Access Shared Resources from Another PC

- On PC2**,** open file explorer**.**
- In the address bar, type the IP of PC1 as: \\192.168.0.1

- Press Enter**.**
- The shared folder (Shared Docs) will appear.
- You can now open, copy, or save files from the shared.

8. Save and Document the Setup

- Note down all assigned IP addresses and shared resource names.
- Capture screenshots of:
  IP configuration window
  Ping result
  Shared folder access
- Save these for your practical record.

XI. Resources used during performance

Table 7.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5**.**
6.
7**.**
8.

XIII. Observation Table

Table 7.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful/ As Expected)	Status (Pass/Fail)
1	Enabled File & Printer Sharing	Sharing option activated		
2	Shared Folder from PC1	Folder visible to PC2		
3	Accessed Shared Folder from PC0	Files accessible successfully		

XIV. Results

……..……...…

……...……...

XV. Interpretation of results

……..……

……...……...……

XVI. Conclusions and Recommendations

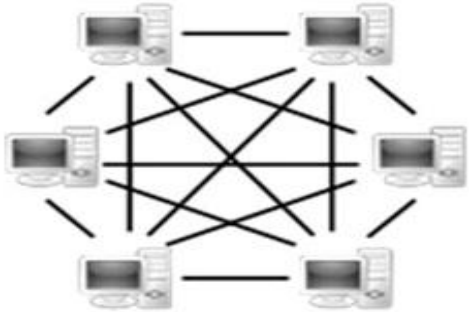
……..……

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of sharing resources in a computer network.
2. Give the advantages of sharing resources in a LAN environment.
3. Explain peer-to-peer network with diagram.
4. Name type of networks shown in following diagram.



[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=QhZpG7U-vpM	Process of File & Printer Sharing

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Proper connection of computers and network devices	10%
2	Correct IP addressing and configuration on all systems	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful resource (file/folder/printer) sharing between computers	10%
2	Verification of connectivity using ping command	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.8: Configuring VPN (Virtual Private Network) using simulator

I. Practical Significance

This practical enables student to configure Virtual Private Network (VPN) using network simulation tools such as Cisco Packet Tracer or GNS3. A VPN provides a secure and encrypted communication channel between geographically separated networks over a public network like the Internet. Through this practical, learners will gain hands-on experience in configuring VPN tunnels between routers, ensuring confidentiality, integrity, and authentication of data. They will also understand how VPNs connect branch offices, remote users, or different LANs securely as if they were part of the same local network.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 8.1 Set up a basic VPN and Connect remote clients securely using Open VPN or Windows VPN.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A Virtual Private Network (VPN) is a technology that enables secure communication over an insecure or public network, such as the Internet. It creates an encrypted tunnel between two endpoints, ensuring that data transmitted between them remains confidential and protected from unauthorized access. VPNs are commonly used by organizations to securely connect branch offices, remote workers, or multiple LANs located at different geographical locations.

Purpose of VPN

1. To secure communication between remote sites or users.
2. To protect sensitive data transmitted over public networks.
3. To reduce cost by using the Internet instead of dedicated leased lines.
4. To provide remote access to employees working from home or other locations.
5. To connect branch offices securely to the main office network.

Types of VPN

1. **Remote Access VPN**
- Allows individual users to connect securely to a corporate network from remote locations.
- Commonly used by work-from-home employees.
2. **Site-to-Site VPN**
- Connects two or more local area networks (LANs) located in different places.
- Used by companies to connect their branch networks securely.
3. **Client-Based VPN**
- Requires client software on the user's device to establish the VPN connection.
4. **SSL VPN**
- Uses Secure Socket Layer (SSL) encryption, usually through a web browser, without needing special client software.

VPN Protocols

1. **PPTP (Point-to-Point Tunnelling Protocol)** – Simple and widely supported but less secure.
2. **L2TP (Layer 2 Tunnelling Protocol)** – Often combined with IPsec for better security.
3. **IPsec (Internet Protocol Security)** – Provides encryption and authentication at the IP layer.
4. **SSL/TLS (Secure Socket Layer / Transport Layer Security)** – Common for web-based VPN connections.
5. **Open VPN** – Open-source protocol using SSL/TLS for encryption and authentication.

VPN Components

1. **VPN Gateway / Router:** Device responsible for managing VPN tunnels.
2. **VPN Client:** Software or device initiating the VPN connection.
3. **VPN Server:** Endpoint accepting the VPN connection.
4. **Encryption Algorithms:** Used to secure data (e.g., AES, DES).
5. **Authentication Methods:** Verify user identity (e.g., passwords, certificates, pre-shared keys).

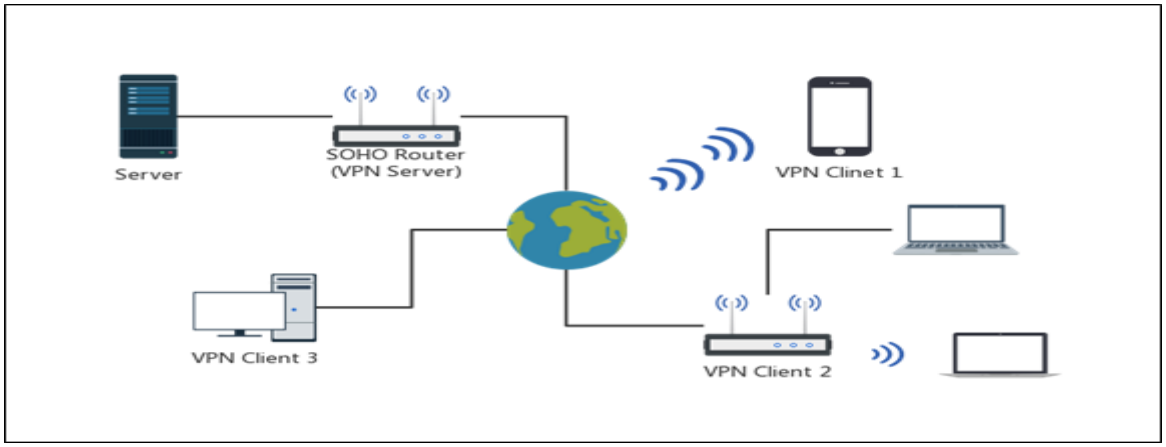


Fig. 8.1: Working as a VPN Server
(Courtesy: https://www.tp-link.com/us/support/faq/2706/)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

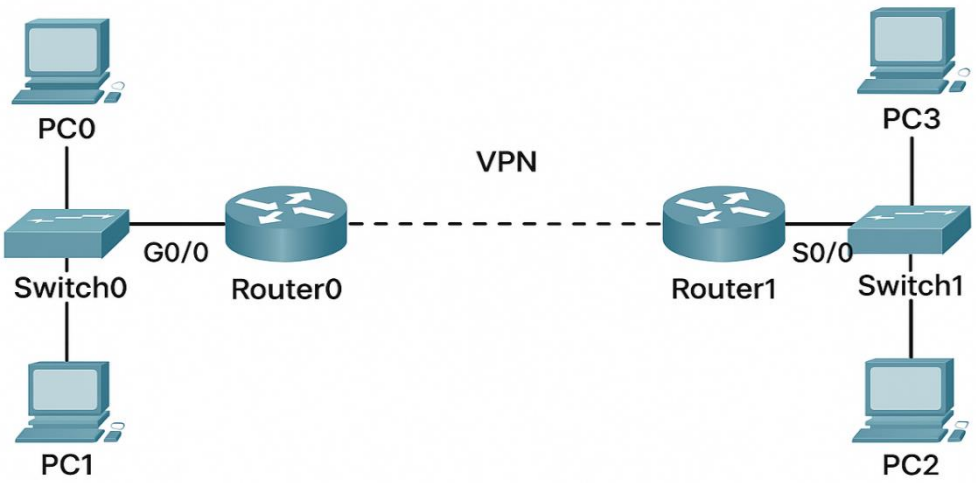


Fig. 8.2: Configuring and Verifying VLANs in Cisco

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 8.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01

IX. Precautions to be followed

1. Ensure all network devices (routers, PCs) are properly connected and powered ON before starting the VPN configuration.
2. Verify that correct IP addresses are assigned to all interfaces involved in the VPN connection.
3. Save the router configuration after successful setup to prevent data loss.

X. Suggested Procedure

1. Prerequisites

- A computer or laptop with Cisco Packet Tracer installed (version 8.0 or above recommended).
- Two routers (e.g., Router0 and Router1).
- Two switches (Switch0 and Switch1).
- Four PCs (two on each LAN – PC0, PC1 connected to Router0; PC2, PC3 connected to Router1).

2. Create the Network Topology

- Launch Cisco Packet Tracer on your computer.
- From the End Devices section, drag and drop four PCs into the workspace**.**
- From the Network Devices section, add two routers and two switches.
- Connect devices as follows:
  PC0 ↔ Switch0
  PC1 ↔ Switch0
  PC2 ↔ Switch1
  PC3 ↔ Switch1
  Switch0 ↔ Router0 (GigabitEthernet0/0)
  Switch1 ↔ Router1 (GigabitEthernet0/0)

Router0 ↔ Router1 (Serial DCE Cable)

3. Assign IP Addresses

- Assign IP addresses to all PCs and router interfaces according to the network design.

PC0: IP – 192.168.1.2 Subnet Mask – 255.255.255.0 (LAN A)
PC1: IP – 192.168.1.3 Subnet Mask – 255.255.255.0 (LAN A)
Router0: IP – 192.168.1.1 Subnet Mask – 255.255.255.0 (Gateway of LAN A)
Router0: IP – 10.0.0.1 Subnet Mask – 255.255.255.252 (VPN Tunnel Side)
Router1: IP – 10.0.0.2 Subnet Mask – 255.255.255.252 (VPN Tunnel Side)
Router1: IP – 192.168.2.1 Subnet Mask – 255.255.255.0 (Gateway of LAN B)
PC2: IP – 192.168.2.2 Subnet Mask – 255.255.255.0 (LAN B)
PC3: IP – 192.168.2.3 Subnet Mask – 255.255.255.0 (LAN B)

4. Configure PCs with IP Addresses

- Click the PC → Desktop → IP Configuration
- Enter the IP Address and Subnet Mask from the table above.
- Set the Default Gateway to the router interface of the same LAN.
  PC0 → Gateway 192.168.1.1
  PC2 → Gateway 192.168.2.1

5. Configure Routers

Router0 Configuration

- Click on Router0 → CLI → Press Enter**.**
- Type the following commands:

```
Router> enable
Router# configure terminal
Router(config)# hostname Router0
Router0(config)# interface gig0/0
Router0(config-if)# ip address 192.168.1.1 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# interface serial0/0/0
Router0(config-if)# ip address 10.0.0.1 255.255.255.252
Router0(config-if)# clock rate 64000
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router0(config)# exit
```

Router1 Configuration

- Click on Router1 → CLI → Press Enter

```
Router> enable
Router# configure terminal
Router(config)# hostname Router1
Router1(config)# interface gig0/0
Router1(config-if)# ip address 192.168.2.1 255.255.255.0
```

Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface serial0/0/0
Router1(config-if)# ip address 10.0.0.2 255.255.255.252
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router1(config)# exit

6. **Verify Basic Connectivity**
   - From Router0, ping Router1 using**:** Router0# ping 10.0.0.2
   - From PC0, ping PC2: C:\> ping 192.168.2.2
7. **Configure VPN (IPsec) Tunnel**
   - Router0
     Router0(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
     Router0(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
     Router0(config)# crypto map MYMAP 10 ipsec-isakmp
     Router0(config-crypto-map)# set peer 10.0.0.2
     Router0(config-crypto-map)# set transform-set MYSET
     Router0(config-crypto-map)# match address 110
     Router0(config)# interface serial0/0/0
     Router0(config-if)# crypto map MYMAP
   - Router1
     Router1(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
     Router1(config)# access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
     Router1(config)# crypto map MYMAP 10 ipsec-isakmp
     Router1(config-crypto-map)# set peer 10.0.0.1
     Router1(config-crypto-map)# set transform-set MYSET
     Router1(config-crypto-map)# match address 110
     Router1(config)# interface serial0/0/0
     Router1(config-if)# crypto map MYMAP
8. **Verify VPN Tunnel**
   - Use the following commands on both routers:
     show crypto isakmp sa
     show crypto ipsec sa
   - Also, check connectivity again:PC0 → ping 192.168.2.2
   - If successful, the VPN configuration is working properly
9. **Save the Configuration**
   - Save the running configuration:
     Router0# copy running-config startup-config
     Router1# copy running-config startup-config
   - Save the project as VPN_Simulation.pkt in Cisco Packet Tracer.

XI. Resources used during performance

Table 8.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.
6.

XIII. Observation Table

Table 8.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/ Fail)
1	Basic network connectivity test (ping	Successful replies		
2	Apply VPN	Tunnel created		
3	Ping between LAN A and LAN B PCs	Encrypted packets exchanged		

XIV. Results

……

……...……

XV. Interpretation of results

……

……...……

XVI. Conclusions and Recommendations

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give importance of Virtual Private Network (VPN).
2. Differentiate between Site-to-Site and Remote Access VPN.
3. List any two VPN protocols and their features.
4. State any two advantages of VPNs in enterprise networks.

[Space for Answers] (If required attach separate page)

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=LlL2DkFkACo&t=606s	VPN Configuration

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Correct assignment of IP addresses and routing setup before VPN configuration	10%
2	Verification of VPN tunnel establishment using simulation tools or commands	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful creation of secure VPN tunnel between remote networks	10%
2	Correct simulation result showing encrypted packet flow between routers	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.9: Installation of Repeater and Bridge

I. Practical Significance

The purpose of this practical is to install, configure, and verify the operation of a bridge and repeater within a data communication network. This practical develops skills to understand the roles of these devices in extending network coverage, maintaining signal strength, and ensuring efficient data transmission across connected network segments. Learners gain practical knowledge of how bridges manage data traffic between network segments and how repeaters regenerate signals to support reliable communication over longer distances.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Implement relevant Network Topology.

IV. Laboratory Learning Outcome

LLO 9.1 Install and test Repeater and Bridge.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A Repeater is a network device that operates at the Physical Layer (Layer 1) of the OSI Model. Its main function is to regenerate and amplify weak signals so that data can travel longer distances without loss or distortion. When data signals travel through a cable, they gradually weaken due to attenuation. A Repeater receives these weak signals, restores them to their original strength and shape, and transmits them further on the network.

Functions of a Repeater

1. **Signal Regeneration:** Restores signal amplitude, shape, and timing.
2. **Extending Network Distance:** Allows data to travel beyond cable length limits.
3. **Maintaining Data Integrity:** Prevents data loss caused by weak or noisy signals.
4. **Connecting Different Media Types:** Used between fiber and copper cables.
5. **Boosting Wireless Range:** In Wi-Fi networks, acts as a range extender.

A Bridge is a Data Link Layer (Layer 2) device in the OSI Model that connects two or more LAN segments and filters traffic between them using MAC (Media Access Control) addresses**.** Its purpose is to divide a large network into smaller segments**,** thereby reducing traffic congestion and improving performance.

Functions of a Bridge

1. **Filtering:** Prevents unnecessary data from being sent to all segments.
2. **Forwarding:** Sends frames only to the segment where the destination device is located.
3. **Learning:** Builds and updates a MAC address table automatically.
4. **Segmentation:** Divides a large LAN into smaller collision domains.

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

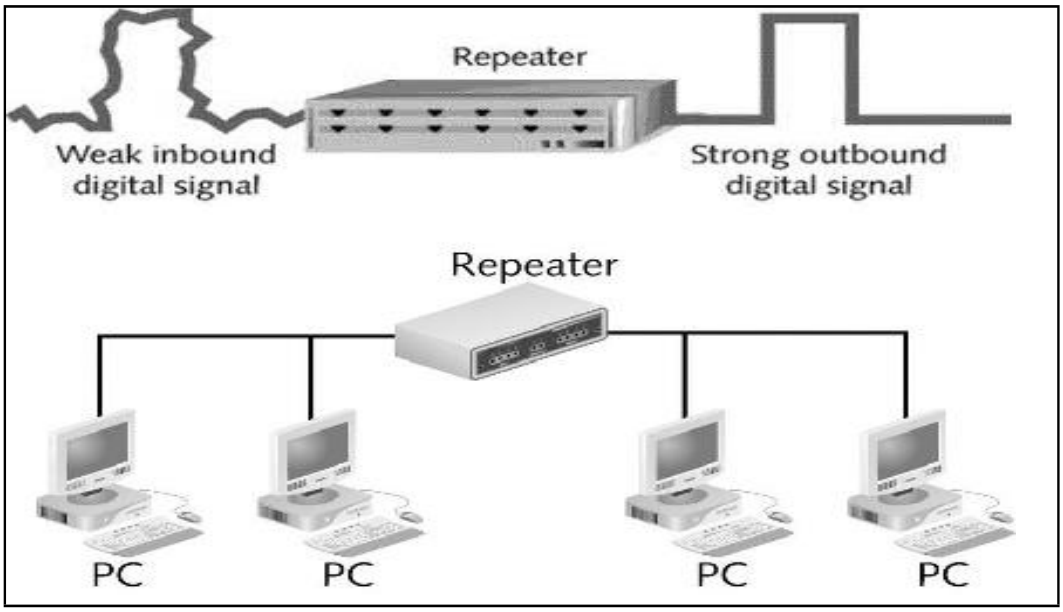


Fig. 9.1: Peer to Peer Network

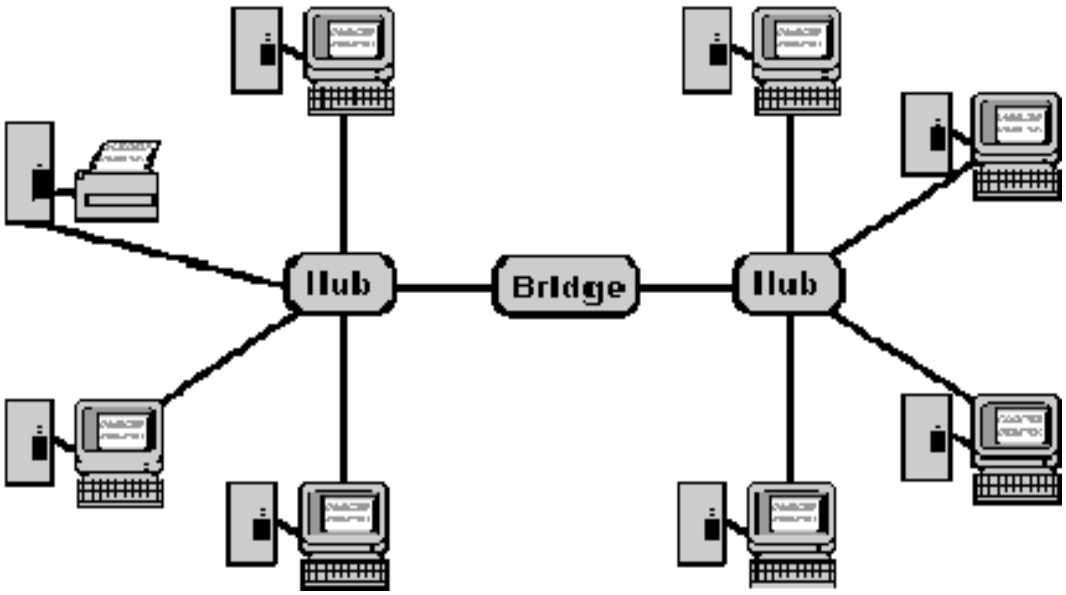


Fig. 9.2: Connection diagram of Bridge in network
(Courtesy: http://www.tutorialspoint.com)

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 9.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	04
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Repeater	Outdoor Band Selective Mobile Signal Repeater suggested	01
5	Bridge	TP-Link standard bridge router	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure both network adapters (Wi-Fi and Ethernet) are properly installed, enabled, and working before creating the bridge.
2. After creating the bridge, restart the system once to ensure proper initialization.
3. Do not unplug network cables or disable adapters during the bridge creation process.

X. Suggested Procedure

Repeater Installation /setup Process

1. Power ON the Repeater

- Plug the Wi-Fi Repeater into a working power socket that is within the range of your main router's Wi-Fi signal.
- Wait until the Power LED lights up and the device is ready.

2. Connect the Computer to the Repeater

- You can connect in either of the two ways.

a) Wireless Connection:

- On your laptop, open Wi-Fi settings → connect to the network named "Wi-Fi-Repeater" **or** "Repeater Setup".
- No password is needed for the first-time setup.

b) Wired Connection:

- Connect one end of an Ethernet cable to the LAN port of the repeater and the other end to your PC/Laptop.

3. Configure IP Addresses

- Press Windows + X → click Network Connections.
- Under Advanced network settings, click more network adapter options.
- In the Network Connections window, right-click Wi-Fi or Ethernet (whichever you are using) → choose Properties.
- Select Internet Protocol Version 4 (TCP/IPv4) → click Properties.
- Choose Use the following IP address and enter:
  IP Address: 192.168.10.2
  Subnet Mask: 255.255.255.0
  Default Gateway: 192.168.10.1
- Leave DNS fields blank → click OK**,** then Close.

4. Access the Repeater's Setup Page

- Open any web browser (Edge, Chrome, or Firefox).
- In the address bar, type http://192.168.10.1 → press Enter**.**
- When the login screen appears, enter:
  Username: admin
  Password: admin
- Click Login **t**o open the Repeater Setup Wizard.

5. Configure Wireless Repeater Mode

- On the setup page, select Repeater Mode / Range Extender Mode**.**
- Click Scan / Search / Refresh List to view nearby Wi-Fi networks.
- Select your main router's SSID (the Wi-Fi network you want to extend)**.**
- Enter the Wi-Fi password of your router in the Pre-Shared Key or Password field.
- Click Apply / Save Settings**.**
- Wait for the repeater to reboot automatically.

6. Verify the Repeater Connection

- After reboot, disconnect the Ethernet cable**.**

- Open your Wi-Fi settings again.
- You should now see a new network name such as**.**
  HomeNetwork_EXT**,** or
  YourNetworkName-Plus
- Connect to this extended Wi-Fi network.
- Open Command Prompt → type:
  ping google.com
- If you receive replies, your repeater is configured successfully.

Bridge Installation /setup Process

1. Use the Windows key + X to open the Power User menu and select Network Connections.
2. Right-click the bridge adapter and select Properties**.**

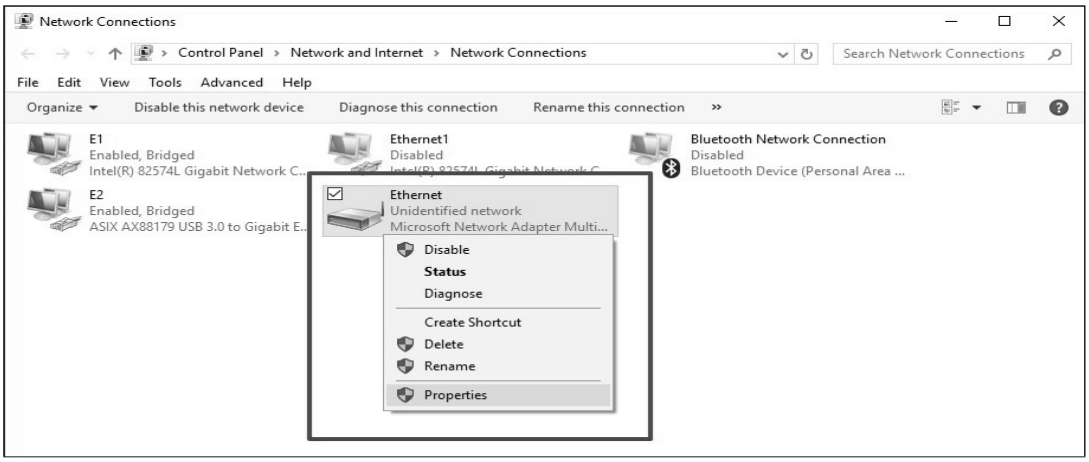


Fig. 9.3: Network Connections

3. Select the network adapter that connects to the internet.
4. Select Internet Protocol Version 4 (TCP/IPv4).
5. Click Properties**.**

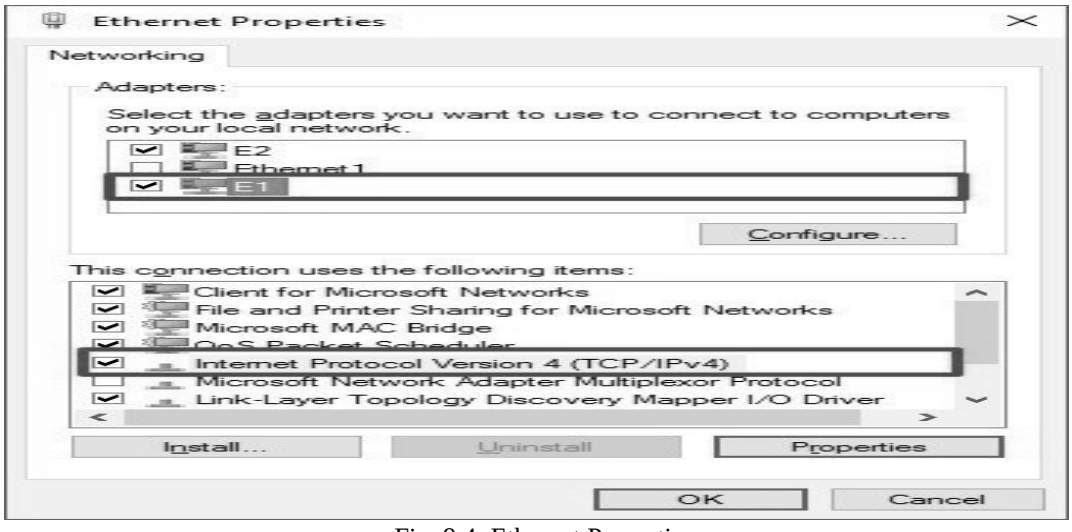


Fig. 9.4: Ethernet Properties

6. Select the Use the following IP address option.
7. Use the IP address information you collected at the beginning of this guide to assign a static IP address like is shown in the screenshot below.

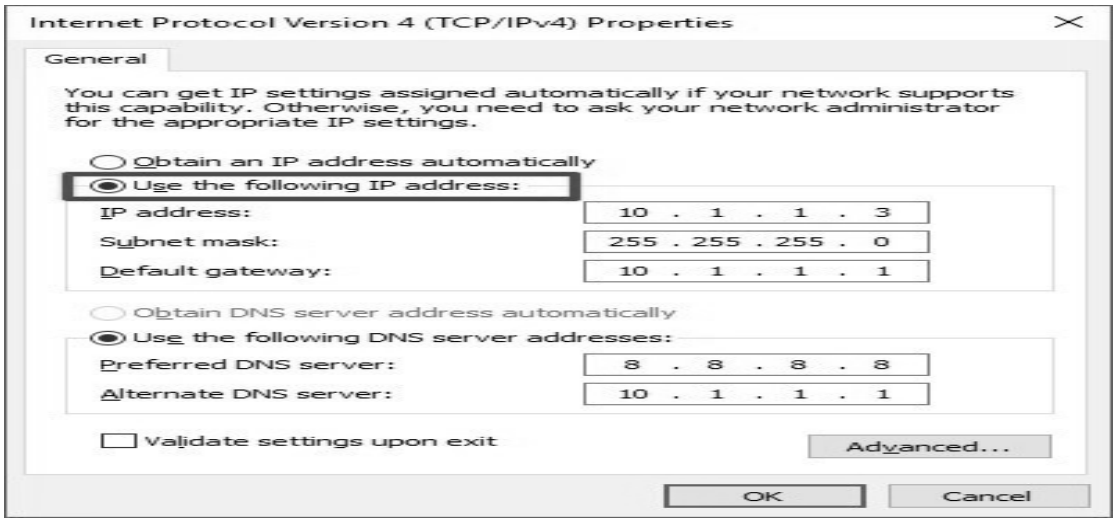


Fig. 9.5: Internet Protocol Version 4 (TCP/IPv4) Properties

8. Click OK.
9. Click Close to complete the task.

XI. Resources used during performance

Table 9.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.

XIII. Observation Table

Table 9.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful/ As Expected)	Status (Pass/Fail)
1	Connected LAN segments using Repeater	Power LED ON, Link Active		
2	Connected Bridge between two LANs	Bridge initialized		
3	Ping between PCs in different LANs	Successful replies		

XIV. Results

……..……

……...……..……

XV. Interpretation of results

……...……

……...……...

XVI. Conclusions and Recommendations

……...……

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. List the components required for this practical.
2. Describe how a repeater helps in extending the range of a data communication network.
3. List the steps involved in installing and verifying the operation of repeater.
4. Difference in operation between a bridge and a repeater based on the OSI model layers.

[Space for Answers] (If required attach separate page)

…….

…….

…….

…….

…….

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=Ke-vYlKUcnY	Bridge and Repeater Installation Demo

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Correct connection and device configuration	10%
2	Setting up bridge and repeater as per network design	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Network successfully extended using bridge and repeater	10%
2	Checking connectivity across network segments	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.10: *Troubleshoot computer network using given commands

I. Practical Significance

This practical enables student to identify, analyze, and resolve common network connectivity problems using essential network troubleshooting commands. It helps learners develop hands-on skills in diagnosing issues related to IP configuration, connectivity, and routing. By using commands such as ping, ipconfig and tracert, student gain practical experience in verifying network status, locating faults, and ensuring efficient data communication.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Select relevant network model and Transmission Media for data communication system.

IV. Laboratory Learning Outcome

LLO 10.1 Execute TCP/IP network commands: ipconfig, ping, tracert.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

In computer networks, data transmission may fail due to configuration errors, cable faults, IP conflicts, or routing issues. To detect and solve these problems, network troubleshooting commands **are used.**

1. Ipconfig Command

Ipconfig stands for Internet Protocol Configuration**.** This Command Displays detailed information about all adapters, including the IP address, subnet mask, default gateway, DHCP server, and DNS servers etc. Used without parameters ipconfig displays the IP address, subnet mask, and default gateway for all adapters. By default, this command displays only the IP address, subnet mask, and default gateway for each adapter bound to TCP/IP.

Syntax:

ipconfig [/all compartments] [/? | /all | /renew [adapter] | /release [adapter] |/renew6 [adapter] [classid] |/showclassid6 adapter | /setclassid6 adapter [classid]

Following table shows use of ipconfig command with different options:

Table 10.1

Parameter	Description
/?	Displays the help message
/all	Displays complete configuration information
/release	Uses DHCP to release the IP address for the specified adapter
/release6	Uses DHCPv6 to release the IPv6 address for the specified adapter
/renew	Uses DHCP to renew the IP address for the specified adapter
/renew6	Uses DHCPv6 to renew the IPv6 address for the specified adapter
/flushdns	Purges the DNS cache
/registerdns	Uses DHCP to refresh all DHCP leases and re-registers DNS names
/displaydns	Displays the contents of the DNS cache
/showclassid	Displays all the DHCP class IDs allowed for the adapter
/setclassid	Modifies the DHCP class ID
/showclassid6	Displays all the DHCPv6 class IDs allowed for the adapter
/setclassid6	Modifies the DHCPv6 class ID

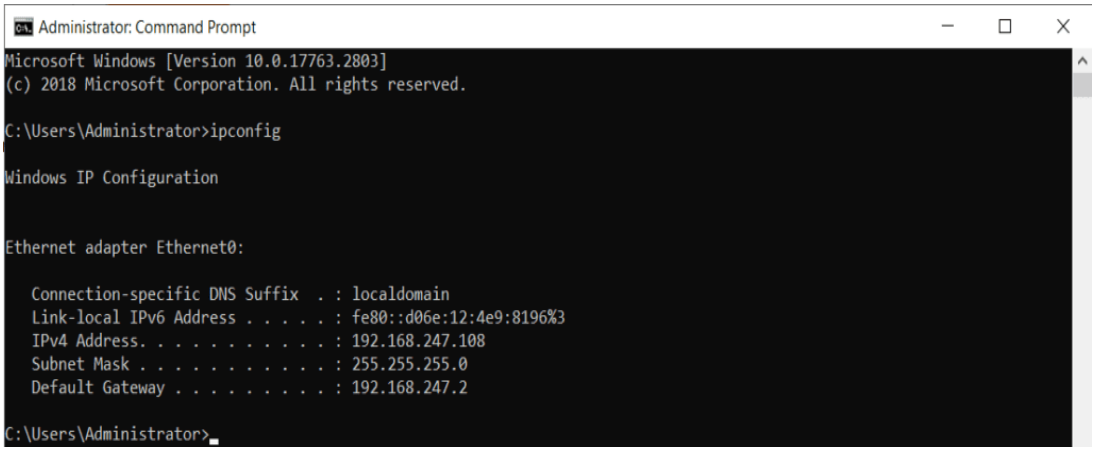


Fig. 10.1: Output screen of command C:\>ipconfig

2. Ping Command

Ping (Packet Internet groper): The ping command is the basic troubleshooting tool for TCP/IP. It is a command used to verify the network connectivity of a computer. It uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply. This command is used to test a machine‘s connectivity to another system and to verify that the target system is active. Usually, this command is the first step to any troubleshooting if a connectivity problem is occurring between two computers. The Ping utility executes an end-to-end connectivity test to other devices and obtains the round-trip time between source and destination device. Ping uses the ICMP Echo and

Echo Reply packets to test connectivity. Excessive usage may appear to be a denial of service (DoS) attack.

Syntax: ping <ip address>

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS][-r count] [-s count] [[-j host-list] | [-k host-list]][-w timeout] [-R] [-S srcaddr] [-c compartment] [-p][-4] [-6] target_name

Following table shows use of ping command with different options:

Table 10.2

Parameter	Description
-t	Pings the specified host until interrupted (press Ctrl+C to stop sending).
-a	Resolves addresses to hostnames.
-n count	Indicates the number of Echo Requests to send.
-l size	Sends a specific size of data. If this size is greater than the local network can handle, the sender will generate fragmented packets directly on the network.
-f	Sets the Don _t Fragment flag in the packet.
-i TTL	Sets the Time to Live value in the packet.
-vTOS	Sets the type of service in the packet.
-r count	Indicates that the Ping process should record the route for the number of count hops specified.
-s count	Indicates that the Ping process should maintain Timestamp information for the number of count hops specified.
-j host_list	Indicates that the Ping process should follow a loose source route path along the host_list path.
-k host_list	Indicates that the Ping process should follow a strict source route along the host_list path.
-w timeout	Indicates the number of milliseconds the host should wait for each reply.
-R	Use the router header to test the reverse route as well (IPv6 only).
-S srcaddr	What address to use to source ping from.
-p	Ping yper-V Network Virtualization provider address.
-4	Use IPv4 specifically.
-6	Use IPv6 specifically.

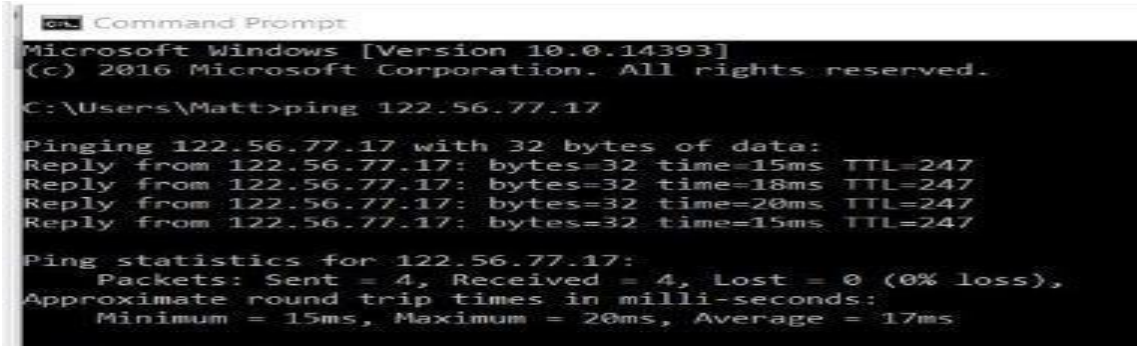


Fig. 10.2: Output screen of command C:\>ping

3. Tracert (traceroute) Command

In the internet, data packets travel through a series of routers before reaching their destination. Tracert is a command that allows you to trace this path. It traces the route taken by your data, revealing each hop (router) it encounters and the time it takes to reach it.

Syntax: tracert<ip address>

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Following table shows use of tracert command with different options:

Table 10.3

Parameter	Description
-d	Prevents tracert from resolving IP addresses to hostnames. This speeds up the display of results.
-h maximum_hops	Specifies the maximum number of hops (routers) that tracert will search for the target. The default is 30.
-j host_list	Specifies loose source routing along the host list (IPv4 only). Packets follow the listed routers but can pass through other routers as needed.
-w timeout	Specifies the time, in milliseconds, to wait for each reply. The default is 4000 milliseconds (4 seconds).
-R	Traces the round-trip path (IPv6 only). Tests the path from source to destination and back.
-f	Sets the starting TTL (Time To Live) value. Useful when testing beyond certain hops.
-r count	Records the route for a specified number of hops (less commonly used in Windows but supported in some systems).
-4	Forces tracert to use IPv4.
-6	Forces tracert to use IPv6.

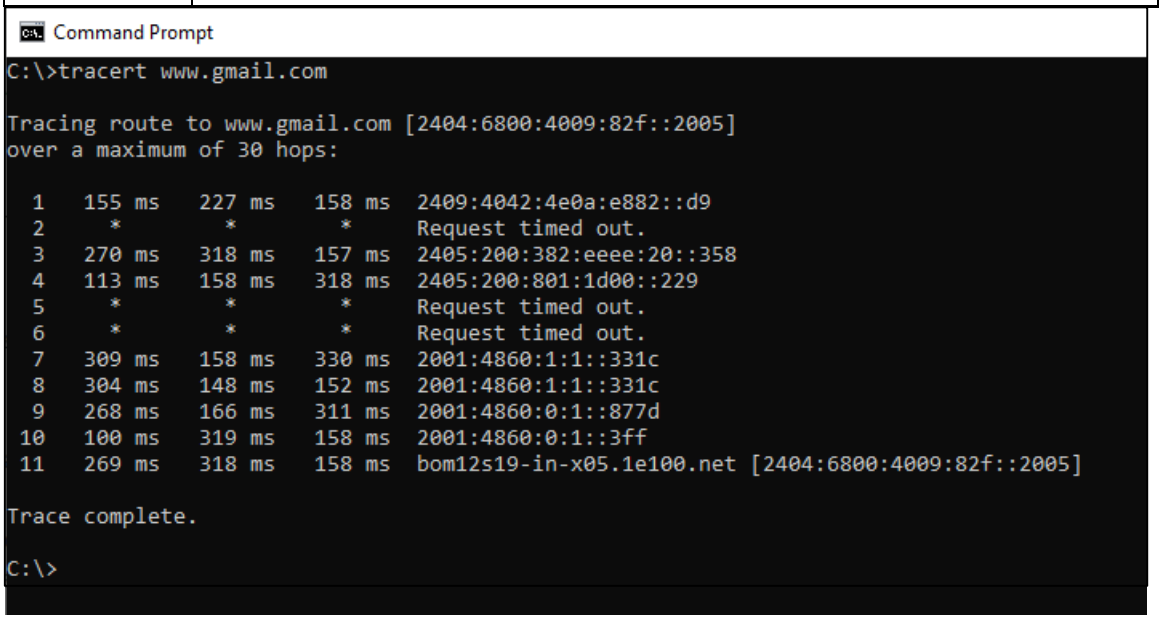


Fig. 10.3: Output screen of command C:\> tracert

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

NA

B. Actual Block Diagram

NA

VIII. Required Resources/apparatus/equipment with specifications

Table 10.4

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Internet Connectivity	LAN or Wi-Fi	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all network cables and connectors are properly attached before starting troubleshooting.
2. Record each command and observation carefully in the practical record book.
3. Save and close all open configurations properly after completing the troubleshooting process.

X. Suggested Procedure

1. Prerequisites

- All network devices are powered on and properly configured.
- IP addresses are assigned either manually or through DHCP.
- Command Prompt is accessible on all systems

2. Using the ipconfig Command

- Click on Start → Search → cmd and open the Command Prompt.
- Type the command: ipconfig
- Observe the displayed details such as IPv4 Address, Subnet Mask, and Default Gateway.
- To view detailed configuration, type: ipconfig /all
- Note the Physical (MAC) address, DNS servers, and DHCP status.
- Verify that the system has a valid IP address within the network range.

3. Using the ping Command

- Open Command Prompt on your system.

- Type the command to test loopback address: ping 127.0.0.1
- Ping your own IP address to check network card status: ping <your_IP_address>
- Ping another computer or device on the same network: ping <destination_IP_address>
- Ping an external website to check internet connectivity: ping www.google.com
- Observe the reply time (ms), TTL, and packet loss values.
- Interpret results:
  Reply received → Network path is working
  Request timed out → Network or connectivity problem exists

4. Using the tracert Command

- Open Command Prompt.
- Type the command: tracert www.google.com
- Observe each hop (router or gateway) the data passes through.
- Note the IP addresses, hop count, and response time of each node.
- Identify where packet loss or delay occurs to locate network issues.
- Save the results for analysis in your report.

5. Verification

- Check whether the local system and remote systems are reachable.
- Confirm that the routing path displayed by tracert matches the expected network design**.**

6. Result

- The network is successfully tested and troubleshoot using ipconfig, ping, and tracert commands. Network connectivity, configuration, and routing paths are verified for proper communication**.**

XI. Resources used during performance

Table 10.5

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

4.

5.

6.

7.

XIII. Observation Table

Table 10.6

Sr. No.	Action Performed	Expected Output	Actual Output(Successful/As Expected)	Status (Pass/ Fail)
1	Executed ipconfig command	Display of IPv4 address, Subnet Mask, and Default Gateway		
2	Executed ping 127.0.0.1 (loopback test)	Reply from 127.0.0.1 indicating TCP/IP is working		
3	Executed tracert www.google.com	Display of route and intermediate hops to destination		

XIV. Results

……

……...…….

XV. Interpretation of results

……..……..……

……...……...……..……

XVI. Conclusions and Recommendations

……..……

……...……...

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give the name of commands to find out hostname and MAC address of computer.
2. Give a syntax of tracert command.
3. State the importance of verifying IP configuration before performing connectivity tests.
4. Mention the command used to release and renew the IP address of a system.

[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=rurs7cdT5cc	Basic Networking Commands

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Execution of Commands	10%
2	Correct identification of PC, network cables, and connectivity	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Troubleshooting and Analysis	10%
2	Verification of Results	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.11: *Troubleshoot computer network using given commands

I. Practical Significance

This practical enables student to execute and analyze key TCP/IP network commands such as route, netstat, and pathping. It provides hands-on experience in monitoring routing tables, examining active network connections, and tracing packet paths to evaluate network performance. Through systematic command execution and interpretation, learners enhance their ability to identify routing issues, diagnose communication faults, and ensure efficient data transmission across interconnected networks. This activity strengthens both technical understanding and practical troubleshooting proficiency essential for effective network management.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Select relevant network model and Transmission Media for data communication system.

IV. Laboratory Learning Outcome

LLO 11.1 Execute TCP/IP network commands: route, netstat, pathping.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

1. Route Command

This command manipulates network routing tables. Route command is only available if the TCP/IP protocol is installed as a component in the properties of a network adapter. Route command displays or modifies the computer's routing table information. For a typical computer that has a single network interface and is connected to a local area network (LAN) that has a router, the routing table is pretty simple. If user facing trouble in accessing other computers or other networks, user can use the route command to investigate bad entry that affect in the computer's routing table. For a computer with more than one interface and that's configured to work as a router, the routing table is often a major source of trouble. Setting up the routing table properly is a key part of configuring a router to work. Earlier tracert command is used to trace the travel of packet from source to destination over a network. This command is capable to modify routing table entries hence the route command is established. To display the routing table (both IPv4 and IPv6) in Windows, use the route print command.

Syntax:

route [-f] [-p] [-4|-6] command [destination][MASK netmask] [gateway] [METRIC metric] [IF interface]

Following table shows use of route command with different options:

Table 11.1

Parameter	Description
-f	Clears the routing table
-P	When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, Which always affect the appropriate persistent routes.
Command	The command to run (add, change, delete, print)
-4	Force using IPv4
-6	Force using IPv6
Destination	Network destination of the route
mask Netmask	The netmask (subnet mask) associated with the network destination
Gateway	Specifies gateway
metric Metric	Specifies the metric, ie. Cost for the destination.
Interface	The interface number for the specified route.
/?	Command help

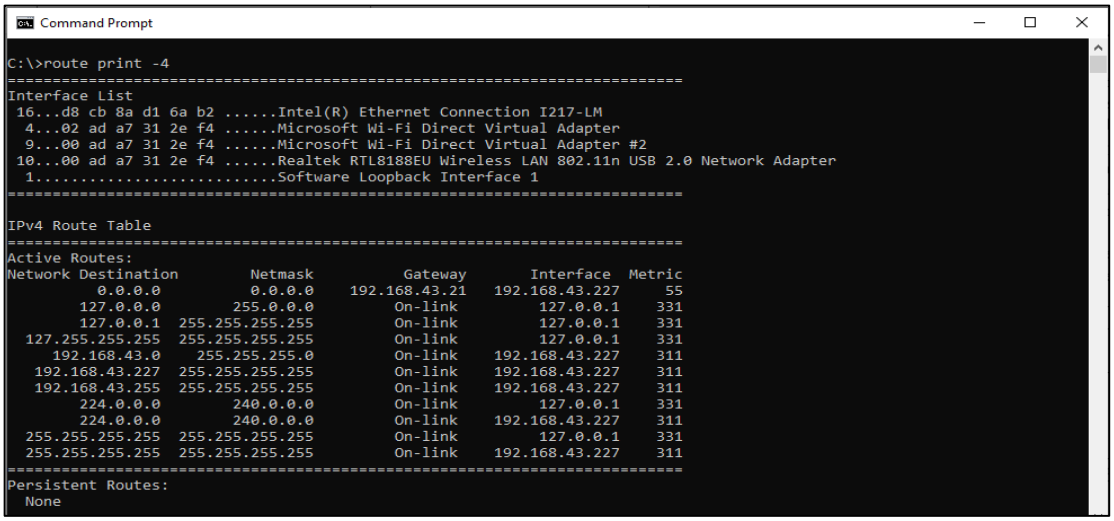


Fig. 11.1: Output of route command

2. Netstat Command

Netstat displays protocol statistics and current TCP/IP network connections. Netstat allows users to display network-related information and diagnose various networking issues. The command has several options that can be combined to retrieve specific details.

Syntax:

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

Following table shows use of netstat command with different options:

Table 11.2

Parameter	Description
-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-f	Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q	Displays all connections, listening ports, and bound no listening TCP ports. Bound no listening ports may or may not be associated with an active Connection.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays Network Direct connections, listeners, and shared endpoints.
-y	Displays the TCP connection template for all connections. Cannot be Combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

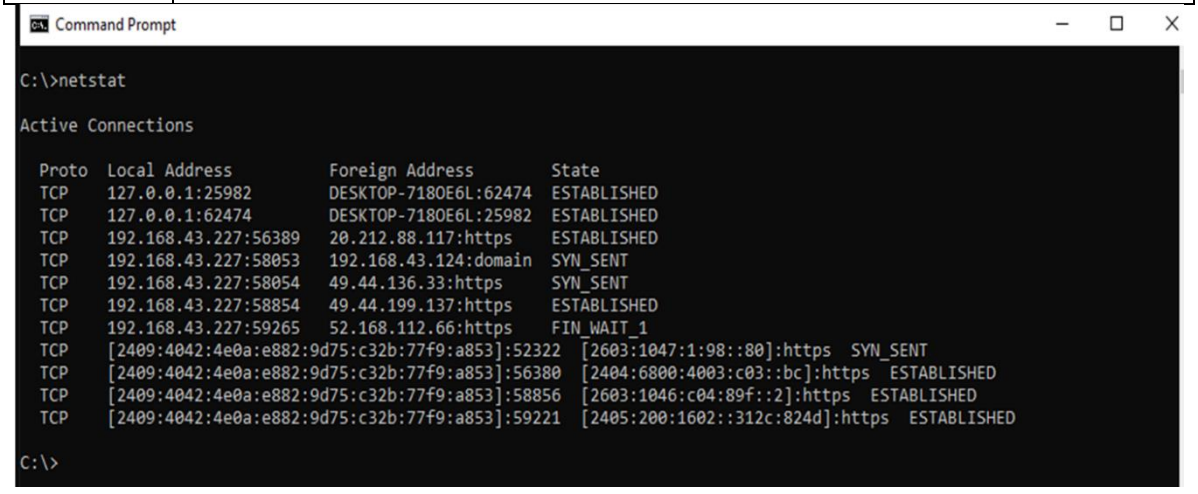


Fig. 11.2: Output of netstat command

3. **Pathping Command**

This network utility is a more advanced version of the Ping tool, which performs a ping to each hop along the route to the destination (unlike Ping, which just pings from the originating device to the destination device). It is extremely useful in diagnosing packet loss, and can help with diagnosing slow speed faults. Pathping is a TCP/IP based utility (command-line tool) that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address. It does this by sending echo requests via ICMP and analyzing the results.

Syntax:

pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries][-w timeout][-4] [-6] target_name

Following table shows use of pathping command with different options:

Table 11.3

Parameter	Description
-g <host-list>	Loose source route along host-list.
-h <maximum_hops>	Maximum number of hops to search for target
-i <address>	Use the specified source address.
-n	Do not resolve addresses to hostnames.
-p <period>	Wait period milliseconds between pings.
-q <num_queries>	Number of queries per hop.
-w <timeout >	Wait timeout milliseconds for each reply.
-4	Force using IPv4.
-6	Force using IPv6.

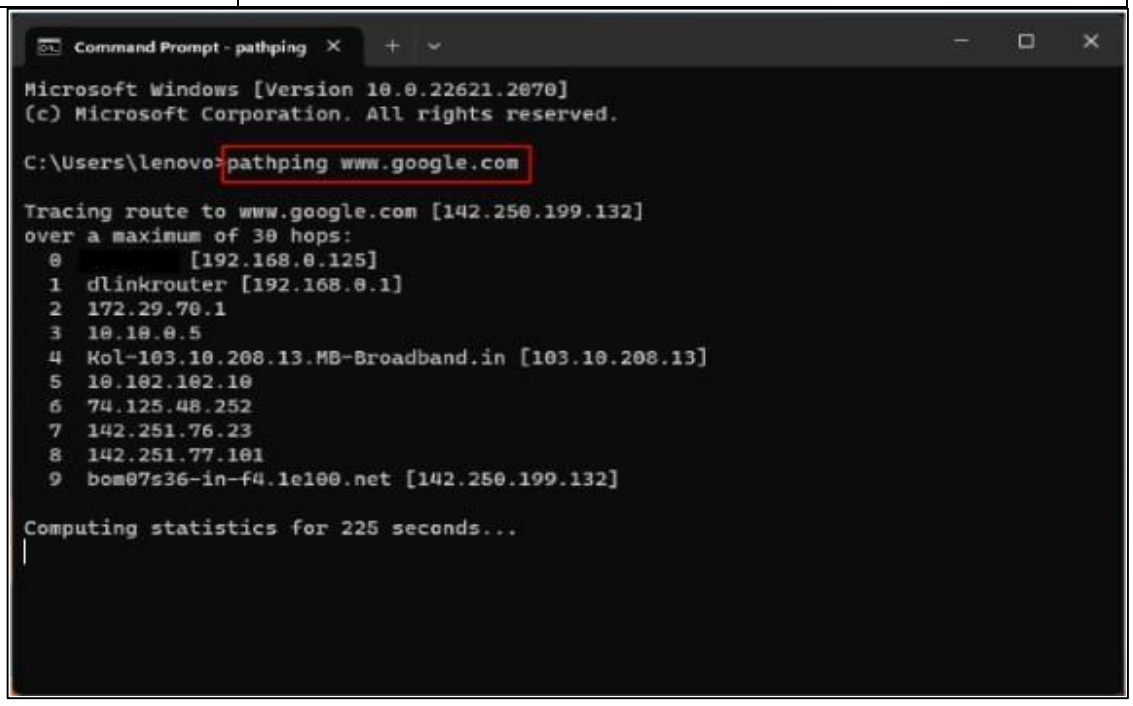


Fig. 11.3: Output of pathping command

VII. Circuit diagram / block diagram / flowchart

A. Suggestive Block Diagram

NA

B. Actual Block Diagram

NA

VIII. Required Resources/apparatus/equipment with specifications

Table 11.4

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Internet Connectivity	LAN or Wi-Fi	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all network cables and connectors are properly attached before starting troubleshooting.
2. Record each command and observation carefully in the practical record book.
3. Save and close all open configurations properly after completing the troubleshooting process.

X. Suggested Procedure

1. Prerequisites

- A computer system with Windows or Linux OS installed.
- LAN connection established or Internet connectivity available.
- The Command Prompt (cmd) is accessible with administrative rights.

2. Check IP Configuration

- Click on Start → Search → cmd and open the Command Prompt.
- Type the command: ipconfig
- Note the IP address, Subnet Mask, and Default Gateway of the system.
- Ensure the IP configuration is correct and the network is active.

3. Execute the route Command

- Display the current routing table: route print
- Observe the entries for destination, network mask, gateway, and interface.
- Add a static route: route add 192.168.20.0 mask 255.255.255.0 192.168.10.1

- Adds a route to the 192.168.20.0 network via gateway 192.168.10.1
- Delete an unwanted route: route delete 192.168.20.0
- Recheck the routing table using: route print

4. Execute the netstat Command

- To view all active connections and listening ports: netstat -a
- To view routing table information: netstat -r
- To display connections numerically (IP addresses and ports): netstat -an
- To identify which process is using each port: netstat -ano
- Observe the Local Address, Foreign Address, and State (e.g., ESTABLISHED, LISTENING.

5. Execute the pathping Command

- Type the following command to trace the route and analyze packet loss: pathping google.com
- The command first traces the route (like tracert) and then calculates packet loss and latency at each hop**.**
- Wait until the complete analysis is displayed.
- Identify any hop with high latency or packet loss.

6. Result

- The commands route, netstat, and pathping were executed successfully. The system's routing table, active network connections, and path analysis were displayed correctly, verifying proper TCP/IP network configuration and connectivity.

XI. Resources used during performance

Table 11.5

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

4.

5.

6.

7.

8.

XIII. Observation Table

Table 11.6

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Executed route print command	Display of current routing table showing destination, network mask, gateway, and		
2	Executed netstat -an command	List of all active TCP/UDP connections with local and foreign addresses and port status		
3	Executed pathping www.google.com command	Display of route with hop numbers, latency, and packet loss statistics for each hop		

XIV. Results

……..……

……..……..

XV. Interpretation of results

……..……

……..……...

XVI. Conclusions and Recommendations

……..…….

……..…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give syntax of commands for adding, deleting IP addresses from routing table.
2. State the purpose of the route command in a TCP/IP network.
3. State the function of the pathping command in analyzing network paths.
4. Mention the use of the netstat command to display network statistics.

[Space for Answers] (If required attach separate page)

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=bxFwpm4IobU	Netstat Command
2	https://www.youtube.com/watch?v=ynUGngoK8sU	Pathping Command
3	https://www.youtube.com/watch?v=2L8oPYkw26M	Route Command

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Execution of Commands	10%
2	Correct use of syntax to display, add, or delete routes and interpret the routing table	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Route traced successfully with hop-wise statistics and minimal packet loss	10%
2	Verification of Results	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.12: *Prepare a standard network straight cable by using crimping tool

I. Practical Significance

This practical enables student to perform the process of preparing a standard Ethernet straight-through cable using a crimping tool and RJ-45 connectors. It helps learners gain hands-on experience in selecting the correct wire standard (T568A or T568B), arranging the colour codes, and crimping the cable properly to ensure reliable data transmission. Through this activity, student develop practical skills in assembling and testing network cables, which are essential for creating physical connections between devices such as computers, switches, and routers in a LAN environment. This practical also enhances knowledge of basic cabling standards, signal transmission, and the importance of proper termination for efficient network performance.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Select relevant network model and Transmission Media for data communication system.

IV. Laboratory Learning Outcome

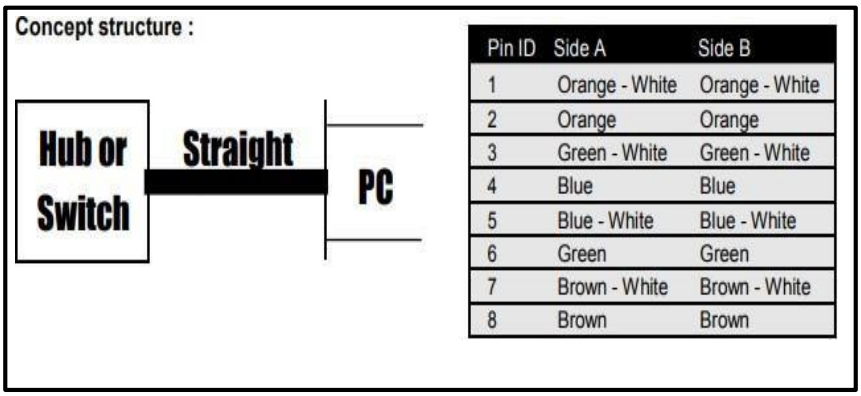
LLO 12.1 Prepare a straight patch cord cable to connect the devices in the LAN.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

Straight-through cables will be used to connect different of hosts to each other. This means that whenever you are connecting a computer to a router, a router to a switch, and so on, you will have to use a straight-through cable for the hosts to communicate with each other.



Pin ID	Side A	Side B
1	Orange - White	Orange - White
2	Orange	Orange
3	Green - White	Green - White
4	Blue	Blue
5	Blue - White	Blue - White
6	Green	Green
7	Brown - White	Brown - White
8	Brown	Brown

Fig. 12.1 Colour Code on Both Side

RJ45 Connector

The RJ-45 (Registered Jack 45) connector is an 8-pin modular plug used primarily for terminating Ethernet cables (UTP or STP) in computer networking. It serves as the physical interface between network cables and networking devices such as computers, switches, routers, and hubs. RJ-45 connectors are standardized under the EIA/TIA-568 wiring standards, ensuring compatibility and uniformity across all Ethernet installations. Each RJ-45 connector has eight metal contacts (pins) that correspond to the eight wires inside a twisted-pair cable. These contacts are responsible for transmitting and receiving data signals. The connector body is made of transparent plastic, allowing easy verification of correct wire order before crimping.

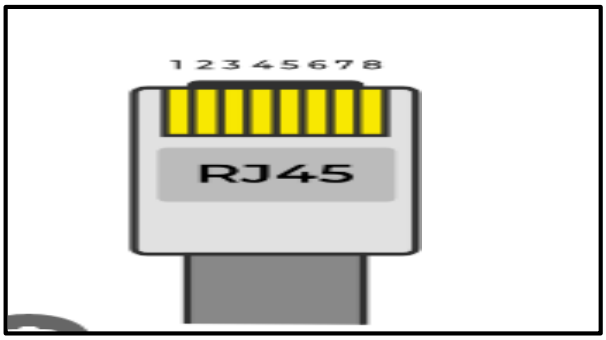


Fig. 12.2 RJ 45 Connector

Crimping Tool

A crimping tool is a hand-held device used to attach connectors, such as RJ-45 plugs, to the ends of network cables like Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) cables. It performs a mechanical operation called crimping, which involves pressing and securing the metal pins of the connector into the individual copper wires inside the cable. This ensures a firm electrical contact and a secure mechanical connection between the cable and connector.

Fig. 12.3 Crimping Tool

Cable Tester

A Cable Tester is an electronic device used to verify the integrity and correctness of network cables, such as Ethernet (UTP/STP) cables terminated with RJ-45 connectors. It checks whether each wire within the cable is properly connected and whether there are any faults like open circuits, short circuits, crossed pairs, or miswiring.

Fig. 12.4 Cable Tester

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

NA

B. Actual Block Diagram

NA

VIII. Required Resources/apparatus/equipment with specifications

Table 12.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Connector (RJ45 connector)	8-pin (8P8C) modular connector, used with Cat5e/Cat6 UTP cables, gold-plated contacts; follows T568A/B standard, supports up to 1–10 Gbps	02
4	Crimping tool	Handheld tool for cutting, stripping, and crimping RJ-45 connectors, supports Cat5e/Cat6 cables, steel body with PVC grip	01
5	Line tester or cable tester	LAN cable tester with main and remote unit, 8 LED indicators, 9V battery operated; tests continuity, pairing, and wiring faults (open, short, cross)	01
6	Network Cable (UTP Cable)	Category 5e or 6 Unshielded Twisted Pair (UTP) cable, 4 twisted pairs (8 copper wires); used for Ethernet LAN connections; supports up to 1 Gbps (Cat5e) or 10 Gbps (Cat6)	As required

IX. Precautions to be followed

1. Ensure the power supply is disconnected before connecting or testing network cables.
2. Use proper wire colour sequence (T568B or T568A) at both ends of the cable.
3. Check for correct pin alignment before pressing the crimp handle.
4. After crimping, verify continuity using a cable tester before actual network use.

X. Suggested Procedure

1. Collect the Required Materials

- Gather the necessary components and tools: UTP cable (Cat5e or Cat6), two RJ-45 connectors, crimping tool, wire stripper or cutter, and LAN cable tester.

2. Measure and Cut the Cable

- Take the required length of UTP cable using a measuring scale.
- Use the cutter section of the crimping tool to cut the cable neatly.

3. Strip the Outer Sheath

- Using the stripper section of the crimping tool, remove about 1 inch (2.5 cm) of the outer insulation from both ends of the cable.
- Be careful not to damage the inner twisted pairs.

Fig. 12.5 Cut cable plastic cover

4. Untwist and Arrange Wires

- Separate and slightly untwist the four colour pairs of wires (total eight):
  1. Orange–White / Orange
  2. Green–White / Green
  3. Blue–White / Blue
  4. Brown–White / Brown

Fig. 12.6 Separate pair wires

- Untwist the pairs slightly and arrange the wires in the T568B colour code sequence:
  1. Orange-White
  2. Orange
  3. Green-White
  4. Blue
  5. Blue-White
  6. Green

7. Brown-White
8. Brown

5. Straighten and Trim the Wires

- Align the wires flat, side by side, in the correct order.
- Cut all wires evenly to about ½ inch (1.3 cm) from the sheath end**.**

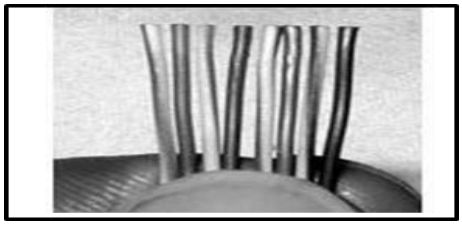


Fig. 12.7 Straighten Wire

6. Insert Wires into RJ-45 Connector

- Hold the RJ-45 connector with the clip facing down.
- Carefully insert the wires into the connector so that each wire goes fully into its slot and touches the metal contacts.
- Ensure the colour order remains correct and the cable sheath fits slightly inside the connector for support.

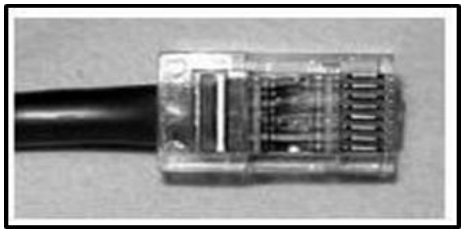


Fig. 12.8 Fit cable in to Connector

7. Crimp the Connector

- Place the connector (with cable inserted) into the crimping slot of the tool.
- Press the handles firmly until you hear a click, ensuring the pins pierce the wires and the connector is locked securely.

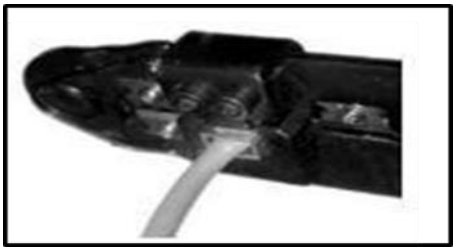


Fig. 12.9 Crimping the cable

- Repeat the same steps for the other end of the cable.

8. Test the Cable

- Connect one end of the cable to the main unit and the other to the remote unit of the cable tester.
- Switch on the tester and observe the LED indicators.
- If all eight LEDs light up in order, the cable is correctly made and functional.
- If any LED fails to light or glows out of order, recheck the wiring and redo the crimping if necessary.

Fig. 12.10 Cable or line Tester

XI. Resources used during performance

Table 12.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.
2.
3.
4.
5.
6.
7.

XIII. Observation Table

Table 12.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Arranged wires in T568B color code	Correct color sequence obtained		
2	Inserted wires into RJ-45 connector	All eight wires fully inserted in correct order and visible at connector end		
3	Crimped the RJ-45 connector using crimping tool	Connector pins properly pressed into wires ensuring firm		
4	Tested cable using LAN cable tester	All 8 LEDs glow in proper sequence indicating correct wiring		

XIV. Results

……..……

……...……..

XV. Interpretation of results

……..……

……...……..……

XVI. Conclusions and Recommendations

……..…….

……..…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of preparing a straight-through Ethernet cable.
2. Mention the function of the RJ-45 connector in LAN networks.
3. Give the names of RJ45 pin out for each pin along with pin number.
4. Describe the role of the crimping tool in cable preparation.

[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=Uw8FSXx4dnU	Process of straight-through cable by using crimping tool

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Proper selection and use of tools (UTP cable, RJ-45 connector, crimping tool, cable tester)	10%
2	Correct wire arrangement as per T568B colour code standard	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Accuracy of wiring sequence	10%
2	Correct wiring sequence verified using cable tester	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.13: *Create cross-over network straight cable by using crimping tool

I. Practical Significance

This practical enables student to perform the process of preparing a cross-over Ethernet cable using a crimping tool and RJ-45 connectors. Student gain hands-on experience in selecting and applying the correct wiring standards (T568A and T568B) on opposite ends of the cable, arranging the colour codes, and crimping the connectors properly to ensure reliable data transmission. Through this activity, student develop practical skills in assembling and testing network cables, which are essential for creating direct device-to-device connections, such as connecting two computers or switches without an intermediate hub in a LAN environment. This practical also enhances knowledge of cabling standards, signal transmission, and the importance of proper termination for efficient and error-free network performance.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Select relevant network model and Transmission Media for data communication system.

IV. Laboratory Learning Outcome

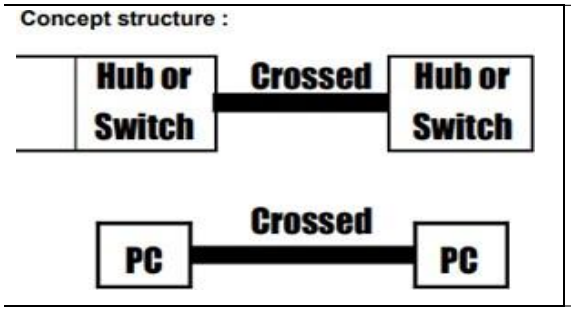
LLO 13.1 Prepare cross-connection cables to connect the devices in the LAN.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

A cross-over cable is a type of Ethernet cable in which the transmit and receive wire pairs are crossed between the two ends. Unlike a straight-through cable, where both ends follow the same wiring standard (T568A–T568A or T568B–T568B), a cross-over cable uses T568A on one end and T568B on the other.



Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white

Fig. 13.1 Colour code on both side

RJ45 Connector

The RJ-45 (Registered Jack 45) connector is an 8-pin modular plug used primarily for terminating Ethernet cables (UTP or STP) in computer networking. It serves as the physical interface between network cables and networking devices such as computers, switches, routers, and hubs. RJ-45 connectors are standardized under the EIA/TIA-568 wiring standards, ensuring compatibility and uniformity across all Ethernet installations. Each RJ-45 connector has eight metal contacts (pins) that correspond to the eight wires inside a twisted-pair cable. These contacts are responsible for transmitting and receiving data signals. The connector body is made of transparent plastic, allowing easy verification of correct wire order before crimping.

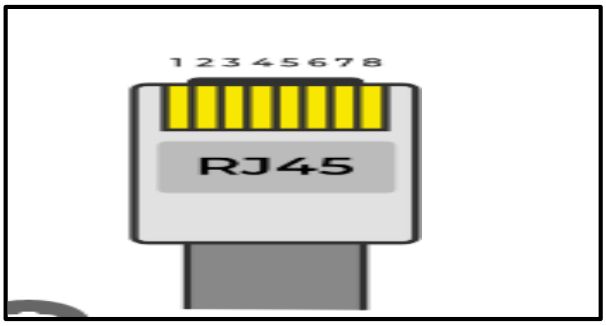


Fig. 13.2 RJ 45 Connector

Crimping Tool

A crimping tool is a hand-held device used to attach connectors, such as RJ-45 plugs, to the ends of network cables like Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) cables. It performs a mechanical operation called crimping, which involves pressing and securing the metal pins of the connector into the individual copper wires inside the cable. This ensures a firm electrical contact and a secure mechanical connection between the cable and connector.

Fig. 13.3 Crimping Tool

Cable Tester

A Cable Tester is an electronic device used to verify the integrity and correctness of network cables, such as Ethernet (UTP/STP) cables terminated with RJ-45 connectors. It checks whether each wire within the cable is properly connected and whether there are any faults like open circuits, short circuits, crossed pairs, or miswiring.

Fig. 13.4 Cable Tester

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

NA

B. Actual Block Diagram

NA

VIII. Required Resources/apparatus/equipment with specifications

Table 13.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Connector (RJ45 connector)	8-pin (8P8C) modular connector, used with Cat5e/Cat6 UTP cables, gold-plated contacts; follows T568A/B standard, supports up to 1–10 Gbps	02
4	Crimping tool	Handheld tool for cutting, stripping, and crimping RJ-45 connectors, supports Cat5e/Cat6 cables, steel body with PVC grip	01
5	Line tester or cable tester	LAN cable tester with main and remote unit, 8 LED indicators, 9V battery operated; tests continuity, pairing, and wiring faults (open, short, cross)	01
6	Network Cable (UTP Cable)	Category 5e or 6 Unshielded Twisted Pair (UTP) cable, 4 twisted pairs (8 copper wires); used for Ethernet LAN connections; supports up to 1 Gbps (Cat5e) or 10 Gbps (Cat6)	As required

IX. Precautions to be followed

1. Ensure the power supply is disconnected before connecting or testing network cables.
2. Use the correct wiring standards (T568A at one end and T568B at the other).
3. Check for correct pin alignment before pressing the crimp handle.
4. After crimping, verify continuity using a cable tester before actual network use.

X. Suggested Procedure

1. Collect the Required Materials

- Gather the necessary components and tools: UTP cable (Cat5e or Cat6), two RJ-45 connectors, crimping tool, wire stripper or cutter, and LAN cable tester.

2. Measure and Cut the Cable

- Take the required length of UTP cable using a measuring scale.
- Use the cutter section of the crimping tool to cut the cable neatly.

3. Strip the Outer Sheath

- Using the stripper section of the crimping tool, remove about 1 inch (2.5 cm) of the outer insulation from both ends of the cable.
- Be careful not to damage the inner twisted pairs.

Fig. 13.5 Cut cable plastic cover

4. Untwist and Arrange Wires

- Separate and slightly untwist the four colour pairs of wires (total eight):
  1. Orange–White / Orange
  2. Green–White / Green
  3. Blue–White / Blue
  4. Brown–White / Brown

Fig. 13.6 Separate pair wires

- Arrange the wires according to cross-over wiring:

  One end – T568A Standard:

  1. Orange-White
  2. Orange
  3. Green-White
  4. Blue
  5. Blue-White
  6. Green

7. Brown-White
8. Brown

Other end – T568B Standard:

1. Green-White
2. Green
3. Orange-White
4. Brown-White
5. Brown
6. Orange
7. Blue
8. Blue-White

5. Straighten and Trim the Wires

- Align the wires flat, side by side, in the correct order.
- Cut all wires evenly to about ½ inch (1.3 cm) from the sheath end**.**

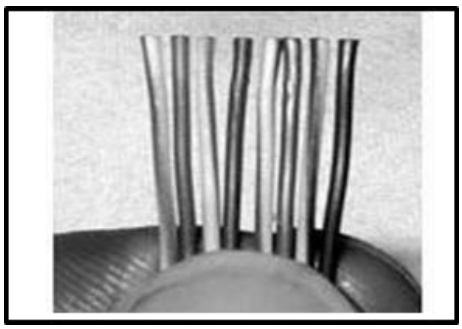


Fig. 13.7 Straighten Wire

6. Insert Wires into RJ-45 Connector

- Hold the RJ-45 connector with the clip facing down.
- Carefully insert the wires into the connector so that each wire goes fully into its slot and touches the metal contacts.
- Ensure the colour order remains correct and the cable sheath fits slightly inside the connector for support.

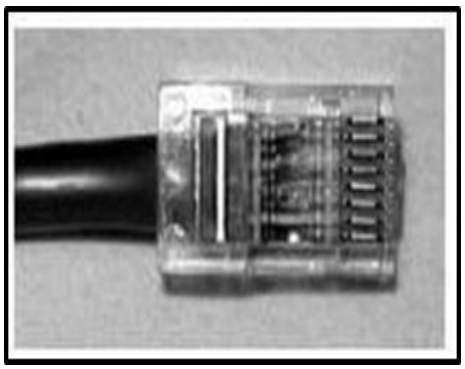


Fig. 13.8 Fit cable in to Connector

7. Crimp the Connector

- Place the connector (with cable inserted) into the crimping slot of the tool.
- Press the handles firmly until you hear a click, ensuring the pins pierce the wires and the connector is locked securely.

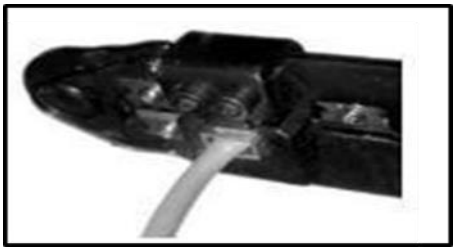


Fig. 13.9 Crimping the cable

- Repeat the same steps for the other end of the cable.

8. Test the Cable

- Connect one end of the cable to the main unit and the other to the remote unit of the cable tester.
- Switch on the tester and observe the LED indicators.
- If all eight LEDs light up in order, the cable is correctly made and functional.
- If any LED fails to light or glows out of order, recheck the wiring and redo the crimping if necessary.

Fig. 13.10 Cable or line Tester

XI. Resources used during performance

Table 13.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

4.

5.

XIII. Observation Table

Table 13.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful/As Expected)	Status (Pass/Fail)
1	Arranged wires in T568A standard at one end and T568B standard at the other end	Correct cross-over wiring sequence obtained		
2	Inserted wires into RJ-45 connector	All eight wires fully inserted in correct order and visible at connector end		
3	Crimped both RJ-45 connectors using crimping tool	Connector pins properly pressed into wires ensuring firm connection		

XIV. Results

……..……

……...……...

XV. Interpretation of results

……..……

……...……...……

XVI. Conclusions and Recommendations

……..…….

……..…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of preparing a cross-over Ethernet cable.
2. Mention the difference between straight-through and cross-over cables.
3. State the sequence of wires at each end of a cross-over cable.

[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=VZZq7MbvAuE	Process of cross-over cable by using crimping tool

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Proper selection and use of tools (UTP cable, RJ-45 connector, crimping tool, cable tester)	10%
2	Correct wire arrangement at each end according to T568A and T568B standards	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Accuracy of wiring sequence	10%
2	Correct wiring sequence verified using cable tester	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.14: *Use PDU tool to analyse layers of OSI Model

I. Practical Significance

This practical enables student to analyze and visualize how data is encapsulated and transmitted across the different layers of the OSI model using a PDU (Protocol Data Unit) tool. Student gain hands-on experience in observing the process of segmentation, addressing, and encapsulation at each layer, from the application layer down to the physical layer. Through this learners develop practical skills in understanding network communication, protocol interaction, and data flow, which are essential for designing, troubleshooting, and optimizing network operations. This practical also enhances knowledge of OSI layer functions, protocol behaviour, and the role of headers and trailers in efficient and reliable data transmission across networks.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Select relevant network model and Transmission Media for data communication system.

IV. Laboratory Learning Outcome

LLO 14.1 Capture Protocol Data Unit information of the TCP/IP and OSI Model using network simulator.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

The OSI (Open Systems Interconnection) Model is a conceptual framework used to understand and standardize the functions of a telecommunication or computing system without regard to its underlying internal structure and technology. It divides network communication into seven distinct layers, each with specific responsibilities:

1. **Application Layer (Layer 7):** Provides network services directly to applications, such as email, file transfer, and web browsing.
2. **Presentation Layer (Layer 6):** Translates data formats, performs encryption/decryption, and handles data compression.
3. **Session Layer (Layer 5):** Establishes, manages, and terminates communication sessions between applications.
4. **Transport Layer (Layer 4):** Ensures reliable data transfer, error detection, and flow control using protocols like TCP and UDP.
5. **Network Layer (Layer 3):** Determines logical addressing and routing of data packets across multiple networks (IP addressing, routing).

6. **Data Link Layer (Layer 2):** Handles physical addressing (MAC), error detection, and frames data for transmission over the physical medium.
7. **Physical Layer (Layer 1):** Deals with the transmission and reception of raw bit streams over a physical medium (cables, wireless signals).

PDU (Protocol Data Unit) Tool:

A PDU tool allows learners to simulate and analyze how data moves through the OSI layers. It generates and displays PDUs at each layer of the OSI model:

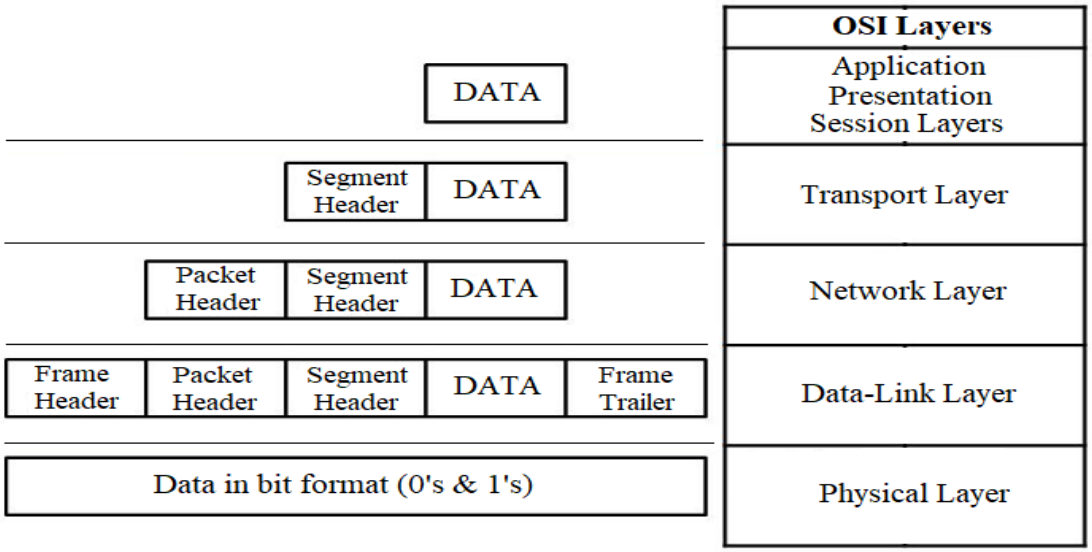


Fig. 14.1 Data Encapsulation at each OSI layer

(Courtesy:https://www.ques10.com/p/66119/discuss-data-encapsulation-process-on-the-osi-mode/)

VII. Circuit diagram / block diagram

A. Suggestive Block Diagram

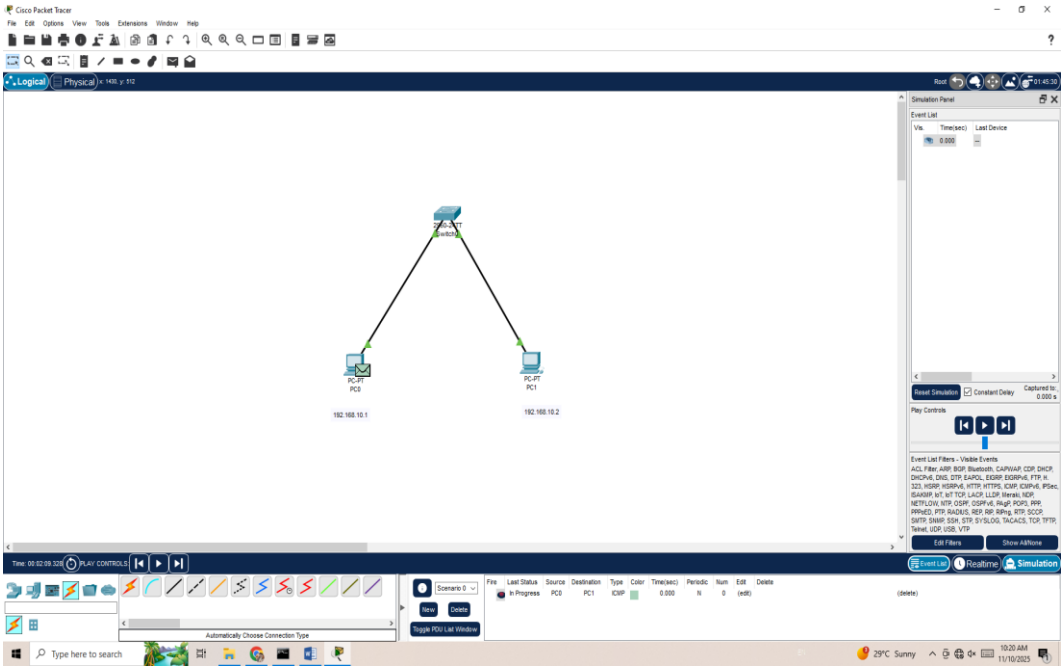


Fig. 14.2 Topology Block Diagram

B. Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 14.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch-4/8/16/24/32	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure the network simulator software is properly installed and functional before starting the practical.
2. Verify that the PDU tool module is correctly configured for the selected devices.
3. Select the correct source and destination devices to avoid errors in PDU generation.
4. Observe all PDU headers, trailers, and encapsulation steps carefully without skipping layers.

X. Suggested Procedure

1. Prerequisite

- Computer with network simulator software (e.g., Cisco Packet Tracer or similar).
- PDU tool/module in the simulator.
- Pre-configured simple network topology (e.g., two PCs connected via a switch).

2. Launch the PDU Tool

- Open the network simulator and select the PDU tool option.
- Choose the source and destination devices between which you want to analyze data flow.

Fig. 14.3 Simulation Mode

3. Select Protocol and Message Type

- Choose the protocol (TCP, UDP, ICMP, etc.) to be used for the PDU.
- Enter the message or data to be transmitted for simulation.

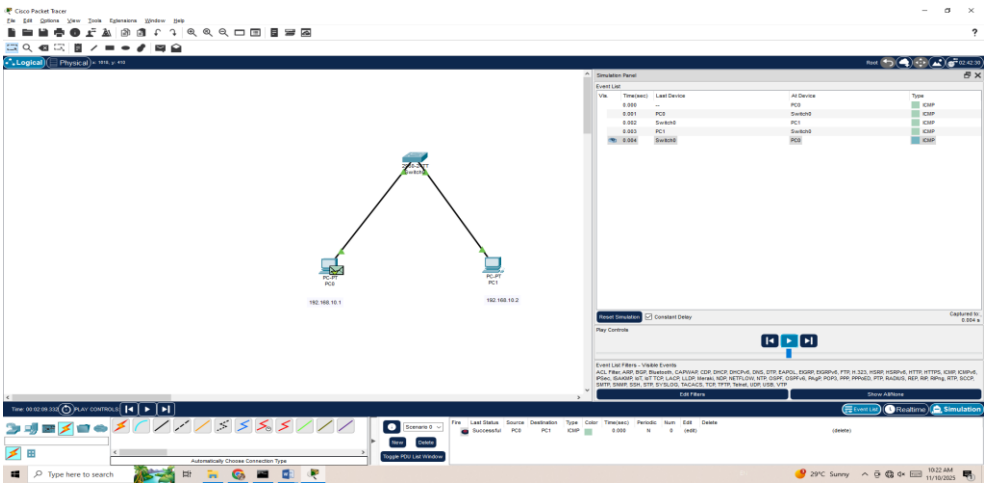


Fig. 14.4 Simulation of ICMP Packet for PDU

4. Generate the PDU

- Click “Send” or “Create PDU” to simulate data transfer from source to destination.
- Observe the PDU creation and encapsulation as it passes through the OSI layers.

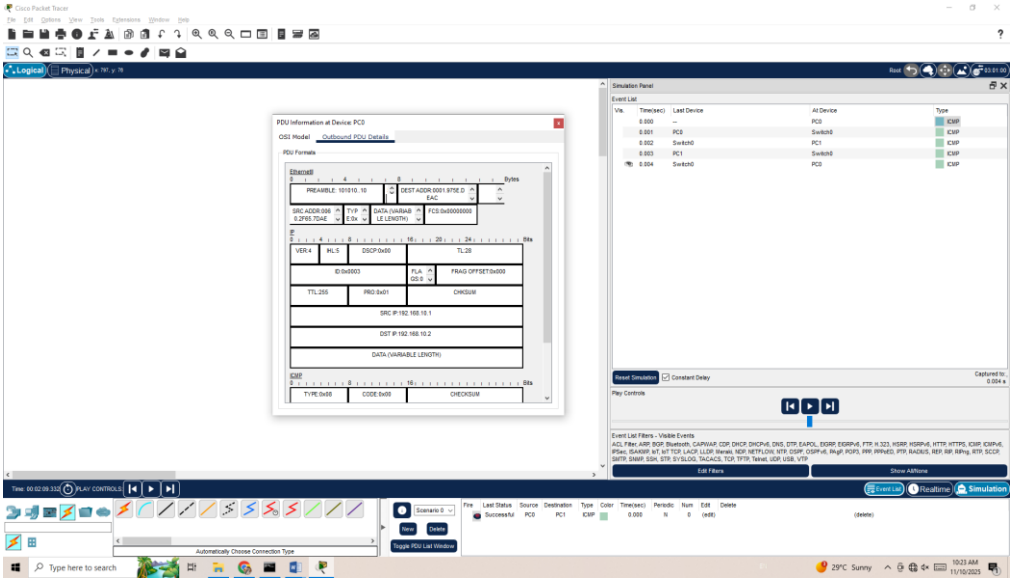


Fig. 14.5 PDU Details

5. Analyze PDU at Each Layer

- Examine the Application Layer to see the actual data/message.
- Check the Transport Layer segment, noting port numbers and headers.
- Observe the Network Layer packet, including source/destination IP addresses.
- Inspect the Data Link Layer frame, including MAC addresses and error-checking information.
- Review the Physical Layer representation as bits or binary data.

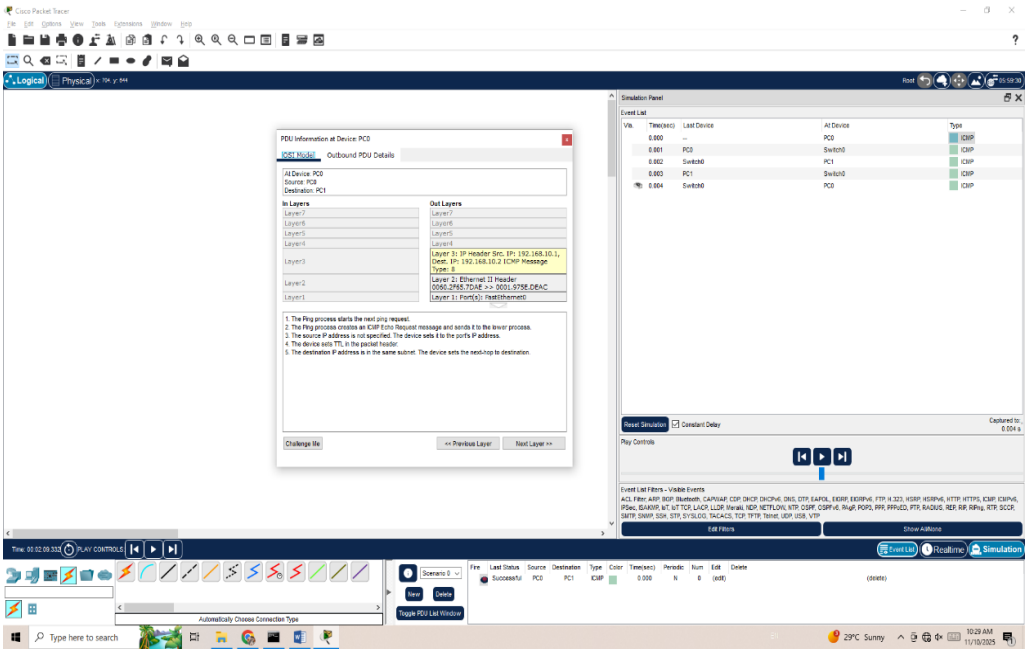


Fig. 14.6 PDU Details at each layer

6. **Trace the Path and Encapsulation**
   - Follow the PDU as it traverses through the network devices.
   - Note how encapsulation is added at each layer and removed at the destination (de-encapsulation).
7. **Record Observations**
   - Fill in the observation table with details of PDUs at each layer.
   - Note any anomalies or points of interest, such as header/trailer changes or packet drops.
8. **Repeat with Different Protocols or Devices**
   - Generate PDUs using TCP, UDP, or ICMP to compare encapsulation differences.
   - Test with different source/destination devices to observe addressing changes.

XI. Resources used during performance

Table 14.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

4.

5.

6.

7.

XIII. Observation Table

Table 14.3

Sr. No.	Action Performed	Expected Output	Actual Output(Successful /As Expected)	Status (Pass/Fail)
1	Generated PDU using ICMP protocol	PDU created with Transport layer segment containing correct port information		
2	Observed PDU at Network layer	Packet contains correct source and destination IP		
3	Observed PDU at Data Link layer	Frame contains source/destination MAC addresses and trailer information		
4	Verified ICMP echo request and reply	Destination device sends ICMP echo reply successfully		

XIV. Results

……..……

……...……..…….

XV. Interpretation of results

……...…

……...……...…

XVI. Conclusions and Recommendations

……...…

…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of PDU tool in network simulation.
2. Mention the method to trace a PDU through all OSI layers.
3. Describe the function of the Transport Layer in data encapsulation.
4. State the method to verify encapsulation and de-encapsulation in the simulation.

[Space for Answers] (If required attach separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.youtube.com/watch?v=BQel5VyhUZA	PDU tool to analyses layers of OSI Model

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Proper selection and use of PDU tool	10%
2	Correct step-by-step observation of PDUs at each OSI layer	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct creation of PDU with proper encapsulation	10%
2	Proper identification of addressing (MAC, IP, ports)	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.15: Implementation of the Hamming code using C programming language to detect error

I. Practical Significance

This practical enables student to implement the Hamming code algorithm using the C programming language to detect single-bit errors in data transmission. Student gain hands-on experience in encoding data, generating parity bits, and identifying errors during transmission. Through this, learners develop practical skills in error detection and correction techniques, which are essential for ensuring data integrity in digital communication systems. This practical also enhances knowledge of binary arithmetic, parity calculation, and locating errors, strengthening the ability to maintain reliable and efficient data transmission in computer networks and digital systems.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Troubleshoot transmission errors and flow control of the data in Data Link Layer.

IV. Laboratory Learning Outcome

LLO 15.1 Develop and test 'C' program for error detection using Hamming code.

V. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader or a team member.
2. Follow ethical practices.

VI. Relevant Theoretical Background

In digital communication systems, errors can occur when data is transmitted over noisy channels. The Hamming Code, developed by Richard W. Hamming in 1950, is one of the earliest and most widely used error detection and correction codes. It not only detects single-bit errors but can also correct them automatically, improving the reliability of data transmission.

Key Concepts:

1. **Error Detection**
   - Single-bit errors occur when data is transmitted through noisy channels.
   - Hamming Code detects these errors using parity bits embedded in the data.
2. **Parity Bits**
   - For m data bits, the number of parity bits r is chosen such that: $2^r \geq m + r + 1$
   - Parity bits are placed at positions that are powers of 2: 1, 2, 4, 8…

- Each parity bit covers certain bits according to the binary representation of positions.

3. **Codeword Formation**
   - Data bits are placed in positions not occupied by parity bits.
   - Parity bits are calculated using even parity.
4. **Error Detection Process**
   - The receiver recalculates parity bits.
   - Discrepancies indicate the presence of an error.
   - The syndrome (binary value from parity check) identifies the erroneous bit position.
   - For error detection only, the system identifies the error but does not correct it.

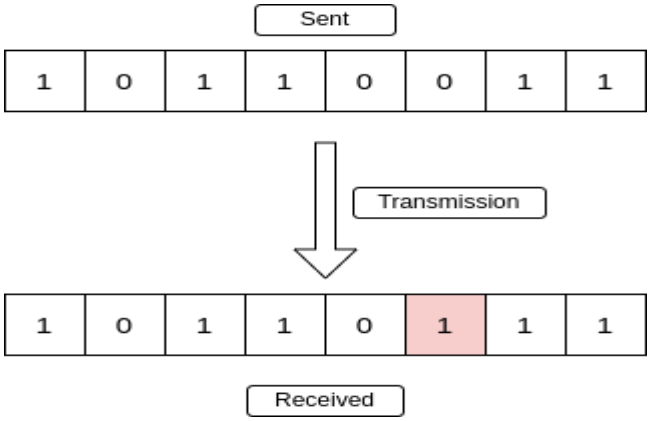


Fig. 15.1 Single bit error

The following program will demonstrate implementation of Hamming code using C programming language to detect errors.

```
#include <stdio.h>
#include <math.h>
// Generate Hamming code with parity bits
void generateHammingCode(int data[], int m, int codeword[], int *r) {
   int i, j, k = 0;
   while(pow(2, *r) < (m + *r + 1)) (*r)++;
   int totalBits = m + *r;
   for(i = 1, j = 1; i <= totalBits; i++) {
      if(i == pow(2, j-1)) codeword[i] = 0, j++;
      else codeword[i] = data[k++];
   }
   for(i = 0; i < *r; i++) {
      int parityPos = pow(2, i), count = 0;
      for(j = parityPos; j <= totalBits; j++)
         if(j & parityPos) count += codeword[j];
      codeword[parityPos] = count % 2;
   }
}
```

```
// Detect single-bit error
int detectError(int codeword[], int totalBits, int r) {
   int errorPos = 0;
   for(int i=0;i<r;i++) {
      int parityPos = pow(2,i), count = 0;
      for(int j=1;j<=totalBits;j++)
         if(j & parityPos) count += codeword[j];
      if(count % 2 != 0) errorPos += parityPos;
   }
   return errorPos;
}

int main() {
   int data[20], codeword[20], m, r=0, totalBits;
   printf("Enter number of data bits: ");
   scanf("%d", &m);
   printf("Enter data bits (from LSB to MSB): ");
   for(int i=0;i<m;i++) scanf("%d",&data[i]);
   generateHammingCode(data,m,codeword,&r);
   totalBits = m+r;
   printf("\nGenerated Hamming Code: ");
   for(int i=totalBits;i>=1;i--) printf("%d",codeword[i]);
   int errorBit;
   printf("\n\nEnter bit position to introduce error (0 for none): ");
   scanf("%d",&errorBit);
   if(errorBit != 0 && errorBit <= totalBits) codeword[errorBit] = !codeword[errorBit];
   printf("\nReceived Codeword: ");
   for(int i=totalBits;i>=1;i--) printf("%d",codeword[i]);
   int errorPos = detectError(codeword,totalBits,r);
   if(errorPos==0) printf("\n\nNo error detected in the received codeword.\n");
   else printf("\n\nError detected at bit position: %d\n", errorPos);
   return 0;
}
```

Output:

```
Enter number of data bits: 5
Enter data bits (from LSB to MSB): 1 0 1 1 1
Generated Hamming Code: 111100111
Enter bit position to introduce error (0 for none): 4
Received Codeword: 111101111
Error detected at bit position: 4
```

VII. Circuit diagram / block diagram / flowchart

A. Suggestive Flowchart

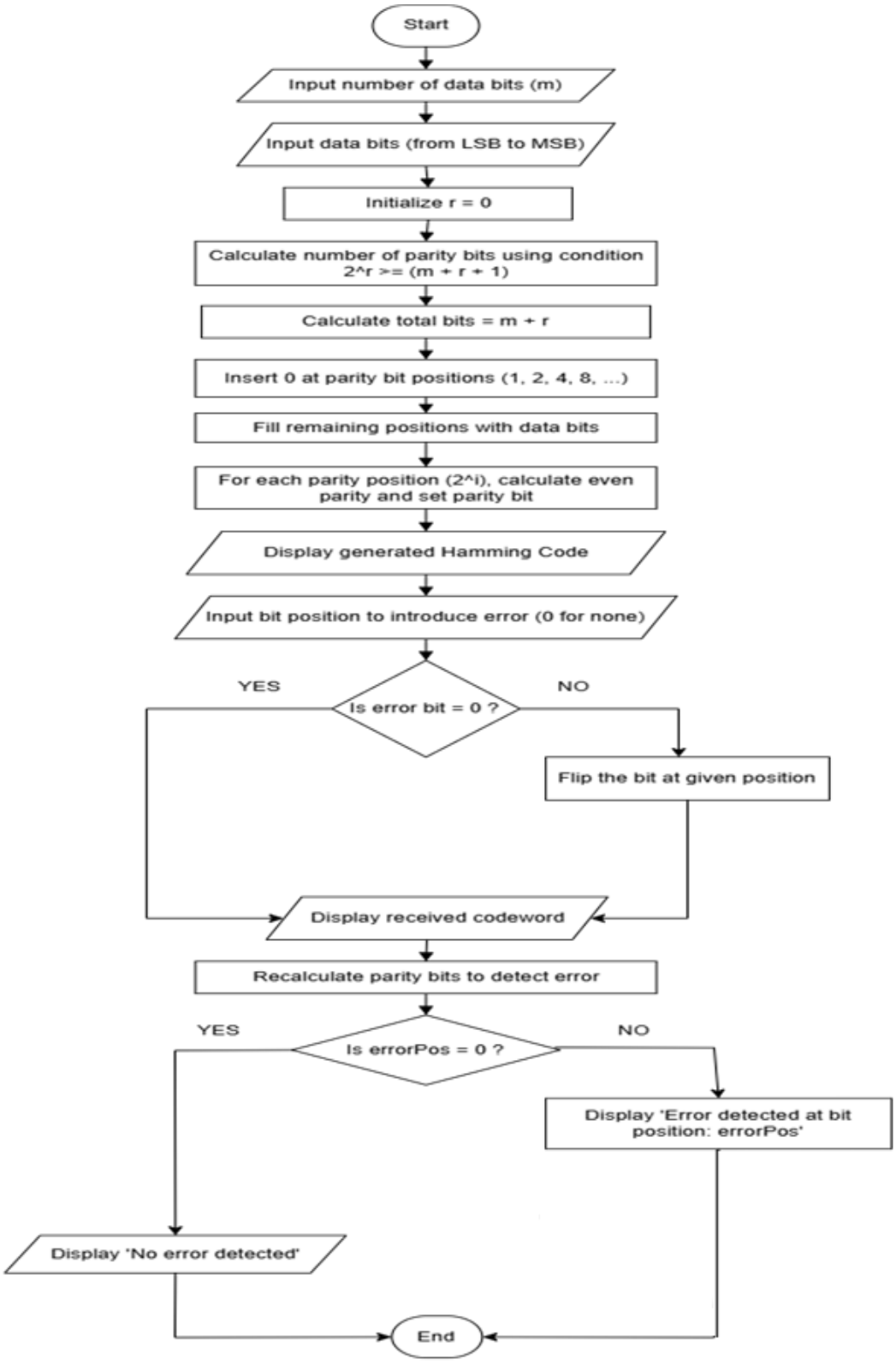


Fig. 15.2 Flowchart for Hamming code to detect error

B. Actual Flowchart

VIII. Required Resources/apparatus/equipment with specifications

Table 15.1

Sr. No.	Name of Resource	Suggested Broad Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Turbo C++ for Windows 10/11	Turbo C++ 3.2 or Turbo C++ 4.5 (with DOSBox support)	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure Turbo C is properly installed and configured before starting the experiment.
2. Verify all input bits are binary (0 or 1).
3. Avoid syntax errors by maintaining correct C syntax and logical expressions.
4. Use clear comments and meaningful variable names to improve code readability.

X. Suggested Procedure

1. Prerequisite

Before starting the practical, make sure you have:

- A computer running Windows 10/11 (Turbo C installed) or any C compiler such as GCC.
- Minimum 2 GB RAM and 200 MB free disk space.
- Turbo C or Turbo C++ IDE properly configured.
- Basic knowledge of C programming and error detection concepts.

2. **Start Turbo C:** Open the Turbo C software on your computer.
3. **Create a New File:** In the Turbo C IDE, go to the File menu. Click New to open a blank source code window.
4. **Type the Program:** Type the complete C program for Hamming Code as given in the lab manual.
5. **Save the Program:** Go to file → Save As. Enter the filename as haming.c and click Save. The program file will now appear in the Turbo C workspace.
6. **Compile the Program:** Press Alt + F9 to compile. The compiler will check your code for syntax errors. If any errors or warnings appear, correct them and compile again. Ensure that the message "0 Errors, 0 Warnings" is displayed.
7. **Run the Program:** After successful compilation, press Ctrl + F9 to run the program. The output window will appear at the bottom of the screen (press Alt + F5 if hidden).
8. **Enter Number of Data Bits:** When prompted, enter the 4 number of data bits. Press Enter to continue.
9. **Enter Data Bits:** The program will ask: "Enter data bits (from LSB to MSB):" Enter the bits one by one, separated by spaces (for example: 1 0 1 1). Press Enter

after entering all bits.

10. **View Generated Hamming Code:** The program will calculate and display the generated Hamming code with parity bits inserted at correct positions.
    Example output:
    Generated Hamming Code: 1010110
11. **Test Error Detection:** The program will prompt:
    - "Enter bit position to introduce error (0 for none):"
    - To test error correction, enter any valid bit position (e.g., 3) to simulate an error.
    - Enter 0 if you don't want to introduce an error.
    - Press Enter.
12. **View Error Detection:** The program will:
    - If an error exists, it will display the bit position of the error.
    - Example: Error detected at bit position: 3
    - If no error exists, it will display: No error detected in the received codeword.
13. **Observe and Record Output:** Record the following:
    - Number of data bits entered
    - Generated Hamming code
    - Error position introduced
    - Error position detected by the program
14. **Save Your Work:** Go to File → save to save any modifications.
15. **End of Practical:** After verifying that the program works correctly, close the output window. Exit the Turbo C IDE using File → Exit. Your Hamming Code practical is now complete.

XI. Resources used during performance

Table 15.2

Sr. No.	Name of Resource	Specifications	Quantity

XII. Actual Procedure (If required attach separate page)

1.

2.

3.

XIII. Observation Table

NA

XIV. Results

……

……

XV. Interpretation of results

……

……

XVI. Conclusions and Recommendations

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Describe the process to detect single-bit error in Hamming Code.
2. For 7 data bits, find the total number of bits in the Hamming codeword.
3. Describe the process for checking errors in a received codeword using a C program.
4. For 4 data bits, calculate the number of parity bits required for Hamming Code.

[Space for Answers] (If required attach separate page)

……

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/hamming-code-in-computer-network/	C implementation of Hamming Code
2	https://www.scaler.in/what-is-hamming-code/	What is Hamming code?
3	https://www.vlab.andcollege.du.ac.in/heyming	Hamming code Virtual Lab

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related : 15 Marks		**60%**
1	Correct C program logic for Hamming Code	10%
2	Successful compilation and execution in Turbo C	20%
3	Following procedure and maintaining lab discipline	20%
4	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct generation of encoded bits	10%
2	Error detection verification	05%
3	Conclusion	05%
4	Answer to sample questions	15%
5	Submitting the journal in time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.16: *Implementation of Hamming code using C programming language to correct error

I. Practical Significance

This practical enables students to implement and analyse Hamming Code for error detection and correction. Through this practical, Students gain hands-on experience in identifying and correcting single-bit errors, thereby enhancing data reliability during transmission.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Troubleshoot transmission errors and flow control of the data in Data Link Layer.

IV. Laboratory Learning Outcome

LLO 16.1 Develop and test 'C' program for error correction using Hamming code.

V. Relevant Affective Domain related outcomes

- Demonstrate working as a leader or a team member.
- Maintain computer systems and software tools in good working condition.
- Demonstrate ethical behaviour in coding and reporting results.

VI. Relevant Theoretical Background

In digital communication systems, errors can occur when data is transmitted over noisy channels. The Hamming Code, developed by Richard W. Hamming in 1950, is one of the earliest and most widely used error detection and correction codes. It not only detects single-bit errors but can also correct them automatically, improving the reliability of data transmission.

The main purpose of Hamming Code is to:

1. Detects and corrects single-bit errors.
2. Detect (but not correct) two-bit errors.

This is achieved by adding redundant (parity) bits to the data bits, forming a longer encoded message called a codeword. To enable error detection and correction, redundancy is introduced in the form of parity bits. Each parity bit checks a specific combination of data and parity bits in the codeword.

Let:

m = number of data bits

r = number of redundant (parity) bits

n=m+r is total number of bits in the transmitted codeword

The relation between m and r is given by:

$$2^r \geq m + r + 1$$

where m = number of data bits, and r = number of redundant bits.

This ensures that there are enough parity bits to cover all data bits and uniquely identify the position of any single-bit error. Parity bits are placed at positions that are powers of 2: 1,2,4,8,16,… For example: P1 is at position 1, P2 is at position 2, P4 is at position 4, etc. The remaining positions (not powers of 2) are filled with data bits. Each parity bit covers certain positions in the codeword based on the binary representation of their position numbers.

For example:

- P1 covers all positions whose binary representation has a 1 in the least significant bit (positions 1, 3, 5, 7, 9, 11, …)
- P2 covers all positions whose binary representation has a 1 in the second bit (positions 2, 3, 6, 7, 10, 11, …)
- P4 covers all positions whose binary representation has a 1 in the third bit (positions 4–7, 12–15, …)
- Each parity bit ensures even parity (or odd parity, depending on system convention) over the bits it checks.

When the receiver gets the codeword:

- It recomputes all parity checks.
- The results form a binary number called the syndrome.
- The value of this syndrome directly points to the bit position in error (if any).
- If the syndrome = 0 then No error.
- If syndrome ≠ 0 then Error detected and corrected (by flipping the bit at that position).

The following program will demonstrate implementation of Hamming code using C programming language to correct errors.

```
#include <stdio.h>
#include <math.h>
// Function to calculate parity bits and generate the Hamming codeword
void generateHammingCode(int data[ ], int m, int codeword[ ], int *r) {
   int i, j, k = 0; // i, j are loop variables; k is used for data index
   // Find number of parity bits required using condition 2^r >= (m + r + 1)
   while (pow(2, *r) < (m + *r + 1)) {
      (*r)++;
   }
   int totalBits = m + *r; // Total bits = data bits + parity bits
   // Insert 0 at parity bit positions (1, 2, 4, 8, ...) and fill data bits in remaining
positions
   for (i = 1, j = 1; i <= totalBits; i++) {
      if (i == pow(2, j - 1)) { // Check if position is a power of 2
         codeword[i] = 0; // Placeholder for parity bit
         j++;
      } else {
         codeword[i] = data[k]; // Insert data bit
```

```
            k++;
        }
    }
    // Calculate parity bits using even parity
    for (i = 0; i < *r; i++) {
        int parityPos = pow(2, i); // Position of current parity bit
        int count = 0; // To count 1s for parity calculation

        for (j = parityPos; j <= totalBits; j++) {
            if (j & parityPos) { // Check if bit position contributes to this parity
                count += codeword[j];
            }
        }
        codeword[parityPos] = count % 2; // Set parity bit (even parity)
    }
}
// Function to detect and correct single-bit error in received codeword
int detectError(int codeword[ ], int totalBits, int r) {
    int errorPos = 0; // To store position of error (if any)
    // Recalculate parity bits and check for mismatch
    for (int i = 0; i < r; i++) {
        int parityPos = pow(2, i); // Position of current parity bit
        int count = 0; // To count 1s for this parity bit
        for (int j = 1; j <= totalBits; j++) {
            if (j & parityPos) { // Include bits relevant to this parity
                count += codeword[j];
            }
        }
        if (count % 2 != 0) { // Parity check fails
            errorPos += parityPos; // Add to error position
        }
    }
    return errorPos; // Return position of error (0 means no error)
}
int main() {
    int data[20], codeword[20]; // Arrays to hold data bits and codeword
    int m, r = 0, totalBits, errorBit; // m = number of data bits, r = parity bits count
    printf("Enter number of data bits: ");
    scanf("%d", &m); // Read number of data bits

    printf("Enter data bits (from LSB to MSB): ");
    for (int i = 0; i < m; i++) {
        scanf("%d", &data[i]); // Read data bits
    }
```

```
    generateHammingCode(data, m, codeword, &r); // Generate Hamming code
    totalBits = m + r; // Calculate total number of bits in codeword
    printf("\nGenerated Hamming Code: ");
    for (int i = totalBits; i >= 1; i--) {
        printf("%d", codeword[i]); // Display generated codeword (MSB to LSB)
    }
    printf("\n\nEnter bit position to introduce error (0 for none): ");
    scanf("%d", &errorBit); // Read position to introduce error manually
    if (errorBit != 0 && errorBit <= totalBits) {
        codeword[errorBit] = !codeword[errorBit]; // Flip bit to simulate error
    }
    printf("\nReceived Codeword: ");
    for (int i = totalBits; i >= 1; i--) {
        printf("%d", codeword[i]); // Display received codeword
    }
    int errorPos = detectError(codeword, totalBits, r); // Detect error position
    if (errorPos == 0) {
        printf("\n\nNo error detected in the received codeword.\n");
    } else {
        printf("\n\nError detected at bit position: %d\n", errorPos);
        codeword[errorPos] = !codeword[errorPos]; // Correct the error
        printf("Corrected Codeword: ");
        for (int i = totalBits; i >= 1; i--) {
            printf("%d", codeword[i]); // Display corrected codeword
        }
        printf("\n");
    }
    return 0;
}
```

Output:

```
Enter number of data bits: 4
Enter data bits (from LSB to MSB): 1 0 1 1
Generated Hamming Code: 1010110
Enter bit position to introduce error (0 for none): 3
Received Codeword: 1000110
Error detected at bit position: 3
Corrected Codeword: 1010110
```

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Flowchart

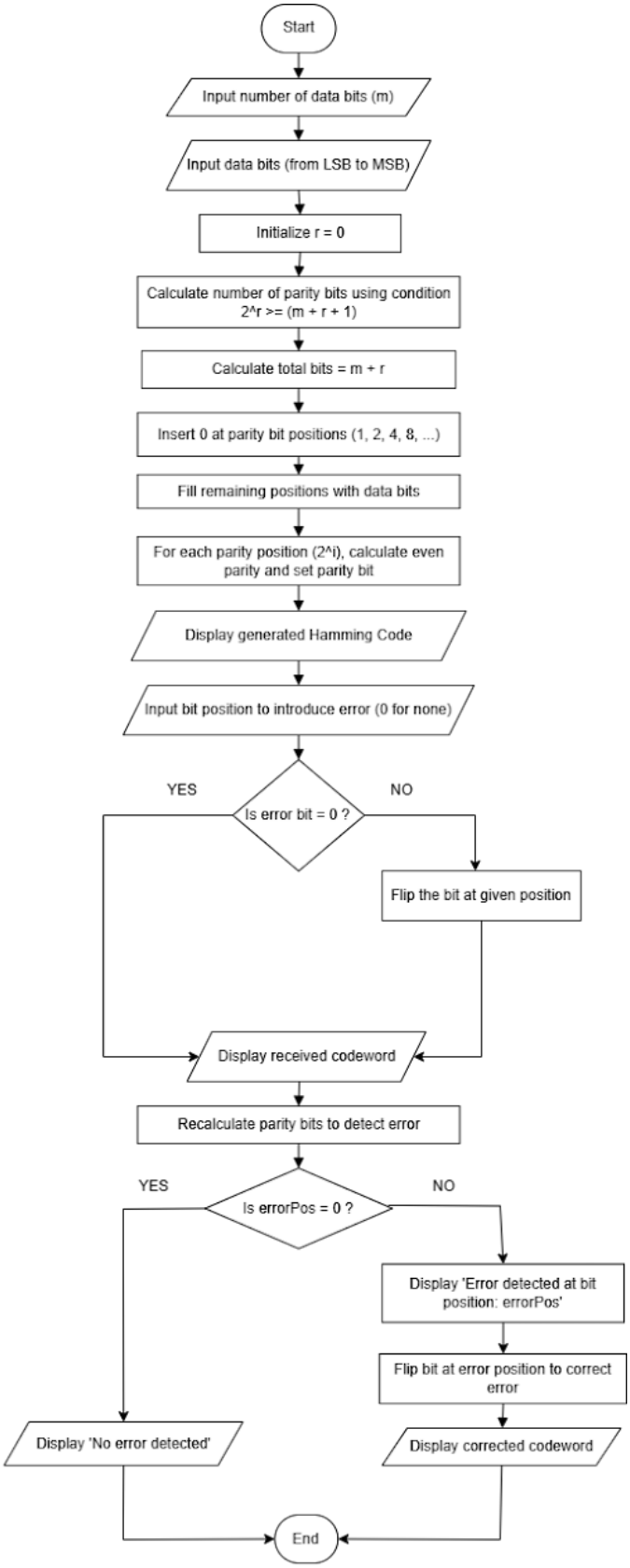


Fig 16.1: Flowchart for Hamming code to correct errors

B) Actual Flowchart

VIII. Required Resources/apparatus/equipment with specifications

Table 16.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Turbo C++ for Windows 10/11	Turbo C++ 3.2 or Turbo C++ 4.5 (with DOSBox support)	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure Turbo C is properly installed and configured before starting the experiment.
2. Verify all input bits are binary (0 or 1).
3. Avoid syntax errors by maintaining correct C syntax and logical expressions.
4. Save the program frequently to prevent data loss.
5. Use clear comments and meaningful variable names to improve code readability.

X. Suggested Procedure

1. Prerequisites

- Before starting the practical, make sure you have:
  - A computer running Windows 10/11 (Turbo C installed) or any C compiler such as GCC.
  - Minimum 2 GB RAM and 200 MB free disk space.
  - Turbo C or Turbo C++ IDE properly configured.
  - Basic knowledge of C programming and error detection concepts.

2. Start Turbo C: Open the Turbo C software on your computer.

3. Create a New File: In the Turbo C IDE, go to the File menu. Click New to open a blank source code window.

4. Type the Program: Type the complete C program for Hamming Code as given in the lab manual.

5. Save the Program: Go to File → Save As. Enter the filename as HAMMING.C and click Save. The program file will now appear in the Turbo C workspace.

6. Compile the Program: Press Alt + F9 to compile. The compiler will check your code for syntax errors. If any errors or warnings appear, correct them and compile again. Ensure that the message "0 Errors, 0 Warnings" is displayed.

7. Run the Program: After successful compilation, press Ctrl + F9 to run the program. The output window will appear at the bottom of the screen (press

Alt + F5 if hidden).

8. **Enter Number of Data Bits:** When prompted, enter the 4 number of data bits. Press Enter to continue.
9. **Enter Data Bits:** The program will ask: "Enter data bits (from LSB to MSB):" Enter the bits one by one, separated by spaces (for example: 1 0 1 1). Press Enter after entering all bits.
10. **View Generated Hamming Code:** The program will calculate and display the generated Hamming code with parity bits inserted at correct positions.

    Example output:
    Generated Hamming Code: 1010110
11. **Test Error Detection:** The program will prompt:
    - "Enter bit position to introduce error (0 for none):"
    - To test error correction, enter any valid bit position (e.g., 3) to simulate an error.
    - Enter 0 if you don't want to introduce an error.
    - Press Enter.
12. **View Error Detection and Correction:** The program will:
    - Show the received codeword (with or without error).
    - Detect the position of the error, if any.
    - Automatically correct the error bit and display the corrected codeword.

    Example output:
    Received Codeword: 1000110
    Error detected at bit position: 3
    Corrected Codeword: 1010110
13. **Observe and Record Output:** Record the following:
    - Number of data bits entered
    - Number of parity bits generated
    - Generated Hamming code
    - Error position introduced
    - Error position detected by the program
    - Corrected Hamming code
14. **Save Your Work:** Go to File → Save to save any modifications.
15. **End of Practical:** After verifying that the program works correctly, close the output window. Exit the Turbo C IDE using File → Exit. Your Hamming Code practical is now complete.

XI. Resources used during performance

Table 16.2

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……..……

……..…

XV. Interpretation of result

……..

……..

XVI. Conclusion and recommendation

……...

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of Hamming Code.
2. Give the formula to find the number of redundant bits required in Hamming Code.
3. List the applications of Hamming Code in computer networks
4. Describe the placement of parity bits in Hamming Code.

[Space for Answers] (If required attached separate page)

……

……

……

……..……..…

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/hamming-code-in-computer-network/	C implementation of Hamming Code
2	https://www.scaler.in/what-is-hamming-code/	What is Hamming code?
3	https://www.vlab.andcollege.du.ac.in/heyming	Hamming code Virtual Lab
4	https://virtual-labs.github.io/exp-hamming-codes-iiith/	Encoding Hamming Code.

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct C program logic for Hamming Code	30%
2	Successful compilation and execution in Turbo C	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct generation of encoded bits	20%
2	Error correction verification	10%
3	Answer to Practical Related Questions	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.17: Implementation of Cyclic Redundancy Check (CRC) using C Programming Language

I. Practical Significance

This practical exercise aims to illustrate the working principle of CRC as an error detection mechanism in Computer Network. It Develops skills to understand how CRC codes are generated, transmitted, and verified to ensure accuracy and integrity of data during transmission across computer networks.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'

III. Course Level Learning Outcome

Troubleshoot transmission errors and flow control of the data in Data Link Layer.

IV. Laboratory Learning Outcome

LLO 17.1 Write a 'C' program for Cyclic Redundancy Check (CRC).

V. Relevant Affective Domain related outcomes

- Demonstrate working as a leader or a team member.
- Maintain computer systems and software tools in good working condition.
- Demonstrate ethical behaviour in coding and reporting results.

VI. Relevant Theoretical Background

Cyclic Redundancy Check (CRC) is one of the most widely used error detection methods in data communication. It uses polynomial division to generate a checksum (CRC code) that helps the receiver verify data integrity. In CRC, the sender appends a sequence of redundant bits (CRC bits) to the data frame. These bits are computed using a predefined generator polynomial. At the receiver side, the same polynomial division is performed; if the remainder is zero, the transmission is error-free.

Key Concepts:

- Data word: Original binary message to be transmitted.
- Generator Polynomial (G(x)): A fixed binary pattern agreed upon by sender and receiver.
- Code word: Data word + CRC bits appended.
- Division Rule: The remainder obtained when the dataword × x^n (where *n* is the degree of G(x)) is divided by the generator polynomial forms the CRC bits.

Example:

Let Data word = 1101, Generator Polynomial = 1011 (degree = 3)

Step 1: Append three zeros to data word → 1101 000
Step 2: Divide 1101000 by 1011 using XOR division
Step 3: Remainder (CRC) = 011
Step 4: Codeword = 1101011 (Data + CRC)
At receiver side, dividing 1101011 by 1011 gives remainder = 000, which confirms no error. The following program will demonstrate implementation of Cyclic Redundancy Check (CRC) using C Programming to detect Error.

```
#include <stdio.h>
#include <string.h>
// Function to perform XOR between two binary strings
void xorOperation(char dividend[ ], char divisor[ ], int start) {
   for (int i = 0; i < strlen(divisor); i++) {
      // Perform XOR only when bits differ
      dividend[start + i] = (dividend[start + i] == divisor[i]) ? '0' : '1';
   }
}
// Function to perform CRC division and get the remainder
void crcDivision(char data[ ], char generator[ ], char remainder[ ]) {
   int dataLen = strlen(data);
   int genLen = strlen(generator);
   char temp[50];
   strcpy(temp, data); // Copy data to temp for manipulation
   // Perform modulo-2 division
   for (int i = 0; i <= dataLen - genLen; i++) {
      if (temp[i] == '1') {
         xorOperation(temp, generator, i);
      }
   }
   // Extract remainder (last genLen-1 bits)
   strncpy(remainder, temp + dataLen - genLen + 1, genLen - 1);
   remainder[genLen - 1] = '\0';
}
int main() {
   char data[50], generator[50], remainder[50], transmittedData[50];
   printf("Enter the data bits: ");
   scanf("%s", data);
   printf("Enter the generator polynomial: ");
   scanf("%s", generator);
   int dataLen = strlen(data);
   int genLen = strlen(generator);
   // Append (genLen - 1) zeros to data for division
   char appendedData[50];
   strcpy(appendedData, data);
```

```
    for (int i = 0; i < genLen - 1; i++) {
        appendedData[dataLen + i] = '0';
    }
    appendedData[dataLen + genLen - 1] = '\0';
    // Perform CRC division to find remainder
    crcDivision(appendedData, generator, remainder);
    // Append remainder to original data to form transmitted codeword
    strcpy(transmittedData, data);
    strcat(transmittedData, remainder);
    printf("\nCRC Remainder: %s", remainder);
    printf("\nTransmitted Codeword: %s", transmittedData);
    // ---- Receiver Side ----
    printf("\n\nEnter received codeword: ");
    char received[50], recvRem[50];
    scanf("%s", received);
    crcDivision(received, generator, recvRem);
    // Check if remainder is all zeros
    int error = 0;
    for (int i = 0; i < strlen(recvRem); i++) {
        if (recvRem[i] == '1') {
            error = 1;
            break;
        }
    }
    if (error == 0)
        printf("\nNo Error Detected! Data received correctly.\n");
    else
        printf("\nError Detected in received data!\n");
    return 0;
}
```

Output:

```
Enter the data bits: 11010011101100
Enter the generator polynomial: 1011
CRC Remainder: 100
Transmitted Codeword: 11010011101100100
Enter received codeword: 11010011101100100
No Error Detected! Data received correctly.
```

If an error is introduced:

```
Enter received codeword: 11010011101100101
Error Detected in received data!
```

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Flow Chart

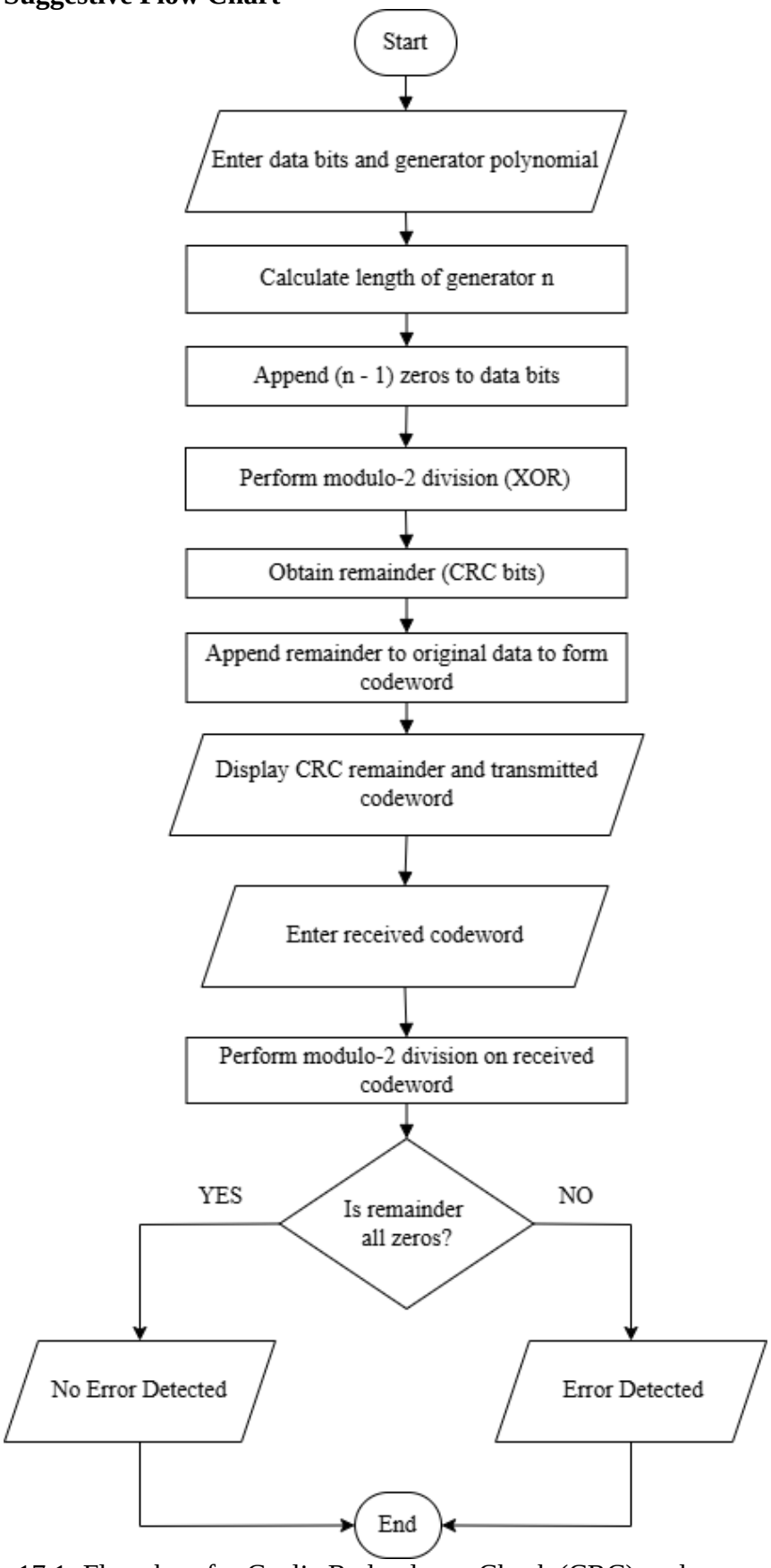


Fig 17.1: Flowchart for Cyclic Redundancy Check (CRC) to detect errors

B) Actual Flow Chart

VIII. Required Resources/apparatus/equipment with specifications

Table 17.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Turbo C++ for Windows 10/11	Turbo C++ 3.2 or Turbo C++ 4.5 (with DOSBox support)	01
4	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that Turbo C compiler is properly installed and configured.
2. Enter only binary input (0s and 1s) for dataword and generator.
3. Maintain correct input order for data bits and generator bits.
4. Save the program periodically while editing in Turbo C.
5. Validate results with known examples to ensure correctness.

X. Suggested Procedure

1. Prerequisites

- Before starting the practical, make sure you have:
    - A computer running Windows 10/11 with Turbo C installed, or any compatible C compiler (e.g., GCC).
    - Minimum 2 GB RAM and 200 MB of free disk space.
    - Turbo C or Turbo C++ IDE properly configured and tested.
    - Basic understanding of C programming, binary operations, and error detection techniques.
    - A copy of the CRC implementation C program.

2. Start Turbo C: Open the Turbo C software on your computer. Wait until the Turbo C IDE window appears with the main menu bar at the top.

3. Create a New File: In the Turbo C IDE, go to the File menu. Click New to open a blank source code window. The editor window will now be ready to type your program.

4. Type the Program: Type the complete C program for Cyclic Redundancy Check (CRC) implementation as given in lab manual. Carefully type the code, maintaining correct syntax, braces, and function names. Example functions may include:

- crc(), xorOperation(), and mod2div().

5. Save the Program: Go to File → Save As. Enter the filename as CRC.C and click Save. The program file will now be visible in the Turbo C workspace.

6. Compile the Program: Press Alt + F9 to compile the program. The compiler will check your code for syntax errors. If any errors or warnings appear, correct them and recompile until you get: 0 Errors, 0 Warnings

7. Run the Program: After successful compilation, press Ctrl + F9 to run the program. The output window will appear at the bottom of the screen. If it's hidden, press Alt + F5 to make it visible.

8. Enter Input Data: The program will prompt:

- Enter data bits: Type the binary dataword to be transmitted (For Example. 1101).

Next, it will prompt:

- Enter generator polynomial: Enter the binary polynomial (For Example. 1011).

9. Observe the Output: The program will perform Modulo-2 Division (XOR operation) between the data word and the generator polynomial and display: The Remainder (CRC bits) generated at the sender side. The Code word (data word + CRC bits) that will be transmitted.

Example Output:

Data word: 1101
Generator Polynomial: 1011
Remainder (CRC bits): 011
Transmitted Codeword: 1101011

10. Test for Error Detection: The program will now prompt to enter the received codeword:

Enter received codeword: Enter the received bits (you can modify one bit intentionally to simulate an error).

Example: 1101111

The program performs Modulo-2 division again on the received codeword using the same generator polynomial.

11. Check Result: If the remainder after division is all zeros, then the message is error-free. If the remainder is non-zero, then an error is detected during transmission.

Example Output:

Remainder after checking: 000
No Error Detected.
or
Remainder after checking: 010
Error Detected in Received Codeword.

12. Record the Output: Record the following observations in your journal:

- Data word entered
- Generator polynomial used
- Remainder (CRC bits) generated
- Transmitted codeword
- Received codeword
- Remainder at receiver side
- Result (Error detected / No error)

13. Save Work: Go to File → Save to save final program and output. If required, take a screenshot of the output window for documentation.

14. End of Practical: After verifying that the program works correctly, close the output window. Exit the Turbo C IDE using File → Exit. CRC Implementation Practical is now complete.

XI. Resources used during performance

Table 17.2

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……...……

……

XV. Interpretation of result

……...…

……..……

XVI. Conclusion and recommendation

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of CRC.
2. Give the formula used to compute CRC bits.
3. Describe the purpose of a CRC in data communication.
4. Enlist errors that CRC detect.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/error-detection-in-computer-networks/	Implementation details for CRC in C
2	https://www.scaler.com/topics/computer-network/cyclic-redundancy-check/	Cyclic Redundancy Check
3	https://www.gatevidyalay.com/cyclic-redundancy-check-crc-error-detection/	Cyclic Redundancy Check (CRC) Example

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Write correct logic for CRC computation	30%
2	Compile and execute program successfully	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct CRC and transmitted codeword output	20%
2	Code structure, comments, and clarity	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.18: *Use PPP Protocol to establish a direct connection between two PCs

I. Practical Significance

The purpose of this practical is to implement the Point-to-Point Protocol (PPP), which is widely used to establish a direct communication link between two computers using a crossover Ethernet, serial cable. This Practical develops skills to implement PPP in creating point-to-point connectivity, configuring network settings, and verifying successful data transfer between the connected systems.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Troubleshoot transmission errors and flow control of the data in Data Link Layer.

IV. Laboratory Learning Outcome

LLO 18.1 Configure PPP (Point to Point Protocol) on Cisco packet tracer.

V. Relevant Affective Domain related outcomes

- Demonstrate working as a leader or a team member.
- Demonstrate ethical behavior in coding and reporting results.
- Follow systematic procedures for setting up and testing network connections.
- Maintain laboratory equipment responsibly and ensure safe cabling connections.

VI. Relevant Theoretical Background

The Point-to-Point Protocol (PPP) is a Data Link Layer (Layer 2) protocol used to establish a direct connection between two nodes. It provides essential services such as framing, error detection, authentication, and link control. PPP can be implemented over a variety of physical media including serial cables, telephone lines, fibre optic links, and other point-to-point channels. PPP is widely used in WAN (Wide Area Network) connections, dial-up Internet access, and router-to-router links. It ensures reliable data transfer and supports multiple network layer protocols such as IP (Internet Protocol), IPX (Internetwork Packet Exchange).

Main Components of Point-to-Point Protocol (PPP)

1. **Encapsulation:** PPP encapsulates network layer packets (like IP datagrams) into PPP frames for transmission. It defines a standard method for framing data so that the receiver can identify the beginning and end of each frame.

2. **Link Control Protocol (LCP):** LCP is responsible for establishing, configuring, and testing the data link connection. It negotiates link parameters such as authentication type, compression, and frame size before communication begins.
3. **Network Control Protocol (NCP):** NCP allows PPP to configure and enable different network layer protocols. Each supported network layer protocol (like IP or IPX) has its own control protocol.

PPP Frame Format: The Point-to-Point Protocol (PPP) frame is the basic data unit used for communication between two directly connected devices.

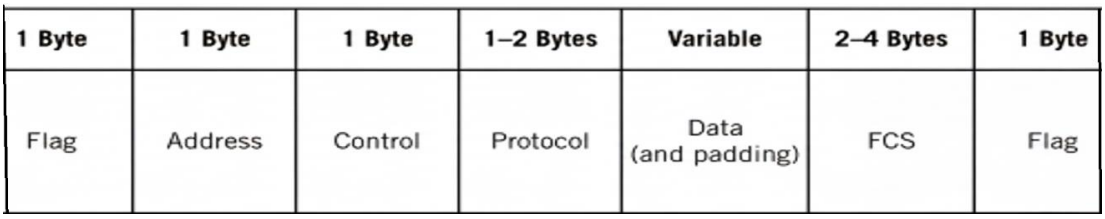


Fig 18.1: Point-to-Point Protocol (PPP) Frame Format

It defines how data is encapsulated and transmitted over a point-to-point link. Each field in the PPP frame serves a specific purpose to ensure reliable and error-free data transfer. Below is the explanation of each field in the PPP frame shown in the Fig 18.1:

Table 18.1 PPP Frame Fields

Field Name	Size	Description
Flag	1 byte	Marks the beginning and end of a PPP frame. The bit pattern is 01111110. This helps the receiver identify frame boundaries.
Address	1 byte	Fixed value 11111111 (0xFF). It represents a broadcast address (used even though PPP is point-to-point).
Control	1 byte	Usually set to 11000000 (0x03). It indicates that the frame is an Unnumbered Information (UI) frame, meaning PPP does not provide sequencing or acknowledgment at the Data Link Layer.
Protocol	1 or 2 bytes	Identifies the type of data carried in the payload field. For example: •0x0021→IP(Internet Protocol) •0xC021→LCP(Link Control Protocol) • 0x8021 → IPCP (IP Control Protocol)
Payload (Information Field)	Variable	Contains the actual data being transmitted, such as a network layer packet (e.g., IP datagram). The size of this field depends on the Maximum Transmission Unit (MTU).
Frame Check Sequence (FCS)	2 or 4 bytes	Used for error detection. It contains a Cyclic Redundancy Check (CRC) value that allows the receiver to detect any errors that occurred during transmission.
Flag (End)	1 byte	Marks the end of the frame. It uses the same bit pattern 01111110 as the starting flag.

PPP Operation Phases

PPP operates in several phases to establish and manage communication:

1. **Link Establishment Phase (LCP):** The connection between the two devices is initialized, and link parameters are negotiated.
2. **Authentication Phase (Optional):** Devices may authenticate each other using protocols like PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).
3. **Network Layer Protocol Phase (NCP):** NCP configures and enables network layer protocols (e.g., IPCP for IP).
4. **Data Transmission Phase:** Once the link is established and protocols configured, data packets are transmitted using PPP framing.
5. **Link Termination Phase:** When communication ends or an error occurs, LCP terminates the link gracefully.

Key Features of PPP

- Supports multiple network layer protocols.
- Provides error detection through Frame Check Sequence (FCS).
- Offers authentication using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).
- Automatically negotiates link parameters.
- Can detect and avoid looped links.
- Supports optional compression and encryption.

Advantages of PPP

- Simple, standardized, and widely supported.
- Ensures reliable and error-free communication.
- Provides security through authentication.
- Works over various types of physical links.
- Suitable for both WAN and dial-up connections.

Applications of PPP

- Dial-up Internet connections between PC and ISP.
- Router-to-router WAN connections using serial links.
- PPP over Ethernet (PPPoE) for DSL and broadband services.
- Point-to-point leased lines in enterprise networks.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

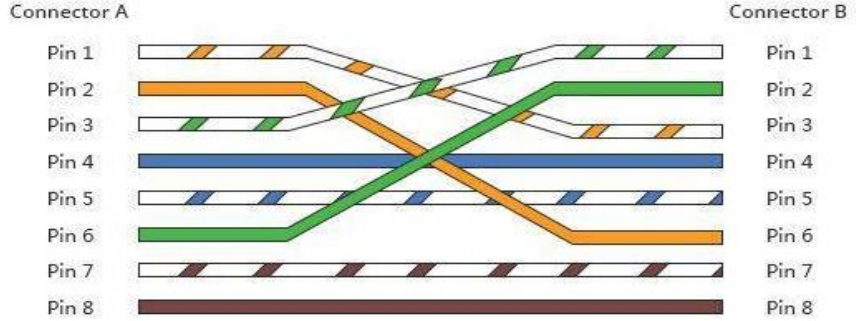


Fig 18.2 Crossover cable wiring Scheme

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 18.2

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Serial Cable (DTE–DCE)	RS-232 / DB-9 serial crossover cable for point-to-point communication	01
4	USB-to-Serial Converter (if PCs lack serial ports)	Compatible with RS-232 cable; required for modern PCs	02
5	Network Interface Card (NIC)	Built-in or external (for serial or Ethernet interface)	02
6	CAT6 UTP Cable	02 Meters CAT6 Unshielded Twisted pair cable with 8 wires inside	01
7	RJ45 Crimping Tool	RJ45 Crimping Tool	01
8	RJ45 Connectors	8-pin modular plugs used on Ethernet cables	02
9	Cable stripper or cutter	Cable stripper or cutter	01
10	Generic/Basic LAN Tester	Tests continuity, open circuit, short circuit, and miswires via sequential LED indicators (1 to 8 and G for ground). Often compatible with RJ45, RJ11, and RJ12. Typically battery-powered (9V) and includes a main and remote unit for testing installed cables.	01
11	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Validate results with known examples to ensure correctness.
2. Ensure both PCs are powered off before connecting the serial cable.
3. Configure the same baud rate, parity, and stop bits on both systems.
4. Verify proper COM port selection before running the program.
5. Avoid tight bending or pulling of cables.
6. Save and test programs periodically.
7. Use only text-based binary data for transmission during testing.

X. Suggested Procedure

1. Prerequisites: Before starting the practical, make sure you have:

- Two desktop or laptop computers running Windows 10 or Windows 11 (with administrative access).
- Minimum 2 GB RAM and 200 MB free disk space on each system.
- Network Interface Cards (NICs) properly installed and enabled.
- A Crossover Ethernet cable (for LAN cards) or a Serial Null Modem cable (RS-232) for serial ports
- Optional: USB-to-Serial adapters, if computers do not have physical COM ports.
- Basic knowledge of IP addressing, network configuration, and PPP concepts.
- Both systems should be free from firewalls or antivirus restrictions blocking local connections.
- **Procedure to create Crossover Ethernet cable:**

  1. Cut the Cable: Cut the Ethernet cable to desired length using a wire cutter.

  2. Strip the Outer Jacket: Strip about **1 inch (2.5 cm)** of the outer insulation at both ends. Be careful not to damage the inner twisted pairs.

  3. Untwist and Arrange the Wires: Untwist the pairs just enough to straighten them. Arrange them in the correct **color order as shown in Fig 18.2:**

    - One end in T568A: Connector A
    - The other end in T568B: Connector B

  4. **Trim the Wires Evenly:** Line them up flat and trim to about **half inch (1.25 cm)** from the jacket so all wires are the same length.
  5. **Insert Wires into RJ-45 Connector:** Hold the connector with the clip facing down and gold pins up. Insert the wires carefully into the connector, making sure each wire goes fully to the end. Verify the color order again before crimping.
  6. **6. Crimp the Connector:** Place the connector into the crimping tool and press firmly until it clicks. The metal contacts should pierce the wire insulation and hold the wires securely.

7. Repeat for the Other End: Wire the second connector in the **other standard** (T568A or T568B, opposite of the first end). Crimp and inspect carefully.

8. Test the Cable: Use a cable tester to ensure all connections are correct and there are no shorts or open wires. The tester should indicate a "crossed" connection between transmit and receive pairs.

2. Prepare the Hardware

- Connect PC1 and PC2 directly using:
  - A Crossover Ethernet cable (for Ethernet ports)
- Make sure both PCs are powered ON and network adapters are enabled.
- Check the network LEDs on both computers — they should glow, indicating an active physical link.

3. Configure Network Settings on PC 1

- Open Control Panel → Network and Internet → Network and Sharing Center.
- Click Change adapter settings on the left sidebar.
- Right-click the connected network adapter → Properties.
- Select Internet Protocol Version 4 (TCP/IPv4) → click Properties.
- Assign a static IP address as follows:
  - IP Address: 192.168.1.1
  - Subnet Mask: 255.255.255.0
  - Default Gateway: (Leave blank)
  - Click OK → Close to save changes.

4. Configure Network Settings on PC 2

- Repeat the same steps on PC 2.
- Assign the following static IP address:
  - IP Address: 192.168.1.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: (Leave blank)
  - Click OK → Close to apply the configuration.
- Both PCs are now on the same subnet and ready to communicate.

5. Enable PPP or Direct Connection Support (Windows 10/11)

Note: In Windows 10/11, the PPP protocol is not listed as a separate checkbox in adapter properties. It is automatically used when you create dial-up, VPN, or direct serial connections.

To ensure PPP functionality is available:

- Open Control Panel → Network and Sharing Center → Set up a new connection or network.
- Choose Set up a dial-up connection (for modem or virtual PPP) or Connect directly using a serial port (COM) if available.
- Ensure that the following Windows services are Running:
  - Remote Access Connection Manager
  - Telephony
    (Open Run → services.msc → start these if stopped.)
- PPP will be automatically activated when the dial-up or direct connection is established.

6. Set Up Direct or Dial-Up Connection

On PC 1 (Incoming Connection):

- Go to Control Panel → Network and Sharing Center.
- Click Set up a new connection or network.
- Choose Set up an incoming connection → Next.
- Select the users allowed to connect, or Create a new user account (e.g., Username: admin, Password: 1234).
- Select the connection device:
  - COM port (for serial), or
  - Ethernet adapter (for direct LAN).
- Click Allow access to create the incoming PPP connection.

On PC 2 (Outgoing Connection):

- Open Network and Sharing Center → Set up a new connection or network.
- Choose Connect to a workplace → Use my Internet connection (VPN or Dial-up).
- Select Dial-up and enter:
  - The IP address or computer name of PC 1.
  - The same username and password you configured on PC 1.
- Click Connect to initiate the PPP link.

7. Authenticate the Connection

- The Remote Access Connection window will appear.
- Enter the username and password created for the incoming connection.
- Wait for authentication to complete.
- Once verified, the status will show "Connected", confirming successful PPP link establishment.

8. Test the Connection

- On PC 1, open Command Prompt and type:
  - ping 192.168.1.2
- On PC 2, type:
  - ping 192.168.1.1
- If replies are received (e.g., "Reply from 192.168.1.1: bytes=32 time<1ms TTL=128"), the PPP connection is working correctly.
- If the ping fails, verify cable connection, IP settings, and firewall configuration.

9. Transfer Data (Optional): After establishing the PPP link, you can Share files using Windows File Sharing.

10. Record Observations: Record practical observations as shown below:

Parameter	**Observation**
IP Address of PC 1	192.168.1.1
IP Address of PC 2	192.168.1.2
Cable Type Used	Crossover / Serial Null Modem
Connection Type	Direct (PPP)
Authentication Used	Username/Password
Ping Result	Successful / Failed
Connection Status	Connected / Disconnected

11. End of Practical

- After verifying communication, disconnect the PPP link:
  - Go to Network Connections → Right-click PPP connection → Disconnect.
- Save the ping result or screenshots for documentation.

- Properly shut down or disconnect the cable connections.
- The PPP Implementation practical is now complete.

XI. Resources used during performance

Table 18.3

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……

……

XV. Interpretation of result

……...…

……...…

XVI. Conclusion and recommendation

……...

……..…….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give the purpose of the Point-to-Point Protocol (PPP).
2. Explain the role of Link Control Protocol (LCP) in PPP.
3. State the functions of Frame Check Sequence (FCS).
4. Draw and explain the PPP frame format.

[Space for Answers] (If required attached separate page)

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/ppp-full-form/	What is Point-to-Point Protocol (PPP)?
2	https://www.studytonight.com/computer-networks/pointtopoint-protocol	Point-to-Point Protocol
3	https://www.geeksforgeeks.org/computer-networks/point-to-point-protocol-ppp-frame-format/	Point-to-Point Protocol (PPP) Frame Format

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correctly connecting two PCs using crossover or serial cable and verifying link lights	30%
2	Correctly assigning IP addresses and subnet masks on both PCs	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Both PCs connected via PPP successfully	20%
2	Successful ping between both PCs	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.19: Measure types of transmission delays using CISCO Packet Tracer

I. Practical Significance

The purpose of this practical is to measure and analyse different types of transmission delays such as propagation delay, transmission delay, queuing delay, and processing delay using Cisco Packet Tracer. This practical develops skills to evaluate how data packets experience various delays in real network scenarios and how parameters like bandwidth, distance, and data size influence overall transmission performance.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Maintain Network layer and Transport layer.

IV. Laboratory Learning Outcome

LLO 19.1 Capture TCP and UDP packet using CISCO Packet Tracer.

V. Relevant Affective Domain related outcomes

- Demonstrate working as a leader or a team member.
- Follow systematic steps while designing and simulating networks.
- Maintain and use the Cisco Packet Tracer environment responsibly.
- Display professional ethics, teamwork, and clear documentation while performing and recording experiments.

VI. Relevant Theoretical Background

In a computer network, transmission delay represents the total time required for a data packet to travel from the source to the destination. The overall delay in data transmission is not determined by a single factor but is the sum of multiple types of delays that occur at different stages of the communication process. Understanding these delay components is essential for evaluating network performance, optimizing routing strategies, and ensuring Quality of Service (QoS) in real-time applications such as video conferencing and online gaming.

Types of Transmission Delays

- **Processing Delay (Tproc):**

Processing delay is the time taken by a router or a network device to analyse the packet header, check for bit-level errors, and determine the appropriate outgoing link for forwarding.

1. Depends on: Device processing power, routing table complexity, and packet size.
2. Typical Range: Microseconds to milliseconds, depending on hardware performance.

3. Example: A high-performance router introduces minimal processing delay compared to a low-end device.

- **Queuing Delay (Tq):**

Queuing delay occurs when packets wait in the output buffer (queue) of a router or switch before transmission. When network traffic is high, queues grow longer, increasing delay.

1. Depends on: Network congestion level, buffer size, and scheduling algorithms (FIFO, priority queuing, etc.).
2. Observation: Queuing delay varies dynamically and is the most unpredictable component of total delay.
3. Typical Scenario: During peak network usage, queuing delay can become significant.

- **Transmission Delay (Tt):**

Transmission delay is the time required to place all bits of a packet onto the transmission medium. It depends on the size of the packet and the available bandwidth of the link.

1. Formula: Tt=Packet Size (in bits)/Bandwidth (in bps)
2. Depends on: Packet size and link bandwidth.
3. Example: Larger packets or lower bandwidth links result in higher transmission delay.

- **Propagation Delay (Tp):**

Propagation delay is the time taken for a signal to travel through the physical medium (like copper cable or fiber optic) from the sender to the receiver.

1. Formula: Tp=Propagation Speed (in m/s)/Distance (in meters)
2. Depends on: Physical distance and propagation speed of the medium (typically m/s for fiber).
3. Example: Long-distance WAN links introduce noticeable propagation delays compared to LANs.

- **Total Delay (Ttotal):** The total delay will be given by, Ttotal=Tt+Tp+Tq +Tproc

Where, T_t → Transmission Delay, T_p → Propagation Delay, Tq → Queuing Delay, Tproc → Processing Delay

Example:

If a 1 MB file (8×10^6 bits) is sent over a 10 Mbps link covering 1000 km,

Transmission Delay:

$$T_t = (8 \times 10^6) / (10 \times 10^6) = 0.8 \text{ sec}$$

Propagation Delay:

$$T_p = (1000 \times 10^3) / (3 \times 10^8) = 0.0033 \text{ sec}$$

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

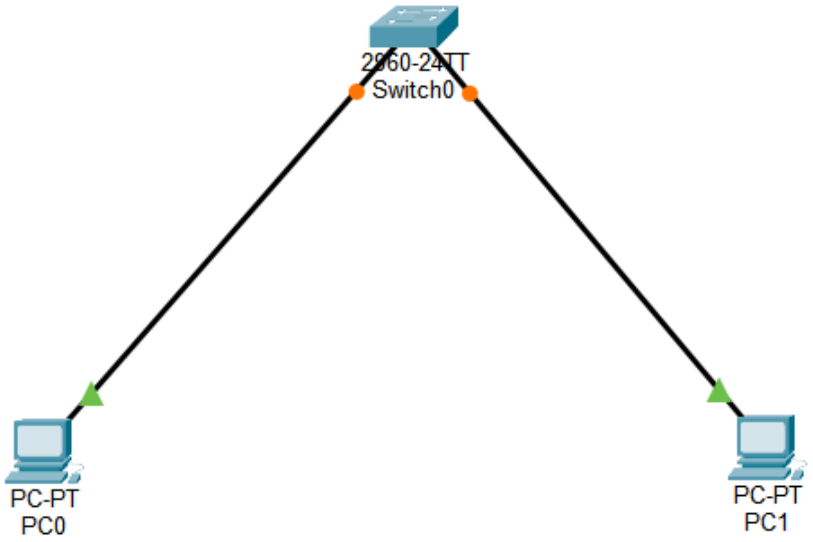


Fig 19.1 Simple Topology using switch

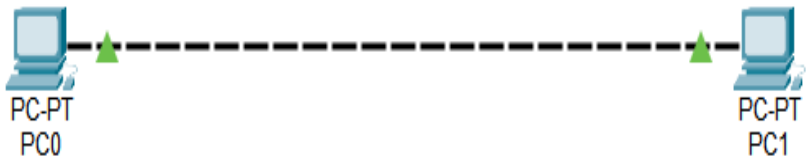


Fig 19.2 Simple Topology without switch

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 19.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
4	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
5	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that Cisco Packet Tracer is properly installed and functional.
2. Use correct IP addressing and connection types between devices.
3. Avoid overlapping cables and devices while designing the topology.
4. Save simulation file frequently to avoid data loss.
5. Check simulation speed settings (Real-time vs Simulation Mode).
6. Run multiple test packets to ensure consistent results.

X. Suggested Procedure

1. **Prerequisites:** Before starting the practical, make sure following things will be available:
   - A computer or laptop running Windows 10/11 with Cisco Packet Tracer (version 8.0 or above) installed.
   - Minimum 4 GB RAM and 1 GB free disk space.
   - Basic knowledge of IP addressing, ping command, and Packet Tracer simulation environment.
   - A Packet Tracer project file folder ready to save practical work.
2. **Open Cisco Packet Tracer**
   - Launch Cisco Packet Tracer software from desktop or Start menu.
   - Wait for the workspace to load completely.
3. **Create a Simple Network Topology**
   - From the Device Panel, drag and drop two PCs **(**PC0 and PC1**)** onto the workspace.
   - To interconnect them, choose one of the following methods:
     - **Using a Switch as shown in Fig 19.1:**

        - Drag one Switch (2960) from the Network Devices → Switches section.
        - Use Copper Straight-Through Cables to connect:
            - PC0 → Switch (FastEthernet0/1)
            - PC1 → Switch (FastEthernet0/2)
    - **Direct Connection (without Switch) as shown in Fig 19.2:**
        - Use a Copper Cross-Over Cable to connect PC0's FastEthernet0 port directly to PC1's FastEthernet0 port.
- Verify that green link lights appear on both ends, indicating a successful physical connection.

4. **Assign IP Addresses**
    - Click on PC0 → Desktop → IP Configuration.
    - Enter the following details:
        - IP Address**:** 192.168.1.1
        - Subnet Mask**:** 255.255.255.0
        - Default Gateway**:** (Leave blank)
    - Click Close to save the settings.
    - Repeat the same steps for PC1, and assign:
    - IP Address**:** 192.168.1.2
    - Subnet Mask**:** 255.255.255.0
    - Both PCs are now configured in the same subnet (192.168.1.0/24).
5. **Configure the Simulation Settings**
    - At the bottom-right of the window, click the Simulation Mode button (next to Real-Time) as shown in Fig 19.3

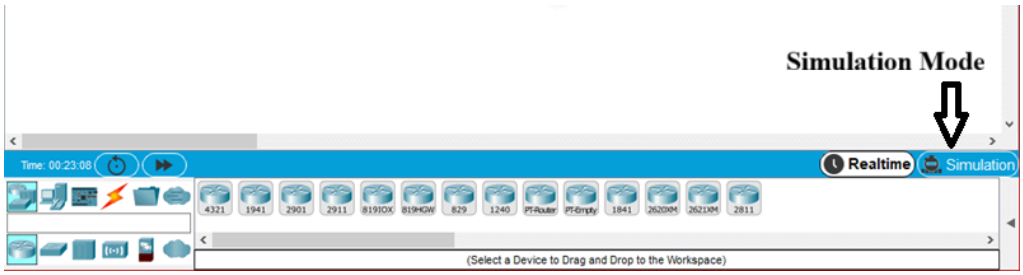


Fig 19.3 Simulation Mode Option in Packet Tracer

    - This mode allows to observe packet movement and measure transmission delays step by step.
    - Open the Event List Filters and ensure that relevant events are displayed for analysis.
6. **Generate Network Traffic**
    - Select PC0 → Desktop → Command Prompt.
    - Type the following command to initiate communication with PC1:
        - ping 192.168.1.2
    - Observe the ICMP Echo Request and Echo Reply packets being generated.
    - (Optional) The Traffic can be generated using Applications → HTTP or FTP on PC0 to simulate data transfer across the link.

7. **Observe Packet Transmission**
   - In Simulation Mode, click Auto Capture/Play or Capture/Forward to follow packet movement.

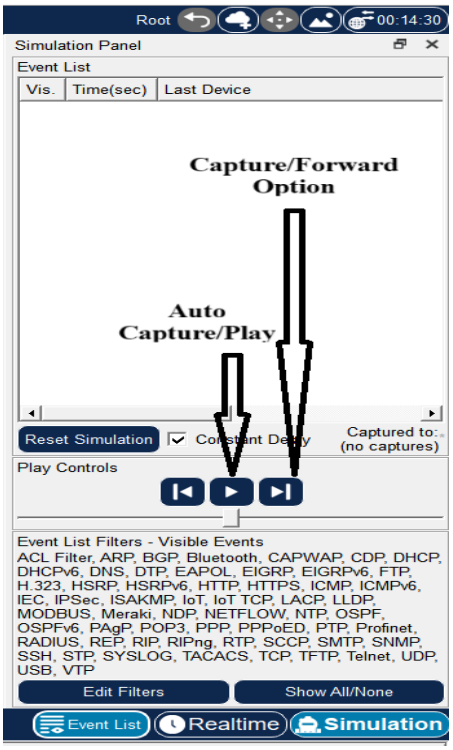


Fig 19.4 Auto Capture/Play or Capture/Forward Option in Simulation mode of Packet Tracer

   - Open Event List Filters and enable the following:
     - Transmission Delay
     - Propagation Delay
     - Queuing Delay
     - Processing Delay
   - Click on individual events or packets to open PDU Details and observe the delay times at each stage of transmission.

8. **Record the Delay Values**
   - For each packet, note the values of delays displayed in the Event List or PDU Details window.
   - Record the following parameters in lab observation table:

Parameter	**Description / Observed Value**
Transmission Delay (Tt)	Time to push packet bits onto the link
Propagation Delay (Tp)	Time for the signal to travel between PCs
Queuing Delay (Tq)	Time spent waiting in the transmission queue
Processing Delay (Tproc)	Time taken for packet header processing
Total Delay (Ttotal)	Sum of all delays observed

9. **Repeat for Multiple Packets**
   - Send multiple ping requests or increase packet size using the command:
     - ping 192.168.1.2 -l 1000
       (where -l specifies packet size in bytes).

- Observe how Transmission Delay and Queuing Delay vary with packet size and network load.
- Note the difference in delays for each test case.

10. Analyze the Results

- Compare the delay components and analyze their dependency:
  - Transmission Delay **(**Tt): Increases with larger packet sizes or lower bandwidth.
  - Propagation Delay **(**Tp**):** Increases with physical distance between nodes.
  - Queuing Delay **(**Tq**):** Increases with higher network traffic or congestion.
  - Processing Delay **(**Tproc**):** Depends on the device's processing speed.
- Identify which delay type has the greatest impact in simulation scenario.

11. End of Practical

- Save project file:
  - Click File → Save As → enter filename

  (e.g., Transmission_Delay_Analysis.pkt).
- Switch back to Real-Time Mode to verify connectivity and close Cisco Packet Tracer after completion.
- The Transmission Delay Measurement Practical is now complete.

Sample Scenario for Calculating transmission delays in Cisco Packet Tracer as per Topology shown in Fig 19.1:

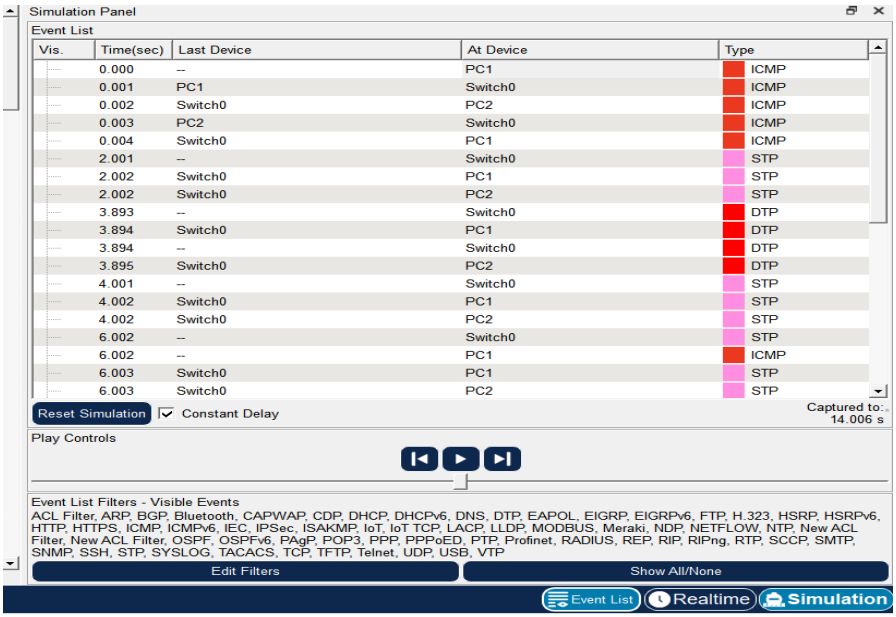


Fig 19.5 Events in Simulation for calculating transmission delays

Assumptions: Change it as per required Scenario. Below presented calculations are as per Fig 19.5

- ICMP packet size = **1500 bytes** = **12,000 bits**.
- Link bandwidth = **100 Mbps** = **100,000,000 bits/s**.
- Distance PC1 ↔ Switch0 = **100 m** and Switch0 ↔ PC2 = **100 m** (two links).
- Signal propagation speed = **2×10^8 m/s** (typical in copper/fiber).

- Switch processing time (per packet) = **0.5 ms** = **0.0005 s** (typical small-store processing).
- Use the timestamps gave as the observed timeline; relevant events used below:
  - Packet generated at PC1 at **0.000 s**.
  - Packet observed at Switch0 at **0.001 s**.
  - Switch0 forwards packet to PC2 and that event is logged at **0.004 s** (so arrival at PC2 is taken as 0.004 s).
  - **Total observed end-to-end time (PC1 → PC2)** = **0.004 − 0.000 = 0.004 s** = **4.000 ms**.

Calculations:

1) **Transmission delay (per link)**
   Packet size = 12,000 bits. Link rate = 100,000,000 bits/s.
   Transmission delay (per link) = packet_size / bandwidth
   = 12,000 / 100,000,000 s
   = 0.00012 s = **0.12 ms**
   Transmission delay (two links total) = 2 × 0.00012 s = **0.00024 s = 0.24 ms**

2) **Propagation delay (per link)**
   Distance = 100 m. Propagation speed = 2×10^{8} m/s.
   Propagation delay (per link) = distance / speed
   = 100 / (2×10^{8}) s
   = 5.0×10^{-7} s = **0.0000005 s = 0.0005 ms**
   Propagation delay (two links total) = 2 × 0.0000005 s = **0.000001 s = 0.001 ms**

3) **Processing delay (total)**
   Assumed switch processing time = **0.0005 s = 0.5 ms**.
   Processing delay (total used) = **0.0005 s = 0.5 ms**

4) **Queuing delay (total, inferred from observed timestamps)**
   Observed total end-to-end (PC1→PC2) from simulation panel = **0.004 s = 4.000 ms**.
   Sum of known components (transmission + propagation + processing) =
   = Transmission total (two links) + Propagation total (two links) + Processing total
   = 0.00024 s + 0.000001 s + 0.0005 s
   = 0.000741 s = **0.741 ms**
   *Residual = Observed total − Sum
   = 0.004000 s − 0.000741 s
   = **0.003259 s = 3.259 ms**
   So **Queuing delay (total, inferred)** = **0.003259 s = 3.259 ms**
   *****In the simulation, the total observed end-to-end delay between PC1 and PC2 was 4.000 ms. The calculated values for transmission, propagation, and processing delays accounted for 0.741 ms in total. The remaining unaccounted time, known as the residual delay (3.259 ms), represents the queuing delay and other minor delays not explicitly modeled. This residual delay occurs when packets wait in the switch

buffer before transmission due to internal processing or temporary congestion. In real networks, queuing delay varies with traffic load, buffer size, and link utilization. Therefore, in this analysis, the residual (3.259 ms) is considered as the queuing delay, completing the total end-to-end delay of 4.000 ms observed in the simulation.

5) Total End-to-End Delay

Transmission (total) = **0.00024 s = 0.24 ms**
Propagation (total) = **0.000001 s = 0.001 ms**
Processing (total) = **0.0005 s = 0.5 ms**
Queuing (total, inferred) = **0.003259 s = 3.259 ms**
Total = 0.00024 + 0.000001 + 0.0005 + 0.003259 s
= **0.004000 s = 4.000 ms**

Final numeric summary

- **Observed total end-to-end (PC1 → PC2):** 0.004000 s = **4.000 ms**
- **Transmission delay (per link):** 0.000120 s = **0.120 ms**
- **Transmission delay (two links total):** 0.000240 s = **0.240 ms**
- **Propagation delay (per link):** 0.0000005 s = **0.0005 ms**
- **Propagation delay (two links total):** 0.000001 s = **0.001 ms**
- **Processing delay (total assumed at switch):** 0.000500 s = **0.500 ms**
- **Queuing delay (inferred residual):** 0.003259 s = **3.259 ms**
- **Total (sum of components):** 0.004000 s = **4.000 ms**

XI. Resources used during performance

Table 19.2

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

7.

XIII. Observation Table

Table 19.3

Sr. No.	Parameter	Symbol	Formula / Description	Observed / Measured Value	Remarks
1	Transmission Delay	T_t	T_t = (Packet Size in bits) / (Bandwidth in bps)	_____ sec	Depends on packet size and link bandwidth
2	Propagation Delay	T_p	T_p = (Distance in meters) / (Propagation Speed in m/s)	_____ sec	Depends on physical link distance
3	Queuing Delay	Tq	Time spent waiting in router/switch buffer before transmission	_____ sec	Increases with network congestion
4	Processing Delay	Tproc	Depends on device speed and routing complexity.	_____ sec	Depends on hardware speed
5	Total End-to-End Delay	Ttotal	Ttotal=Tt+Tp+Tq +Tproc	_____ sec	Overall data transmission delay

XIV. Result

……...

……...

……...

……...

XV. Interpretation of result

……...

……...

XVI. Conclusion and recommendation

……...

……...

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Differentiate between transmission delay and propagation delay.
2. Describe factors that affect queuing delay in a network.
3. State the formula for calculating transmission delay.
4. Describe the role of bandwidth in determining total delay.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/delays-in-computer-network/	Delay types and formulas
2	https://www.tutorialspoint.com/what-are-transmission-and-propagation-delay	What are transmission and propagation delay?
3	https://www.gatevidyalay.com/delay-in-computer-networks/	Delays in Computer Networks-
4	https://www.baeldung.com/cs/propagation-vs-transmission-delay	Propagation Delay vs Transmission Delay
5	https://takeuforward.org/computer-network/different-types-of-delays	Different types of delays

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Create correct topology and configuration in Cisco Packet Tracer	30%
2	Correctly simulate and record delay parameters	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Accurate observation and explanation of delay types	20%
2	Successful ping between both PCs	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.20: Installation of Modem and Router

I. Practical Significance

The purpose of this practical is to install, configure, and verify the operation of a modem and router within a data communication network. This practical develops skills to understand the roles of these devices in establishing internet connectivity, managing network traffic, and facilitating efficient and secure data exchange between multiple devices in a local and wide area network environment.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Maintain Network layer and Transport layer.

IV. Laboratory Learning Outcome

LLO 20.1 Install and test Modem and Router.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing and recording experiments.
- Follow systematic procedures for installation and configuration.
- Handle network devices carefully and maintain lab safety standards.
- Show responsibility in using authorized network equipment and configurations.
- Document observations clearly and ethically.

VI. Relevant Theoretical Background

A modem (modulator-demodulator) and a router are fundamental devices in modern data communication networks. Together, they enable computers and other networked devices to access the internet, share data, and communicate efficiently. Understanding their functions, configurations, and interconnections is essential for setting up and maintaining reliable network communication systems.

1. Modem

A modem is a communication device that performs two key functions — modulation and demodulation. It converts digital signals generated by computers into analog signals suitable for transmission over traditional communication media (such as telephone lines or coaxial cables), and vice versa. This process allows digital data to be transmitted across long distances using analog infrastructure.

Functions and Purpose:

- **Signal Conversion:** The modem modulates outgoing digital data into analog form for transmission and demodulates incoming analog signals back into digital form for computer interpretation.

- **ISP Connectivity:** It serves as the interface between a local network or single computer and the Internet Service Provider (ISP), establishing the primary internet connection.
- **Data Synchronization:** The modem maintains synchronization with the ISP's transmission system to ensure accurate and continuous data exchange.

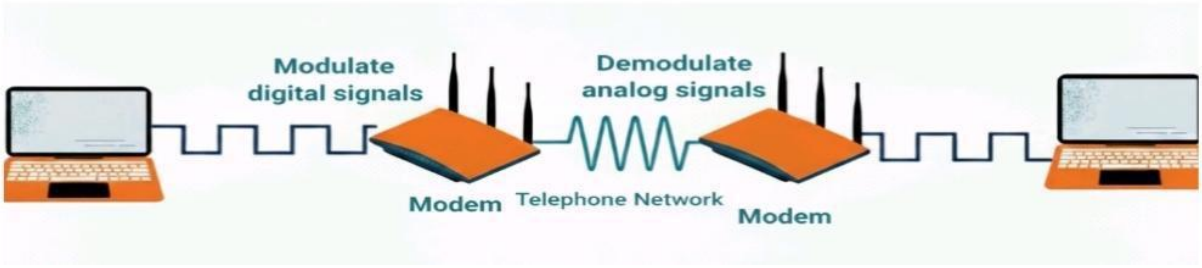


Fig 20.1 Modem working

Types of Modems:

1. **DSL (Digital Subscriber Line) Modem:**
   - Utilizes standard telephone lines for data transmission.
   - Allows simultaneous voice and internet use over a single line.
   - Commonly used in home and small office networks.
2. **Cable Modem:**
   - Uses a coaxial cable connection (the same used for cable TV).
   - Provides higher bandwidth than DSL and is suitable for high-speed broadband connections.
3. **Fiber Modem (Optical Network Terminal – ONT):**
   - Used in fiber-optic networks to convert light signals into electrical signals and vice versa.
   - Supports extremely high-speed data transmission with low latency.

Modem Configuration:

- Configuration involves setting up ISP credentials (username and password), communication protocols (PPP, PPPoE), and connection modes.
- Some modems include built-in routing capabilities, combining both modem and router functions in one device (e.g., DSL router or gateway).

2. Router

A router is a networking device responsible for forwarding data packets between computer networks. It connects multiple devices within a Local Area Network (LAN) and directs their data to the appropriate destinations, either within the same network or toward the internet through the modem.

Functions and Purpose:

- Packet Forwarding: The router determines the best path for data packets to reach their destination using IP routing tables**.**
- **Network Segmentation:** It divides large networks into smaller, manageable segments to improve performance and security.
- **Internet Sharing:** Provides internet access to all connected devices by managing communication between the LAN and the modem.

- **Address Assignment:** Uses DHCP (Dynamic Host Configuration Protocol) to automatically assign IP addresses to network devices.
- **Security Management:** Implements firewall rules and supports Network Address Translation (NAT) to protect internal devices from external threats.

Key Features and Protocols:

- NA**T (Network Address Translation):** Enables multiple devices in a private network to share a single public IP address when accessing the internet.
- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses, subnet masks, and gateway information to devices.
- **Firewall Settings:** Filter incoming and outgoing traffic to safeguard against unauthorized access.
- **Routing Protocols:** Routers use dynamic protocols (like RIP, OSPF, and EIGRP) to discover and maintain optimal data paths within larger networks.

Router Configuration:

- Configuration involves setting up LAN IP ranges, DHCP parameters, wireless SSIDs (if applicable), and security settings such as WPA3 encryption.
- Routers can be accessed and configured through a web interface or command-line interface (CLI), depending on the device type and manufacturer.

Understanding the roles, configurations, and interaction between these two devices is crucial for establishing a stable and secure network infrastructure, ensuring efficient data transmission and reliable internet connectivity.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

Fig 20.2 Typical Modem and router Setup

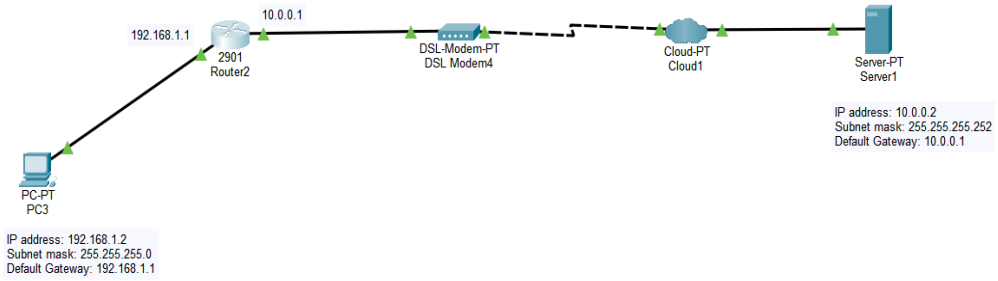


Fig 20.3 Typical Router and Modem Setup in Cisco Packet Tracer

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 19.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Router	Router with 256MB Memory, Wireless and Ethernet Connectivity, Compatible with Desktop/Laptop, Rack Mountable, Supports NAT, DHCP, and Firewall Configuration Connectivity	01
4	Modem	DSL/Cable/Fiber Modem (as per ISP type), Supports PPP/PPPoE Configuration, Input: ISP Line, Output: Ethernet Port to Router	01
5	Network cables	Cat5e or Cat6 Ethernet Patch Cables, Standard RJ45 Connectors, Length as per setup requirement	02
6	Internet Connection (ISP Line)	Active Internet Service Line for Practical Demonstration and Testing	01
7	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
8	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all devices are switched off before making connections.
2. Use proper Cat5e or Cat6 cables for all network links.
3. Check power supply and use a UPS to avoid interruptions.
4. Label all cables and ports correctly.
5. Enter correct configuration settings before connecting to the ISP line.
6. Keep modem and router away from heat or magnetic sources.
7. Use proper IP addressing to avoid conflicts.
8. Change default usernames and passwords for security.
9. In simulation, verify correct connections and interface settings.
10. Save simulation work frequently.
11. Test connections step by step using ping or tracert.
12. Record all configuration details for future use.

X. Suggested Procedure

A) Offline Physical Installation of Modem and Router with ISP Line

1. Prerequisites: Before beginning the practical, ensure that following things will be available-

- A broadband Internet connection (DSL, Fiber, or Cable) with an active ISP line.
- A wireless/wired router (e.g., TP-Link, D-Link, Netgear, Cisco home router).
- A modem (if not built into the router).
- Ethernet (LAN) cables (Cat5e or Cat6).
- A computer/laptop with an Ethernet port or Wi-Fi capability.
- Basic understanding of network devices**,** IP addressing**,** and browser-based configuration.

2. Identify and Prepare Equipment

- Place the modem and router on a flat, well-ventilated surface near the ISP line entry point.
- Check power adapters for both devices.
- Ensure cables are in good condition and having label for easy identification.

3. Connect the Modem to the ISP Line

- Connect the ISP line (telephone cable for DSL or coaxial cable for cable Internet) to the modem's WAN/DSL port as shown in Fig. 20.4

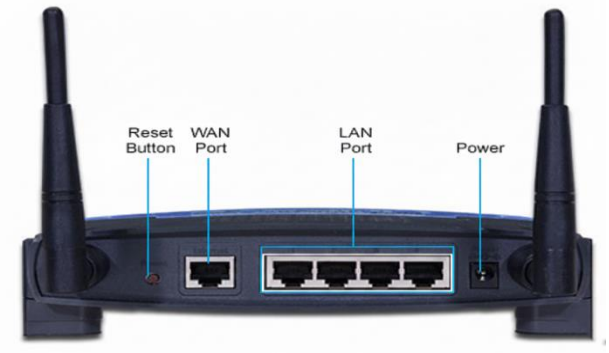


Fig 20.4 Typical Modem Back View of Ports

- Plug in the modem's power adapter and switch it on.
- Wait until the Power and DSL/Internet LEDs turn solid green, indicating a successful connection with the ISP.

4. Connect the Router to the Modem

- Using an Ethernet cable, connect:
  - Modem LAN port → Router WAN/Internet port as shown in Fig. 20.5

Fig 20.5 Typical Modem Back View of Ports

- Connect computer/laptop to one of the router's LAN ports using another Ethernet cable (or via Wi-Fi after configuration) as shown in Fig. 20.5

5. Power ON and Check Connections

- Power on the router and wait until all indicator lights stabilize.
- Verify that:
  - The Internet/WAN light on the router is ON.
  - The LAN light corresponding to PC connection is ON.
- If the lights remain off or blinking abnormally, recheck cable connections.

6. Configure Router Settings

- On computer, open a web browser.
- Type the router's default IP address (commonly 192.168.0.1 or 192.168.1.1) in the address bar.

Fig. 20.6 Routers Configuration Page for TP-Link's Router WR841N

- Log in using the default credentials (found on the router's label).
- Configure the WAN/Internet settings based on ISP using options as shown in Fig. 20.6
  - PPPoE: Enter username and password provided by the ISP.
  - Dynamic IP: Automatically obtains IP from ISP.
  - Static IP: Enter ISP-assigned IP, Subnet Mask, Gateway, and DNS.
- Save and reboot the router.

7. Configure Wireless Settings

- Navigate to the Wireless Settings menu as shown in Fig. 20.6
- Set:
  - SSID (Network Name) — e.g., MyHomeNetwork
  - Security Mode — WPA2/WPA3
  - Password — a strong passphrase. Don't use Common Passwords.
- Save and apply changes.

8. Verify Internet Connectivity

- Open Command Prompt and type:
- ping 8.8.8.8
  - If replies are received, Internet connectivity is established.
- Test access to a website (e.g., www.google.com).
- If unsuccessful, check ISP connection, PPPoE credentials, or contact ISP support.

9. Secure and Finalize Setup

- Change the router's default admin password for security.
- Save configuration and backup settings if supported.
- Place the router centrally for optimal wireless coverage.
- The physical installation and configuration of the modem and router are now complete.

B) Installation of Modem and Router in Cisco Packet Tracer (Simulation Mode) as shown in Fig 20.3

1. Prerequisites

Before starting, ensure:

- Cisco Packet Tracer version 8.0 or above is installed on computer.
- Basic knowledge of router interfaces, IP configuration, and network simulation.
- A dedicated folder to save Packet Tracer project files.
- Familiarity with real-time and simulation modes in Packet Tracer.

2. Open Cisco Packet Tracer

- Launch Cisco Packet Tracer from the Start menu or desktop.
- Wait for the workspace to load completely.

3. Create a Basic Topology

- From the Network Devices → Routers section, drag a Router (e.g., 2901) to the workspace.

- From Network Devices → WAN Emulation→drag a DSL Modem into the workspace.
- From End Devices, drag one PC (PC0) and one Server (Server0) into the workspace.
- From Network Devices → WAN Emulation→drag a Cloud-PT0 into the workspace.

Connections:

- Connect Router → PC0 (LAN interface).
- Connect Modem → Router (use appropriate cable: Copper Straight-Through).
- Connect Modem→CloudPT0 through Phone Cable
- Connect CloudPT0 → Server0 to simulate an ISP or DNS service.

4. **Assign IP Addresses**

On Router:

- Click the Router → CLI Tab.
- Configure interfaces:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# interface gigabitEthernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# no shutdown
Router(config)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

On PC0:

- Desktop → IP Configuration:
  - IP Address: 192.168.1.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.1.1

On Server0 (simulating ISP):

- IP Address: 10.0.0.2
- Subnet Mask: **255.255.255.252**

5. **Configure the Modem (Simulated)**
   - Click on the Modem → Config Tab.
   - In DSL tab, select modem4 and ethernet6 in DSL option, click Add Button which will add modem4 to Ethernet6 port in the port list.
6. **Verify Connectivity**
   - From PC0 → Command Prompt, type:
     - ping 192.168.1.1(Test Router)
     - ping 10.0.0.2 (Test ISP Server)
   - Successful replies indicate connectivity through modem and router.

7. **Save and Document**
   - Save project:
     - File → Save As → Modem_Router_Installation.pkt
   - Record IP configurations, connectivity test results, and observations in lab manual.
8. **End of Practical**
   - Switch back to Real-Time Mode to verify continuous connectivity.
   - Close Cisco Packet Tracer after saving.
   - The simulation-based installation of a modem and router is now complete.

XI. Resources used during performance

Table 19.2

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……

……

XV. Interpretation of results

……

……

XVI. Conclusion and recommendation

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State is the function of a modem.
2. Differentiate between a modem and a router.
3. Describe the purpose of the WAN and LAN ports on a router.
4. State the reason why DHCP is used in routers.
5. List the steps to check network connectivity on a PC.

[Space for Answers] (If required attached separate page)

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/difference-between-modem-and-router/	Comparison and configuration guide
2	https://www.geeksforgeeks.org/techtips/how-to-install-a-modem/	How To Install a Modem?
3	https://www.geeksforgeeks.org/computer-networks/steps-to-configure-initial-router-settings/	Steps to Configure Initial Router Settings
4	https://www.geeksforgeeks.org/computer-networks/router-configuration-with-cisco-packet-tracer/	Router Configuration with Cisco Packet Tracer

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correctly connect modem and router hardware	30%
2	Configure router for internet and LAN	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful network and internet operation	20%
2	Successful ping between both PCs	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.21: Implement IPv6 Addressing Scheme on a Network

I. Practical Significance

This practical develops skills to implement basic IPv6 configuration on routers and hosts address with IPv6 notation and types. It also enables learners to verify end-to-end IPv6 connectivity, enhancing their understanding of modern IP addressing and its role in scalable and future-ready network design.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Maintain Network layer and Transport layer.

IV. Laboratory Learning Outcome

LLO 21.1 Create IPv6 environment in a small network using simulator.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing and recording experiments.
- Follow systematic procedures for installation and configuration.
- Handle network devices carefully and maintain lab safety standards.
- Show responsibility in using authorized network equipment and configurations.
- Document observations clearly and ethically.
- Maintain documentation and save project files responsibly.

VI. Relevant Theoretical Background

The Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), designed to replace IPv4, which has been the foundation of internet communication since its inception. IPv6 was developed by the Internet Engineering Task Force (IETF) to address key issues in IPv4, such as the limited address space**,** growing network complexity, and increasing demand for globally unique IP addresses driven by the rapid expansion of the internet and connected devices. IPv6 uses 128-bit addressing, compared to IPv4's 32-bit scheme, resulting in a vastly larger pool of unique addresses — approximately 3.4×10^{38} (340 undecillion) possible combinations. This enormous address space ensures that every device, sensor, or user can have a unique IP address, making IPv6 ideal for modern technologies such as Internet of Things (IoT)**,** 5G networks**,** cloud computing, and autonomous systems. IPv6 is a crucial evolution of the Internet Protocol, ensuring the continued scalability, performance, and security of global networks.

IPv6 Configuration and Routing

IPv6 can be configured either manually (static addressing) or automatically using:

- **Stateless Address Autoconfiguration (SLAAC):** Devices automatically generate their own IPv6 addresses based on router advertisements.
- **DHCPv6:** Similar to DHCP in IPv4 but designed for IPv6 address assignment and network configuration.

IPv6 Address Representation

- IPv6 addresses are represented in hexadecimal notation, divided into eight groups of four hexadecimal digits (also called hex), separated by colons (:).
  Example:
  - 2001:0db8:0000:0000:0000:ff00:0042:8329
- To simplify representation, IPv6 allows two key shortening techniques:
  - **Leading Zero Omission:** Any leading zeros within a hex can be removed.
    Example:2001:0db8:0000:0000:0000:ff00:0042:8329→
    2001:db8:0:0:0:ff00:42:8329
  - **Zero Compression (::):** Consecutive sections of zeros can be replaced by a double colon (::), but this can only be used once per address to avoid ambiguity.
    Example: 2001:db8:0:0:0:ff00:42:8329 → 2001:db8::ff00:42:8329

IPv6 Address Structure

Table 21.1

Portion	Bits	Meaning	Example
Network Prefix	64 bits	Identifies network	2001:db8:1::/64
Interface ID	64 bits	Identifies host/device	::10

IPv6 uses Prefix Length instead of subnet masks:

Example:

2001:db8:1::10/64

Common Types of IPv6 Addresses

Table 21.2

Address Type	Prefix / Rule	Example	Purpose
Global Unicast	2000::/3	2001:db8:2::10	Public, Internet-routable
Link-Local	fe80::/10	fe80::1a2b:3c4d:5e6f:abcd	Local link, auto-configured
Unique Local	fc00::/7	fd12:3456:789a::1	Private organization network
Multicast	ff00::/8	ff02::1 (all nodes)	One-to-many communication
Anycast	Uses Global Unicast format	Same address configured on multiple routers	Nearest service access

IPv6 does not support Broadcast**,** reducing unnecessary traffic**.** IPv6 provides security, scalability, huge address space, and modern routing support, making it the foundation of future networks.

Advantages of IPv6 Over IPv4:

- Virtually unlimited address space (128-bit vs. 32-bit).
- Simplified header structure improves routing efficiency.
- Integrated security through IPSec (mandatory in IPv6).
- Built-in support for mobility and autoconfiguration.
- Elimination of NAT (Network Address Translation), allowing true end-to-end communication.
- Improved multicast and anycast capabilities.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

Fig 21.1 IPv6 Network Implementation in Cisco Packet Tracer

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 21.3

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Verify IPv6 support is enabled on all devices.
2. Use correct prefix lengths; /64 is recommended for LAN segments.
3. Do not overlap global unicast prefixes when designing networks.
4. Save configuration frequently during the lab.
5. Ensure correct interface assignment to avoid misconfiguration.

X. Suggested Procedure

1. Prerequisites

Before starting the practical, ensure the following requirements are met:

- A computer with Cisco Packet Tracer or any other network simulation software installed.
- Basic understanding of IPv6 addressing concepts**,** router configuration, and network topology design.
- Familiarity with basic router commands such as enable, configure terminal, and interface configuration.
- Ensure that the simulation tool is properly installed and tested by opening a sample topology.

2. Create Network Topology

- Open Cisco Packet Tracer on computer. Wait until the workspace loads completely.
- Drag and drop the following devices into the workspace as shown in 21.1:
  - 1 Router (e.g., Cisco 1841)
  - 2 PCs (PC0 and PC1)
- Connect the devices using Copper Straight-Through cables as follows:
  - PC0 ↔ Router FastEthernet0/0

- PC1 ↔ Router FastEthernet0/1
- Verify that each cable connection is shown as green (indicating a proper physical link).

3. Configure Router Interfaces

- Click on Router0 → CLI tab to open the command-line interface.
- Enter privileged EXEC mode and global configuration mode using the following commands:
  - enable
  - configure terminal
- Enable IPv6 routing globally to allow IPv6 packet forwarding:
  - ipv6 unicast-routing
- Configure FastEthernet0/0 interface (connected to PC0):
  - interface FastEthernet0/0
  - ipv6 address 2004::1/64
  - no shutdown
  - exit
- Configure FastEthernet0/1 interface (connected to PC1):
  - interface FastEthernet0/1
  - ipv6 address 2008::1/64
  - no shutdown
  - exit
- Save the configuration to prevent loss after reboot:

4. Configure IPv6 Addresses on PCs

- Click on PC0 → Desktop tab → IP Configuration.
  - Select IPv6 section and enter the following:
    - IPv6 Address**:** 2004::10
    - Prefix Length**:** 64
    - Default Gateway**:** 2004::1
- Click on PC1 → Desktop tab → IP Configuration.
  - In the IPv6 section, enter:
    - IPv6 Address**:** 2008::10
    - Prefix Length**:** 64
    - Default Gateway**:** 2008::1
- Close both configuration windows once the addresses are assigned.

5. Verify IPv6 Configuration

- Go to Router0 CLI and check IPv6 interface status:
- show ipv6 interface brief
- Expected Output**:** Both FastEthernet interfaces should display their assigned IPv6 addresses with status up/up.
- If any interface shows administratively down, recheck connections and ensure the no shutdown command was used.

6. Test IPv6 Connectivity

- On PC0, open Command Prompt:
  - **ping 2008::10**

Expected Result**:** Successful ping replies indicate that IPv6 addressing and routing are functioning correctly.

- For reverse testing, go to PC1, open Command Prompt, and type:
  - **ping 2004::10**

Successful replies confirm end-to-end IPv6 connectivity between both PCs through the router.

7. **Additional Verification and Troubleshooting**
   - View IPv6 neighbour discovery table on the router:
     - show ipv6 neighbours

     This displays the IPv6 addresses and link-layer (MAC) mappings of connected devices.
   - Display detailed interface configurations:
     - show ipv6 interface FastEthernet0/0
     - show ipv6 interface FastEthernet0/1
   - Review the router's running configuration for confirmation:
     - show running-config
8. **Record Observations**

   In lab journal, note the following details:
   - IPv6 addresses assigned to each interface and device.
   - Ping test results between PC0 and PC1.
   - Status of interfaces (up/up).
   - Neighbour table entries and verification commands used.
9. **Save and Exit**
   - Save Packet Tracer file using File → Save As for future reference.
   - Exit the simulation environment once all steps are verified successfully.
   - The IPv6 Addressing and Configuration Practical is now complete.

XI. Resources used during performance

Table 21.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

Table 21.5

Sr. No.	Parameter	Formula / Description	Observed / Measured Value	Remarks
1	IPv6 Address of PC0	Manually assigned as per configuration		
2	IPv6 Address of PC1	Manually assigned as per configuration		
3	Router Interface (Fa0/0) Address	Configured using ipv6 address command		
4	Router Interface (Fa0/1) Address	Configured using ipv6 address command		
5	Default Gateway for PC0	Gateway address for PC0		
6	Default Gateway for PC1	Gateway address for PC1		
7	Ping Test (PC0 → PC1)	ping 2008::10		
8	Ping Test (PC1 → PC0)	ping 2004::10		

XIV. Result

……

……

XV. Interpretation of result

……

……

XVI. Conclusion and recommendation

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the length of an IPv6 address.
2. Describe the difference between Link-Local and Global Unicast addresses.
3. Explain Commands to Configure Router Interfaces in cisco packet tracer.
4. Write the following address with o Leading Zero Omission:
   2001:0db8:0000:0000:0000:ff00:0042:8329

[Space for Answers] (If required attached separate page)

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/how-to-configure-ipv6-on-cisco-router/	Implementation of IPv6
2	https://www.geeksforgeeks.org/computer-networks/internet-protocol-version-6-ipv6/	Examples and explanation of IPv6 address types and structure
3	Rohit Kautkar Youtube Channel- How to Configure IPv6 in Packet Trace	https://www.youtube.com/watch?v=ydDxYT0nkXk

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct IPv6 addressing & routing	30%
2	Verification using commands	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Connectivity success	20%
2	Interpretation and result writing	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.22: *Implement IP Addresses for Intranet in Class A, Class B, Class C

I. Practical Significance

The purpose of this practical is to implement and assign IP addresses for an intranet using Class A, Class B, and Class C addressing schemes. This practical develops skills to segment a network, allocate IP addresses, configure subnet masks, and verify network connectivity. It enables learners to understand the principles of efficient local network design and ensures effective communication between devices within a structured network environment.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Maintain Network layer and Transport layer.

IV. Laboratory Learning Outcome

LLO 22.1 Implement Classful Address in a for class A, Class B, Class C network node in CISCO packet tracer.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing and recording experiments.
- Follow systematic procedures for IP address assignment and network configuration.
- Maintain lab safety standards while handling networking devices.
- Document IP addressing and network configurations clearly and ethically.
- Show responsibility in using authorized devices and addressing schemes.

VI. Relevant Theoretical Background

IP Addressing

An IP (Internet Protocol) address is a unique numerical identifier assigned to every device connected to a network. It enables communication between devices by specifying both the source and destination of data packets. Essentially, it serves two key functions:

1. Identification – Distinguishes each device on the network.
2. Location addressing – Defines where the device is located within the network structure.

Every device-such as a computer, printer, server, or router—requires an IP address to communicate effectively, whether in a Local Area Network (LAN) or across the Internet.

Versions of IP

A. IPv4 (Internet Protocol version 4)

IPv4 is the most widely used version of the Internet Protocol. It utilizes a 32-bit address divided into four octets, each ranging from 0 to 255, separated by dots (e.g., 192.168.1.1).

- **Total Address Space:** Approximately 4.3 billion unique addresses.
- **Format:** Decimal dotted notation (e.g., 172.16.0.1).
- **Structure:** Each address consists of a network portion and a host portion. The division depends on the subnet mask.

IPv4 is commonly used in both public networks (Internet) and private networks (Intranet). However, due to the limited address pool, private IP ranges have been reserved for internal use.

B. IPv6 (Internet Protocol version 6)

IPv6 was developed to overcome the address exhaustion problem of IPv4. It uses 128-bit addresses written in hexadecimal and separated by colons (e.g.,2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 allows for a vastly greater number of unique addresses and introduces features like auto configuration, improved routing, and enhanced security. Although IPv6 adoption is increasing, IPv4 remains dominant in private intranets and most LAN environments, making it essential to understand IPv4 addressing and subnetting.

IPv4 Address Classes

IPv4 addresses are categorized into five major classes (A to E) based on the **first octet value**. This classification helps determine the default network mask, network size, and intended use.

Table 22.1

Sr. No.	Class	Range (First Octet)	Default Subnet Mask	Max Hosts per Network	Use Case / Description
1	A	1-126	255.0.0.0	16,777,214	Used for very large organizations with extensive networks. The first octet identifies the network, while the remaining three octets identify hosts.
2	B	128-191	255.255.0.0	65,534	Suitable for medium-sized organizations, universities, or government departments. The first two octets represent the network portion, while the last two identify hosts.
3	C	192-223	255.255.255.0	254	Commonly used in small networks or LANs. The first three octets represent the network, and the last octet represents the host portion.
4	D	224-239	N/A	N/A	Reserved for multicast communication, such as streaming or conferencing.
5	E	240-255	N/A	N/A	Reserved for experimental and research purposes, not used in standard networking.

The address range 127.x.x.x is reserved for loopback testing, typically 127.0.0.1, which allows a device to test its own network interface without sending data over the network.

Private IP Address Ranges (for Intranet Implementation)

For internal or private networks (intranets), certain IP ranges are reserved so they cannot be used on the public Internet. These are defined by the Internet Assigned Numbers Authority (IANA).

They are as follows:

Table 22.2

Class	Private IP Range	Subnet Mask	Typical Use Case
A	10.0.0.0 – 10.255.255.255	255.0.0.0	Used for very large intranet systems such as large corporations or ISPs.
B	172.16.0.0 – 172.31.255.255	255.255.0.0	Used for medium-sized enterprise networks such as universities or organizations with multiple departments.
C	192.168.0.0 – 192.168.255.255	255.255.255.0	Commonly used in home networks, small offices, and LANs.

These private ranges are implemented behind routers or firewalls, typically using Network Address Translation (NAT) to communicate with external (public) networks if needed.

Practical Implementation in Class A, B, and C Networks

1. **Class A Implementation**
   - **Example Network:** 10.0.0.0
   - **Subnet Mask:** 255.0.0.0
   - **Available Hosts:** 16,777,214
   - **Application:** Used for large enterprises or ISPs with thousands of users.
   - **Example Host Assignment:**
     - Network ID: 10.0.0.0
     - First usable host: 10.0.0.1
     - Last usable host: 10.255.255.254
     - Broadcast address: 10.255.255.255
2. **Class B Implementation**
   - **Example Network:** 172.16.0.0
   - **Subnet Mask:** 255.255.0.0
   - **Available Hosts:** 65,534
   - **Application:** Medium-sized organizations such as universities or corporations with multiple departments.
   - **Example Host Assignment:**
     - Network ID: 172.16.0.0
     - First usable host: 172.16.0.1
     - Last usable host: 172.16.255.254
     - Broadcast address: 172.16.255.255

3. Class C Implementation

- **Example Network:** 192.168.1.0
- **Subnet Mask:** 255.255.255.0
- **Available Hosts:** 254
- **Application:** Small office or departmental network.
- **Example Host Assignment:**
  - Network ID: 192.168.1.0
  - First usable host: 192.168.1.1
  - Last usable host: 192.168.1.254
  - Broadcast address: 192.168.1.255

In a typical intranet environment, Class C addressing is most common because it offers an adequate number of hosts for small networks and is easy to manage. Class A and B addresses are used when the organization needs to accommodate a significantly larger number of devices across multiple branches or campuses.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

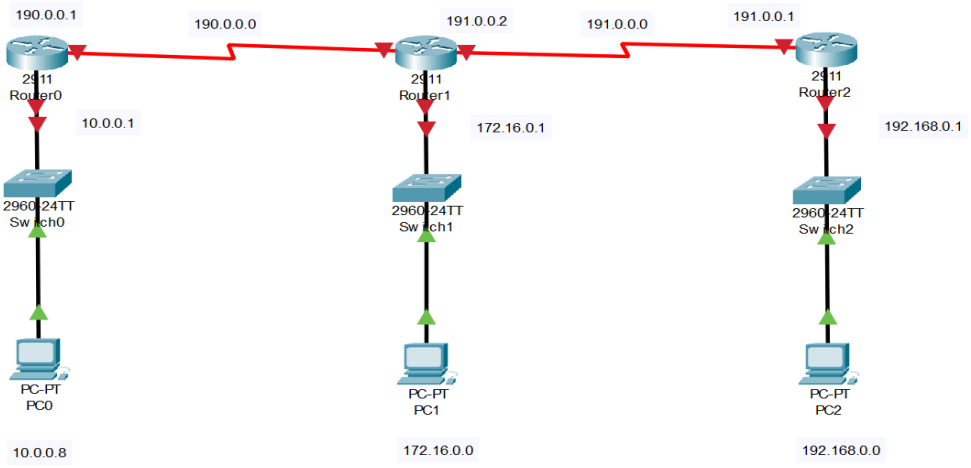


Fig 22.1: Simple Network Topology for implementation of Class A, Class B and Class C in Cisco Packet Tracer

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 22.3

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure all devices are powered off before connecting cables.
2. Assign IP addresses according to the designated class and subnet.
3. Avoid duplicate IP addresses in the same network.
4. Verify all connections before testing network connectivity.
5. Document IP addresses and subnet masks accurately.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following requirements are met:

- A computer with Cisco Packet Tracer (or any equivalent network simulation software) installed.
- Basic understanding of IPv4 addressing**,** subnetting, and router configuration commands.
- Familiarity with device connectivity using Copper Straight-Through and Serial DCE/DTE cables.
- Verify that the simulation tool is correctly installed by opening and testing a sample topology.

2. Create Network Topology

- Open Cisco Packet Tracer and wait until the workspace loads completely.
- Drag and drop the following network devices into the workspace as shown in the topology:
  - 3 Routers (Router0, Router1, and Router2 – model 2911)
  - 3 Switches (2960-24TT)
  - 3 PCs (PC0, PC1, PC2)
- Adding HWIC-2T in Cisco Packet Tracer (Mandatory Step)
  - Step 1: Power Off the Router

- Before adding or removing any hardware module, the router must be powered off.
- Click on the router icon in Packet Tracer.
- Click the "Power" button (a red switch on the left side) to turn it off.

- **Step 2: Select the HWIC-2T Module**
  - Go to the Physical tab of the router window.
  - Under the list of available WIC slots, locate HWIC-2T (or similar serial WAN interface card).
  - Drag and drop the HWIC-2T card into an empty WIC slot (usually WIC 0 or WIC 1).
- **Step 3: Power On the Router**
  - After inserting the module, click the Power button again to turn the router back on.

- Connect the devices using the following cables:
  - Copper Straight-Through cables for PC-to-Switch and Switch-to-Router connections.
  - Serial DCE cables (red lines) for Router-to-Router WAN connections.
- Ensure all link indicators turn green, confirming proper physical connections.

3. Assigning IP Addresses in the Class A Network (Left Segment) as shown in Fig 22.1

Network**:** 10.0.0.0

Connected Devices**:** Router0, Switch0, PC0

- **Configure PC0:**
  - Click PC0 → Desktop → IP Configuration
  - Enter the following values:
    - IP Address: 10.0.0.8
    - Subnet Mask: 255.0.0.0
    - Default Gateway: 10.0.0.1
- **Configure Router0 LAN Interface:**
  - Click Router0 → CLI tab and type the following commands:
    - enable
    - configure terminal
    - interface gigabitEthernet 0/0
    - ip address 10.0.0.1 255.0.0.0
    - no shutdown
    - exit
- **Verify LAN Link:**
  - On PC0 Command Prompt, type:
    - ping 10.0.0.1

  Successful replies indicate that LAN connectivity between PC0 and Router0 is functioning correctly.

4. **Assigning IP Addresses in the Class B Network (Middle Segment)**
   Network: 172.16.0.0
   Connected Devices**:** Router1, Switch1, PC1
   - **Configure PC1:**
     - Click PC1 → Desktop → IP Configuration
     - Enter the following values:
       - IP Address: 172.16.0.8
       - Subnet Mask: 255.25.0.0
       - Default Gateway: 172.16.0.1
   - **Configure Router1 LAN Interface:**
     - Click Router1 → CLI tab and enter:
       - enable
       - configure terminal
       - interface gigabitEthernet 0/0
       - ip address 172.16.0.1 255.255.0.0
       - no shutdown
       - exit
   - **Verify Connectivity:**
     - On PC1 Command Prompt, test communication with:
       - ping 172.16.0.1

     A successful ping confirms local connectivity within the Class B network.
5. **Assigning IP Addresses in the Class C Network (Right Segment)**
   Network: 192.168.0.0
   Connected Devices**:** Router2, Switch2, PC2
   - **Configure PC2:**
     - Click PC2 → Desktop → IP Configuration
     - Enter:
       - IP Address: 192.168.0.8
       - Subnet Mask: 255.255.255.0
       - Default Gateway: 192.168.0.1
   - **Configure Router2 LAN Interface:**
     - Click Router2 → CLI tab and type:
       - enable
       - configure terminal
       - interface gigabitEthernet 0/0
       - ip address 192.168.0.1 255.255.255.0
       - no shutdown
       - exit
   - **Verify Connectivity:**
     - On PC2 Command Prompt, type:
       - ping 192.168.0.1

     Successful ping replies verify proper LAN configuration on the Class C network.

6. **Configure WAN (Serial DCE/DTE) Connections Between Routers**
   - **Link 1: Between Router0 and Router1**
     - Network: 190.0.0.0
     - Router0 Serial0/3/0: 190.0.0.1
     - Router1 Serial0/3/0**:** 190.0.0.2
     - Cable Type**:** Serial DCE (set clock rate on DCE side)
   - **Configuration Commands:**
     - On Router0 (DCE side):
       - enable
       - configure terminal
       - interface serial 0/3/0
       - ip address 190.0.0.1 255.255.255.0
       - clock rate 64000
       - no shutdown
       - exit
     - On Router1 (DTE side):
       - enable
       - configure terminal
       - interface serial 0/3/0
       - ip address 190.0.0.2 255.255.255.0
       - no shutdown
       - exit
   - **Link 2: Between Router1 and Router2**
     - Network: 191.0.0.0
     - Router1 Serial0/3/1: 191.0.0.2
     - Router2 Serial0/3/0: 191.0.0.1
     - Serial DCE
   - **Configuration Commands:**

     On **Router1** (DCE side):
     - interface serial 0/3/1
     - ip address 191.0.0.2 255.255.255.0
     - clock rate 64000
     - no shutdown
     - exit

     On **Router2** (DTE side):
     - interface serial 0/3/0
     - ip address 191.0.0.1 255.255.255.0
     - no shutdown
     - exit
7. **Configure Static Routing Between Routers**

   To ensure communication between all three LANs (10.0.0.0, 172.16.0.0, and 192.168.0.0), static routes must be configured.
   - **On Router0:**

- ip route 172.16.0.0 255.255.0.0 190.0.0.2
- ip route 192.168.0.0 255.255.255.0 190.0.0.2

- **On Router1:**
  - ip route 10.0.0.0 255.0.0.0 190.0.0.1
  - ip route 192.168.0.0 255.255.255.0 191.0.0.1
- **On Router2:**
  - ip route 10.0.0.0 255.0.0.0 191.0.0.2
  - ip route 172.16.0.0 255.240.0.0 191.0.0.2

8. Verify Network Configuration and Connectivity

- Check interface status:
  - show ip interface brief

  All interfaces should show status up/up**.**
- Verify routing tables:
  - show ip route

  Ensure all three networks (10.0.0.0, 172.16.0.0, and 192.168.0.0) appear in each router's routing table.
- Ping Tests:
  - From PC0, ping PC1 and PC2 as shown in Fig 22.2
  - From PC2, ping PC0 and PC1.

  Successful replies confirm complete end-to-end connectivity across all networks.

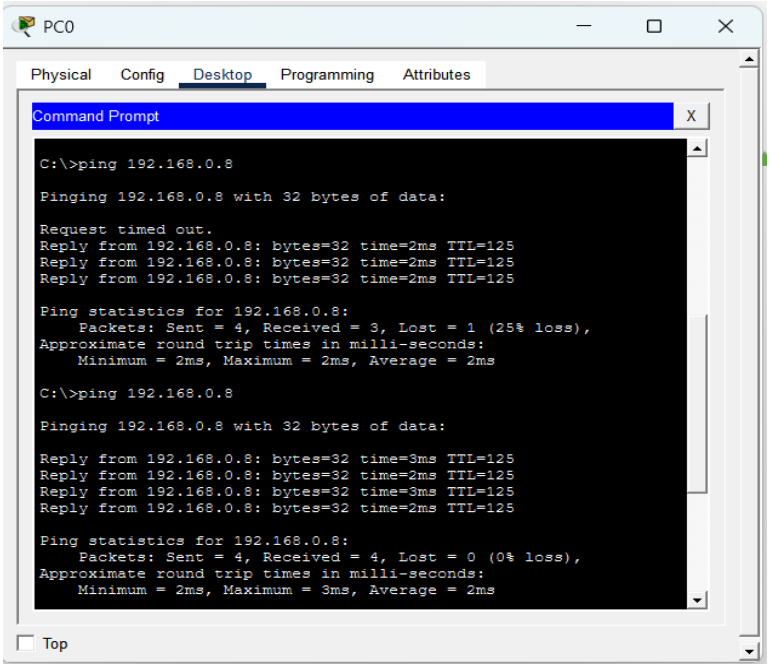


Fig 22.2 Results of Successful Ping Test from PC0 to PC1 and PC2

9. Record Observations

In lab journal, note:

- IP addresses assigned to each router interface and PC.
- Subnet masks and default gateways used.
- Results of ping tests between all devices.
- Status of router interfaces and routing table verification.

10. Save and Exit

- Save Packet Tracer file using File → Save As for future reference.
- Exit the simulation once all configurations are verified and tested successfully.

Table 22.4

Device	Interface	IP Address	Subnet Mask	Network	Default Gateway / Next Hop	Description
Router0	Gigabit Ethernet 0/0	10.0.0.1	255.0.0.0	10.0.0.0	—	LAN interface for Class A network
Router0	Serial0/3/0	190.0.0.1	255.255.255.0	190.0.0.0	—	WAN link to Router1 (DCE side)
Router1	Serial0/3/0	190.0.0.2	255.255.255.0	190.0.0.0	190.0.0.1	WAN link to Router0 (DTE side)
Router1	Serial0/3/1	191.0.0.2	255.255.255.0	191.0.0.0	—	WAN link to Router2 (DCE side)
Router1	Gigabit Ethernet 0/0	172.16.0.1	255.255.0.0	172.16.0.0	—	LAN interface for Class B network
Router2	Serial0/3/0	191.0.0.1	255.255.255.0	191.0.0.0	191.0.0.2	WAN link to Router1 (DTE side)
Router2	Gigabit Ethernet 0/0	192.168.0.1	255.255.255.0	192.168.0.0	—	LAN interface for Class C network
PC0	NIC	10.0.0.8	255.0.0.0	10.0.0.0	10.0.0.1	End device in Class A network
PC1	NIC	172.16.0.8	255.255.0.0	172.16.0.0	172.16.0.1	End device in Class B network
PC2	NIC	192.168.0.8	255.255.255.0	192.168.0.0	192.168.0.1	End device in Class C network

XI. Resources used during performance

Table 22.5

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……

……

XV. Interpretation of results

……

……

XVI. Conclusion and recommendation

……

……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Identify the class range that supports the maximum number of hosts.
2. State the total number of octets in an IPv4 address.
3. Specify an example of a valid IPv4 address.
4. Determine the IP class for the address 172.16.10.5.

[Space for Answers] (If required attached separate page)

……

……

……

……..…..…
……...…
……...
……...…
……...…
……...…
……...…
……...…
……...…
……...…

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/introduction-of-classful-ip-addressing/	Explanation of IP Classes with examples
2	https://www.geeksforgeeks.org/computer-networks/internet-protocol-version-6-ipv6/	Examples and explanation of IPv6 address types and structure
3	https://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm	IPv4 - Address Classes

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correctly assign IP addresses	30%
2	Configure subnet masks & gateway	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Connectivity success	20%
2	Successful intranet operation	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.23: Configuration and Testing of basic Firewall

I. Practical Significance

The purpose of this practical is to understand, configure, and test a basic firewall on both Windows operating systems to ensure secure network communication. This practical develops skills to manage and implement firewall rules, monitoring network traffic, and safeguarding systems from unauthorized access. It enables learners to comprehend the role of firewalls as a critical component of network security, ensuring the protection of data and maintaining the integrity of communication within a secure network environment.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 23.1 Configure basic firewall using Windows/Linux.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing and recording firewall configuration experiments.
- Follow systematic procedures for configuring and testing firewall rules on Windows and Linux operating systems.
- Maintain lab safety and security standards while handling networked systems and security configurations.
- Show responsibility in using authorized systems, adhering to security guidelines, and implementing ethical practices in network protection.

VI. Relevant Theoretical Background

A firewall is a critical component of network security designed to monitor, filter, and control the flow of incoming and outgoing network traffic based on a defined set of security rules. It acts as a protective barrier between a trusted internal network and untrusted external networks, such as the Internet, ensuring that only authorized traffic is allowed while potentially harmful data is blocked. Firewalls are fundamental to maintaining data confidentiality, integrity, and availability within modern digital infrastructures.

Types of Firewalls

1. **Packet Filtering Firewall** –

This is the most basic type of firewall that inspects network packets individually, making decisions based on parameters such as source and destination IP addresses, port numbers, and protocols. It operates primarily at the network layer of the OSI model. Although efficient, it does not track the state of connections, which can limit its effectiveness against more sophisticated attacks.

2. **Stateful Inspection Firewall** –
   Also known as a dynamic packet filtering firewall, this type goes beyond simple packet inspection by maintaining a state table that tracks active connections. It evaluates packets in the context of an existing session, ensuring that only legitimate packets belonging to established connections are allowed. This makes it more secure than basic packet filtering firewalls.
3. **Application Firewall** –
   Operating at the application layer, this firewall inspects and filters traffic based on application- specific data, such as HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), or SMTP (Simple Mail Transfer Protocol) requests. It can identify and block malicious activities hidden within application data streams, offering granular control over network communication. Application firewalls are widely used to protect web servers and application services from sophisticated threats like SQL injection or cross-site scripting (XSS).

Firewalls on Operating Systems

Both Windows and Linux operating systems provide built-in firewall solutions to manage and secure local network communication. Understanding their configuration and operation is essential for ensuring system security and compliance with organizational policies.

A. Windows Firewall Options

Windows systems incorporate Windows Defender Firewall, which offers both Graphical User Interface (GUI) and command-line tools for configuration.

- The GUI-based configuration allows users to easily enable or disable rules, create exceptions, and monitor firewall activity.
- The command-line tools such as PowerShell and Command Prompt (netsh or Set-NetFirewallRule) provide advanced control for scripting and automation, enabling network administrators to manage firewall settings efficiently across multiple systems.

Windows Firewall operates as a stateful firewall, meaning it monitors and records the state of active connections to ensure that only valid traffic is permitted.

B. Linux Firewall Options

Linux systems offer multiple firewall frameworks and tools, each designed to cater to different levels of user expertise and network complexity. Some of the most common and significant firewall solutions include:

- **IPCop:**
  A dedicated Linux-based firewall distribution aimed at providing network perimeter protection and gateway services for small businesses and home

networks. IPCop features a web-based graphical interface that simplifies configuration, monitoring, and maintenance. It is commonly used as a standalone security appliance.

- **Shorewall (Shoreline Firewall):**
  A high-level firewall management tool built on top of iptables. It simplifies the creation and management of complex firewall rules for systems with multiple network interfaces. Shorewall is often preferred by experienced administrators who manage large-scale or segmented network environments.
- **UFW (Uncomplicated Firewall):**
  UFW is a user-friendly command-line interface designed to simplify the configuration of iptables for both beginners and system administrators. It provides a simplified syntax for creating, enabling, or disabling firewall rules, making it an excellent choice for quick setup and basic security configurations.
- **iptables**:The most fundamental and widely used firewall framework in Linux systems. Operating at the kernel level through the netfilter framework, iptables allows detailed control over packet filtering, Network Address Translation (NAT), and packet mangling. It enables administrators to define rules that determine how packets are handled, ensuring fine-grained control over network traffic. Many higher-level tools, such as UFW and Shorewall, internally rely on iptables to enforce their firewall rules. This makes iptables the core firewall engine for most Linux distributions and an essential concept for anyone studying or working in the field of Linux network security.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

NA

B) Actual Block Diagram

NA

VIII. Required Resources/apparatus/equipment with specifications

Table 23.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01

Sr. No.	Name of Resource	Specification	Quantity
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure administrator/root privileges before configuration.
2. Avoid blocking essential system ports (e.g., 22, 80, 443) unless required.
3. Always verify connectivity after rule changes.
4. Save or export firewall rules after successful configuration.
5. Disable firewall rules carefully when testing.

X. Suggested Procedure

A. Firewall Configuration on Windows

- **Prerequisites**

  Before starting the practical, ensure the following:
  - A computer running Windows 10 or Windows 11 with administrative privileges.
  - Basic understanding of networking concepts, including ports, protocols, and IP addressing.
  - Internet access (optional) to test firewall rules and connectivity.
  - The system should have Windows Defender Firewall enabled by default.
  - If any third-party firewall or antivirus software is installed, disable it temporarily to avoid conflicts.
- **Open Windows Defender Firewall**
  - Windows provides two interfaces for managing firewall settings:
    - A basic interface through the Control Panel and
    - An advanced configuration console called Windows Defender Firewall with Advanced Security (WFAS).
- **Option 1: Open Using Control Panel**
  - Click the Start button on the taskbar.
  - Type Control Panel in the search box and press Enter.
  - In the Control Panel window, click System and Security.
  - Click Windows Defender Firewall.
  - The main window displays the firewall status for Domain, Private, and Public networks. You can see whether the firewall is currently enabled or disabled for each profile as shown in Fig 23.1

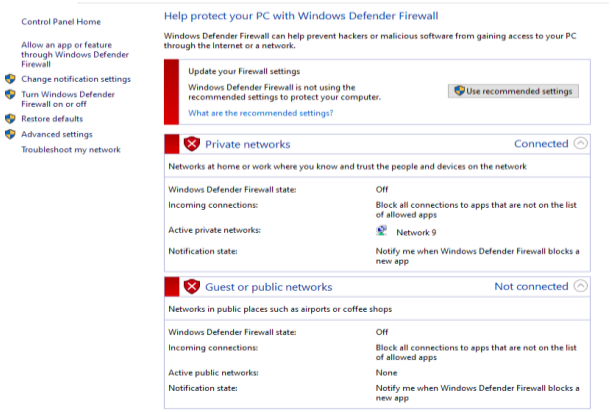


Fig 23.1 Firewall status for Domain, Private, and Public networks

- **Option 2: Open Using Advanced Security Console**
  - From the same Windows Defender Firewall window, click Advanced settings on the left panel.
  - This opens the Windows Defender Firewall with Advanced Security console.
  - The left pane contains sections such as Inbound Rules, Outbound Rules, and Monitoring.
  - The right-hand pane shows Actions where you can create new rules or manage existing ones.

  This console allows administrators to create specific rules for ports, IP addresses, and programs.
- **Enable or Disable the Firewall**

  Windows Defender Firewall can be turned on or off using either the Control Panel or the Advanced Security console.
  - **Enable or Disable from Control Panel**
    - Open Control Panel → System and Security → Windows Defender Firewall.
    - In the left panel, click Turn Windows Defender Firewall on or off.
    - Two sections will appear: Private network settings and Public network settings as shown in Fig 23.2

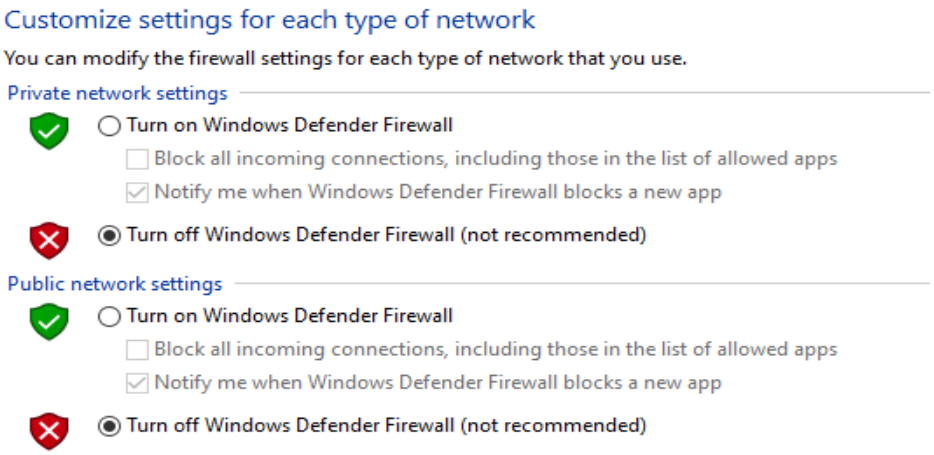


Fig 23.2 Firewall status for Domain, Private, and Public networks

- Under each section, select Turn on Windows Defender Firewall. Optional: Check Block all incoming connections, including those in the list of allowed apps for stronger protection.
- Click OK to save the changes.

Enabling the firewall protects the system from unauthorized access on both private and public networks.

- **Enable or Disable from Advanced Security Console**
  - Open Windows Defender Firewall with Advanced Security.
  - In the right-hand Actions pane, click Windows Defender Firewall Properties.
  - A dialog box appears with four tabs: Domain Profile, Private Profile, Public Profile, and IPsec Settings as shown in Fig 23.3

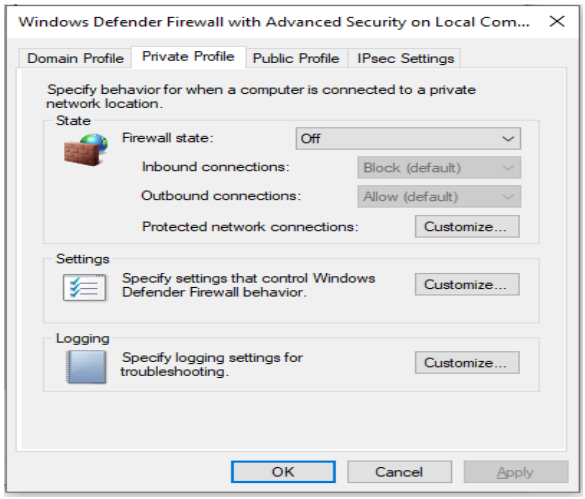


Fig 23.3 Windows Defender Firewall Properties

  - Under each of the first three tabs, locate the Firewall state section.
  - Select On (recommended) to enable or Off to disable the firewall for that profile.
  - Click Apply and then OK.

This method allows administrators to enable or disable the firewall separately for each network profile.

- **Allow a Specific Application or Port**

Sometimes, a trusted application or service needs permission to communicate through the firewall. You can create a rule to allow an application or a port.

- **Allowing an Application**
  - Open Control Panel → System and Security → Windows Defender Firewall.

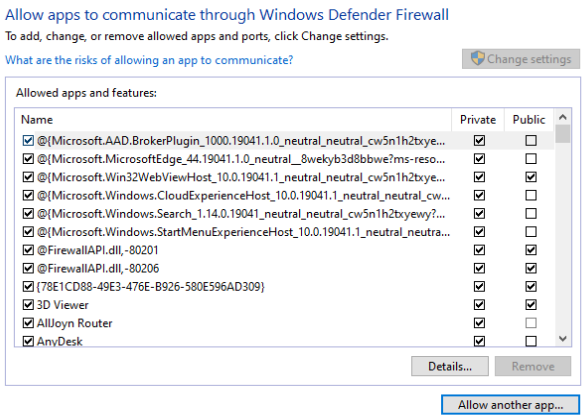


Fig 23.4 Allow an app or feature through Windows Defender Firewall

- In the left panel, click Allow an app or feature through Windows Defender Firewall as shown in Fig 23.4
- Click the Change settings button to make the list editable.
- To add a new application, click Allow another app.
- In the dialog box, click Browse and navigate to the application's executable file (for example, C:\Program Files\AppName\App.exe).
- Click Open, then Add.
- Select the network types (Private and/or Public) where the app should be allowed.
- Click OK to apply the settings.

This creates an exception that allows the selected application to send and receive network traffic through the firewall.

- **Allowing a Specific Port**
  - Open Windows Defender Firewall with Advanced Security.
  - In the left pane, click Inbound Rules.
  - In the right-hand Actions pane, click New Rule.
  - In the New Inbound Rule Wizard, select Port and click Next.
  - Choose the required protocol (TCP or UDP).
  - Select Specific local ports and enter the port number (for example, 80 for HTTP or 443 for HTTPS).
  - Click Next.
  - Select Allow the connection and click Next.
  - Choose the network profiles (Domain, Private, and/or Public) where this rule should apply.
  - Click Next.
  - Enter a name such as Allow HTTP Port 80, then click Finish.

  The firewall now allows data through the specified port number.
- **Block a Specific IP Address or Program**

  Blocking rules are used to prevent network traffic from a specific program, IP address, or IP range.
  - Open Windows Defender Firewall with Advanced Security.
  - In the left pane, click Inbound Rules.

- In the right-hand Actions pane, click New Rule.
- Select Custom and click Next.
- Under Program, select either All programs or This program path and browse to the desired executable file.
- Click Next.
- Under Protocol and Ports, leave the default settings or specify the desired protocol and port number. Click Next.
- Under Scope, select These IP addresses under the remote IP section.
- Click Add, and enter the IP address or range you wish to block (for example, 192.168.1.0/24).
- Click OK, then Next.
- Under Action, select Block the connection, then click Next.
- Under Profile, choose when the rule should apply (Domain, Private, Public). Click Next.
- Enter a descriptive name such as Block Unknown Host, then click Finish.

Any network traffic from the specified program or IP address range will now be blocked by the firewall.

- **Verify Firewall Configuration**

  After configuring the firewall, you can verify its current status and rules using command-line tools.

  - Right-click the Start button and select Windows Terminal (Admin) or Command Prompt (Admin).
  - Type the following commands one by one and press Enter after each.

  netsh advfirewall show allprofiles

  netsh advfirewall firewall show rule name=all

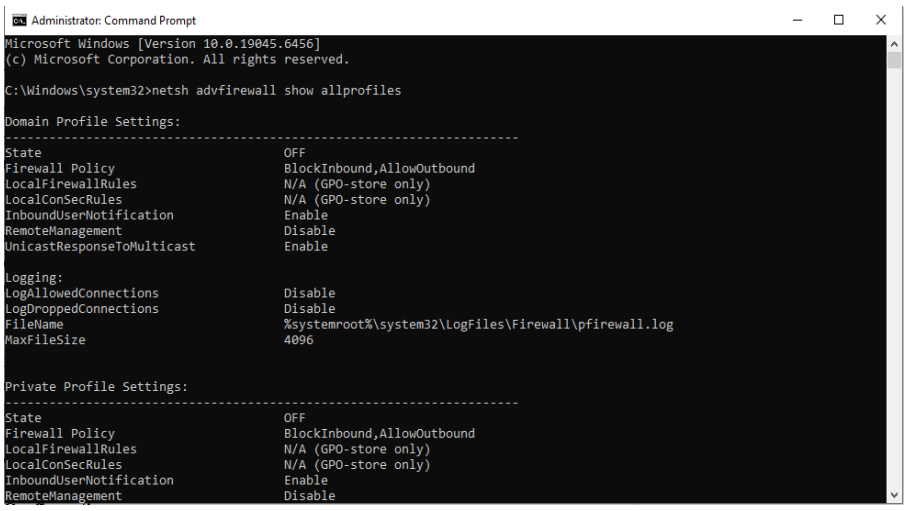


Fig 23.5 Output of netsh advfirewall show all profiles command

It will show output as shown in Fig 23.5. The first command displays the status of all firewall profiles. The second command lists all the firewall rules currently active on the system.

- **Test Firewall Behaviour**

  After configuration, it is important to test whether the firewall rules work correctly.
  - Open Command Prompt.
  - Use ping or telnet commands to test connectivity between systems.
    Example:

    ping <target_IP>

    telnet <target_IP> 80
  - If the connection is allowed, you should receive a reply or connection success message.
  - If the connection is blocked, the command will show a timeout or connection failure.

  Testing verifies that the firewall is functioning as configured and that allowed and blocked rules are enforced properly.
- **Record Observations**

  Record practical results in the following format:

Parameter	**Observation**
Firewall Enabled	Yes / No
Network Profile Used	Domain / Private / Public
Rule Type Created	Allow / Block
Port Number	Example: 80
IP Address (if blocked)	Example: 192.168.1.10
Test Result	Successful / Failed
Connection Status	Connected / Blocked

B. Firewall Configuration on Linux (Ubuntu using UFW)

- **Check UFW Status**
  - Open the terminal and type:
  - sudo ufw status
  - If UFW is inactive, proceed to enable it.
- **Enable the Firewall**
  - Activate UFW using the command:
  - sudo ufw enable
  - Confirm the firewall is active and protecting the system.
- **Allow Specific Services or Ports**
  - Permit commonly used network services by specifying port numbers or service names:
    - sudo ufw allow 22/tcp # Allow SSH
    - sudo ufw allow 80/tcp # Allow HTTP
    - sudo ufw allow 443/tcp # Allow HTTPS
  - Each command adds a new rule to the firewall configuration.
- **Block a Specific IP Address**
  - To deny traffic from a specific IP:
  - sudo ufw deny from 192.168.1.100
  - This rule prevents communication from the listed IP address.
- **Allow a Specific IP Address**

- To allow a trusted IP:
- sudo ufw allow from 192.168.1.10
- This ensures only the specified IP is permitted through the firewall.

- **View All Active Rules**
  - Display all configured rules in a numbered list:
  - sudo ufw status numbered
- **Delete or Modify a Rule**
  - Identify the rule number from the list and remove it as needed:
  - sudo ufw delete <rule-number>
  - This command helps maintain an updated and relevant firewall configuration.
- **Test Configuration**
  - From another machine on the network, test the applied rules using **ping**, **telnet**, or a web browser.
  - Attempt connections to both allowed and blocked services.
  - Observe successful communication for allowed ports (e.g., SSH or HTTP) and failed attempts for blocked IPs or ports.

C. Verification and Testing

After configuring both systems, perform a series of validation tests to confirm that firewall rules function as intended.

Table 23.2

Sr. No.	Test Description	Command	Expected Result
1	Check Firewall Status (Windows)	netsh advfirewall show allprofiles	Firewall should be ON for all profiles
2	Check Firewall Status (Linux)	sudo ufw status	UFW should display as active with configured rules
3	Test Allowed Port	telnet <IP> 80	Connection should be successful
4	Test Blocked IP	ping <blocked_IP>	Response should be Request Timed Out
5	View Active Rules (Linux)	sudo ufw status numbered	Displays a numbered list of all active firewall rules

D. Record Observations

In the lab journal, note the following details:

- List of allowed and blocked ports configured on both systems.
- IP addresses or programs that were restricted or permitted.
- Commands used for enabling, disabling, or modifying rules.
- Results of connectivity tests verifying firewall effectiveness.
- Screenshots (if required) showing command outputs and rule configurations.

E. Save and Exit

- Ensure all configurations are properly verified and tested.
- Save the system or lab environment snapshot for documentation purposes.
- Close the firewall management consoles and terminal windows.

XI. Resources used during performance

Table 23.3

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

NA

XIV. Result

……..……..

……..……..

XV. Interpretation of result

……...…

……...…

XVI. Conclusion and recommendation

……...……

……..….

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the main purpose of a firewall.
2. Name two types of firewalls based on packet inspection.
3. Write the command to enable firewall on Linux using UFW.
4. Describe the process to check active firewall rules on Windows.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/	Windows Firewall documentation
2	https://help.ubuntu.com/community/UFW	Ubuntu UFW official documentation
3	https://www.geeksforgeeks.org/ethical-hacking/how-to-configure-firewalls-in-windows/	Simple firewall setup examples on Windows
4	https://www.geeksforgeeks.org/linux-unix/linux-firewall/	Simple firewall setup examples on Linux

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct firewall configuration (Windows/Linux)	30%
2	Verification of configuration	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful blocking/allowing traffic	20%
2	Interpretation and results	10%
3	Answer to Practical Related Question	05%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.24: *Use FTP protocol to transfer files from one system to another system

I. Practical Significance

The purpose of this practical is to implement and analyze the functioning of the File Transfer Protocol (FTP) for transferring files between two systems. This practical develops an understanding of how FTP facilitates reliable and organized file exchange between client and server systems within a network environment. Through this practical, students gain essential skills in configuring and testing FTP operations, reinforcing the importance of file transfer mechanisms in network management and data communication.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 24.1 Create FTP Server using network simulation software.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing
- Follow systematic procedures for setting up, configuring, and analyzing FTP operations between client and server systems using Cisco Packet Tracer.
- Maintain lab safety, equipment functionality, and software tools in proper working condition during FTP experiments.
- Document FTP setup details, configuration parameters, and test outcomes clearly, accurately, and ethically.
- Demonstrate responsibility in using authorized systems, adhering to network security guidelines, and practicing ethical conduct during file transfer simulations.

VI. Relevant Theoretical Background

The File Transfer Protocol (FTP) is one of the earliest and most widely used application-layer protocols designed for transferring files between computer systems over a Transmission Control Protocol/Internet Protocol (TCP/IP) network. It provides a reliable, structured, and efficient mechanism for sharing data between a client (the requesting system) and a server (the responding system). FTP plays a crucial role in network administration, web hosting, and remote data management, where files such as documents, software, and configuration data need to be moved securely and efficiently between connected systems.

FTP operates using the client–server architecture, where the client initiates communication with the server to perform actions such as authentication, file upload, download, renaming, or deletion. The server, in turn, manages access permissions, directory structures, and user requests. Communication in FTP is based on two separate channels, each serving a specific purpose:

1. Control Channel (TCP Port 21): This channel is responsible for establishing and maintaining the control session between the FTP client and server. It is used to transmit commands (such as login credentials and file operation instructions) from the client to the server and to receive responses or acknowledgment codes from the server. This channel remains open throughout the FTP session and handles administrative exchanges rather than the actual file data.

2. Data Channel (TCP Port 20):

The data channel is dedicated to the actual transmission of files and directory listings. Unlike the control channel, it is opened and closed as needed for each data transfer operation. The data channel carries the contents of files being uploaded or downloaded, ensuring that the data is transmitted reliably using the underlying TCP protocol, which provides error detection, retransmission, and sequencing of packets.

FTP supports two distinct modes of operation for managing the data connection, based on how the data channel is established:

- **Active Mode:**

  In this mode, the client opens a random port above 1023 and informs the server of this port number. The server then initiates the data connection from its port 20 to the client's specified port. However, this mode may encounter issues when firewalls or NAT (Network Address Translation) devices block incoming connections initiated by the server.

- **Passive Mode:**

  Passive mode overcomes the limitations of active mode by allowing the client to initiate both control and data connections. Here, the server provides a port number for the client to connect to for data transfer. This mode is more firewall-friendly and is commonly used in modern network environments where security restrictions are in place.

To enhance security, FTP can be extended to FTPS (File Transfer Protocol Secure**)**, which uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security**)** encryption to protect the confidentiality and integrity of data during transmission. Unlike standard FTP, which transmits data and credentials in plaintext, FTPS ensures that sensitive information such as usernames, passwords, and file contents are encrypted, thus preventing unauthorized access and eavesdropping. FTP sessions involve a sequence of commands and responses that facilitate communication between the client and server. These commands follow a well-defined syntax and enable various file operations.

Key Concepts of FTP

Table 24.1

Sr. No.	Concept	Detailed Description
1	**FTP Server**	The FTP server is a dedicated system or software service that stores, manages, and shares files over the network. It listens on port 21 for incoming client requests, authenticates users, enforces access permissions, and facilitates file transfer operations. Examples include FileZilla Server, vsftpd, and Windows IIS FTP service.
2	**FTP Client**	The FTP client is an application or system that connects to an FTP server to perform operations such as uploading, downloading, renaming, or deleting files. Common FTP clients include FileZilla, WinSCP, and the command-line FTP utility. Clients send FTP commands and interpret server responses to perform specific actions.
3	**TCP Port 21**	This port is reserved for the control connection and is responsible for transmitting commands and responses between the client and server. It ensures session management, user authentication, and operational control throughout the communication process.
4	**TCP Port 20**	Used primarily for data transfer in active mode, this port facilitates the actual exchange of file contents or directory listings between the FTP client and server. The data connection is temporary and is established separately from the control channel.

Table 24.2

Command	Function
ls	Lists files on the remote FTP server.
dir	Also lists files — sometimes shows more details depending on the FTP server implementation.
get filename	Downloads a file from the FTP server.
put filename	Uploads a file to the FTP server.
bye or quit	Ends the FTP session.

FTP is an essential protocol for network-based file sharing, built upon TCP to ensure reliable, ordered, and error-checked delivery of data. Understanding FTP involves not only knowing its ports and operational modes but also being aware of its security implications and practical applications in both academic and professional network environments. Through hands-on implementation and analysis using tools like Cisco Packet Tracer, learners can develop a deeper understanding of FTP operations, network communication, and secure file transfer mechanisms in modern networking systems.

VII. Circuit diagram / block diagram

A) Suggestive Block Diagram

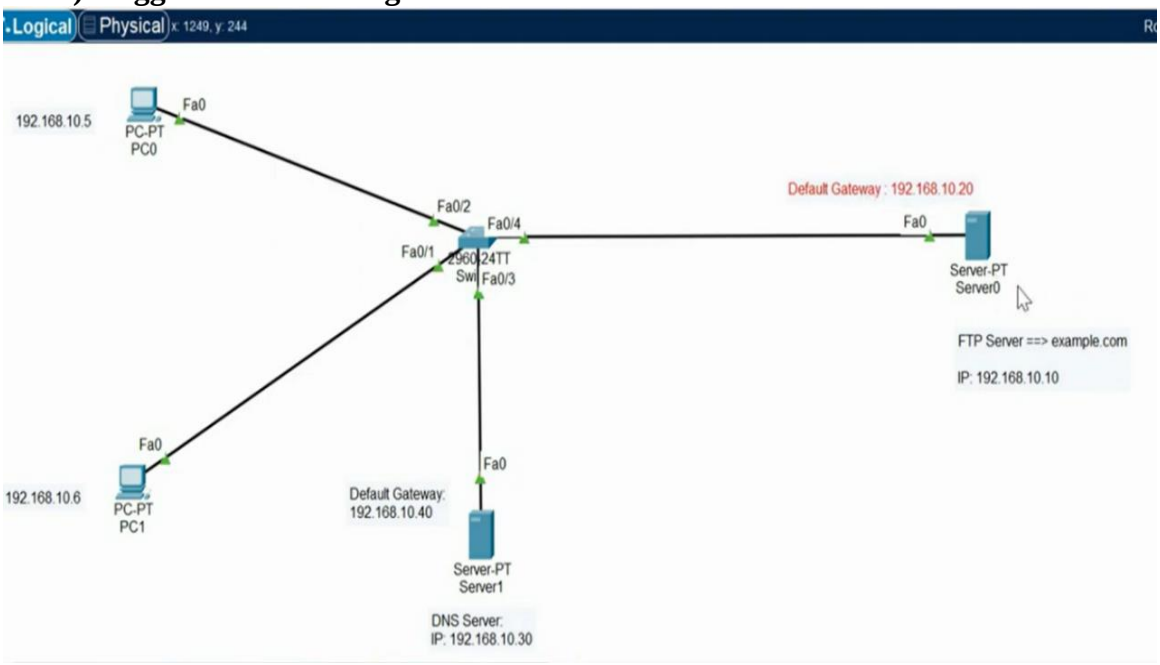


Fig 24.1 Typical FTP Server Implementation in Cisco Packet Tracer

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 24.3

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	02
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all devices are properly connected and powered ON in Cisco Packet Tracer.
2. Configure correct IP addresses for all systems.
3. Verify connectivity using PING before starting FTP configuration.
4. Use proper usernames and passwords while configuring FTP.
5. Save the simulation frequently to prevent data loss.

X. Suggested Procedure

- **Prerequisites**

Before beginning the practical, ensure the following requirements are met:

- A computer with **Cisco Packet Tracer** (or an equivalent network simulation software) properly installed and functioning.
- Basic understanding of **networking concepts**, including IPv4 addressing, subnet masks, default gateways, and DNS configuration.
- Familiarity with **client-server architecture**, particularly the operation of FTP (File Transfer Protocol) and DNS (Domain Name System).
- Knowledge of **connecting network devices** using **Copper Straight-Through Cables** within Cisco Packet Tracer.
- Keep an **IP addressing plan** ready for all devices, including PCs, FTP Server, and DNS Server, as per the practical diagram.
- Verify that all network interfaces (FastEthernet ports) show **green link lights**, indicating successful physical connections before configuration.

A. Configuration and Testing of FTP Server in Cisco Packet Tracer

- **Start Cisco Packet Tracer**

- Launch Cisco Packet Tracer on computer.
- Open a new workspace and ensure that all device categories (End Devices, Switches, and Servers) are accessible from the bottom panel.
- Familiarize with the basic tools for connecting devices and configuring IP addresses.

- **Create the Network Topology**
  - Place the following devices in the workspace as shown in the diagram:
    - Two PCs (PC0 and PC1)
    - One Switch (2960-24TT)
    - Two Servers (Server0 and Server1)
  - Connect the devices using Copper Straight-Through Cables:
    - PC0 → Switch (Fa0/1)
    - PC1 → Switch (Fa0/2)
    - Server0 (FTP Server) → Switch (Fa0/4)
    - Server1 (DNS Server) → Switch (Fa0/3)

  Ensure that each connection shows a green link light, indicating an active physical connection.
- **Assign IP Addresses to Devices**

  Assign the IP addresses as shown in the diagram to ensure all devices are in the same network (192.168.10.0).

Table 24.4

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	Fa0	192.168.10.5	255.255.255.0	192.168.10.40
PC1	Fa0	192.168.10.6	255.255.255.0	192.168.10.40
Server0 (FTP Server)	Fa0	192.168.10.10	255.255.255.0	192.168.10.20
Server1 (DNS Server)	Fa0	192.168.10.30	255.255.255.0	192.168.10.40

- **Configure the FTP Server (Server0)**
  - Click on Server0 to open its configuration window.
  - Go to Services → FTP tab.
  - Turn FTP Service: ON to enable the FTP functionality.
  - Create a user account for FTP login:
    - Username: ftpuser
    - Password: ftp123
  - Add or upload files to the FTP directory, such as:
    - example.txt
    - datafile.docx
  - Note the FTP Server Name**:** example.com
    - This name can later be mapped to the server's IP address using DNS.

  Server0 is now ready to accept FTP client connections for file uploads and downloads.

- **Configure the DNS Server (Server1)**
  - Click on Server1 → Services → DNS tab.
  - Turn DNS Service: ON.
  - Create a new DNS record for the FTP Server:
    - Name: example.com
    - Address: 192.168.10.10
  - Click Add to save the record.

  This allows clients to access the FTP server using the hostname example.com instead of its IP address.
- **Configure FTP Clients (PC0 and PC1)**
  - Click on PC0 → Desktop → IP Configuration, and verify the following details:
    - IP Address: 192.168.10.5
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.10.40
    - DNS Server: 192.168.10.30
  - Repeat the same steps for PC1 with IP 192.168.10.6.
  - Both PCs should be configured to use the DNS Server (Server1) for name resolution.
- **Verify Network Connectivity**
  - Open the Command Prompt on PC0. Test connectivity using the ping command:

    ping 192.168.10.10
  - A successful reply confirms that PC0 can reach the FTP server.
  - Also, test DNS name resolution:

    ping example.com

  If the DNS server is correctly configured, the hostname example.com should resolve to 192.168.10.10. Repeat the same test from PC1 to ensure connectivity.
- **Access the FTP Server from PC Clients**
  - On PC0, open Desktop → Command Prompt.
  - Type the following command to connect using the FTP protocol:

    ftp example.com

    or directly using the server's IP:

    ftp 192.168.10.10
  - When prompted, enter the credentials created earlier:
    - Username: ftpuser
    - Password: ftp123
  - Once connected, perform the following operations:
    - To list files:

      ls
    - To download a file from the server:

      get example.txt

- To upload a file to the server:
  put newdata.txt
- To exit the FTP session**:**
  bye

Repeat the same process on PC1 to verify multi-client FTP access.

- **Verify File Transfer**
  - Open PC0 → Desktop → Files and confirm that the file example.txt has been successfully downloaded.
  - On the FTP Server (Server0), check the FTP directory to ensure that the file newdata.txt uploaded by the client is present.
  - A successful transfer of files in both directions indicates that the FTP service and client-server communication are functioning correctly.
- **Record Observations**
  Record the configuration details and results in lab journal as follows:

Parameter	**Observation**
FTP Server Name	example.com
FTP Server IP	192.168.10.10
DNS Server IP	192.168.10.30
PC0 IP	192.168.10.5
PC1 IP	192.168.10.6
Username Used	ftpuser
File Download Status	Successful / Failed
File Upload Status	Successful / Failed
DNS Resolution	Working / Not Working
Connection Status	Connected / Disconnected

- **End of Practical**
  - Review all results and confirm that FTP connections, file transfers, and DNS name resolution are operating as expected.
  - Save Cisco Packet Tracer project file (.pkt) for future reference.
  - Close all open configuration windows and exit Cisco Packet Tracer.

  This completes the FTP Server Configuration and Testing Practical using Cisco Packet Tracer, demonstrating client-server communication, DNS name resolution, and secure file exchange over a simulated TCP/IP network.

XI. Resources used during performance

Table 24.5

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

Table 24.6

Step	Action Performed	Expected Output	Actual Output (Successful/As Expected/File Downloaded/ File uploaded/ Verified)	Status (Pass/ Fail)
1	Ping between PC0 and Server0 (FTP Server)	Successful reply from 192.168.10.10		
2	Ping between PC0 and Server1 (DNS Server)	Successful reply from 192.168.10.30		
3	Resolve FTP server domain using ping command (ping example.com)	Domain name resolves to IP 192.168.10.10		
4	Establish FTP connection from PC0 to FTP Server	"Connected to 192.168.10.10" or "Connected to example.com"		

Step	Action Performed	Expected Output	Actual Output (Successful/As Expected/File Downloaded/ File uploaded/ Verified)	Status (Pass/ Fail)
5	Login using FTP credentials (ftpuser / ftp123)	Login successful message displayed		
6	Execute ls command on FTP client	List of available files displayed from server directory		
7	Execute get example.txt command	File successfully downloaded to PC0		
8	Execute put newdata.txt command	File successfully uploaded to FTP Server		
9	Verify transferred files on both client and server	Files appear correctly in their respective directories		
10	Test FTP access from PC1 to FTP Server	FTP session established and files accessible		

XIV. Result

……..…..……

……...…

XV. Interpretation of result

……...…

……...…

XVI. Conclusion and recommendation

……...…

……..

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. Give the purpose of the FTP protocol.
2. State ports are used by FTP for control and data transfer.
3. Differentiate between active and passive FTP modes.
4. List any four FTP commands and their functions.
5. Enlist various FTP clients.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/file-transfer-protocol-server-configuration-using-cisco-packet-tracer/	FTP working and commands
2	Rohit Kautkar Youtube Channel-Configure FTP in Packet Tracer | How to configure an FTP | Simulating FTP Server using Packet tracer	https://www.youtube.com/watch?v=PZ4Fd7bgCws
3	https://www.tutorialspoint.com/what-is-the-ftp	What is the FTP?
4	https://www.scaler.com/topics/computer-network/file-transfer-protocol/	File Transfer Protocol (FTP)

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct FTP configuration in Cisco Packet Tracer	30%
2	Successful connection and file transfer	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct upload/download of files	10%
2	Verification of file transfer	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.25: *Use of Packet Tracer as Packet Sniffer

I. Practical Significance

The purpose of this practical is to develop skills and analyze the transmission of data packets within a network using the Packet Sniffer feature in Cisco Packet Tracer. This practical develops skills to capture, inspect, and interpret network packets, providing insights into network behavior, error detection, and protocol operations. Through this practical, students develop essential skills in monitoring and troubleshooting network communication, reinforcing the significance of packet analysis in effective network management and performance optimization.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 25.1 Block/unblock specific ports and test using TELNET.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing
- Demonstrate ethical and responsible practices while performing network monitoring and analysis activities, respecting data privacy and system integrity.

VI. Relevant Theoretical Background

A packet sniffer, also known as a network or protocol analyzer, is a specialized tool used to capture, monitor, and examine data packets as they travel across a network. It enables students to understand how devices exchange information, how different network protocols operate, and how data integrity and reliability are maintained during transmission.

In Cisco Packet Tracer, the Simulation Mode acts as an integrated packet sniffer, allowing users to visualize and analyze packet movement through networking devices such as routers, switches, and PCs. When activated, it displays each transmitted packet along with details such as source and destination address, encapsulated protocol headers, and the path followed. This provides a clear view of communication processes across the OSI or TCP/IP layers.

This practical exercise focuses on managing network traffic by blocking and unblocking specific ports—particularly TELNET (port 23)—using Access Control Lists (ACLs). By using Simulation Mode to monitor TELNET packets before and after ACL implementation, students can observe how access rules affect packet flow. This

hands-on approach enhances understanding of port-based traffic control, network security, and policy enforcement.

Key Concepts

Table 25.1

Sr. No	Concept	Description
1	Packet Sniffer	A software or tool that captures and analyzes network packets to study network traffic and diagnose issues.
2	Encapsulation	The process of adding headers and trailers to data as it passes through OSI layers to prepare it for transmission.
3	Decapsulation	The reverse process, where protocol headers are removed as data travels up the OSI layers at the receiver's end.
4	Simulation Mode	A feature in Cisco Packet Tracer that enables packet tracking, allowing users to view the detailed journey of packets through a simulated network.
5	Protocol Stack	The layered structure (such as OSI or TCP/IP model) showing how data is formatted, transmitted, and interpreted across the network.

Common Uses of Packet Sniffer in Packet Tracer

- **Network Troubleshooting:** Identifying and diagnosing connectivity issues, packet loss, or incorrect routing configurations.
- **Protocol Study:** Observing how various protocols such as HTTP (Hypertext Transfer Protocol), ICMP (Internet Control Messaging Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), and TCP (Transmission Control Protocol)/UDP (User Datagram Protocol) function during communication.
- **Traffic Analysis:** Understanding how data flows between devices, determining bandwidth usage, and analyzing latency or delays.
- **Educational Demonstration:** Providing a visual understanding of theoretical networking concepts like encapsulation, addressing, and data exchange.
- **Security Monitoring:** Recognizing unusual traffic patterns that could indicate potential security threats or unauthorized access attempts.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

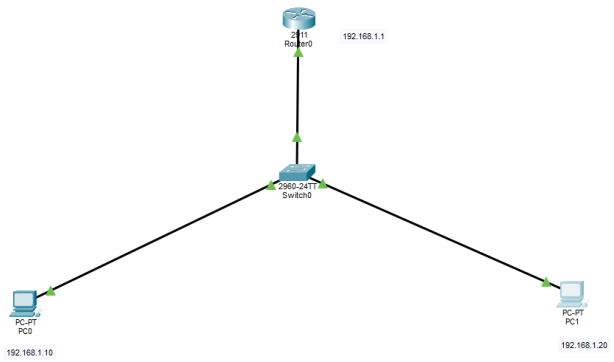


Fig 25.1 Typical network topology for capture, monitor, and analyze data

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 25.2

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all devices (Router, Switch, PCs) are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Configure correct IP addresses and subnet masks on all devices to avoid connectivity issues.

3. Verify basic network connectivity using PING between devices before configuring TELNET or ACLs.
4. Use correct usernames and passwords when configuring TELNET access on the router to prevent login failures.
5. Carefully apply and verify Access Control Lists (ACLs) to avoid unintentionally blocking legitimate traffic.
6. Use Packet Tracer's simulation mode to monitor and confirm the effects of ACLs on TELNET traffic.
7. Save the Packet Tracer project frequently to prevent loss of configuration and simulation data.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following:

- Cisco Packet Tracer (version 8.0 or later) is installed on computer.
- The basics of IPv4 addressing, subnetting, and router configuration.
- Fundamental of TELNET, Access Control Lists (ACLs), and Packet Sniffer tools in Packet Tracer.
- Verify Packet Tracer functionality by opening and running a sample topology.

2. Create Network Topology

- Open Cisco Packet Tracer and wait for the workspace to load completely.
- Drag and drop the following devices as shown in the provided topology diagram:
  - 1 Router (Router0 – Model 2911)
  - 1 Switch (2960-24TT)
  - 2 PCs (PC0, PC1)
- Connect the devices using Copper Straight-Through Cables:
  - PC0 → Switch0 (FastEthernet 0/1)
  - PC1 → Switch0 (FastEthernet 0/2)
  - Switch0 → Router0 (GigabitEthernet 0/0)
- Ensure all links show green lights (active connections).

3. Assign IP Addresses

Assign IP addresses to PCs and the router as shown below:

Table 25.3

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.20	255.255.255.0	192.168.1.1
Router0	GigabitEthernet0/0	192.168.1.1	255.255.255.0	—

a) Configure PC0

- Click PC0 → Desktop → IP Configuration
- Enter:
  - IP Address: 192.168.1.10
  - Subnet Mask: 255.255.255.0

- Default Gateway: 192.168.1.1

b) Configure PC1

- Click PC1 → Desktop → IP Configuration
- Enter:
  - IP Address: 192.168.1.20
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.1.1

c) Configure Router0

- Click Router0 → CLI and type:
  - enable
  - configure terminal
  - interface gigabitEthernet 0/0
  - ip address 192.168.1.1 255.255.255.0
  - no shutdown
  - exit
  - Verify the interface status:
  - show ip interface brief

It should show up/up for GigabitEthernet 0/0.

4. **Verify Basic Connectivity**
   - On PC0, open Command Prompt and type:
     - ping 192.168.1.1
     - ping 192.168.1.20
   - Successful replies confirm LAN connectivity between all devices.
5. **Enable TELNET Service on Router0**
   - Access Router0 CLI and configure TELNET login:
     - enable
     - configure terminal
     - line vty 0 4
     - password cisco
     - login
     - transport input telnet
     - exit
     - enable secret class
   - Test TELNET connectivity from PC0:
   - On PC0 → Desktop → Command Prompt as shown in Fig 25.2:
     - telnet 192.168.1.1
   - When prompted, enter:
     - Password: cisco
   - Successful login indicates TELNET is functioning.

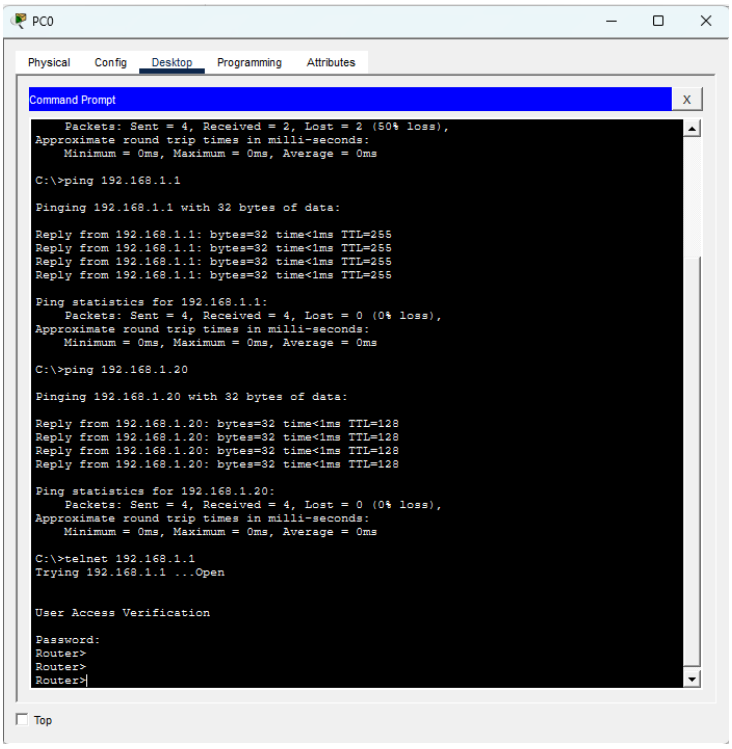


Fig 25.2 Telnet Login from PC0 to Router 0

6. **Configure Access Control List (ACL) to Block TELNET from PC1**

   We will create a Standard ACL on Router0 to block TELNET access for PC1 (192.168.1.20).

   - Go to Router0 CLI:
     - enable
     - configure terminal
     - access-list 10 deny host 192.168.1.20
     - access-list 10 permit any
     - interface gigabitEthernet 0/0
     - ip access-group 10 in
     - exit
     - exit
   - Save configuration:
     - write memory

7. **Test TELNET Access (Blocked and Unblocked)**

   a) From PC0 (Allowed Host)

   - Command Prompt → Type:
     - telnet 192.168.1.1
   - Log in will be successful.

   b) From PC1 (Blocked Host)

   - Command Prompt → Type:
     - telnet 192.168.1.1
   - TELNET connection should fail or show connection refused.

8. **Unblock TELNET Access for PC1**

   To allow TELNET from PC1 again, remove the ACL from the interface.

- On Router 0:
  - enable
  - configure terminal
  - interface gigabitEthernet 0/0
  - no ip access-group 10 in
  - exit
  - exit
- Save:
  - write memory

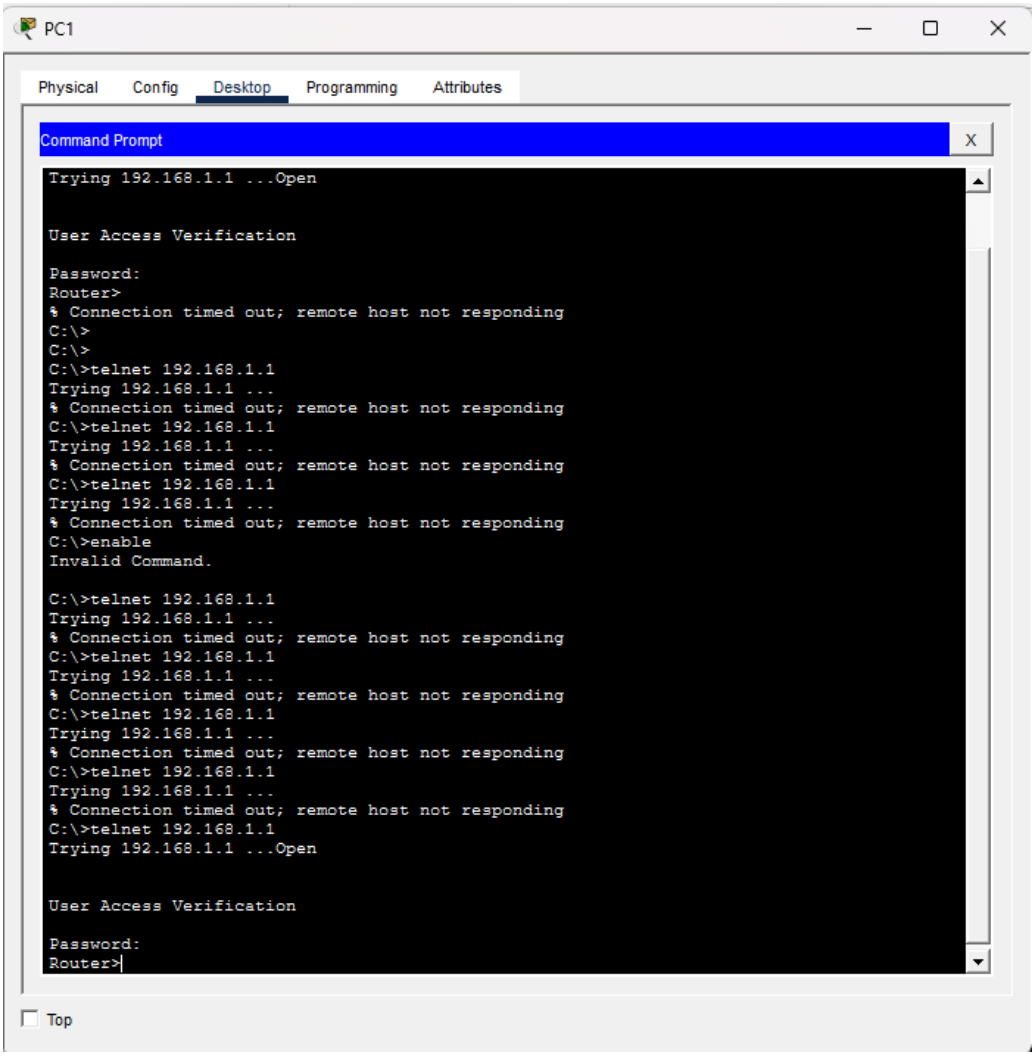


Fig 25.3 After Unblocking PC1 telnet, Successful Login

Now test TELNET again from PC1 — it should succeed as shown in Fig 25.3.

9. Use of Packet Sniffer (Simulation Mode)

a) Switch Packet Tracer to Simulation Mode (bottom right corner).

b) In the Event List Filters, enable as shown in Fig. 25.4:

- TCP
- TELNET

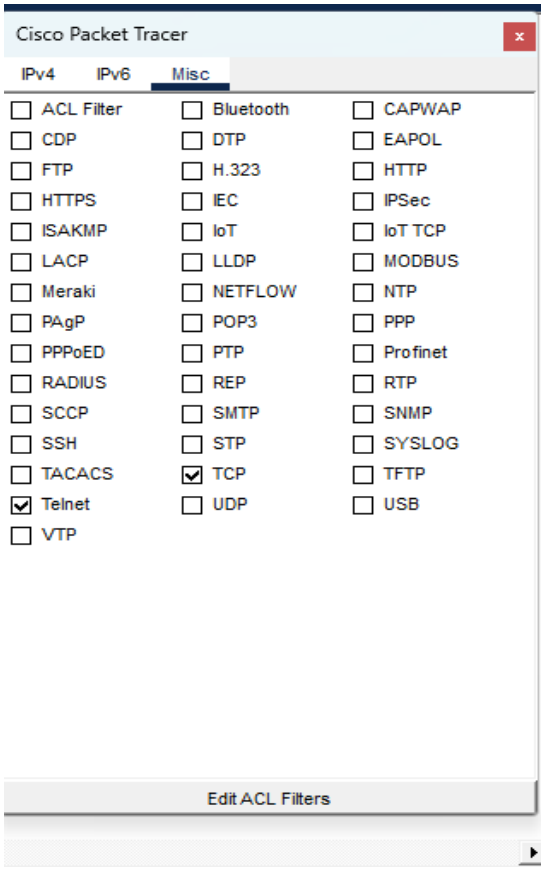


Fig 25.4 Event List Filters, enable Telnet, TCP

c) Start capturing packets:

- Send a TELNET request from PC0 or PC1.
- Observe the packets traveling from the PC to Router0 as shown in Fig 25.5

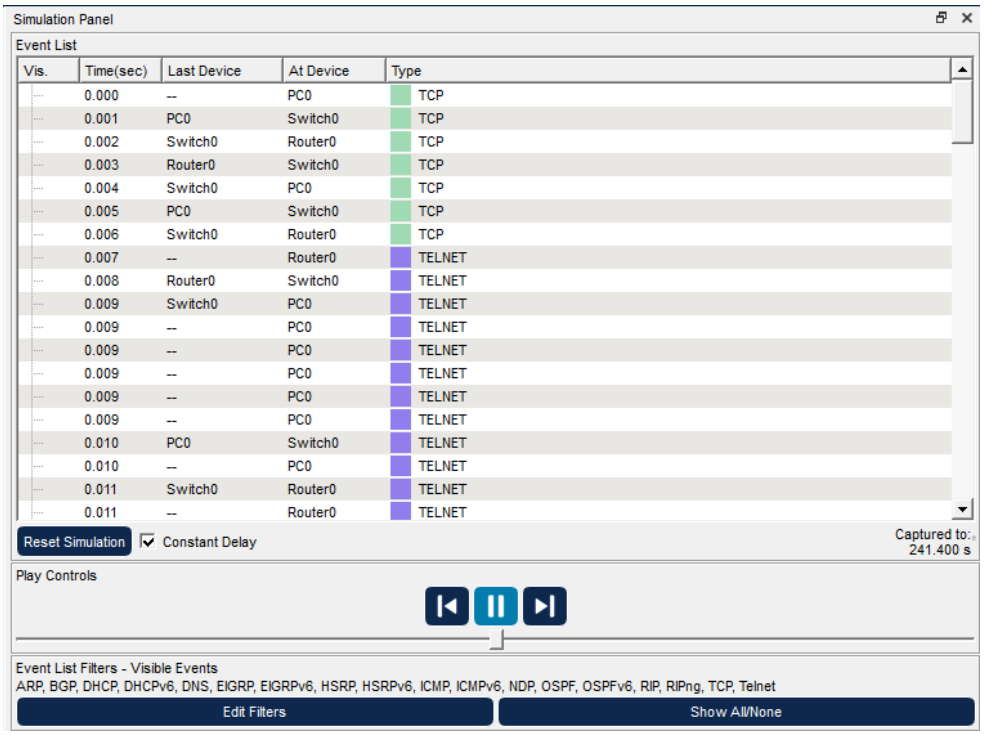


Fig 25.5 TCP and Telnet Packets after Filtering

d) Analyze the packet details:

- Check Source IP, Destination IP, Port numbers, and Protocol (TCP Port 23) as shown in Fig 25.6

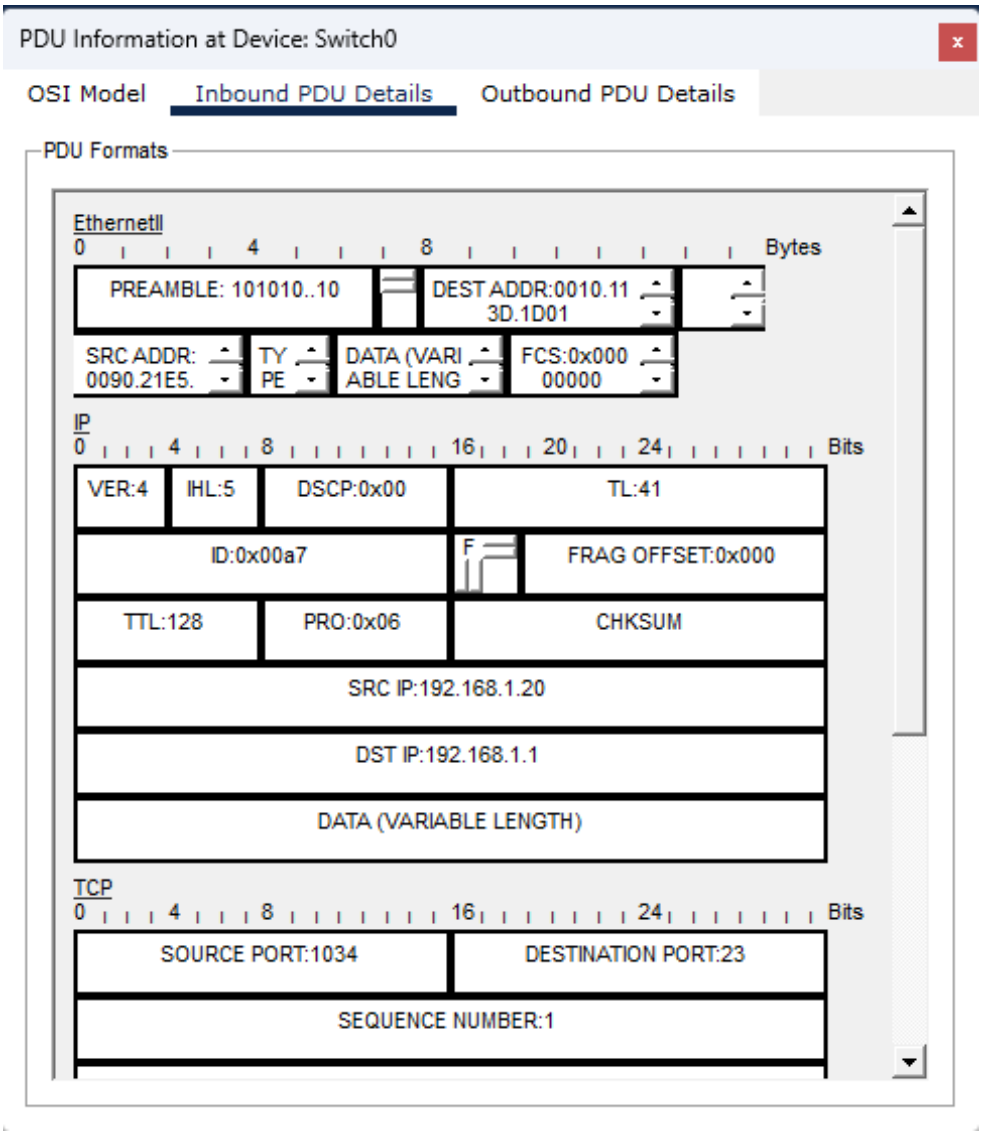


Fig 25.6 Showing Telnet Packet with Destination Port 23

- Note when TELNET is blocked — no successful handshake (SYN/ACK).

10. Record Observations

In lab record, include:

- IP configuration of each device.
- ACL configuration details.
- TELNET test results (before and after blocking).
- Packet Sniffer screenshots showing blocked/unblocked TELNET packets.
- Explanation of how ACLs control traffic based on IP and protocol.

11. Save and Exit

- Save Packet Tracer project using File → Save As → Practical_25_Block_TELNET.pkt
- Exit Packet Tracer after verifying all configurations and results.

XI. Resources used during performance

Table 25.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

Table 25.5

Step	Action Performed	Expected Output	Actual Output (Successful/As Expected/Blocked /Allowed)	Status (Pass/ Fail)
1	Ping between PC0 and Router0	Successful reply from 192.168.1.1		
2	Ping between PC1 and Router0	Successful reply from 192.168.1.1		
3	Establish TELNET connection from PC0 to Router0	TELNET session established successfully		
4	Establish TELNET connection from PC1 to Router0	TELNET session established successfully		
5	Apply ACL on Router0 to block	TELNET connection from PC1 blocked (connection fails)		

Step	Action Performed	Expected Output	Actual Output (Successful/As Expected/Blocked /Allowed)	Status (Pass/ Fail)
	TELNET (port 23) from PC1			
6	Test TELNET connection from PC0 after ACL applied	TELNET connection allowed (successful connection)		
7	Use Packet Sniffer to monitor TELNET packets from PC1	TELNET packets from PC1 dropped by ACL		
8	Use Packet Sniffer to monitor TELNET packets from PC0	TELNET packets from PC0 allowed and forwarded		
9	Remove/Unblock TELNET ACL on Router0	TELNET connection allowed from both PC0 and PC1		
10	Final TELNET connectivity test from both PCs	TELNET sessions successfully established from both PCs		

XIV. Result

……...……

……...…

XV. Interpretation of result

……...…

……...…

XVI. Conclusion and recommendation

……...……

……...…

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the primary purpose of a packet sniffer.
2. State the role of Access Control Lists (ACLs) in controlling network traffic.
3. Give a command used to block TELNET traffic on a Cisco router interface.
4. Describe the effect of blocking TELNET (port 23) on communication between PCs and routers.

[Space for Answers] (If required attached separate page)

……..…

……..……..…

……..…

……..……

……..……

……..……

……..……

……..……

……..……

……..……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/what-is-packet-sniffing/	Overview of packet sniffing techniques
2	Networking with Rich - Using a sniffer in Packet Tracer	https://www.youtube.com/watch?v=gsCSKQAVT2M

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct network setup in Packet Tracer	30%
2	Successful packet capture and analysis	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correct interpretation of packet details	10%
2	Understanding OSI layer operation	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.26: *Implementation of SMTP protocol using CISCO packet tracer

I. Practical Significance

The purpose of this practical is to develops skills for analyzing email communication within a Local Area Network (LAN) using **S**MTP protocol in Cisco Packet Tracer. This practical also develops skills in configuring an Email Server and end devices to facilitate the sending and receiving of emails, providing insights into application layer communication and protocol operations. Through this practical, student gain essential experience in observing, testing, and troubleshooting email transmission processes, reinforcing the importance of protocol understanding in effective network communication and management.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 26.1 Implement SMTP protocol using CISCO packet tracer.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing
- Maintain the simulation environment and associated tools in proper working condition to ensure accurate results.
- Demonstrate patience and accuracy while performing step-by-step configuration of email servers and client devices.
- Exhibit responsibility in maintaining network security and promoting the ethical use of email communication within the LAN.

VI. Relevant Theoretical Background

1. **SMTP (Simple Mail Transfer Protocol)**: SMTP is a standardized application layer protocol responsible for the transmission of outgoing emails across a network. It operates primarily over Port 25 and governs the process of transferring messages from a mail client (such as a PC) to an email server, as well as between different mail servers over the Internet or within a LAN. SMTP ensures that each message is correctly formatted, queued, and delivered to the appropriate recipient's mail server. It uses a store-and-forward mechanism to relay messages efficiently and supports commands such as HELO, DATA for structured communication between clients and servers.
2. **DNS (Domain Name System):** DNS serves as a critical network service that translates human-readable domain names (e.g., mail.example.com) into corresponding IP addresses (e.g., 192.168.10.10). This translation enables devices to locate and communicate with email servers efficiently. Within email communication, DNS plays a crucial role in identifying the Mail Exchange (MX) records that define

which mail server is responsible for receiving emails for a given domain, ensuring accurate and reliable message delivery.

3. **Email Server:** An email server is a dedicated device or software system responsible for managing email communication. It handles the storage of user mailboxes, user authentication, message queuing, and routing of incoming and outgoing emails. The email server integrates both SMTP (for sending) and POP3 (for receiving) functionalities, enabling complete two-way communication within a network. Proper configuration of the email server ensures secure, reliable, and efficient handling of messages within the LAN environment.
4. **Application Layer (OSI Model Layer 7):** The application layer is the topmost layer of the OSI reference model and provides end-user services for network communication. It enables users to interact with network applications such as email, file transfer, and web browsing. Protocols like SMTP and POP3 operate at this layer, allowing user-level communication through standardized message formats and control mechanisms. Understanding the application layer is fundamental to analyzing how user data (such as an email) is encapsulated, transmitted, and interpreted within a networked environment.

Key Concepts

Table 26.1

Sr. No.	Concept	Description
1	**SMTP**	Transfers outgoing emails from client to server and between mail servers using Port 25.
2	**DNS**	Resolves domain names into IP addresses and identifies mail exchange records for routing.
3	**Email Server**	Manages mailboxes, authenticates users, and handles sending and receiving of messages.
4	**Application Layer**	Provides user-level communication services such as email transmission and retrieval.

VII. Circuit diagram / block diagram / flowchart

A) Suggestive Block Diagram

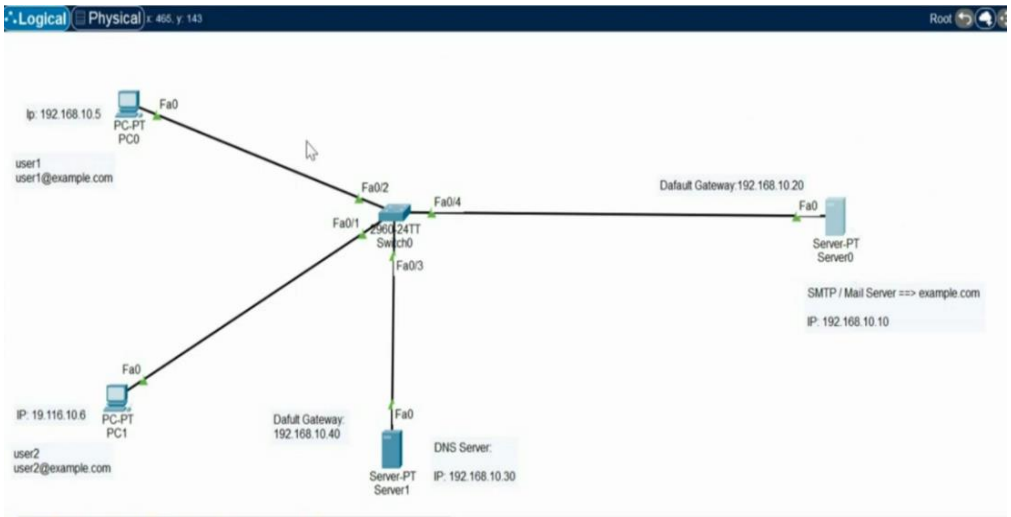


Fig 26.1 Typical network topology for Implementing SMTP Protocol with DNS Server

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 26.2

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all devices (Router, Switch, PCs) are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Configure correct IP addresses and subnet masks on all devices to avoid connectivity issues.
3. Verify basic network connectivity using PING between devices
4. Save the Packet Tracer project frequently to prevent loss of configuration and simulation data.
5. Enable SMTP services on Server.

6. Configure correct username and password for email clients.
7. Check DNS configuration before sending mail.
8. Save Packet Tracer file at every step.

X. Suggested Procedure

1. Prerequisites

   Before beginning the practical, ensure the following:

   - **Cisco Packet Tracer (version 8.0 or later)** is installed on computer.
   - Basic understanding of **IPv4 addressing and switch connectivity.**
   - The fundamental concepts of **DNS (Domain Name System)** and **Email (SMTP/POP3)** services.
   - Verify that Cisco Packet Tracer is working correctly by **opening and running a sample topology**.

2. Create Network Topology
   - Open Cisco Packet Tracer and wait until the workspace fully loads.
   - Place the following network devices in the workspace:
     - 2 PCs → PC0 and PC1
     - 2 Servers → Server0 (Mail Server) and Server1 (DNS Server)
     - 1 Switch → 2960-24TT Switch
3. Connect devices using Copper Straight-Through Cables **as follows**:
     - PC0 → Switch (FastEthernet 0/1)
     - PC1 → Switch (FastEthernet 0/2)
     - Server0 (Mail Server) → Switch (FastEthernet 0/3)
     - Server1 (DNS Server) → Switch (FastEthernet 0/4)
     - Ensure all link lights turn green, indicating active connections between all devices.
     - Assign IP Addresses

Assign IP addresses to all devices as per the following table.

Table 26.3

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	FastEthernet 0	192.168.10.5	255.255.255.0	192.168.10.40
PC1	FastEthernet 0	192.168.10.6	255.255.255.0	192.168.10.40
Server0 (Mail Server)	FastEthernet 0	192.168.10.10	255.255.255.0	192.168.10.40
Server1 (DNS Server)	FastEthernet 0	192.168.10.30	255.255.255.0	192.168.10.40

a) Configure IP on PC0

- Click PC0 → Desktop tab → IP Configuration.
- Enter the following details:
  - IP Address: 192.168.10.5
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.40
  - DNS Server: 192.168.10.30
- Close the window to save the configuration automatically.

b) Configure IP on PC1

- Click PC1 → Desktop tab → IP Configuration.
- Enter:
  - IP Address: 192.168.10.6
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.40
  - DNS Server: 192.168.10.30
- Close the window to save.

c) Configure IP on Mail Server (Server0)

- Click Server0 → Desktop → IP Configuration.
- Set:
  - IP Address: 192.168.10.10
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.40
  - DNS Server: 192.168.10.30

d) Configure IP on DNS Server (Server1)

- Click Server1 → Desktop → IP Configuration.
- Enter:
  - IP Address: 192.168.10.30
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.40
  - DNS Server: 192.168.10.30

4. Configure DNS Server (Server1) as shown in Fig 26.2

- Click Server1 in the workspace.
- Go to the Services tab.
- Select DNS from the left-side service menu.

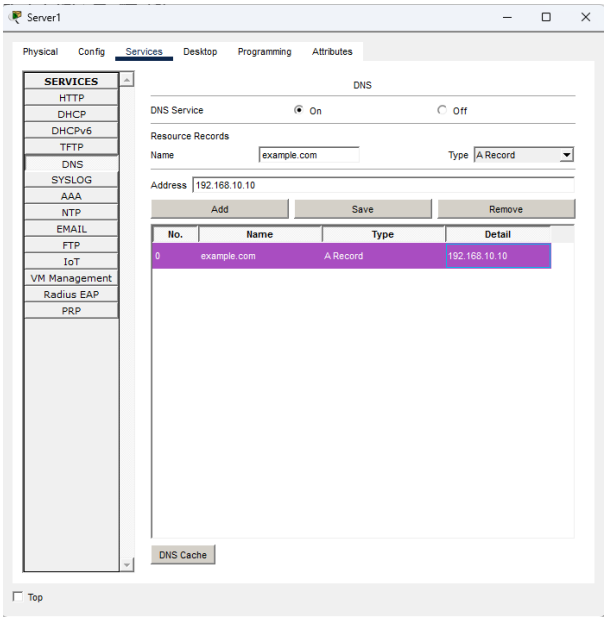


Fig 26.2 Configuring DNS Server

- Turn the DNS Service to ON.

- In the DNS configuration table:
  - Name: example.com
  - Type: A Record
  - Address: 192.168.10.10
- Click Add to save the DNS record.
- Confirm the entry is visible in the DNS table, then close the window.

5. Configure Mail Server (Server0) as shown in Fig 26.3

- Click Server0 → Services tab.
- From the left-side menu, select Email.
- Ensure both SMTP and POP3 services are turned ON.
- Under User Accounts, create the following users:
  - Click Add, then enter:
    1. Username: user1
    2. Password: user1
    3. Email: user1@example.com
  - Click Add again and enter:
    1. Username: user2
    2. Password: user2
    3. Email: user2@example.com
- Verify both user accounts appear in the list.

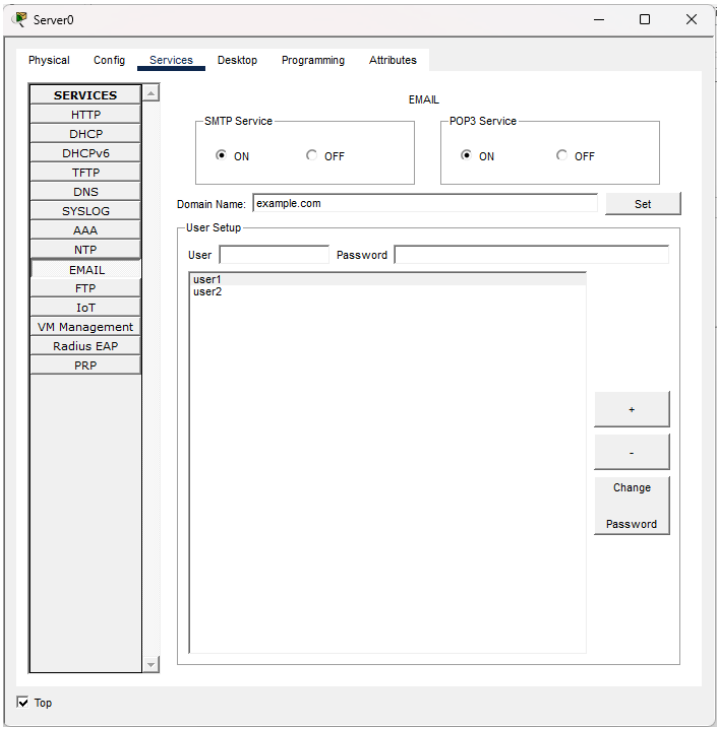


Fig 26.3 Configuring Mail Server

- Confirm default port settings:
  - SMTP Port → 25
  - POP3 Port → 110
- Close the window to save the configuration.

6. Configure Email Account on PC0 (user1) as shown in Fig 26.4

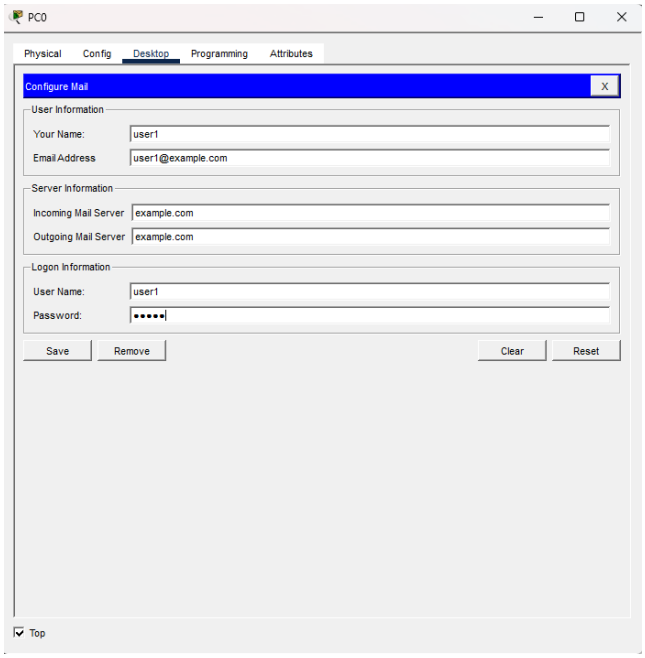


Fig 26.4 Configure Email Account on PC0

- Click PC0 → Desktop tab → Email.
- In the Configure Mail Option, enter:
  - User Name: user1
  - Email Address: user1@example.com
  - Incoming Mail Server: example.com
  - Outgoing Mail Server: example.com
  - Password: user1
- Click Save to apply the configuration.

7. Configure Email Account on PC1 (user2)

- Click PC1 → Desktop tab → Email application.
- In the Configure Mail Option, enter:
- Enter the following details:
  - User Name: user2
  - Email Address: user2@example.com
  - Incoming Mail Server: example.com
  - Outgoing Mail Server: example.com
  - Password: user2
- Click Save to store the configuration.

8. Send Email from PC0 to PC1 as shown in Fig 26.5

- On PC0, open the Email application.
- Click Compose or New Mail.
- Fill in the message details:
  - To: user2@example.com
  - Subject: SMTP Test
  - Message Body: Hello User2! SMTP test mail.

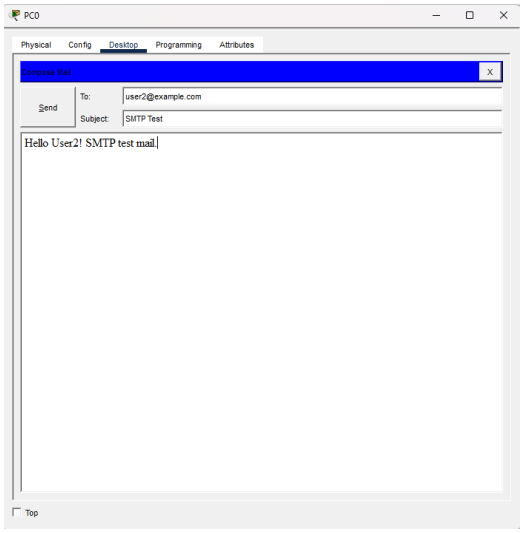


Fig 26.5 Sending Mail from PC0 to PC1

- Click Send.

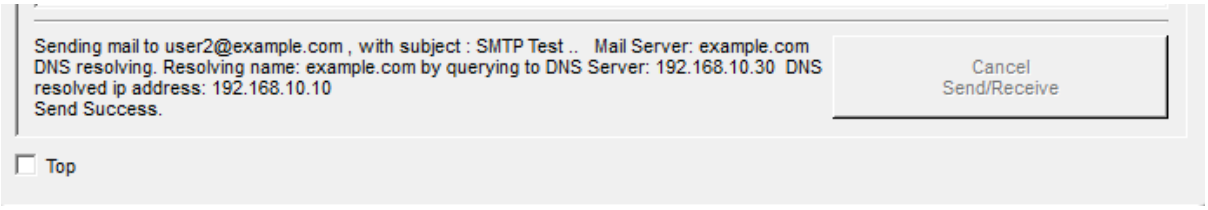


Fig 26.6 Status of Sending Message

- The message will be delivered to the Mail Server via the SMTP protocol & it will show Message as shown in Fig 26.6.

9. Receive Email on PC1

- On PC1, open the Email application.
- Click the Receive button.
- The message from user1@example.com should appear in the inbox, confirming successful delivery.

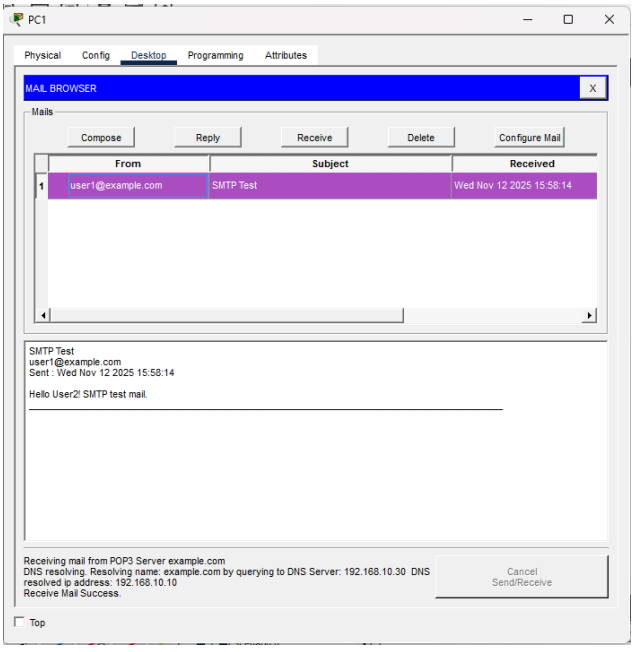


Fig 26.7 **Receive Email Successfully on PC1**

10. Validate Network Connectivity

a) Test Server Connectivity

- On PC0, open Command Prompt (Desktop → Command Prompt).
- Type:
  ping 192.168.10.10
- This checks connectivity to the Mail Server.
- Successful replies confirm the link is active.

b) Test DNS Resolution

- On PC0, type:
  - ping example.com
- If reply messages are received, both network and DNS configurations are correct.

11. Record Observations

In lab record, include the following:

- IP configuration of each device.
- DNS and Mail Server configuration details.
- Screenshots showing email exchange (send and receive).
- Ping test results for both IP and DNS name resolution.
- Short explanation of how DNS and SMTP/POP3 function within this LAN.

12. Save and Exit

- Save your project as:
  File → Save As → Practical_LAN_DNS_Mail_Config.pkt
- Verify all configurations.
- Close Packet Tracer safely.

XI. Resources used during performance

Table 26.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

7.

8.

9.

XIII. Observation Table

Table 26.5

Step	Action Performed	Expected Output	Actual Output (Mail sent/received/Resolved/Shown correctly)	Status (Pass/ Fail)
1	Assign IP addresses and configure DNS & Mail Server	All devices configured properly		
2	Test connectivity between PCs and Server	Successful ping replies		
3	Configure Email accounts on PCs	Email client setup should be successful		
4	Send Email from PC0 (user1) to PC1 (user2)	Email should be sent successfully		
5	Retrieve Email on PC1 (user2)	Email should be received in Inbox		
6	Verify DNS Resolution	Domain → IP resolution should work		
7	Analyze Simulation Mode (Optional)	SMTP/POP3 packets visible in Event List		

XIV. Result

……...……

……...…

XV. Interpretation of result

……...

……...

XVI. Conclusion and recommendation

……...

……...

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the role of SMTP in email communication.
2. State the port number used by SMTP.
3. Write Steps to Configure Mail Server in Cisco Packet Tracer.
4. Write Steps to Send Email from PC0 to PC1.

[Space for Answers] (If required attached separate page)

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/simple-mail-transfer-protocol-smtp/	Simple Mail Transfer Protocol (SMTP)
2	Rohit Kautkar YouTube Channel- How to Configure Email Server in Packet Tracer	https://www.youtube.com/watch?v=JhRTTqcvoCU

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct network setup in Packet Tracer	30%
2	SMTP Configuration	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Interpretation of Packet Flow	10%
2	Understanding App Layer Operations	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.27: Filter ARP and ICMP packets Traffic using network simulation software

I. Practical Significance

The purpose of this practical is to develop skills for analyzing and controlling network traffic within a Local Area Network (LAN) by filtering ARP and ICMP packets using network simulation software. Through this practical, students gain essential experience in configuring filters, observing packet behaviour, and troubleshooting network performance issues, reinforcing the importance of traffic control and protocol analysis in maintaining secure and efficient network operations.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 27.1 Capture ARP and ICMP packet Traffic using packet tracer or any similar network simulation software.

V. Relevant Affective Domain related outcomes

- Display professionalism, teamwork, and clear documentation while performing network simulation and traffic filtering tasks.
- Maintain the simulation environment and filtering tools in proper working condition to ensure accurate monitoring and analysis of network traffic.
- Demonstrate patience, precision, and attention to detail while configuring and testing packet filters.
- Exhibit responsibility in maintaining network integrity and promoting the ethical use of filtering techniques to ensure secure and efficient LAN communication.

VI. Relevant Theoretical Background

In computer networks, efficient communication and data transmission rely on the exchange of packets governed by various network protocols. Two fundamental protocols operating at the Network and Data Link layers are the **Address Resolution Protocol (ARP)** and the **Internet Control Message Protocol (ICMP).** Understanding and managing the behaviour of these protocols is essential for maintaining network performance, security, and stability.

1. **ARP (Address Resolution Protocol):**
    - ARP is a network protocol used to map a device's IP address to its physical MAC address in a local area network (LAN).

- When a host wants to communicate with another host in the same subnet, it broadcasts an ARP request asking "Who has IP X.X.X.X?" and the device with that IP responds with its MAC address.
- Understanding ARP traffic helps in troubleshooting connectivity issues within LANs, detecting IP conflicts, and monitoring network behavior.
- ARP Packet Structure: Includes hardware type, protocol type, sender MAC/IP, and target MAC/IP.

2. ICMP (Internet Control Message Protocol):

- ICMP is primarily used for diagnostic and control purposes in IP networks, such as reporting errors or testing connectivity.
- Common ICMP messages include Echo Request and Echo Reply, which are used by the ping command to check network connectivity.
- Filtering ICMP packets allows network administrators to manage network troubleshooting, control ping floods, and secure the network from certain attacks.
- ICMP Packet Structure: Includes Type, Code, Checksum, and optionally data like timestamp or payload. Various Types of ICMP Messages are shown in Table 27.1

Table 27.1

Type	Message	Code	Meaning
0	Echo Reply	0	No further specification
3	Destination Unreachable	0	Network Unreachable
		1	Host Unreachable
		2	Protocol Unreachable
		3	Port Unreachable
		5	Source Route Failed
		6	Destination Network Unknown
		7	Destination Host Unknown
		8	Source Host Isolated
5	Redirect	0	Redirect Datagram for the Network
		1	Redirect Datagram for the Host
8	Echo Request	0	No further specification
9	Router Advertisement	varies	Information about routers on the network
10	Router Solicitation	0	Request router advertisement
11	Time Exceeded	0	TTL exceeded in transit
		1	Fragment reassembly time exceeded
12	Parameter Problem	0	Pointer indicates error
		1	Missing a required option
		2	Bad length
13	Timestamp Request	0	Request timestamp
14	Timestamp Reply	0	Reply with timestamp

17	Address Mask Request	0	Request subnet mask
18	Address Mask Reply	0	Reply with subnet mask

3. **Packet Filtering and Monitoring in LANs:**
   - Packet filtering is a network security practice used to allow or block specific types of packets based on protocol, source/destination address, or port number.
   - In simulation software like Cisco Packet Tracer, filtering can be observed by using Simulation Mode, which visually displays the path of packets, their types, and the devices they traverse.
   - Monitoring ARP and ICMP traffic helps students understand network device interactions, packet encapsulation, and the role of different protocol layers.
4. **Simulation Mode in Cisco Packet Tracer:**
   - Packet Tracer provides Simulation Mode to examine packet flow in detail as shown in Fig. 27.1. Users can select the packet type to monitor (ARP, ICMP, TCP, UDP) and observe how packets are created, transmitted, and received.

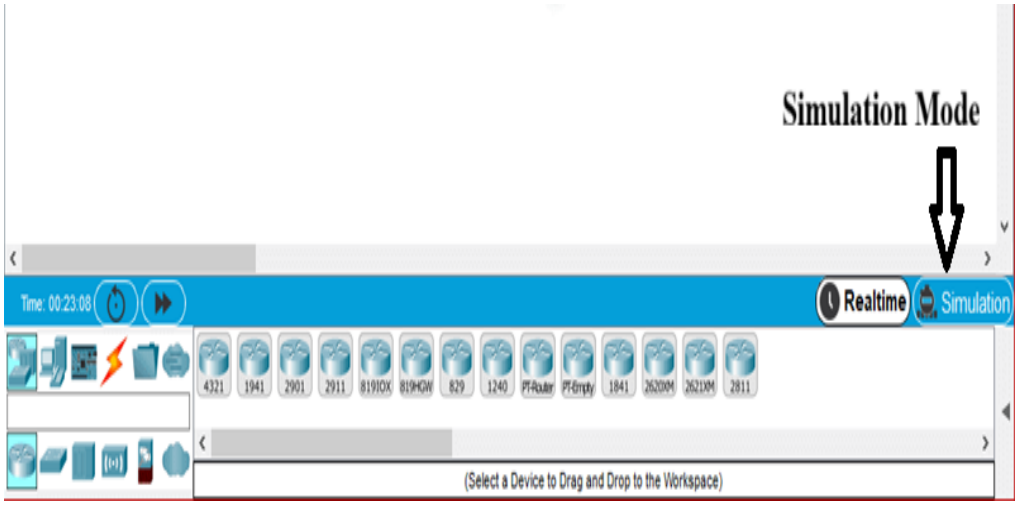


Fig 27.1 Simulation Mode in Cisco Packet Tracer

   - This hands-on approach allows learners to see the practical impact of network commands and configurations, such as using the ping command to generate ICMP traffic or observing ARP broadcasts when a new host joins the network.
5. **Network Troubleshooting Relevance:**
   - Capturing ARP and ICMP traffic allows network administrators to detect problems like:
     - IP conflicts or incorrect subnetting.
     - Host unreachability or high latency visible via ICMP Echo Request/Reply delays.

VII. Circuit diagram / block diagram

A) Suggestive Block Diagram

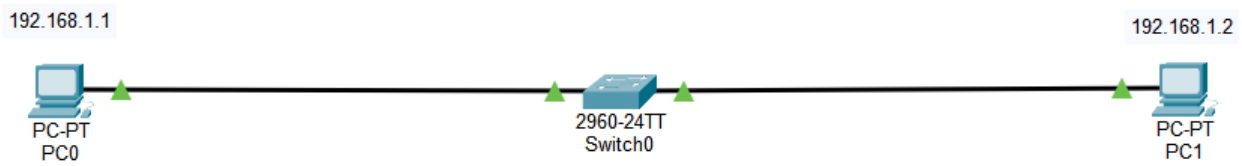


Fig 27.2 Basic Network Topology to Filter ARP and ICMP packets Traffic

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 27.2

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all network devices (Router, Switch, and PCs) are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Assign correct IP addresses and subnet masks to all devices to establish proper network connectivity.
3. Verify network communication between devices using the **ping** command before applying any packet filters.
4. Use proper naming conventions for devices and interfaces to avoid confusion during configuration and analysis.
5. Apply ARP and ICMP filters carefully to avoid blocking essential communication required for network operation.
6. Save the Packet Tracer project file frequently to prevent loss of configuration or simulation progress.
7. After completing the practical, restore normal network settings to ensure that all devices can communicate without restrictions.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following conditions are met:

- Cisco Packet Tracer (version 8.0 or later) is installed and functioning correctly on the laboratory computer system.
- A basic understanding of IPv4 addressing, LAN topology creation, and switch connectivity is developed.
- Familiarity with the basic operation of network protocols such as ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol) is established.
- The Cisco Packet Tracer environment is verified by opening and successfully running a sample network topology.
- All network devices, including PCs and switches, are available in the device list within Cisco Packet Tracer.

2. Create Network Topology

- Open Cisco Packet Tracer and wait until the workspace is completely loaded.
- Place the following network devices in the workspace:
  - 2 PCs → PC0 and PC1
  - 1 Switch → 2960-24TT Switch
- Connect the devices using **Copper Straight-Through Cables** as follows:
  - PC0 → Switch (FastEthernet 0/1)
  - PC1 → Switch (FastEthernet 0/2)
- Ensure that the link lights on all connections turn green, confirming active connectivity between devices.
- Save the initial topology using File → Save As → Practical27_Filter_ARP_ICMP_Topology.pkt to avoid data loss during configuration.

3. Assign IP Addresses

Assign IP addresses to all end devices according to the following Table 27.3:

Table 27.3

Device	IP Address	Subnet Mask
PC0	192.168.1.1	255.255.255.0
PC1	192.168.1.2	255.255.255.0

4. Configure IP Addresses in Cisco Packet Tracer

a) Configure IP Address on PC0

- Select PC0 from the workspace.
- Open the configuration window and choose the Desktop tab.
- Click on IP Configuration from the list of available tools.
- Enter the following details:
  - IP Address: 192.168.1.1
  - Subnet Mask: 255.255.255.0
- Close the window. The configuration will be saved automatically.

b) Configure IP Address on PC1

- Select PC1 from the workspace.
- Open the Desktop tab and click IP Configuration.
- Enter the following details:
  - IP Address: 192.168.1.2
  - Subnet Mask: 255.255.255.0
- Close the window to save the configuration automatically.

5. Switch to Simulation Mode

- Locate the mode selector panel at the bottom-right corner of the Cisco Packet Tracer interface as shown in Fig 27.1.
- Click Simulation to switch from Real-Time Mode to Simulation Mode.
- Ensure that the Simulation Control Panel appears at the bottom of the screen.
- The Simulation panel contains options such as Auto Capture/Play, Capture/Forward, and an Event List displaying captured packets.

6. Generate ICMP Traffic Using Ping

- Select PC0 and open the Desktop tab.
- Click Command Prompt to access the terminal interface.
- Type the following command and press Enter:

  ping 192.168.1.2
- This command initiates ICMP Echo Request and Echo Reply packets between PC0 and PC1.
- Observe that new entries appear in the Event List, representing the generated ICMP traffic.

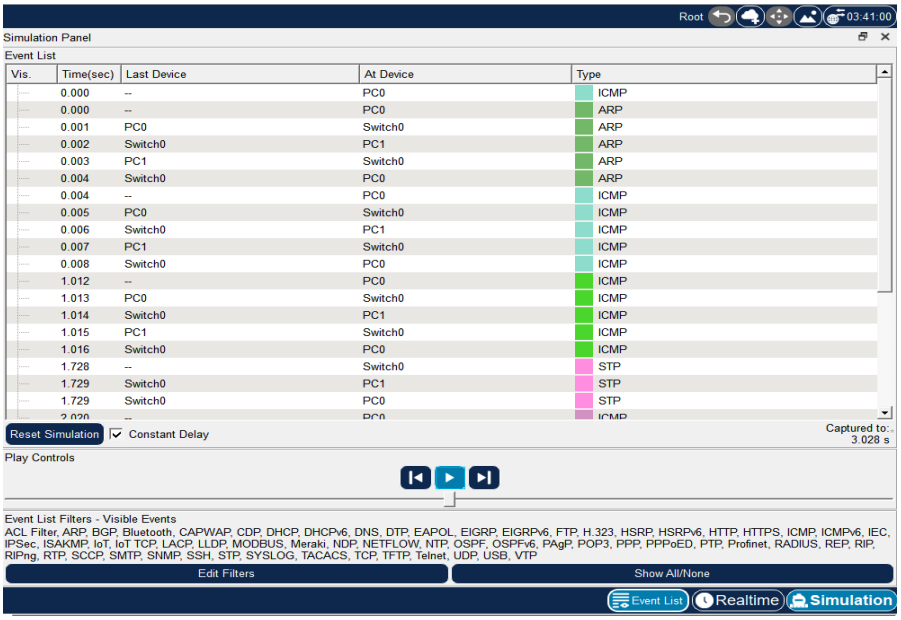


Fig 27.3 Entries of ICMP/ARP Packets in the Event List

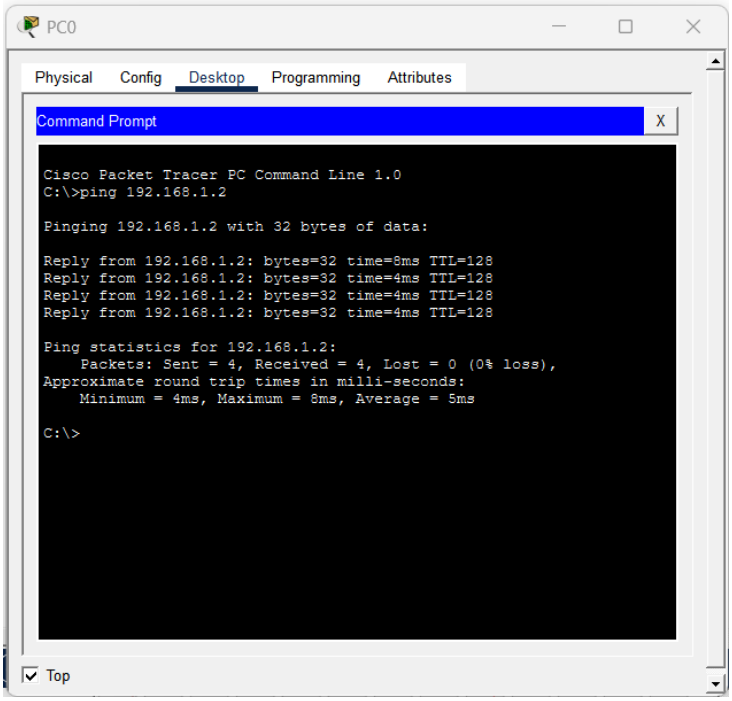


Fig 27.4 Entries of ICMP/ARP Packets in the Event List

7. Apply Protocol Filters for ARP and ICMP

- In the Simulation Panel, click the Event List Filters button (represented by a funnel icon).
- A filter configuration window will open, displaying multiple protocol categories as shown in Fig 27.5.
- Deselect all protocols initially, then enable only the following checkboxes:
  - ARP
  - ICMP
- Click OK to apply the filters.

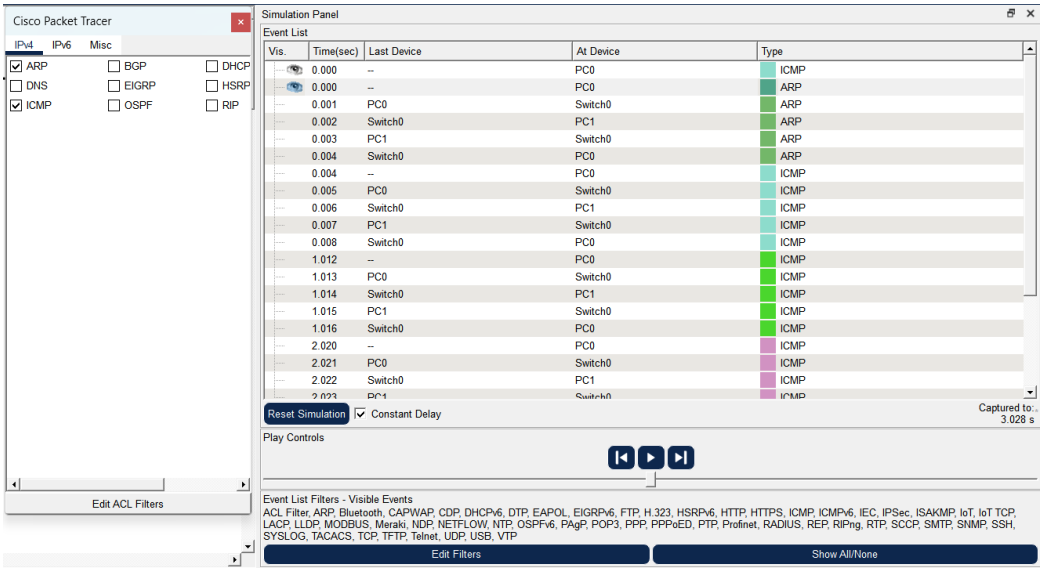


Fig 27.5 Apply Protocol Filters for ARP and ICMP

- Observe that only ARP and ICMP packets are now visible in the Event List, making it easier to study relevant traffic types.

8. Analyze Captured Packets

- Examine the Event List in the Simulation Panel as ARP and ICMP packets are generated.
- Click on individual packets to highlight them.
- Select PDU Details to open a detailed view of the selected packet.
- Analyze the ARP Request packet to understand how a device broadcasts a request to identify the MAC address of another device.
- Observe the ARP Reply packet, which contains the destination device's MAC address in response to the request.

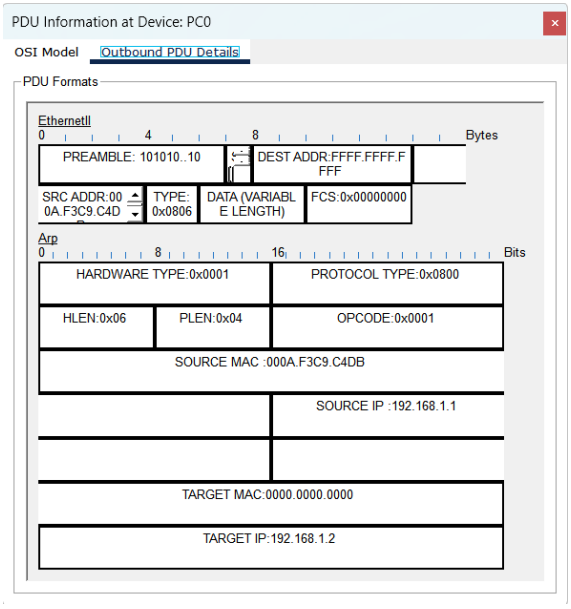


Fig 27.6 PDU details of ARP Packet

- After ARP resolution, review the ICMP Echo Request and Echo Reply packets exchanged between PC0 and PC1.

- Confirm that both protocols function correctly by studying packet fields such as Source IP, Destination IP, MAC addresses, and Frame Information.

10. Record Observations

The following details should be documented in the laboratory record:

- Labeled network topology diagram showing device interconnections.
- IP addressing details of all configured devices.
- Screenshots of the Event List displaying ARP and ICMP packets.
- PDU detail views of ARP Request, ARP Reply, ICMP Echo Request, and ICMP Echo Reply packets.

11. Save and Exit

- Save the final project file as Practical27_ARP_ICMP_Filter.pkt using the File → Save As option.
- Ensure that all configurations and filters have been applied correctly.
- Exit Cisco Packet Tracer safely after verifying that all packet exchanges have been observed and recorded.

XI. Resources used during performance

Table 27.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

7.

XIII. Observation Table

Table 27.5

Step	Action Performed	Expected Output	Actual Output (Packets/Traffic Observed/Displayed Correctly)	Status (Pass/ Fail)
1	Create network topology and connect PC0, PC1, and Switch using Copper Straight-Through cables	All devices connected properly with green link lights indicating active connections	Devices connected successfully; link lights turned green	
2	Assign and configure IP addresses on PC0 and PC1	Correct IP and subnet mask assigned; both devices ready for communication	IP configuration completed successfully on both PCs	
3	Switch from Real-Time Mode to Simulation Mode	Simulation Control Panel displayed with Capture/Forward and Event List options	Simulation panel displayed successfully with all controls active	
4	Generate ICMP traffic using ping command from PC0 to PC1	ICMP Echo Request and Echo Reply packets generated and visible in Event List	ICMP packets successfully generated and displayed in Event List	
5	Apply protocol filters for ARP and ICMP in Event List Filters	Only ARP and ICMP packets visible in Event List for analysis	Event List filtered successfully; only ARP and ICMP packets shown	
6	Analyze captured packets using PDU Details	Detailed ARP and ICMP packet information displayed (Source/Destination IP, MAC, Frame Info)	ARP and ICMP packet details analyzed successfully in PDU window	
7	Visualize communication using Capture/Forward	ARP packets exchanged first, followed by ICMP packets; successful ping replies observed	Sequential ARP and ICMP packet flow visualized correctly; ping successful	
8	Record observations and save Packet Tracer file	Network analysis completed; configuration saved successfully	All observations recorded; project saved without errors	

XIV. Result

……..……

……...……

XV. Interpretation of result

……...……

……...……

XVI. Conclusion and recommendation

……...……

……...…

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of filtering ARP packets.
2. Explain the role of ARP in LAN communication.
3. State the packet type generated during a ping request.
4. Describe what would happen if ARP fails in a network.

[Space for Answers] (If required attached separate page)

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/arp-protocol/	Address Resolution Protocol - ARP
2	https://www.geeksforgeeks.org/computer-networks/internet-control-message-protocol-icmp/	Internet Control Message Protocol (ICMP)

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Proper handling of Cisco Packet Tracer software and devices	30%
2	Correct identification of network devices (PCs, switches, routers) and protocols (ARP, ICMP)	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Correctly captured ARP/ICMP packets	10%
2	Filtering ICMP and ARP Packets	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.28: Configuration of POP3 protocol using CISCO Packet Tracer

I. Practical Significance

The purpose of this practical is to develop skills for configuring and analyzing email communication within a Local Area Network (LAN) using the POP3 protocol in Cisco Packet Tracer. Through this practical, student will gain essential experience in setting up and managing mail servers and client devices, observing the process of retrieving emails from the server, and troubleshooting common email communication issues.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 28.1 Configure a POP3 protocol in Packet Tracer and Test domain.

V. Relevant Affective Domain related outcomes

- Display professionalism, teamwork, and clear documentation while performing configuration and testing in the simulated network environment.
- Maintain the simulation environment, mail servers, and client devices in proper working condition to ensure accurate email retrieval and testing.
- Demonstrate patience, precision, and attention to detail while configuring settings, domain records, and email accounts.
- Exhibit responsibility in maintaining network integrity.

VI. Relevant Theoretical Background

The Post Office Protocol version 3 (POP3) is an application layer protocol used to retrieve emails from a remote mail server to a local client device. It is one of the most widely implemented email retrieval protocols and is particularly useful in scenarios where users require offline access to their messages. POP3 allows clients to download emails from the server to the local machine, enabling them to read messages without a continuous internet connection.

History and Evolution

The POP protocol was first introduced in 1984 as a simple mechanism to access email from a server. It evolved through two major versions, POP2 and POP3. POP3, formalized in 1988 under RFC 1081, was designed to simplify email retrieval while ensuring efficiency and reliability. The protocol has been widely adopted due to its straightforward design, low resource requirements, and compatibility with most email applications, including Microsoft Outlook, Apple Mail, and Gmail.

Working Mechanism

The operation of POP3 follows a client-server model over TCP/IP. Communication typically occurs over port 110, while secure communication using SSL/TLS occurs over port 995. The process of email retrieval via POP3 involves several stages:

1. **Connection Establishment**: The POP3 client establishes a TCP connection with the mail server.
2. **Authentication**: The client provides login credentials, typically a username and password, which the server verifies.
3. **Message Retrieval**: The client requests a list of available emails. The server responds with message identifiers and sizes. The client then requests specific messages for download.
4. **Message Management**: Depending on configuration, the client may leave copies of emails on the server or delete them after download.
5. **Connection Termination**: Once all operations are complete, the client closes the connection, and the server acknowledges before terminating the session.

This sequence allows users to access emails offline while maintaining minimal server storage requirements.

Advantages of POP3

- Emails can be accessed offline after download.
- Reduces server storage usage since emails can be stored locally.
- Simple configuration and compatibility with most email clients.
- Fast local access to messages due to local storage.

Limitations of POP3

- Does not support real-time synchronization between multiple devices.
- Access is typically restricted to a single device per email account.
- Deleting or managing emails on the server is limited compared to IMAP.
- Local storage of emails may expose data to unauthorized access if the system is not secure.

Comparison with IMAP

Unlike POP3, which downloads emails to a single device, IMAP (Internet Message Access Protocol) allows users to manage their email directly on the server, providing access across multiple devices and maintaining folder structures. IMAP supports partial downloads, message synchronization, and server-side operations such as creating, deleting, or renaming emails, which POP3 does not.

Relevance in Cisco Packet Tracer

In Cisco Packet Tracer, POP3 configuration allows student to simulate email retrieval in a controlled LAN environment. Student can configure mail servers, set up user accounts, define domains, and connect client devices to retrieve messages using the POP3 protocol. This simulation enables observation of TCP sessions, authentication exchanges, and message transfers. Additionally, it provides practical insight into troubleshooting common issues, such as incorrect IP addressing, DNS misconfigurations, or authentication failures. Understanding POP3 through simulation reinforces the principles of client-server communication, email protocol operations, and network troubleshooting. It equips students

with essential skills for managing email services within LANs and analyzing application-layer protocol behaviour effectively.

VII. Circuit diagram / block diagram

A) Suggestive Block Diagram

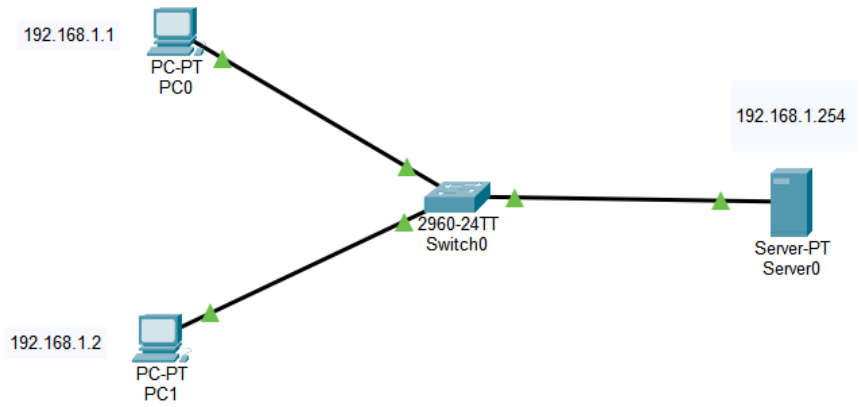


Fig 28.1 Basic Network Topology to Implement POP3 in Cisco Packet Tracer

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 28.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01

Sr. No.	Name of Resource	Specification	Quantity
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all network devices, including the Mail Server, Router, Switch, and PCs, are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Assign accurate IP addresses, subnet masks, and default gateways to all devices to guarantee proper network connectivity.
3. Verify network communication between client PCs and the Mail Server using the ping command.
4. Configure correct DNS settings and domain names to facilitate proper email delivery and retrieval.
5. Use standardized naming conventions for devices, interfaces, and email accounts to maintain clarity during configuration and troubleshooting.
6. Save the Packet Tracer project frequently to avoid loss of configuration or simulation progress.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following conditions are met:

- Cisco Packet Tracer (version 8.0 or later) is installed and functioning correctly on the laboratory computer system.
- A basic understanding of IPv4 addressing, LAN topology creation, and switch connectivity is developed.
- Familiarity with network protocols such as POP3, SMTP, and DNS is established.
- The Cisco Packet Tracer environment is verified by opening and successfully running a sample network topology.
- All network devices, including PCs, Switches, and a Mail Server, are available in the device list within Cisco Packet Tracer.
- Knowledge of configuring email clients and server settings in Cisco Packet Tracer is developed.

2. Create Network Topology

- Open Cisco Packet Tracer and wait until the workspace is fully loaded.
- Place the following devices in the workspace:
  - 2 PCs → PC0 and PC1
  - 1 Switch → 2960-24TT Switch

- 1 Server → Generic Server
- Connect devices using Copper Straight-Through Cables as follows:
  - PC0 → Switch (FastEthernet 0/1)
  - PC1 → Switch (FastEthernet 0/2)
  - Server → Switch (FastEthernet 0/3)
- Verify that the link lights on all connections turn green, confirming active connectivity between devices.
- Save the initial topology using File → Save As → Practical28_POP3_Topology.pkt to avoid data loss during configuration.

3. Assign IP Addresses

Assign IP addresses to all end devices according to the following table 28.2:

Table 28.2

Device	**IP Address**	**Subnet Mask**	**Default Gateway**
PC0	192.168.1.1	255.255.255.0	192.168.1.254
PC1	192.168.1.2	255.255.255.0	192.168.1.254
Server	192.168.1.254	255.255.255.0	192.168.1.254

4. Configure IP Addresses in Cisco Packet Tracer

a) Configure IP Address on PC0:
- Select PC0 from the workspace.
- Open the Desktop tab → IP Configuration.
- Enter IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.254.
- Close the window to save configuration.

b) Configure IP Address on PC1:
- Select PC1 from the workspace.
- Open Desktop tab → IP Configuration.
- Enter IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.254.
- Close the window.

c) Configure IP Address on Server:
- Select the Server → Desktop tab → IP Configuration.
- Enter IP Address: 192.168.1.254, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.254.
- Close the window.

5. Configure DNS and Domain Name on Server as shown in Fig 28.2
- Select the Server → Services → DNS.
- Enter the domain name (e.g., example.com) and associate it with the server's IP address.
- Save the DNS configuration.

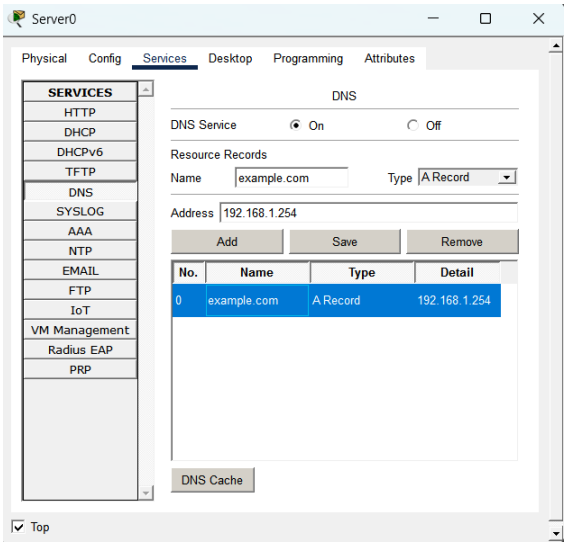


Fig 28.2 Configure DNS Server

6. Configure Email Services on Server as shown in Fig 28.3

- On the Server → Services tab → Email.

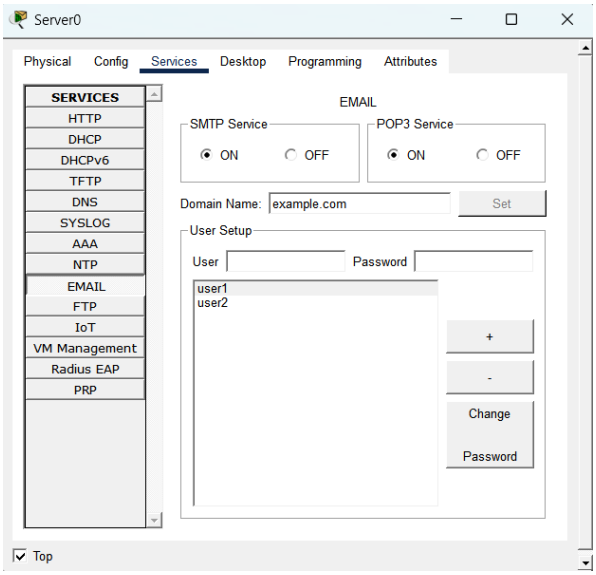


Fig 28.3 Configuring Email server with POP3 Service

- Enable the Email service and select POP3 as the incoming mail protocol.
- Configure user accounts for email clients:
  - User1: user1@example.com, Password: user1
  - User2: user2@example.com, Password: user2
- Verify SMTP is enabled for outgoing mail.

7. Configure Email Clients on PCs

a) PC0 (User1):

- Desktop → Email → Add Account.
- Enter the following:

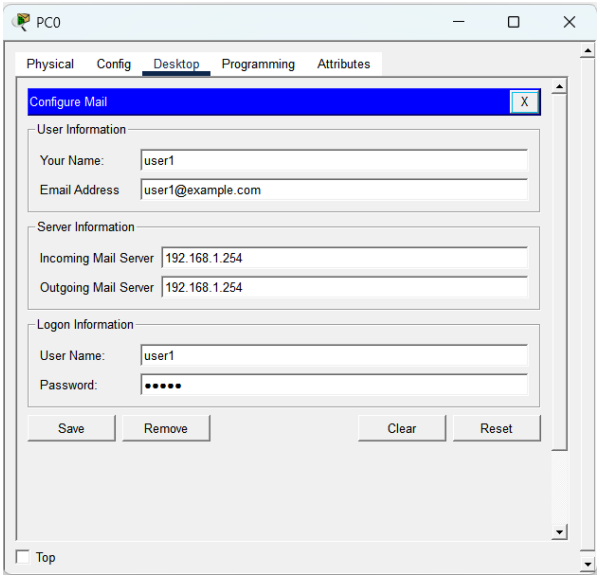


Fig 28.4 Configure Email Clients on PCs

- Incoming Server: 192.168.1.254
- Username: user1
- Password: user1
- Outgoing Server: 192.168.1.254

- Save settings and test configuration.

b) PC1 (User2):

- Desktop → Email → Add Account.
- Enter the following:
  - Incoming Server: 192.168.1.254
  - Username: user2
  - Password: user2
  - Outgoing Server: 192.168.1.254
- Save settings and test configuration.

8. Test POP3 Email Functionality as shown in Fig 28.5

- From PC0, compose and send an email to user2@example.com.

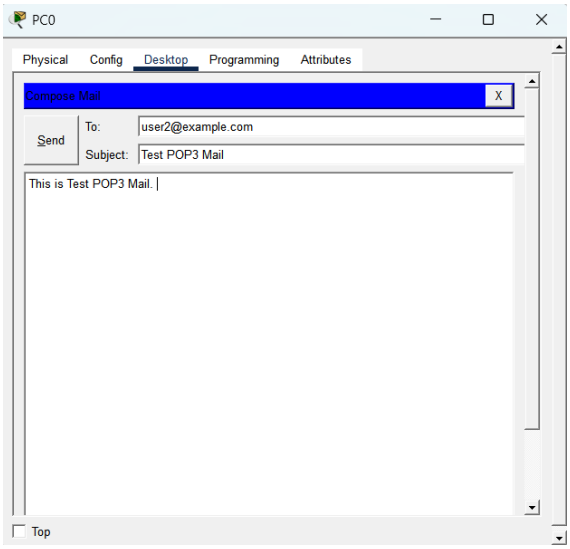


Fig 28.5 Compose Mail from PC0 to PC1 for user2

- Switch to PC1, open the email client, and click Check Mail to receive the message.

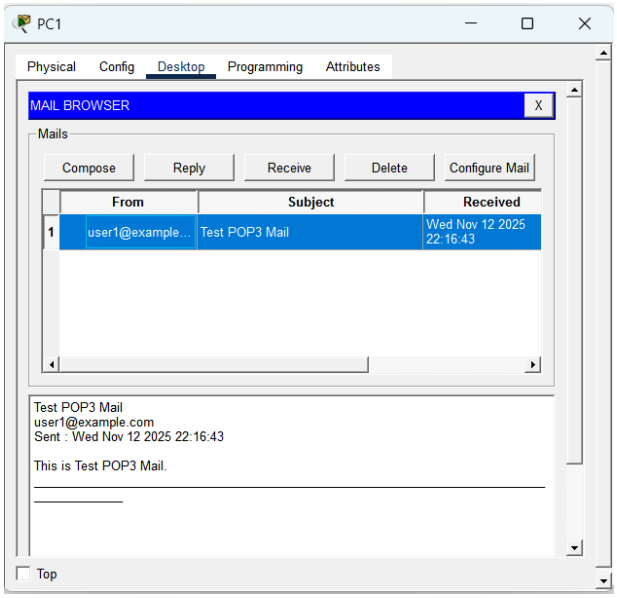


Fig 28.6 Received Mail from User1

- Verify that the email appears in the Inbox as shown in Fig 28.6

9. Switch to Simulation Mode (Optional)

- Use Simulation Mode to observe packet flow between clients and server.
- Monitor SMTP and POP3 packets in the Event List.
- Analyze the PDU details of POP3 commands such as USER, PASS, RETR, and QUIT to understand message retrieval process.

10. Record Observations

Document the following:

- Network topology diagram with device connections.
- IP addresses and domain name details.
- Screenshots of successful email sending and retrieval.
- Simulation capture showing POP3 packet exchange (USER, PASS, RETR).

11. Save and Exit

- Save the final project file as Practical28_POP3.pkt.
- Verify that all configurations are functioning and emails can be sent/received successfully.
- Exit Cisco Packet Tracer safely.

XI. Resources used during performance

Table 28.3

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.
2.
3.
4.
5.
6.
7.
8.
9.

XIII. Observation Table

Table 28.4

Step	Action Performed	Expected Output	Actual Output (Email sent/received/POP3 packets captured)	Status (Pass/ Fail)
1	Assign IP addresses to PCs and Server	All devices configured with correct IP addresses		
2	Configure DNS and domain on Server	Domain resolves correctly to server IP		
3	Configure POP3 service on Server and create user accounts	POP3 service enabled, users added		
4	Configure email accounts on PCs	Email client setup successful		
5	Send email from PC0 (user1) to PC1 (user2)	Email sent successfully via SMTP		
6	Retrieve email on PC1	Email received in Inbox via POP3		
7	Test email sending from PC1 to PC0	Email sent successfully		
8	Retrieve email on PC0	Email received in Inbox via POP3		
9	Verify POP3 packet exchange in Simulation Mode	POP3 commands (USER, PASS, RETR, QUIT) visible		
10	Verify SMTP packet exchange	SMTP packets visible for sent emails		

XIV. Result

……..……

……..……

XV. Interpretation of result

……..……

……..……

XVI. Conclusion and recommendation

……..……

……..……

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the purpose of the POP3 protocol in email communication.
2. Identify the network ports used by the POP3 protocol.
3. Discuss the advantages and limitations of using POP3 for email retrieval in a LAN environment.
4. Describe the process of email retrieval via POP3.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://www.geeksforgeeks.org/computer-networks/what-is-pop3-post-office-protocol-version-3/	What is POP3 (Post Office Protocol Version 3)?
2	https://www.tutorialspoint.com/post-office-protocol-version-3-pop3	Post Office Protocol, Version 3 (POP3)
3	https://www.geeksforgeeks.org/computer-networks/difference-between-smtp-and-pop3/	Difference between SMTP and POP3

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct identification of network devices (PCs, mail server, switches) and protocols (POP3, SMTP)	30%
2	Proper handling of Cisco Packet Tracer software and devices	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Successful configuration of POP3 email accounts on PCs	10%
2	Sending and receiving emails successfully using POP3	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.29: Configuration of a Web Server (HTTP/HTTPS) using Cisco Packet tracer

I. Practical Significance

The purpose of this practical is to develop skills for configuring and analyzing web communication within a Local Area Network (LAN) using the HTTP and HTTPS protocols in Cisco Packet Tracer. This practical also develops skills in setting up a Web Server and end devices to enable access to web pages and secure browsing, providing insights into application layer communication and protocol operations.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

LLO 29.1 Configure a web server and access the website using a client PC using CISCO Packet tracer.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing web server configuration and analysis.
- Maintain the simulation environment and associated tools in proper working condition to ensure accurate configuration and testing results.
- Demonstrate patience and accuracy while performing step-by-step configuration of web servers and client devices.
- Exhibit responsibility in maintaining network security and promoting the ethical use of web services within the LAN.

VI. Relevant Theoretical Background

In computer networks, the **World Wide Web (WWW)** serves as a primary platform for sharing information and providing online services. The communication between a client (such as a web browser) and a web server is facilitated through the **Hypertext Transfer Protocol (HTTP)** and its secure version, **Hypertext Transfer Protocol Secure (HTTPS)**. These protocols operate at the **Application Layer** of the **TCP/IP model**, enabling users to access, retrieve, and interact with web resources hosted on servers.

1. HTTP Protocol

The **HTTP protocol** is a stateless, request-response protocol that governs how messages are formatted and transmitted between clients and servers. When a user enters a URL in a browser, the client sends an HTTP request to the server, typically using methods such as **GET**, **POST**, **PUT**, or **DELETE**. The server processes this request and responds with the requested resource (such as an HTML page, image,

or document) or an error message if the resource is unavailable. HTTP commonly operates on **port 80**.

2. **HTTPS Protocol**
   The **HTTPS protocol** extends HTTP by adding a layer of security through **SSL (Secure Sockets Layer)** or **TLS (Transport Layer Security)** encryption. HTTPS ensures **data confidentiality, integrity, and authentication**, protecting sensitive information from interception or tampering during transmission. HTTPS communication typically operates on **port 443**.
3. **Web Server Configuration**
   A **Web Server** is a software and hardware system that stores, processes, and delivers web content to clients. In Cisco Packet Tracer, the web server can be configured to host web pages and support both HTTP and HTTPS connections. Configuration tasks include assigning IP addresses, enabling HTTP/HTTPS services, uploading web content, and testing connectivity using client devices such as PCs or laptops.
4. **Client–Server Communication Process**
   When a client device sends a request to the web server:
   - The DNS server may resolve the domain name into an IP address.
   - The client initiates a TCP connection with the web server.
   - The HTTP or HTTPS protocol handles the data exchange, delivering the requested web content to the browser.
   - Once the transaction is complete, the TCP session is terminated.

VII. Circuit diagram / block diagram

A) Suggestive Block Diagram

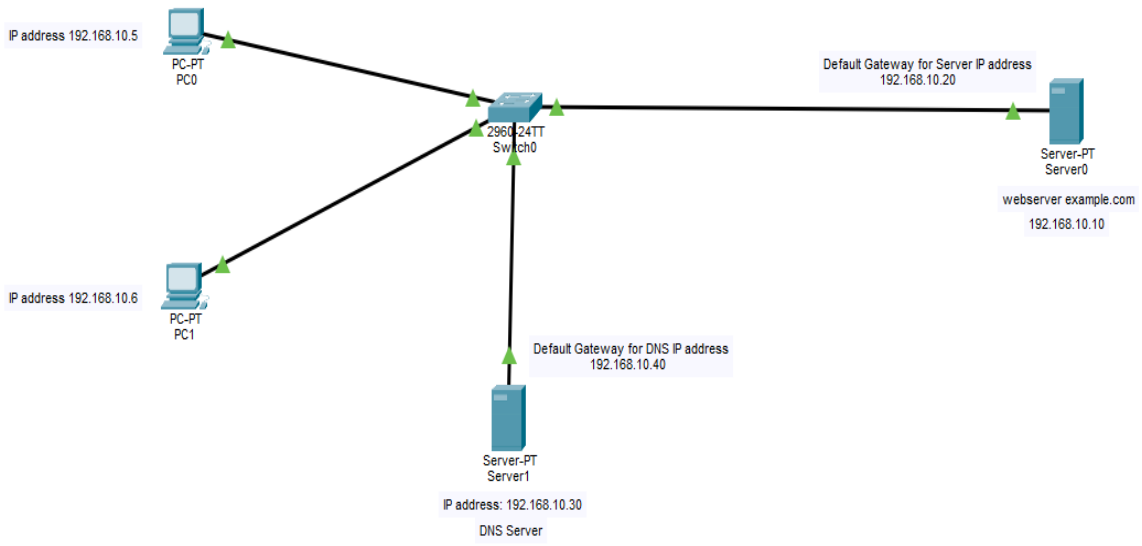


Fig 29.1 Typical network topology for Implementing HTTP/HTTPS Protocol with DNS Server

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 29.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all devices (Router, Switch, PCs) are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Configure correct IP addresses and subnet masks on all devices to avoid connectivity issues.
3. Verify basic network connectivity using PING between devices
4. Save the Packet Tracer project frequently to prevent loss of configuration and simulation data.
5. Enable HTTP/HTTPS services on Server.

6. Save Packet Tracer file at every step.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following:

- Cisco Packet Tracer (version 8.0 or later) is installed on your computer.
- Basic understanding of IPv4 addressing, switch connectivity, and LAN configuration.
- Knowledge of fundamental web protocols such as HTTP and HTTPS.
- Verify that Cisco Packet Tracer is functioning properly by opening and testing a sample network topology.

2. Create Network Topology

- Open Cisco Packet Tracer and wait for the workspace to fully load.
- Place the following network devices in the workspace:
  - 2 PCs → **PC0** and **PC1**
  - 2 Servers → **Server0 (Web Server)** and **Server1 (DNS Server)**
  - 1 Switch → **2960-24TT Switch**
- Connect devices using **Copper Straight-Through Cables** as follows:
  - PC0 → Switch (FastEthernet 0/1)
  - PC1 → Switch (FastEthernet 0/2)
  - Server0 (Web Server) → Switch (FastEthernet 0/3)
  - Server1 (DNS Server) → Switch (FastEthernet 0/4)
- Ensure that all link lights turn **green**, indicating active connections between all devices.

3. Assign IP Addresses

Assign IP addresses to all devices as per the following table.

Table 29.2

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	FastEthernet 0	192.168.10.5	255.255.255.0	192.168.10.40
PC1	FastEthernet 0	192.168.10.6	255.255.255.0	192.168.10.40
Server0 (Web Server)	FastEthernet 0	192.168.10.10	255.255.255.0	192.168.10.20
Server1 (DNS Server)	FastEthernet 0	192.168.10.30	255.255.255.0	192.168.10.40

- **Configure IP on PC0**
  - Click **PC0 → Desktop → IP Configuration**.
  - Enter the following details:
    - IP Address: 192.168.10.5
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.10.40
    - DNS Server: 192.168.10.30
  - Close the window to save the configuration automatically.
- **Configure IP on PC1**
  - Click PC1 → Desktop → IP Configuration.
  - Enter:
    - IP Address: 192.168.10.6

- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.40
- DNS Server: 192.168.10.30

  - Close the window to save the settings.

- **Configure IP on Web Server (Server0)**
  - Click **Server0 → Desktop → IP Configuration**.
  - Set:
    - IP Address: 192.168.10.10
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.10.20
    - DNS Server: 192.168.10.30
- **Configure IP on DNS Server (Server1)**
  - Click **Server1 → Desktop → IP Configuration**.
  - Enter:
    - IP Address: 192.168.10.30
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.10.40
    - DNS Server: 192.168.10.30

4. Configure DNS Server (Server1) as shown in Fig 29.2

- **Click Server1 in the workspace.**
- **Go to the Services tab.**
- **From the left-side menu, select DNS.**
- **Turn the DNS Service to ON.**

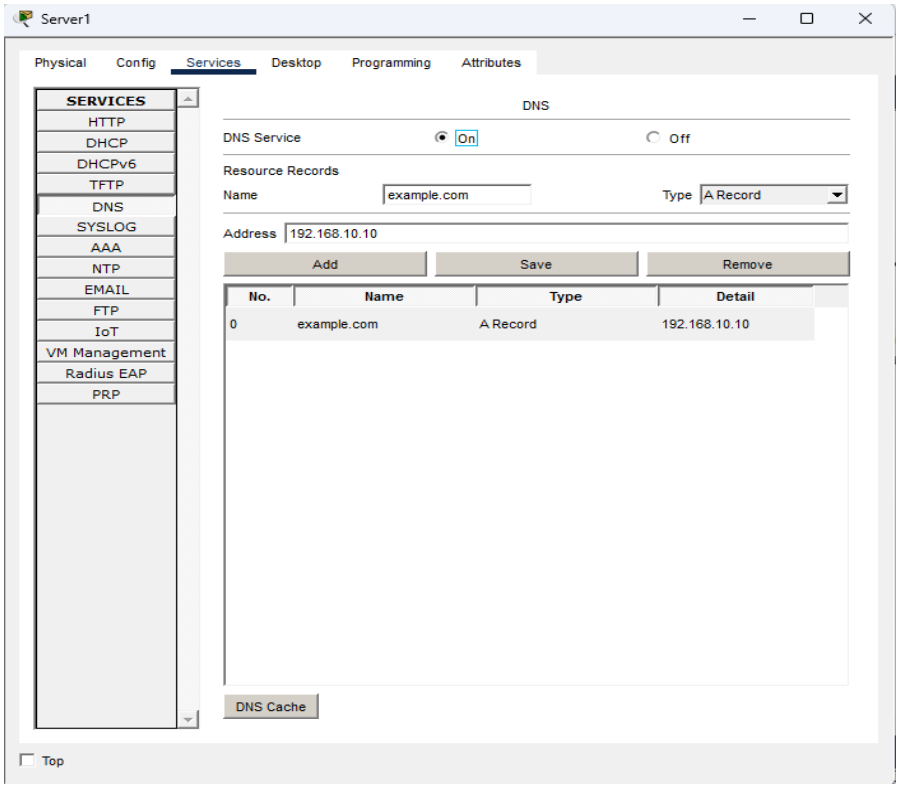


Fig 29.2 DNS Server configuration

- In the DNS configuration table:

- Name: **example.com**
- Type: **A Record**
- Address: **192.168.10.10**

- Click **Add** to save the record.
- Confirm the DNS record is visible in the table.
- Close the window after saving.

5. Configure Web Server (Server0) as shown in Fig 29.3

- Click **Server0 → Services tab**.
- From the left-side menu, select **HTTP**.
- Ensure the **HTTP Service** is turned **ON**.
- Next, scroll down to find **HTTPS Service** and turn it **ON** as well.

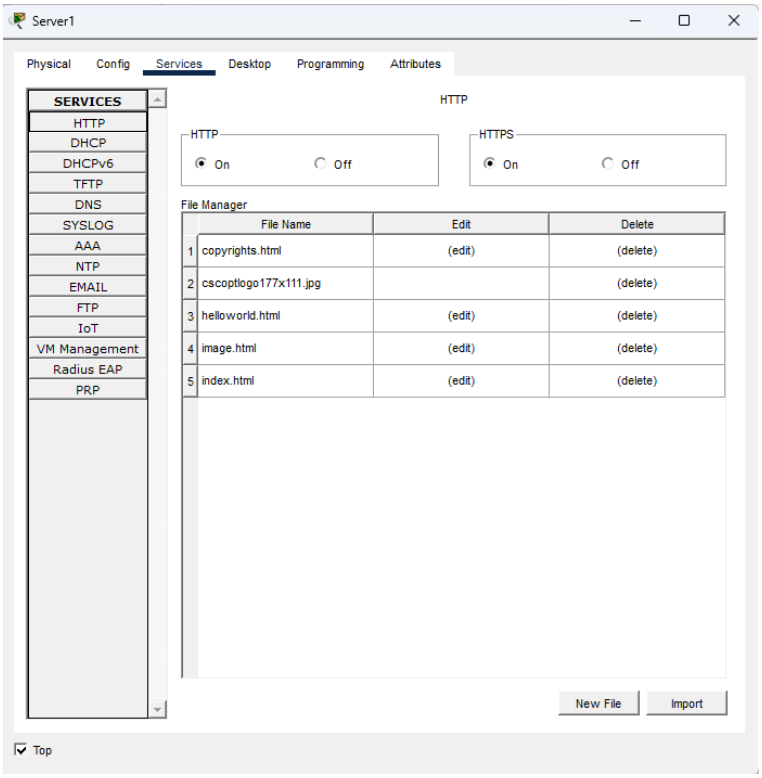


Fig 29.3 Configuring HTTP/HTTPS Service on Webserver

- Under the **Web Page section**, you can edit or upload content:
- Click **Edit** beside *index.html*.
- Replace the default text with as shown in Fig 29.4:

  <html>
  <head><title>Web Server Test Page</title></head>
  <body><h2>Welcome to the Web Server configured using Cisco Packet Tracer!</h2>
  This page is hosted on Server0 using HTTP and HTTPS protocols.
  </body></html>

- Click **Save** to store the webpage. It will ask to replace existing file, click yes as shown in Fig 29.4.

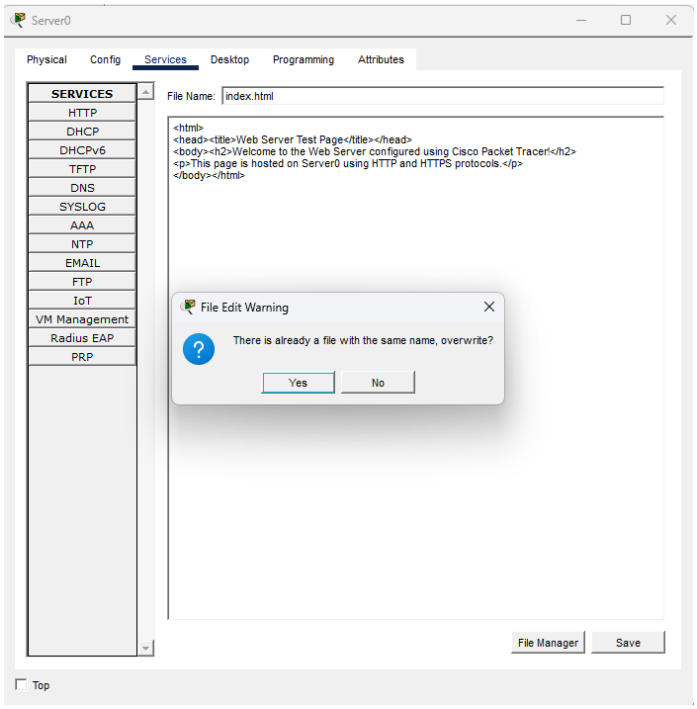


Fig 29.4 Replace code of index.html with new sample code

- Confirm both **HTTP (Port 80)** and **HTTPS (Port 443)** services are active.
- Close the configuration window.

6. Test Web Access from PC0

- Click **PC0 → Desktop → Web Browser**.
- In the address bar, type: http://example.com
- Press **Enter**.
- The webpage hosted on Server0 should appear, confirming successful HTTP configuration as shown in Fig 29.5

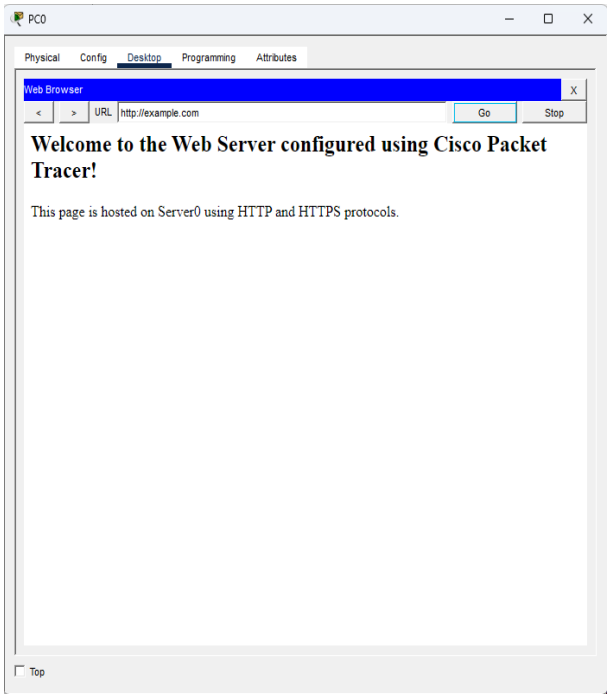


Fig 29.5 Webpage hosted on Server0 displayed confirming successful HTTP request

7. Test Secure Web Access (HTTPS) from PC1
   - Click **PC1 → Desktop → Web Browser.**
   - In the address bar, type:
     https://example.com
   - Press **Enter**.
   - The same webpage should appear, confirming HTTPS functionality as shown in Fig 29.6.

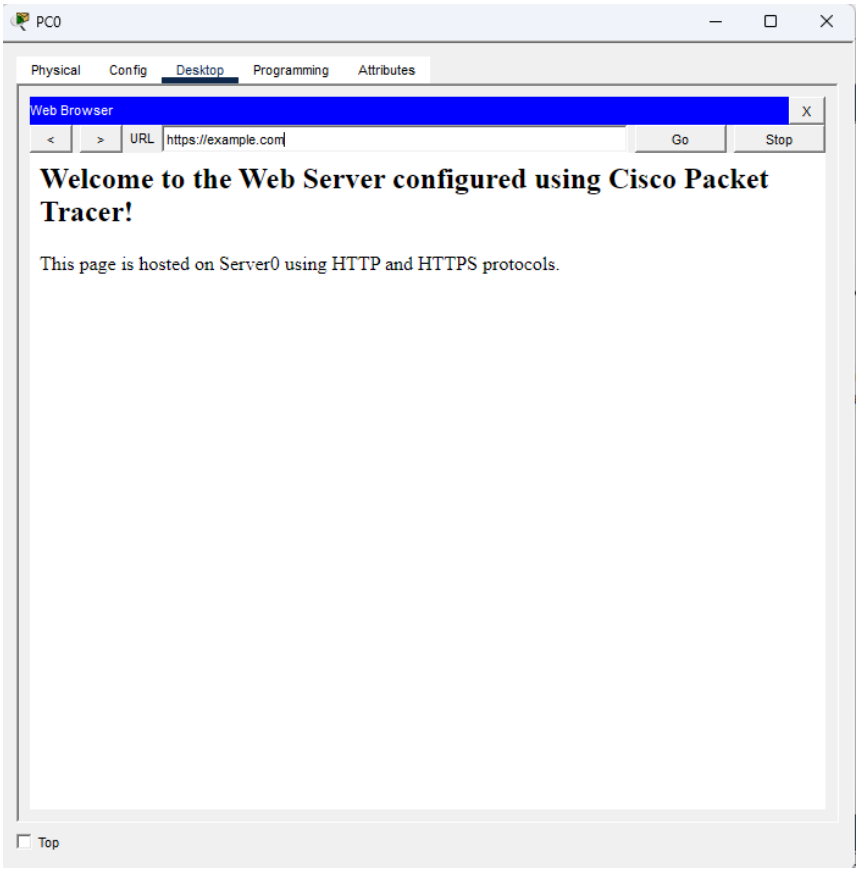


Fig 29.6 Webpage hosted on Server0 displayed confirming successful HTTPS request

8. Validate Network Connectivity
   - **Test Server Connectivity**
     - On **PC0**, open **Command Prompt (Desktop → Command Prompt).**
     - Type: ping 192.168.10.10
     - This checks connectivity to the Web Server.
     - If replies are received, the link is active and communication is successful.
   - Test **DNS Resolution**
     - On **PC0**, in the Command Prompt, type: ping webtest.com
     - If you receive reply messages from **192.168.10.10**, both DNS and network configurations are correct.
9. Record Observations

In the lab record, include the following details:

- IP configuration of each device.

- DNS and Web Server configuration details.
- Screenshots showing webpage access using HTTP and HTTPS.
- Ping test results for both IP and DNS name resolution.
- Short explanation of how HTTP/HTTPS and DNS operate within this LAN.

10. Save and Exit

- Save your project as: File → Save As → Practical_LAN_WebServer_Config.pkt
- Verify all configurations are correct.
- Close **Cisco Packet Tracer** safely.

XI. Resources used during performance

Table 29.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

7.

XIII. Observation Table

Table 29.5

Step	Action Performed	Expected Output	Actual Output (Page loaded/Resolved/ Displayed correctly)	Status (Pass/Fail)
1	Assign IP addresses and configure DNS & Web Server	All devices configured correctly with proper IP and DNS entries		
2	Test connectivity between PCs and Servers	Successful ping replies between all devices		
3	Configure HTTP and HTTPS services on Web Server	Web Server should have both HTTP (Port 80) and HTTPS (Port 443) active		
4	Access website using HTTP (http://example.com) from PC0	Webpage should load successfully via HTTP		
5	Access website using HTTPS (https:// example.com) from PC1	Secure webpage should load successfully via HTTPS		
6	Verify DNS Resolution	Domain name (example.com) should resolve to 192.168.10.10		

XIV. Result

……...

……..

XV. Interpretation of result

……...

……...

XVI. Conclusion and recommendation

……...…

……...…

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the default port numbers used by HTTP and HTTPS.
2. Write the steps to configure a Web Server in Cisco Packet Tracer.
3. Describe various methods of HTTP Protocol.
4. Write the procedure to test webpage accessibility using a web browser on a PC.

[Space for Answers] (If required attached separate page)

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	https://ccnapracticallabs.com/set-up-http-server-packet-tracer/	How to Setup HTTP Server in Packet Tracer
2	Rohit Kautkar YouTube Channel- How to Configure Web Server in Packet Tracer	https://www.youtube.com/watch?v=__pmMEIjcG8
3	https://www.geeksforgeeks.org/computer-networks/how-to-create-web-server-on-packet-tracer/	How to Create Web Server On Packet Tracer?

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct network setup and IP configuration in Packet Tracer	30%
2	Proper configuration of Web Server (HTTP/HTTPS)	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Accurate interpretation of HTTP/HTTPS packet flow	10%
2	Demonstration of application layer communication and protocol functionality	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 30: *Configuration DNS Server using Cisco Packet Tracer

I. Practical Significance

The purpose of this practical is to develop skills for configuring and analyzing domain name resolution within a Local Area Network (LAN) using the DNS (Domain Name System) protocol in Cisco Packet Tracer. This practical also develops skills in setting up a DNS Server and end devices to enable hostname-to-IP address translation, providing insights into application layer communication and protocol operations.

II. Industry/Employer Expected Outcome

This course aims to help the student to attain the following industry-identified outcomes through various teaching learning experiences: 'Maintain and troubleshoot network devices'.

III. Course Level Learning Outcome

Interpret functions of Application layer and Protocols associated with it.

IV. Laboratory Learning Outcome

30.1 Configure a DNS server in Packet Tracer and Test domain.

V. Relevant Affective Domain related outcomes

- Display professional ethics, teamwork, and clear documentation while performing configuration and analysis.
- Maintain the simulation environment and associated tools in proper working condition to ensure accurate configuration and resolution results.
- Demonstrate patience and accuracy while performing step-by-step configuration of servers and client devices.
- Exhibit responsibility in maintaining network integrity

VI. Relevant Theoretical Background

The **Domain Name System (DNS)** is a fundamental component of the Internet and computer networks, responsible for translating human-readable domain names into machine-understandable IP addresses. Since users find it easier to remember names (such as *example.com*) rather than numerical IP addresses (such as *192.168.1.10*), DNS plays a crucial role in simplifying communication between networked devices. It operates at the **Application Layer** of the **TCP/IP model**, providing essential name resolution services that enable efficient and seamless data transmission.

1. Concept of DNS

The Domain Name System functions as a distributed hierarchical database that maps domain names to their corresponding IP addresses. When a user enters a domain name into a browser, a DNS query is generated and sent to a DNS server. The server responds with the IP address of the requested domain, allowing the client to establish a connection with the appropriate host. This translation process is known as **name resolution**.

2. Structure of the DNS Hierarchy

The DNS hierarchy is organized in a tree-like structure that includes:

- **Root Domain (.)** – The top of the DNS hierarchy that directs queries to Top-Level Domains.
- **Top-Level Domains (TLDs)** – Represent general categories such as *.com, .org, .edu,* or country codes like *.in* or *.uk.*
- **Second-Level Domains** – Typically represent organizations or entities (e.g., *example.com*).
- **Subdomains and Hosts** – Define specific services or devices within a domain (e.g., *mail.example.com* or www.example.com).

3. **DNS Records and Their Types**
   DNS servers use different types of resource records to store and manage name resolution information. The most common record types are:
   - **A Record (Address Record):** Maps a domain name to an IPv4 address.
   - **AAAA Record:** Maps a domain name to an IPv6 address.
   - **CNAME (Canonical Name Record):** Provides an alias for another domain name.
   - **MX Record (Mail Exchange):** Specifies mail servers responsible for handling email.
   - **NS Record (Name Server):** Indicates authoritative DNS servers for a domain.
4. **DNS Resolution Process**
   When a client sends a request to access a domain:
   - The DNS client checks its local cache for the IP address.
   - If not found, it sends a query to the configured DNS server.
   - The DNS server searches its database or forwards the request to higher-level servers if necessary.
   - Once the IP address is found, it is sent back to the client for communication establishment.

   This process ensures accurate and efficient mapping of domain names to network addresses.
5. **DNS Configuration in Cisco Packet Tracer**
   In Cisco Packet Tracer, a DNS Server can be configured to provide name resolution services within a LAN. The configuration involves assigning an IP address to the DNS server, enabling the DNS service, and creating domain-to-IP mappings (A records). Client devices must be configured with the correct DNS server address to resolve domain names successfully.
6. **Importance of DNS in Networking**
   DNS enhances network usability, scalability, and manageability by allowing users to access network resources using easily recognizable names instead of numerical addresses. In enterprise networks and simulations, DNS configuration is essential for testing domain-based communication, integrating web and mail services, and ensuring smooth connectivity across networked devices.

VII. Circuit diagram / block diagram

A) Suggestive Block Diagram

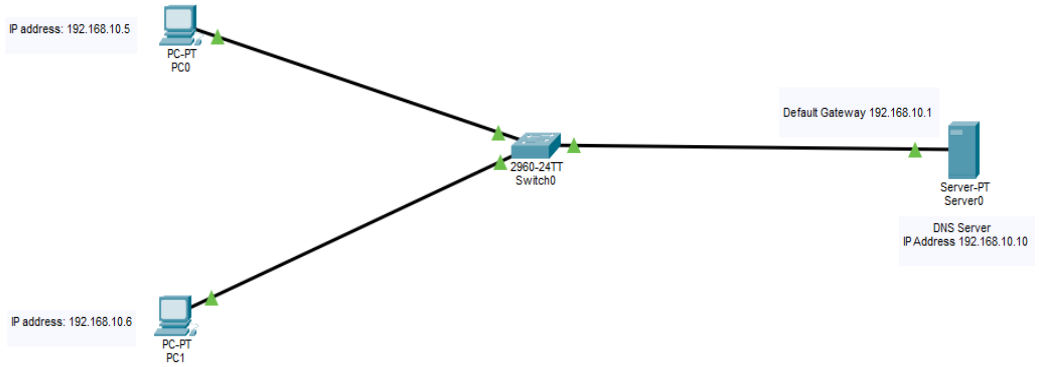


Fig 30.1 Typical network topology for Implementing DNS Server

B) Actual Block Diagram

VIII. Required Resources/apparatus/equipment with specifications

Table 30.1

Sr. No.	Name of Resource	Specification	Quantity
1	Desktop Computer	Intel i3/i5, 8GB RAM, 500GB HDD/256GB SSD, Windows 10/11	01
2	UPS 6 KVA online	Online UPS, 6 KVA capacity, input: 230V AC, output: 230V AC, Backup: 10–15 min, LCD display	01
3	Ethernet Switch	Ethernet Switch- 4/8/16/24/32	01
4	Router	Router-256MB Memory storage capacity, compatible with Desktop and Laptop, Rack Mountable, Wireless Connectivity	01
5	Simulation Software	Simulation Software: CISCO Packet Tracer, CORE Network Emulator, GNS3 or any other simulator	01
6	Antivirus Software	Quick Heal Total Security, Version 24.0 (or the latest available version, or any equivalent antivirus software)	01

IX. Precautions to be followed

1. Ensure that all devices (Router, Switch, PCs) are properly connected and powered ON in Cisco Packet Tracer before starting the practical.
2. Configure correct IP addresses and subnet masks on all devices to avoid connectivity issues.
3. Verify basic network connectivity using PING between devices
4. Save the Packet Tracer project frequently to prevent loss of configuration and simulation data.
5. Enable HTTP/HTTPS services on Server.
6. Save Packet Tracer file at every step.

X. Suggested Procedure

1. Prerequisites

Before beginning the practical, ensure the following:

- Cisco Packet Tracer (version 8.0 or later) is installed on your computer.
- Basic knowledge of IPv4 addressing, LAN connectivity, and switch configuration.
- Fundamental understanding of DNS (Domain Name System) and web communication concepts.
- Verify that Cisco Packet Tracer is functioning properly by opening and testing a sample network topology.

2. Create Network Topology

- Open Cisco Packet Tracer and wait for the workspace to fully load.
- Place the following network devices in the workspace:
  - **2 PCs** → PC0 and PC1
  - **1 DNS Server** → Server0
  - **1 Switch** → 2960-24TT Switch
- Connect devices using **Copper Straight-Through Cables** as follows:
  - PC0 → Switch (FastEthernet 0/1)
  - PC1 → Switch (FastEthernet 0/2)
  - DNS Server (Server0) → Switch (FastEthernet 0/3)
- Ensure all link lights turn green, indicating active connections.

3. Assign IP Addresses

Assign IP addresses to all devices as per the following table:

Table 30.2

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	FastEthernet 0	192.168.10.5	255.255.255.0	192.168.10.1
PC1	FastEthernet 0	192.168.10.6	255.255.255.0	192.168.10.1
DNS Server (Server0)	FastEthernet 0	192.168.10.10	255.255.255.0	192.168.10.1

- **Configure IP on PC0**
  - Click **PC0 → Desktop → IP Configuration**.
  - Enter:
    - IP Address : 192.168.10.5
    - Subnet Mask : 255.255.255.0

- Default Gateway : 192.168.10.1
- DNS Server : 192.168.10.10

- Close the window to save the configuration.

- **Configure IP on PC1**
  - Click **PC1 → Desktop → IP Configuration**.
  - Enter:
    - IP Address : 192.168.10.6
    - Subnet Mask : 255.255.255.0
    - Default Gateway : 192.168.10.1
    - DNS Server : 192.168.10.10
  - Close the window.
- **Configure IP on DNS Server (Server0)**
  - Click **Server0 → Desktop → IP Configuration**.
  - Set:
    - IP Address : 192.168.10.10
    - Subnet Mask : 255.255.255.0
    - Default Gateway : 192.168.10.1
    - DNS Server : 192.168.10.10 (self)
  - Close the window.

4. **Configure DNS Server (Server0) as shown in Fig 30.2**
   - Click **Server0 → Services tab → DNS**.
   - Turn the **DNS Service ON**.
   - In the DNS configuration table, add entries for each PC as shown in Table 30.3:

Table 30.3

Name	Type	Address
pc0	A Record	192.168.10.5
pc1	A Record	192.168.10.6

   - Click **Add** after each entry to save it.

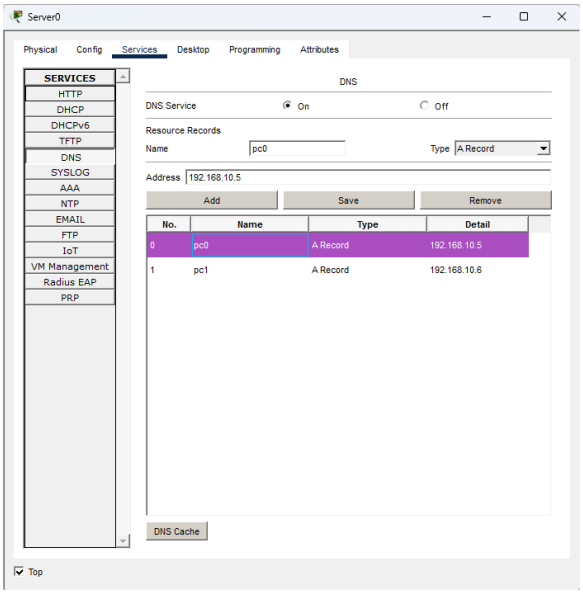


Fig 30.2 Configure DNS Server (Server0)

   - Confirm that both entries are visible in the DNS table.

- Close the configuration window.

5. Test DNS Functionality

- Test connectivity by IP as shown in Fig 30.3
  - On **PC0**, open **Command Prompt.**

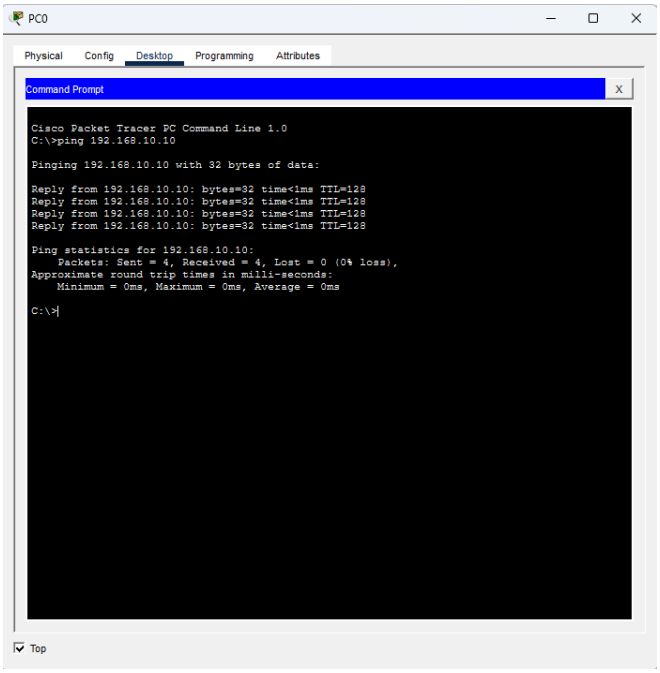


Fig 30.3 Test connectivity by IP

  - Ping the DNS server using its IP:

    ping 192.168.10.10

  - Successful replies confirm connectivity to the DNS server.
- Test connectivity by hostname as shown in Fig 30.4
  - On **PC0**, in Command Prompt, type:

    ping pc1

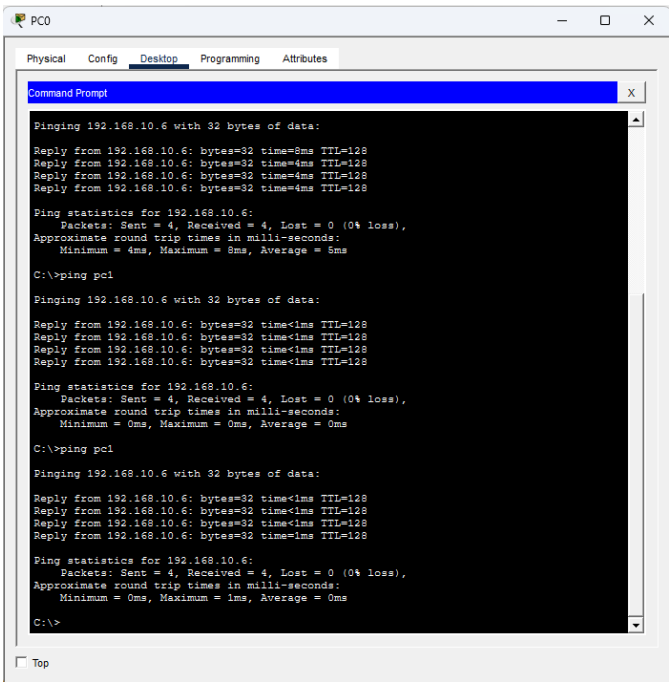


Fig 30.4 Test connectivity by hostname for pc0

- The DNS server resolves pc1 to 192.168.10.6 and returns successful ping replies.
- On **PC1**, repeat using as shown in Fig 30.5:

ping pc0

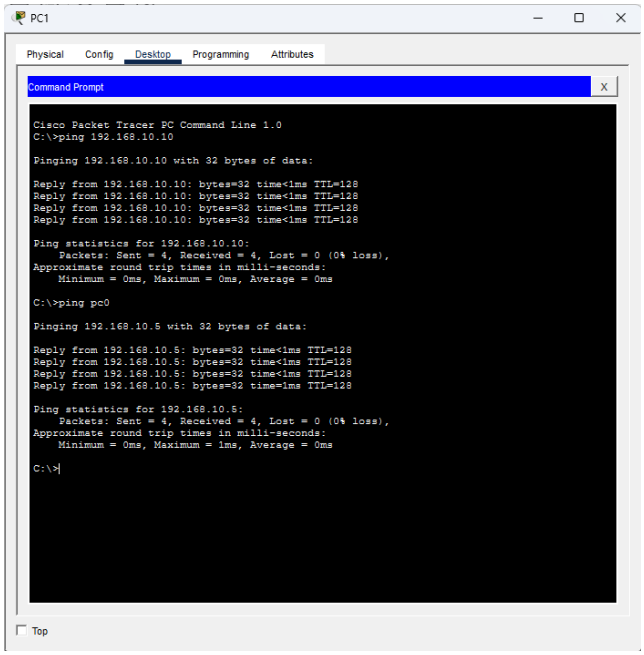


Fig 30.5 Test connectivity by hostname for pc1

- Successful replies confirm DNS name resolution within the LAN.

6. **Record** Observations

   In your lab record, include:
   - IP configuration of all devices.
   - DNS table entries (PC0 and PC1).
   - Screenshots of successful pings using both IP and hostname.
   - Short explanation of how DNS translates hostnames to IP addresses within the LAN.
7. **Save** and Exit
   - Save your project:
   - File → Save As → Practical_LAN_DNS_Config.pkt
   - Verify that all DNS entries and connectivity are correct.
   - Close Cisco Packet Tracer safely.

XI. Resources used during performance

Table 30.4

Sr. No.	Name of Resource	Specification	Quantity

XII. Actual Procedure (If required attached separate sheet)

1.

2.

3.

4.

5.

6.

XIII. Observation Table

Table 30.5

Step	Action Performed	Expected Output	Actual Output (Ping/Resolved/ Displayed Correctly)	Status (Pass/ Fail)
1	Assign IP addresses to PC0, PC1, and DNS Server	All devices configured with correct IP and DNS		
2	Connect PCs and DNS Server to switch	All link lights should turn green		
3	Configure DNS Server entries for PC0 and PC1	DNS table contains entries: pc0 → 192.168.10.5, pc1 → 192.168.10.6		
4	Ping DNS Server from PC0 using IP	Successful replies from 192.168.10.10		

Step	Action Performed	Expected Output	Actual Output (Ping/Resolved/ Displayed Correctly)	Status (Pass/ Fail)
5	Ping PC1 from PC0 using hostname (pc1)	Hostname resolves to 192.168.10.6, successful ping		
6	Ping PC0 from PC1 using hostname (pc0)	Hostname resolves to 192.168.10.5, successful ping		

XIV. Result

……...……

…...……

XV. Interpretation of result

……...

……...

XVI. Conclusion and recommendation

……...

……...

XVII. Practical Related Questions:

Note: Below given are few sample questions for reference. Teacher must design more such questions so as to ensure the achievement of identified CO.

1. State the role of a DNS server in a Local Area Network.
2. State the default port used by DNS protocol.
3. Write the step-by-step procedure to configure a DNS Server in Cisco Packet Tracer.
4. Describe the steps to test DNS resolution from a PC using hostname instead of IP.

[Space for Answers] (If required attached separate page)

……...

……...

……...

……...

……...

……...

……...

……...

……...

……...

……...

XVIII. Suggested references for further reading

Sr. No.	Link / Portal / VLab	Description
1	Rohit Kautkar YouTube Channel- Configure DNS Server in Packet Tracer | How to Configure DNS Server | Set up DNS in Packet Tracer	https://www.youtube.com/watch?v=SP6EnpZPOBQ
2	https://medium.com/@z6157881/configure-dns-server-on-cisco-packet-tracer-e7c412b3b3dd	Configure DNS Server On Cisco Packet Tracer

XIX. Assessment Scheme

Performance Indicators		Weightage
Process Related: 15 Marks		**60%**
1	Correct network setup and IP configuration in Packet Tracer	30%
2	Proper configuration of DNS Server	20%
3	Working in teams	10%
Product Related: 10 Marks		**40%**
1	Accurate interpretation of DNS query and response packet flow	10%
2	Demonstration of application layer communication and protocol functionality	10%
3	Answer to Practical Related Question	15%
4	Submission of Journal on time	05%
Total (25 Marks)		**100 %**

Marks Obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	