DRONACHARYA
College of Engineering

LABORATORY MANUAL

B.Tech. Semester- VI

COMPUTER NETWORK LAB
Subject code: LC-ECE-322G

Prepared by:	**Checked by:**	**Approved by:**
Mr. Hansraj	Mrs. Dimple Saproo	Name : Prof. (Dr.) Isha Malhotra
Sign.: ……	**Sign.: ……**	**Sign.: ……**

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
DRONACHARYA COLLEGE OF ENGINEERING
KHENTAWAS, FARRUKH NAGAR, GURUGRAM (HARYANA)

Table of Contents

1. Vision and Mission of the Institute
2. Vision and Mission of the Department
3. Programme Educational Objectives (PEOs)
4. Programme Outcomes (POs)
5. Programme Specific Outcomes (PSOs)
6. University Syllabus
7. Course Outcomes (COs)
8. CO- PO and CO-PSO mapping
9. Course Overview
10. List of Experiments
11. DOs and DON'Ts
12. General Safety Precautions
13. Guidelines for Students for Report Preparation
14. Lab Assessment Criteria
15. Details of Conducted Experiments
16. Lab Experiments

Vision and Mission of the Institute

Vision:

"Dronacharya College of Engineering, Gurgaon aims to become an Institution of excellence in imparting quality Outcome Based Education that empowers the young generation with Knowledge, Skills, Research, Aptitude and Ethical values to solve Contemporary Challenging Problems"

Mission:

M1: Develop a platform for achieving globally acceptable level of intellectual acumen and technological competence.

M2: Create an inspiring ambience that raises the motivation level for conducting quality research.

M3: Provide an environment for acquiring ethical values and positive attitude.

Vision and Mission of the Department

Vision:

"To become a Centre of Excellence in teaching and research in Information Technology for producing skilled professionals having a zeal to serve society"

Mission:

M1: To create an environment where students can be equipped with strong fundamental concepts, programming and problem solving skills.

M2: To provide an exposure to emerging technologies by providing hands on experience for generating competent professionals.

M3: To promote Research and Development in the frontier areas of Information Technology and encourage students for pursuing higher education

M4: To inculcate in students ethics, professional values, team work and leadership skills.

Programme Educational Objectives (PEOs)

PEO1: To provide students with a sound knowledge of mathematical, scientific and engineering fundamentals required to solve real world problems.

PEO2: To develop research oriented analytical ability among students and to prepare them for making technical contribution to the society.

PEO3: To develop in students the ability to apply state-of-the–art tools and techniques for designing software products to meet the needs of Industry with due consideration for environment friendly and sustainable development.

PEO4: To prepare students with effective communication skills, professional ethics and managerial skills.

PEO5: To prepare students with the ability to upgrade their skills and knowledge for life-long learning.

Programme Outcomes (POs)

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes (PSOs)

PSO1: Analyze, identify and clearly define a problem for solving user needs by selecting, creating and evaluating a computer based system through an effective project plan.

PSO2: Design, implement and evaluate processes, components and/or programs using modern techniques, skills and tools of core Information Technologies to effectively integrate secure IT-based solutions into the user environment.

PSO3: Develop impactful IT solutions by using research based knowledge and research methods in the fields of integration, interface issues, security & assurance and implementation.

University Syllabus

1. Running and using services/commands like ping, trace route, NSLOOKUP, ARP, TELNET, FTP, etc.
2. Network simulation using tools like Cisco Packet Tracer, NetSim, OMNeT++, NS2, NS3, etc.
3. Network Topology – Star, Bus, Ring
4. Simulate the transmission of ping messaged over a network topology and find the number of packets dropped due to congestion.
5. Understanding IP Addressing using the simulation tool.
6. Study of various application protocols using the simulation like FTP, HTTP
7. Understand IP forwarding within a LAN and across a router
8. Understand the working of "Connection Establishment" in TCP using Network simulation using tools
9. Study how the Data Rate of a Wireless LAN (IEEE 802.11b) network varies as the distance between the Access Point and the wireless nodes is varied
10. Study the working and routing table formation of Interior routing protocols, i.e. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)
11. To determine the optimum persistence of a CSMA / CD network
12. Implementation of distance vector routing algorithm
13. Implementation of Link state routing algorithm
14. Study of Network simulator (NS) and simulation of Congestion Control Algorithms using NS
15. Encryption and decryption.

Course Outcomes (COs)

Upon successful completion of the course, the students will be able to

C322.1: Simulate different network topologies.

C322.2: Implement various framing methods of Data Link Layer.

C322.3: Implement various Error and flow control techniques.

C322.4: Implement network routing and addressing techniques.

C322.5: Implement transport and security mechanisms

CO-PO Mapping

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
C322.	3	2	2	2	2	2	2	2	2	2	2	3
C322.	3	2	2	2	2	2	2	2	2	2	2	3
C322.	3	2	2	2	2	2	2	2	2	2	2	3
C322.	3	2	2	2	2	2	2	2	2	2	2	3
C322.	3	2	2	2	2	2	2	2	2	2	2	3
C322	3	2	2	2	2	2	2	2	2	2	2	3

CO-PSO Mapping

	PSO1	PSO2	PSO3
C322.1	2	2	1
C322.2	2	2	1
C322.3	2	2	1
C322.4	2	2	1
C322.5	2	2	1
C322	**2**	**2**	**1**

Course Overview

Computer Networking Lab provides students with hands on training on various topologies and protocols of Networking. It makes students acquainted with an overview of how the information is transferred from source to destination and different layers in networks. Students can come to know that how the routing algorithms work out in the network layer and in what manner the networking techniques that can take place in computer.

A computer network is made of two distinct subsets of components Distributed applications are programs running on interconnected computers; a web server, a remote login server, an e-mail exchanger are examples. Encapsulation of various learning objectives includes: Analysis the different layers in networks; Define, use, and differentiate such concepts as OSI-ISO,TCP/IP; Sending bits from physical layer to data link layer; Simulation of presentation layer, application layer for data compression and network security.

List of Experiments mapped with COs

Sl No.	*Program Name*	*Course Outcome*
1	To study the Comparative Analysis of Network Simulators	C322.1
2	To learn and configuration of networking hardware like RJ-45 connector, Network cables, crimping tool, etc	C322.1
3	To learn and implement basic command of Computer network like PING, traceroute etc.	C322.2
4	Configure and implement a network using Packet Tracer. a. Creating a First Network b. Sending Simple Text Messages in Realtime Mode c. Establishing a Web Server Connection Using the PC's Web Browser	C322.2
5	Configure network devices, such as hubs and switches within a network topology using Packet Tracer software.	C322.3
6	Configure network topology to implement VLANs with trunking using Packet Tracer software.	C322.3
7	Configure and implementation of a router within Network using Packet Tracer.	C322.3
8	Configure network topology and implement static routing using Packet Tracer Software.	C322.4
9	Configure network topology and implement dynamic routing protocol such as RIP, OSPF etc. using Packet Tracer.	C322.5
10	Configure a network and implement remote login of router and Management using Packet Trace	C322.5
11	Configure DHCP Server in the Network using packet tracer software.	C322.5

DOs and DON'Ts

DOs

1. Login-on with your username and password.
2. Log off the Computer every time when you leave the Lab.
3. Arrange your chair properly when you are leaving the lab.
4. Put your bags in the designated area.
5. Ask permission to print.

DON'Ts

1. Do not share your username and password.
2. Do not remove or disconnect cables or hardware parts.
3. Do not personalize the computer setting.
4. Do not run programs that continue to execute after you log off.
5. Do not download or install any programs, games or music on computer in Lab.
6. Personal Internet use chat room for Instant Messaging (IM) and Sites Strictly Prohibited.
7. No Internet gaming activities allowed.
8. Tea, Coffee, Water & Eatables are not allowed in the Computer Lab.

General Safety Precautions

Precautions (In case of Injury or Electric Shock)

1. To break the victim with live electric source, use an insulator such as fire wood or plastic to break the contact. Do not touch the victim with bare hands to avoid the risk of electrifying yourself.
2. Unplug the risk of faulty equipment. If main circuit breaker is accessible, turn the circuit off.
3. If the victim is unconscious, start resuscitation immediately, use your hands to press the chest in and out to continue breathing function. Use mouth-to-mouth resuscitation if necessary.
4. Immediately call medical emergency and security. Remember! Time is critical; be best.

Precautions (In case of Fire)

1. Turn the equipment off. If power switch is not immediately accessible, take plug off.
2. If fire continues, try to curb the fire, if possible, by using the fire extinguisher or by covering it with a heavy cloth if possible isolate the burning equipment from the other surrounding equipment.
3. Sound the fire alarm by activating the nearest alarm switch located in the hallway.
4. Call security and emergency department immediately:

Emergency : Reception

Security : Gate No.1

Guidelines to students for report preparation

All students are required to maintain a record of the experiments conducted by them. Guidelines for its preparation are as follows:-

1) All files must contain a title page followed by an index page. ***The files will not be signed by the faculty without an entry in the index page.***

2) Student's Name, Roll number and date of conduction of experiment must be written on all pages.

3) For each experiment, the record must contain the following

(i) Aim/Objective of the experiment

(ii) Pre-experiment work (as given by the faculty)

(iii) Lab assignment questions and their solutions

(iv) Results/ output

Note:

1. Students must bring their lab record along with them whenever they come for the lab.

2. Students must ensure that their lab record is regularly evaluated.

Lab Assessment Criteria

An estimated 10 lab classes are conducted in a semester for each lab course. These lab classes are assessed continuously. Each lab experiment is evaluated based on 5 assessment criteria as shown in following table. Assessed performance in each experiment is used to compute CO attainment as well as internal marks in the lab course.

Grading Criteria	Exemplary (4)	Competent (3)	Needs Improvement (2)	Poor (1)
AC1: Pre-Lab written work (for last lab class, this may be assessed through viva)	Complete procedure with underlined concept is properly written	Underlined concept is written but procedure is incomplete	Not able to write concept and procedure	Underlined concept is not clearly understood
AC2: Program Writing/ Modeling	Assigned problem is properly analyzed, correct solution designed, appropriate language constructs/ tools are applied, Program/solution written is readable	Assigned problem is properly analyzed, correct solution designed, appropriate language constructs/ tools are applied	Assigned problem is properly analyzed & correct solution designed	Assigned problem is properly analyzed
AC3: Identification & Removal of errors/ bugs	Able to identify errors/ bugs and remove them	Able to identify errors/ bugs and remove them with little bit of guidance	Is dependent totally on someone for identification of errors/ bugs and their removal	Unable to understand the reason for errors/ bugs even after they are explicitly pointed out
AC4:Execution & Demonstration	All variants of input /output are tested, Solution is well demonstrated and implemented concept is clearly explained	All variants of input /output are not tested, However, solution is well demonstrated and implemented concept is clearly explained	Only few variants of input /output are tested, Solution is well demonstrated but implemented concept is not clearly explained	Solution is not well demonstrated and implemented concept is not clearly explained
AC5:Lab Record Assessment	All assigned problems are well recorded with objective, design constructs and solution along with Performance analysis using all variants of input and output	More than 70 % of the assigned problems are well recorded with objective, design contracts and solution along with Performance analysis is done with all variants of input and output	Less than 70 % of the assigned problems are well recorded with objective, design contracts and solution along with Performance analysis is done with all variants of input and output	Less than 40 % of the assigned problems are well recorded with objective, design contracts and solution along with Performance analysis is done with all variants of input and output

LAB EXPERIMENTS

LAB EXPERIMENT 1

OBJECTIVE: To study the Comparative Analysis of Network Simulators

BRIEF DESCRIPTION:

CISCO PACKET TRACER

1. The robust simulation tool used to visualize networks.
2. **Packet Tracer** provides valuable tips and best practices for using Cisco Packet Tracer.
3. Learn the basic operations of Packet Tracer: - File commands, visualization and configuration of networking devices.
4. Simulate the interactions of data traveling through the network.
5. Learn to visualize the network in logical and physical modes.
6. Reinforce your understanding with extensive hands-on networking and IOT activities.
7. Get immediate feedback on your work through built-in quizzes and tests.
8. Connect with the global Cisco Networking Academy community.

System requirement

The following configuration is recommended by Cisco to successfully install and run Packet Tracer 7.0 :

1. Microsoft Windows (7 / 8.1 / 10) or Linux Ubuntu (14.04 64-bits)
2. At least Pentium 4 (2.5 GHz)
3. A minimum of 2GB RAM (4GB recommended)
4. 700 MB of storage space
5. A minimum screen resolution of 1024 x 768

Summary

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows

users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.

NS-2/NS-3

1. ns (from network simulator) is a name for a series of discrete event network simulators, specifically ns-1, and ns-2.
2. All of them are discrete-event computer network simulators, primarily used in research and teaching.

System Requirements

1. Linux (x86 and x86_64): gcc/g++ versions 4.9 and above
2. **Note:** If you are using RHEL or Centos, you will likely need to install a more up-to-date compiler than the default; search for how to enable 'software collections' or 'devtoolset' on these distributions. Other Linux distributions typically have a suitable default compiler (at least version 4.9).
3. MacOS Apple LLVM: version 8.0.0 and above (version 7.0.0 may work)
4. FreeBSD and Linux (x86_64): clang/LLVM version 3.9 and above (older versions down to 3.3 may work)
5. The minimum Python version supported is 2.7 or greater (version 2), or version 3.4 or greater (version 3).

Summary

NETWORK SIMULATOR 3

ns-3 has been developed to provide an open, extensible network simulation platform, for networking research and education.
In brief, *ns-3* provides models of how packet data networks work and perform, and provides a simulation engine for users to conduct simulation experiments.
Some of the reasons to use *ns-3* include to perform studies that are more difficult or not possible to perform with real systems, to study system behavior in a highly controlled, reproducible environment, and to learn about how networks work.

NETWORK SIMULATOR 2

It is not possible to run a simulation in *ns-2* purely from C++ (i.e., as a main() program without any OTcl). Moreover, some components of *ns-2* are written in C++ and others in OTcl.

In *ns-3*, the simulator is written entirely in C++, with optional Python bindings.

Simulation scripts can therefore be written in C++ or in Python.

New animators and visualizers are available and under current development. Since *ns-3* generates pcap packet trace files, other utilities can be used to analyze traces as well.

WIRESHARK

1. Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
2. You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).
3. Wireshark is perhaps one of the best open source packet analyzers available today.

System Requirements

The amount of resources Wireshark needs depends on your environment and on the size of the capture file you are analyzing. The values below should be fine for small to medium-sized capture files no more than a few hundred MB. Larger capture files will require more memory and disk space. If Wireshark runs out of memory it will crash.

1. Microsoft Windows
2. Unix/Linux

Summary

In late 1997 Gerald Combs needed a tool for tracking down network problems and wanted to learn more about networking so he started writing Ethereal (the original name of the Wireshark project) as a way to solve both problems.

In October, 1998 Guy Harris was looking for something better than tcpview so he started applying patches and contributing dissectors to Ethereal.

The list of people who have contributed to the project has become very long since then, and almost all of them started with a protocol that they needed that Wireshark or did not already handle. So they copied an existing dissector and contributed the code back to the team.

In 2006 the project moved house and re-emerged under a new name: Wireshark.

In 2008, after ten years of development, Wireshark finally arrived at version 1.0. This release was the first deemed complete, with the minimum features implemented. Its release coincided with the first Wireshark Developer and User Conference, called Sharkfest.

In 2015 Wireshark 2.0 was released, which featured a new user interface.

OmNet++

1. **OMNeT++ is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.**
2. "Network" is meant in a broader sense that includes wired and wireless communication networks, on-chip networks, queueing networks, and so on.
3. Domain-specific functionality such as support for sensor networks, wireless ad-hoc networks, Internet protocols, performance modeling, photonic networks, etc., is provided by model frameworks, developed as independent projects. OMNeT++ offers an Eclipse-based IDE, a graphical runtime environment, and a host of other tools.
4. There are extensions for real-time simulation, network emulation, database integration, SystemC integration, and several other functions.
5. Although OMNeT++ is not a network simulator itself, it has gained widespread popularity as a network simulation platform in the scientific community as well as in industrial settings, and building up a large user community.

System Requirements

1. simulation kernel library
2. NED topology description language
3. GUI for simulation execution, links into simulation executable (Tkenv)
4. command-line user interface for simulation execution (Cmdenv)
5. utilities (makefile creation tool, etc.)
6. documentation, sample simulations, etc.
7. OMNeT++ IDE based on the Eclipse platform

Summary

OverSim is an OMNeT++-based open-source simulation framework for overlay and peer-to-peer networks, developed at the Institute of Telematics, Karlsruhe Institute of Technology, Germany.

The simulator contains several models for structured (e.g. Chord, Kademlia, Pastry) and unstructured (e.g. GIA) peer-to-peer protocols. An example implementation of the framework is an implementation of a peer-to-peer SIP communications network.

Research tool- OverSim provides a convenient platform for simulating large-scale complex overlay protocols and applications. Though it can be overwhelming at first, you will realize its power when you develop a better understanding of the tool.

PRE EXPERIMENT QUESTIONS:

Q1. What Is Simulation?

Q2. What Is The Need For Simulation?

POST EXPERIMENT QUESTIONS:

Q1. What protocols does ns support?

Q2. What platforms does ns run on and what kind of hardware do I need?

LAB EXPERIMENT 2

OBJECTIVE: To learn handling and configuration of networking hardware like RJ-45 connector, Network cables, crimping tool, etc

BRIEF DESCRIPTION: Familiarize yourself with common networking hardware components, such as RJ-45 connectors, network cables (Ethernet, twisted pair, etc.), crimping tools, cable testers, and cable strippers. Understand the purpose and functionality of each hardware component in a network setup.

STEPS FOR HANDLING NETWORK HARDWARE:

1. RJ-45 Connector Handling:

   Learn the proper handling of RJ-45 connectors to prevent damage and ensure secure connections. Understand the different parts of an RJ-45 connector, including the cable strain relief, wiring channels, and contacts.

2. Network Cable Preparation:
   Learn how to prepare network cables for termination by stripping the outer jacket using a cable stripper. Understand the appropriate length of cable required for specific network connections.

3. Wiring Standard and Color Coding:
   Study the wiring standards for Ethernet connections and the corresponding color codes for each wire. Learn how to arrange the individual wires in the correct order before inserting them into the RJ-45 connector.

4. Crimping Process:
   Practice the crimping process using a crimping tool to secure the wires within the RJ-45 connector. Understand the proper technique for applying pressure while crimping to ensure a reliable connection.

5. Cable Testing and Verification:
   Use a cable tester to verify the continuity and proper wiring of the network cable.
   Learn how to interpret the results displayed by the cable tester to identify any potential issues.

6. Hands-on Practice:
   Engage in hands-on practice by creating various network connections using RJ-45 connectors, network cables, and crimping tools.
   Experiment with different cable types, lengths, and wiring standards to gain proficiency.

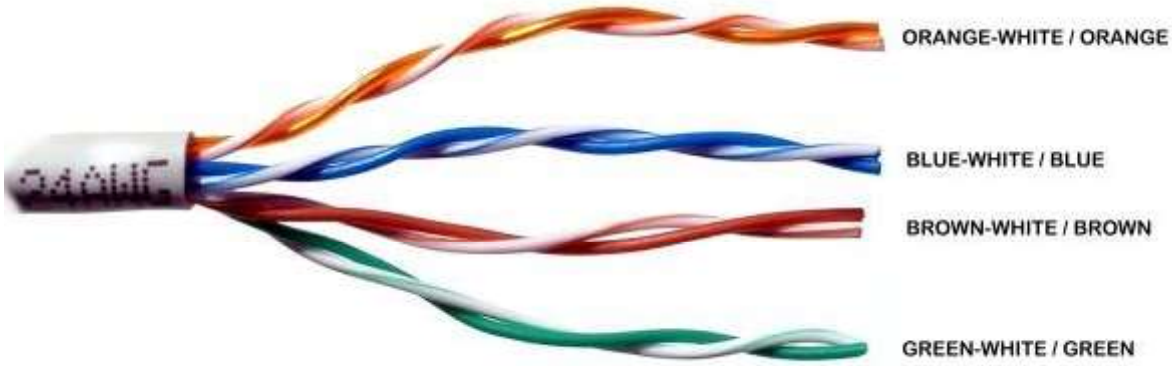
7. Troubleshooting:
   Understand common issues that may arise during the handling and configuration of networking hardware. Learn troubleshooting techniques to identify and resolve problems, such as loose connections, faulty crimps, or incorrect wiring.

PRE EXPERIMENT QUESTIONS:

Q1. What are some examples of networking hardware components that you expect to encounter in this experiment?

Q2. How familiar are you with the purpose and functionality of RJ-45 connectors?

RJ-45 connector



Twisted pair Cable

Climping Tool

POST EXPERIMENT QUESTIONS:

Q1 What is the purpose of an RJ-45 connector in networking hardware?

Q2 How do you properly terminate an Ethernet cable using an RJ-45 connector?

Q3 What are the different types of network cables commonly used in networking hardware?

Q4 Explain the difference between a straight-through cable and a crossover cable.

Q5 What are the steps involved in using a crimping tool to create network cables?

Q6 What safety precautions should be followed while working with networking hardware?

Q7 How do you test the continuity of a network cable using a cable tester?

Q8 What are some common issues that can occur when working with networking hardware, and how would you troubleshoot them?

Q9 Explain the process of creating a network connection between two devices using a switch and network cables.

LAB EXPERIMENT 3

OBJECTIVE: To learn and implement basic command of Computer network like PING, traceroute etc.

BRIEF DESCRIPTION: The experiment aims to familiarize participants with basic network commands such as PING and Traceroute and provide hands-on experience in implementing these commands. The participants will learn how to use these commands to troubleshoot network connectivity issues and gather information about network paths.

STEPS FOR HANDLING NETWORK HARDWARE:

1. Familiarize yourself with the network hardware: Take some time to understand the different networking devices involved, such as routers, switches, and network interface cards (NICs). Learn about their functions and how they connect to form a network.
2. Connect the hardware: Connect the networking hardware according to the network topology you are trying to implement. This may involve connecting computers to switches, switches to routers, or routers to the internet service provider's modem.
3. Verify physical connections: Ensure that all cables are securely connected and properly seated. Check for any loose connections or damaged cables that may affect network connectivity.
4. Power on the devices: Power on the networking devices in the correct order, starting from the modem and moving through the network hierarchy (if applicable). Allow sufficient time for the devices to boot up and establish connections.
5. Configure IP addresses: Assign IP addresses to the network devices, such as computers and routers, using either static IP addressing or dynamic IP assignment protocols like DHCP. Ensure that each device has a unique IP address within the network.
6. Test network connectivity using PING: Open a command prompt or terminal window on a computer connected to the network. Use the PING command followed by the IP address or hostname of another device on the network to check if there is a response. For example, "ping 192.168.0.1" or "ping www.example.com".
7. Perform traceroute: Traceroute is a command used to trace the route that packets take from your computer to a target destination. In the command prompt or terminal, use the "traceroute" command followed by the IP address or domain name of the destination. This will display the hops (routers) the packets take to reach the destination.

8. Analyze the results: Analyze the output of the PING and traceroute commands. Look for any timeouts, high latency, or unexpected routes. This information can help identify network issues and potential bottlenecks.
9. Troubleshoot network problems: If any connectivity issues arise, troubleshoot the network by checking physical connections, verifying IP configurations, and ensuring that network devices are functioning correctly. Use appropriate troubleshooting techniques to identify and resolve the problems.
10. Document and learn from the experiment: Keep a record of your configurations, commands used, and the results obtained. Take note of any lessons learned or challenges faced during the experiment. This documentation will be helpful for future reference and knowledge enhancement.

PRE EXPERIMENT QUESTIONS:

Q1 Explain the concept of round-trip time (RTT) in relation to the PING command.

Q2 How can you interpret the PING command's output to determine if there are any network connectivity issues?

Q3 What are some common options or parameters that can be used with the PING command?

Q4 What is the purpose of the traceroute command in computer networks?

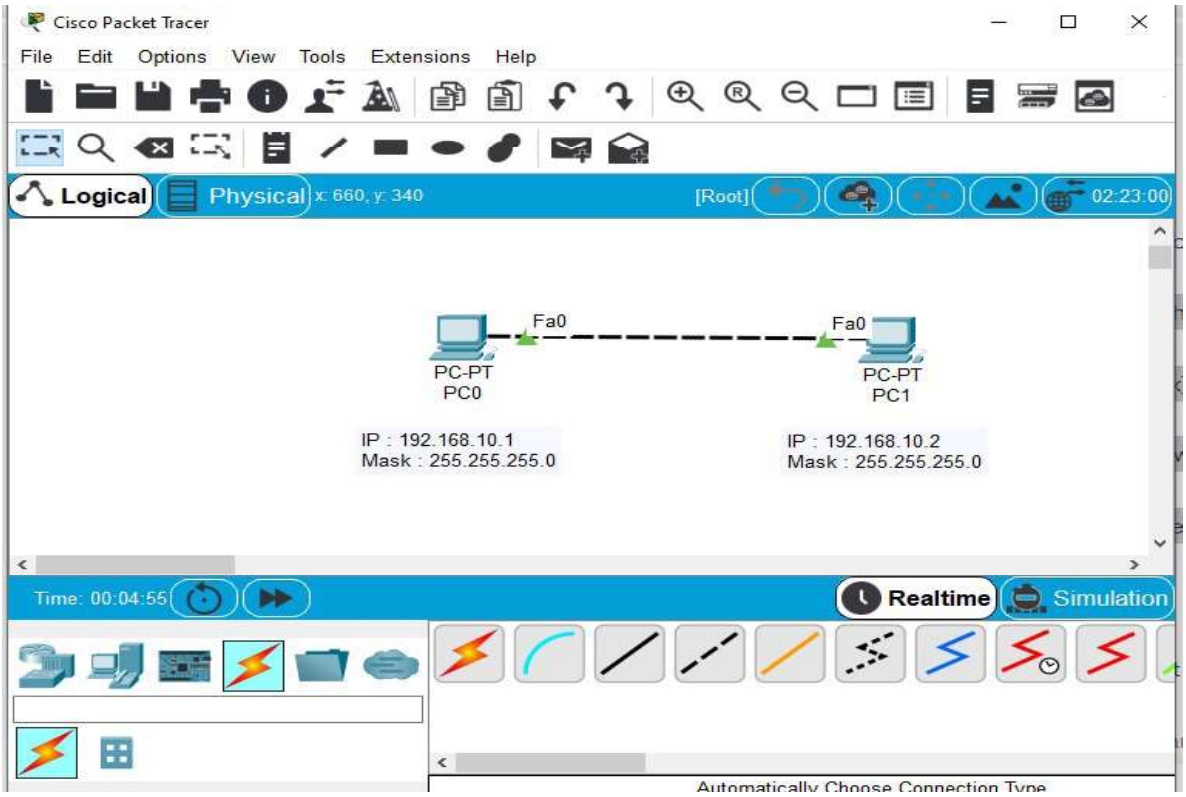
Q5 How do you use the traceroute command to trace the route between your computer and a remote host?

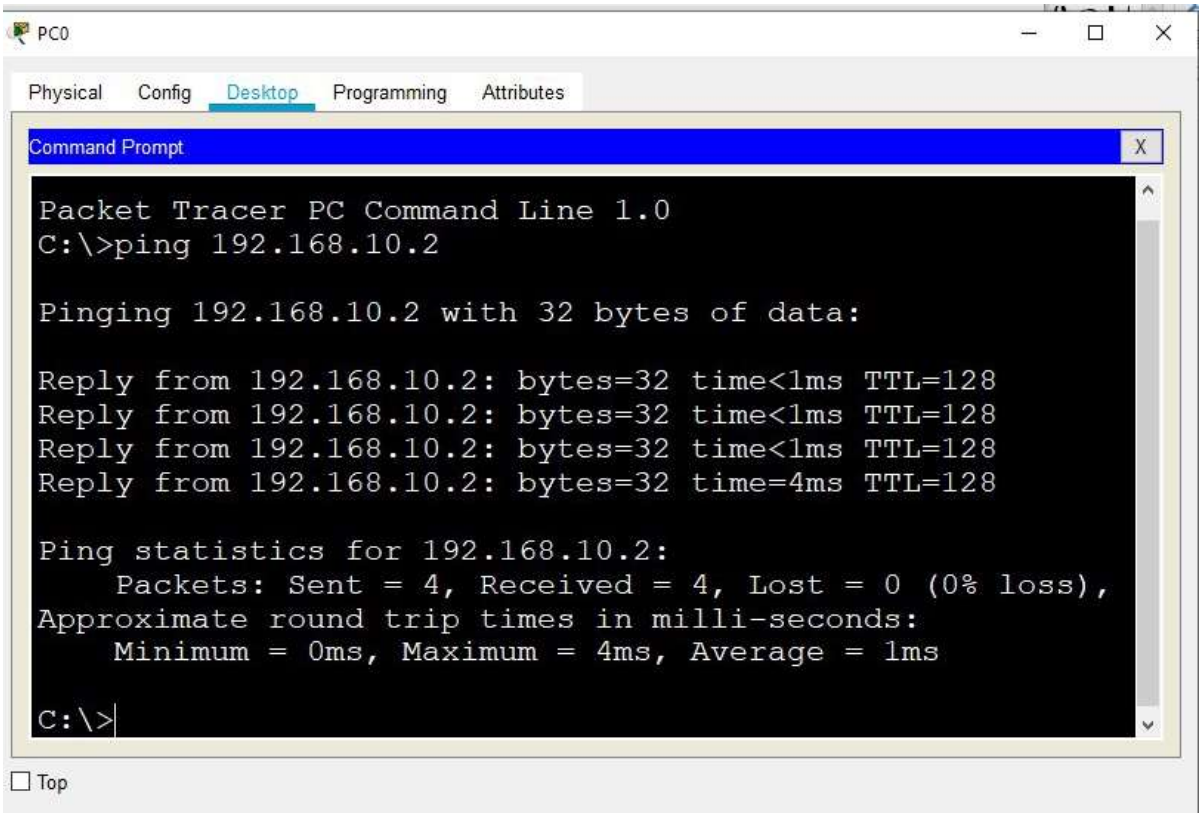
Q6 What information does the traceroute command provide in its output?

Q7 How can you interpret the traceroute command's output to identify network hops and latency?

Q8 Explain the concept of Time to Live (TTL) in relation to the traceroute command.

EXPRIMENT SETUP : Design topology in packet tracer





POST EXPERIMENT QUESTIONS:

Q1 What is the purpose of the ipconfig (Windows) or ifconfig (Unix/Linux) command, and how can it be used to troubleshoot network connectivity issues?

Q2 How do you display the routing table using the route (Windows) or route -n (Unix/Linux) command, and what information does it provide?

Q3 Explain the purpose of the netstat command and how it can be used to view active network connections and listening ports.

Q4 What is the purpose of the arp command, and how can it be used to view or manipulate the ARP (Address Resolution Protocol) cache?

Q5 How do you use the netcat command to test network connectivity and transfer data between devices?

LAB EXPERIMENT 4

OBJECTIVE: Configure and implement a network using Packet Tracer.

a. Creating a First Network
b. Sending Simple Text Messages in Realtime Mode
c. Establishing a Web Server Connection Using the PC's Web Browser

BRIEF DESCRIPTION: The client–server model is a distributed application structure in computing that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server is a host that is running one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.

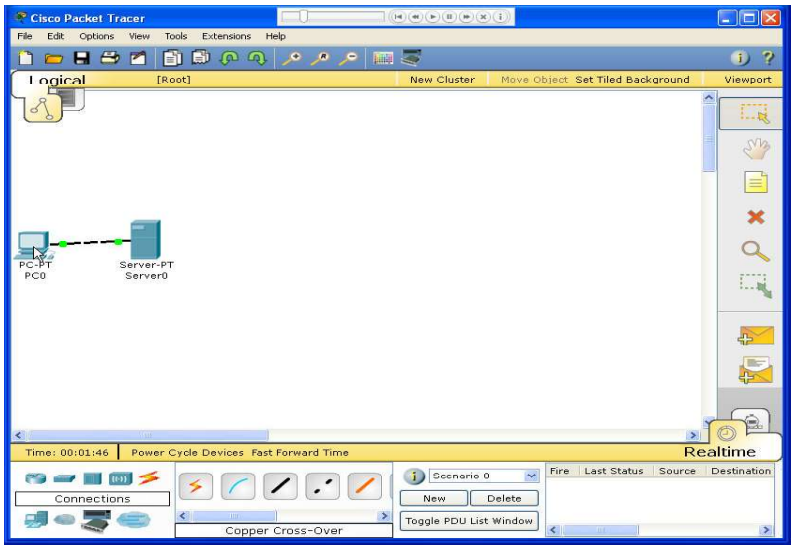
PRE EXPERIMENT QUESTIONS:

Q1 How do you establish connections between devices in Packet Tracer to create a network?
Q2 What are some key considerations when assigning IP addresses to devices in a network?
Q3 What is the purpose of establishing a web server connection using a PC's web browser in Packet Tracer?

STEPS FOR HANDLING NETWORK:

PROGRAM NO – 4 (a)

1. Start creating a network by first selecting the End Devices. Add a Generic PC and a Generic Server to the workspace.
2. Under Connections, select the Copper Straight-through cable (solid black line) and connect the devices with it. The red lights on the link indicate that the connection is not working. Now, use the Delete tool to remove the Copper Straight-through cable, and use a Copper Cross-over cable (dashed line) instead. The lights should turn green at this point. If the mouse pointer is held over either devices, the link status will be shown as "Up." The network should look similar to this:



3. Click on the PC. While paying attention to the link lights, turn the power on, off, and on again. Follow the same steps for the server. The link lights turn red when the device is off. This means that the link is down or is not working. The link lights turn green when the device is turned back on.
4. Try all three ways to learn about the devices. First, mouse over the devices to see basic configuration information about them. Second, click on each device with the Select tool to show the device configuration window, which provides several ways to configure the device. Third, use the Inspect tool to view the tables the network device will build as it learns about the network around it. In this example, open the ARP table. Since the devices have not been configured yet, the ARP tables are empty. Always remember to close the windows after viewing them or they will clutter the workspace.
5. Open the PC configuration window and change the settings using the Config tab. Change the display name to Client and set the DNS server to 192.168.0.105. Under Interface, click FastEthernet and set the IP address as 192.168.0.110. Packet Tracer automatically calculates other parameters. Make sure that the Port Status box is checked. For future reference, note that other Ethernet interface settings, such as bandwidth, duplex, MAC address, and subnet mask can be modified using this window.
6. Go to the Desktop Tab and click on IP Configuration. Notice that the IP address, subnet mask and DNS server can be changed here as well.
7. Open the Server configuration window and go to the Config tab. Change the display name to Web Server. Click FastEthernet and set the IP address as 192.168.0.105. Make sure that the Port Status is also on. Click DNS and set the domain name as www.firstlab.com. Set the IP address as 192.168.0.105 and click Add. Finally, check to make sure that the service for DNS is on.

8. Reposition the network devices by dragging them to a new location. Add a network description by using the "i" button on the upper right corner. Then add some text labels within the Logical Workspace by using the Place Note tool.
9. Load a background grid using the Set Tiled Background button.
10. Save your work using the File > Save As option and create a meaningful filename.

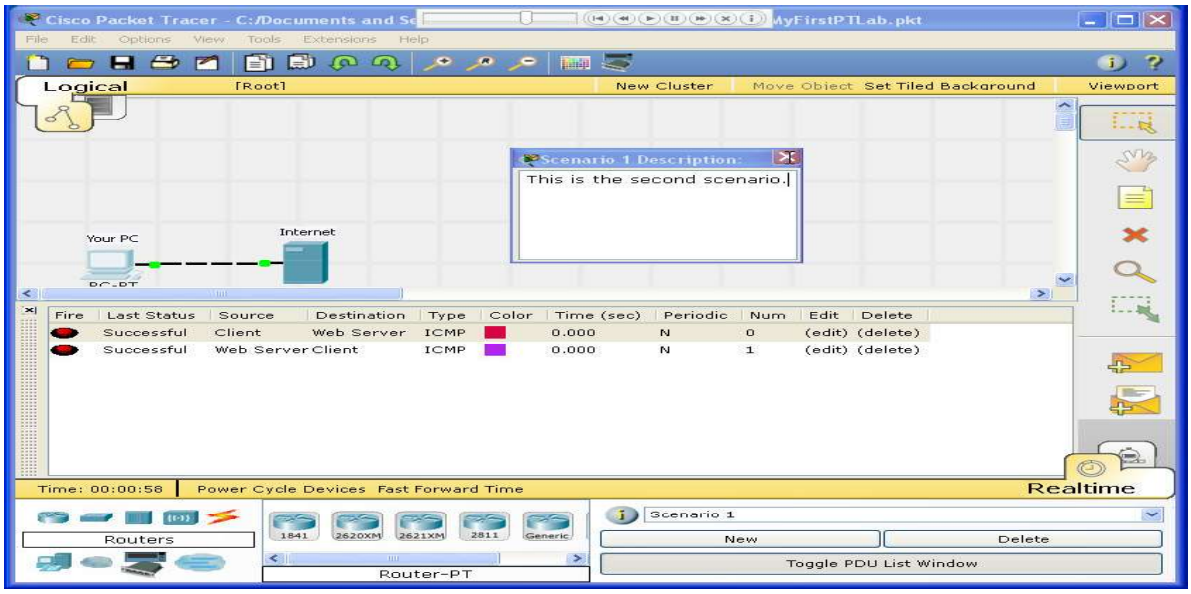
PROGRAM NO – 4 (b)

Aim: Sending Simple Text Messages in Realtime Mode

Objective: This program illustrate the use of Realtime Mode of sending simple text message

Procedure:

1. Start by opening the file saved in the last section.
2. Notice that the file opens in Realtime Mode. Use the Add Simple PDU tool to send a simple one-time ping message, called an echo request, to the server. The server responds with an echo reply because all devices have properly configured IP address settings.
3. Scroll up and down the User Created Packet Window to see the different capabilities of this ping message, including an indication that the ping was successful.
4. Toggle the PDU List Window to see a larger display of this message. One or more of these messages can be saved as a scenario. Scenario 0 is displayed when starting. Label this first scenario with an "i" note. Different scenarios allow the use of the same topology for experiments with different groupings of user created packets.
5. Click New to create a new scenario. New scenarios will initially be blank.
6. Add two packets using the Simple PDU tool, a PDU from the PC to the Server and a different PDU from the Server to the PC. Then add an "i" note describing the scenario, to complete Scenario 1. An example is shown below:



7. Several scenarios can be saved with a single network. Alternate between Scenario 0 and 1.
8. Now, remove Scenario 0 using the Delete button.
9. Scenario 1 is now visible. Go to the last column in the User Created Packet Window and double-click (delete) to remove a PDU.
10. Delete the whole scenario. Notice that the scenario list went back to the default Scenario 0.

PROGRAM NO – 4(c)

Aim: Establishing a Web Server Connection Using the PC's Web Browser

Objective: To study the concept of receiving a web page from server, requested by a client.

Conceptual Background:

The primary function of a web server is to deliver web pages on the request of clients using the Hypertext Transfer Protocol (HTTP). This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets and scripts.

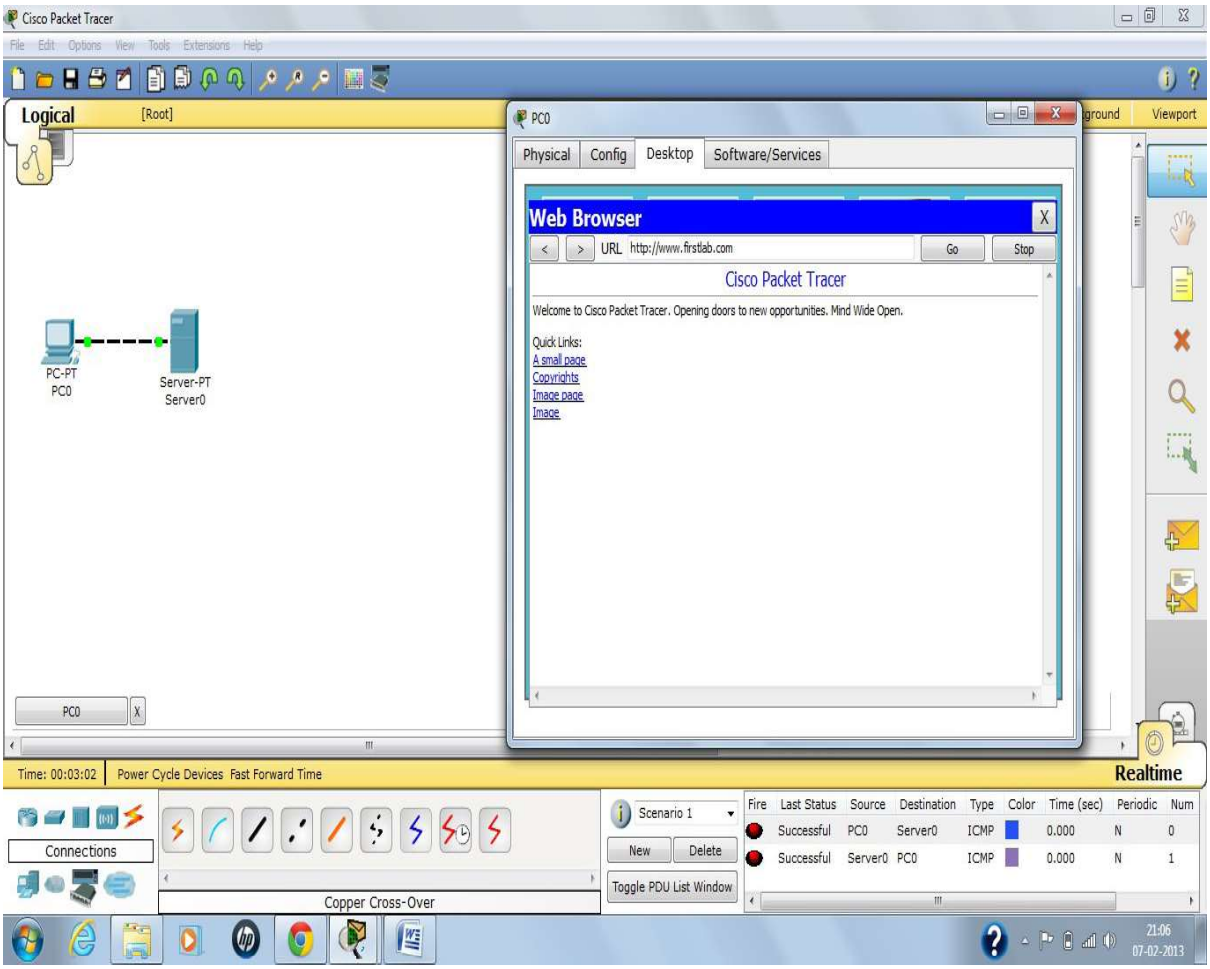
A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if unable to do so. The resource is typically a real file on the server's secondary storage, but this is not necessarily the case and depends on how the web server is implemented.

While the primary function is to serve content, a full implementation of HTTP also includes ways of receiving content from clients. This feature is used for submitting web forms, including uploading of files.

Procedure:

1. Open the file saved from the previous section.

2. Click on the PC to view the configuration window.
3. Select the Desktop tab, and then click Web Browser. Type in www.firstlab.com as the URL and click the Go button. The Packet Tracer welcome page, shown below, appears, indicating that the web connection has been successfully established.
4. Clear the URL, type www and click Go. Since the address entered is not complete, a “Host Name Unresolved” message appears.
5. Type 192.168.0.105 as the URL entry and click on Go. Notice that the Packet Tracer welcome page appears again. This is because the Server IP address can also be used to establish a web connection.
6. Close the window and try the same steps in Simulation Mode. In this mode, the user controls time, so the network can be viewed running at a slower pace, allowing observation of the paths packets take and inspection of packets in detail.
7. Select the PC again and go to the Web Browser in the Desktop tab. Type www.firstlab.com as the URL again and click Go. The welcome page should not appear right away.
8. Switch to the main interface of Packet Tracer without closing the PC configuration window. Notice that a DNS packet is added to the event list.
9. Click Auto Capture/Play or repeatedly click the Capture/Forward button until the HTTP packet appears on the PC. Go back to the PC configuration window. The Packet Tracer welcome page is now shown.
10. Close the PC configuration window.



POST EXPERIMENT QUESTIONS:

Q1 What role does DNS (Domain Name System) play in establishing a connection to a web server, and how is it configured in Packet Tracer?

Q2 What are some common issues that can prevent the PC's web browser from establishing a successful connection to the web server, and how would you troubleshoot them?

LAB EXPERIMENT 5

OBJECTIVE: Configure network devices, such as hubs and switches within a network topology using Packet Tracer software.

BRIEF DESCRIPTION:

ALGORITHM FOR CREATING A TOPOLOGY:

1. Open your Network Topology. Once you've opened your Network Topology on Cisco Packet Tracer, access your network and identify the components of your network, for example; Servers, Routers, End Devices, etc.
2. Complete the cabling. Access the cables section and connect completely and correctly the cables between the networks in order to ensure connectivity between the devices in the network using the connections table given.
3. Using the address table still, correctly and completely configure the IP addresses on all end devices. This can be done by accessing the desktop platform on each device and locating the IP configuration section. The reason for doing this is to enable the devices be on the right network.
4. After configuring the addresses, you will have to test connectivity by opening a command prompt window on the end devices and try pinging the address which the network operates on. If it gives you a reply, it means your network was configured correctly.

The step by procedure of creating Bus topology on Cisco Packet Tracer is shown in Figures 1-6 below

PRE EXPERIMENT QUESTIONS:

Q1. What do you mean by network topology?

Q2. Compare and contrast various different types of network topologies

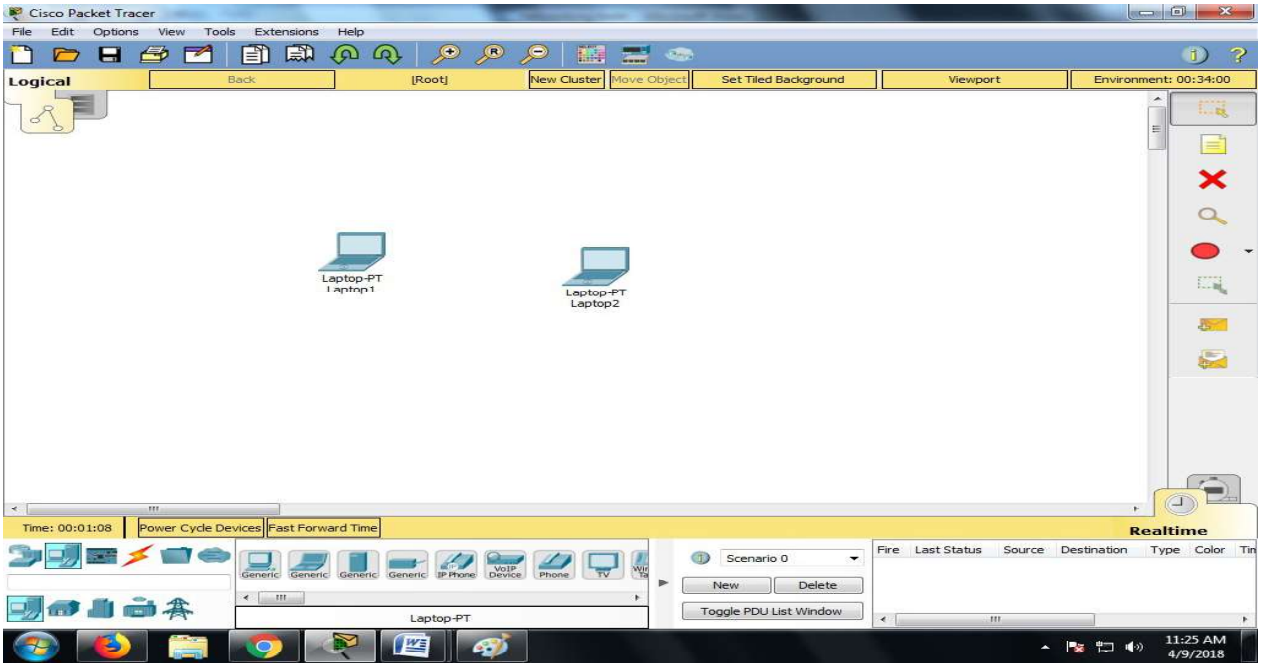


Fig 1: Simulating network devices

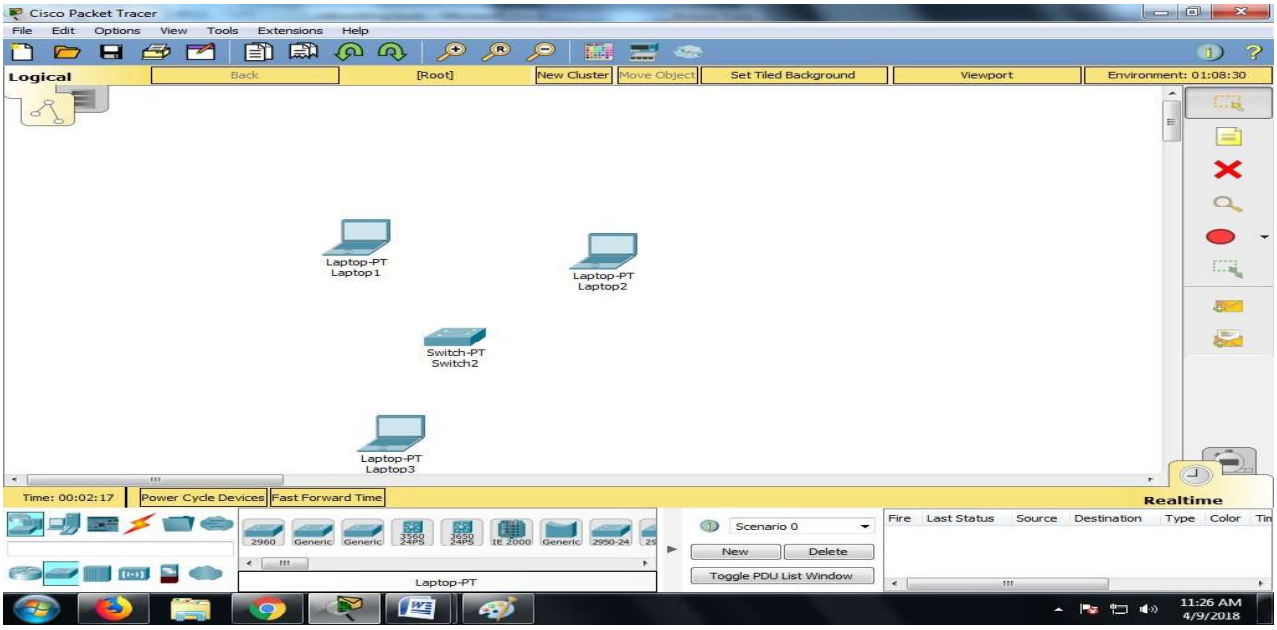


Fig 2: Simulating generic switches

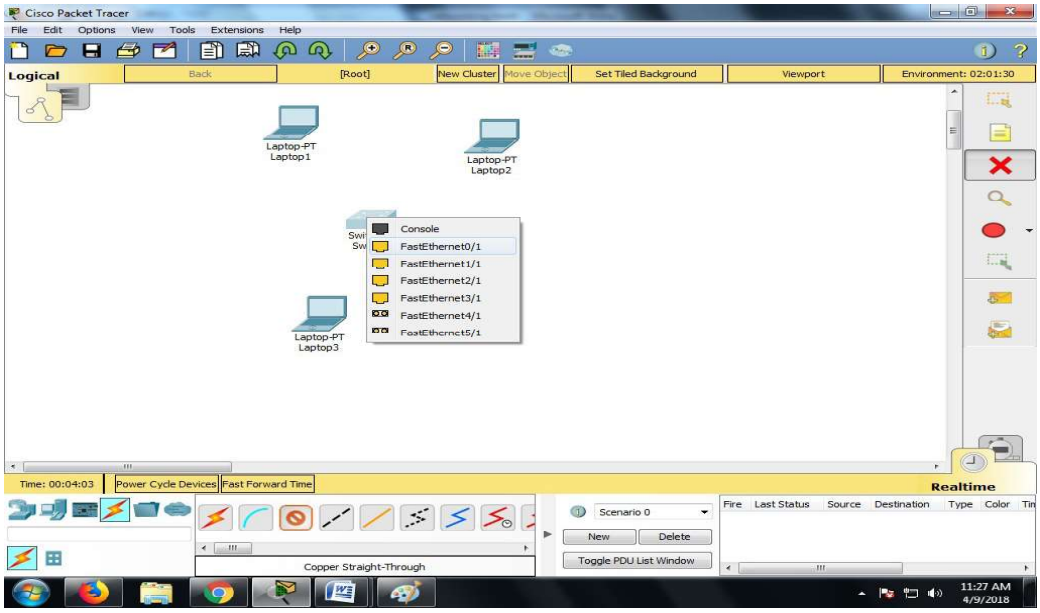


Fig 3: Establish the links between the network devices and generic switches

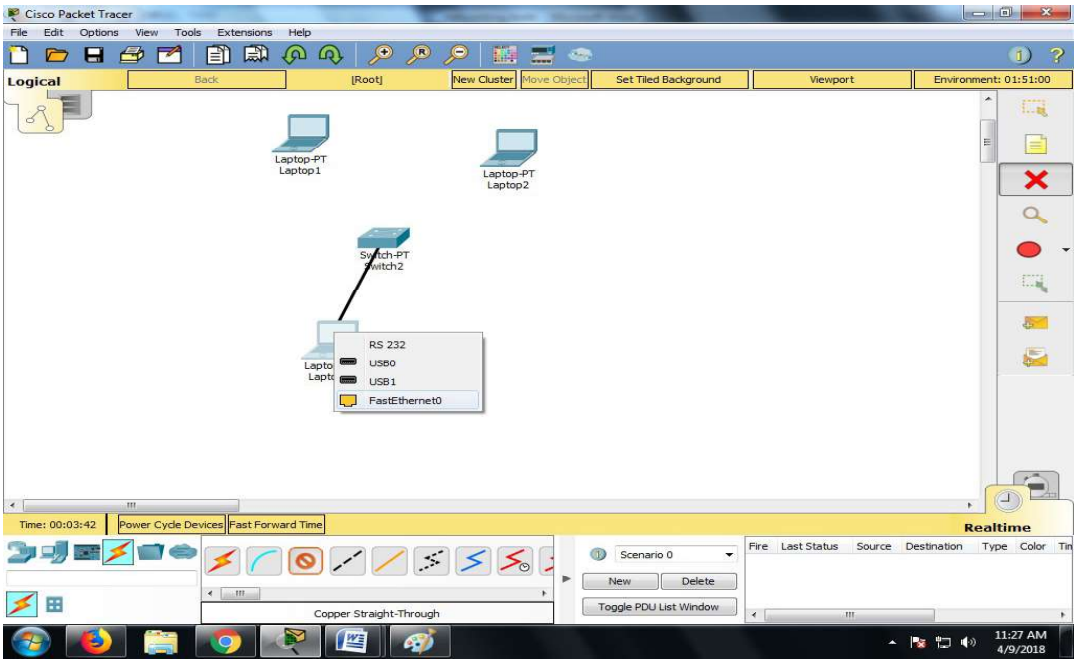


Fig 4: Connect the links

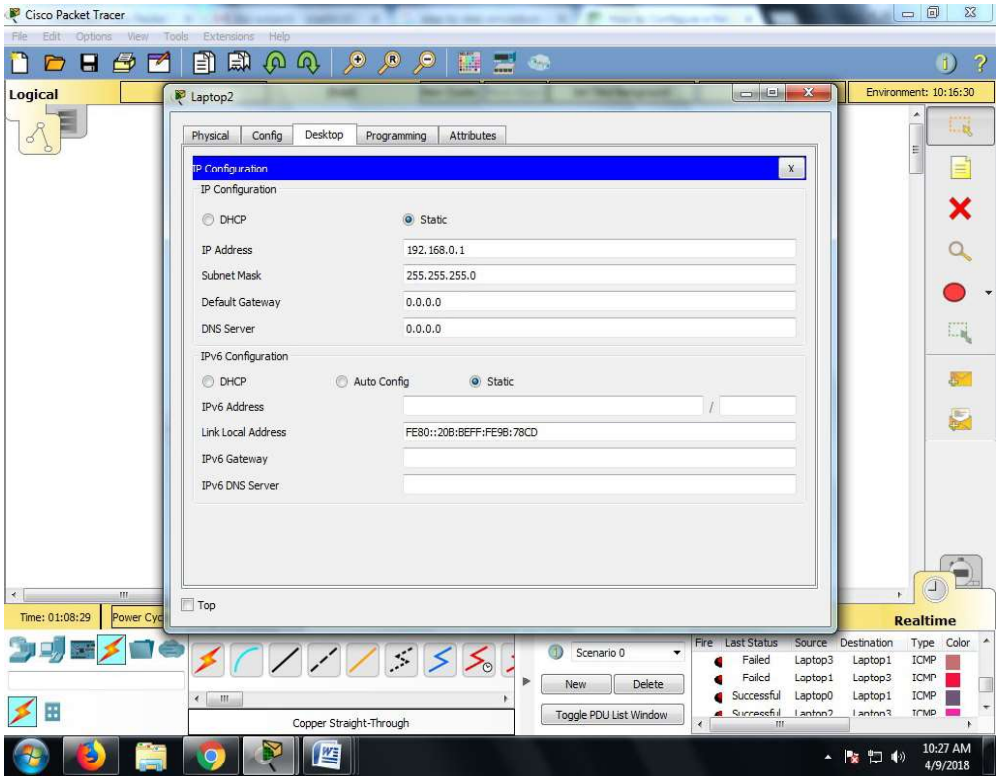


Fig 5: Enter the IP address to each network devices

Bus Topology

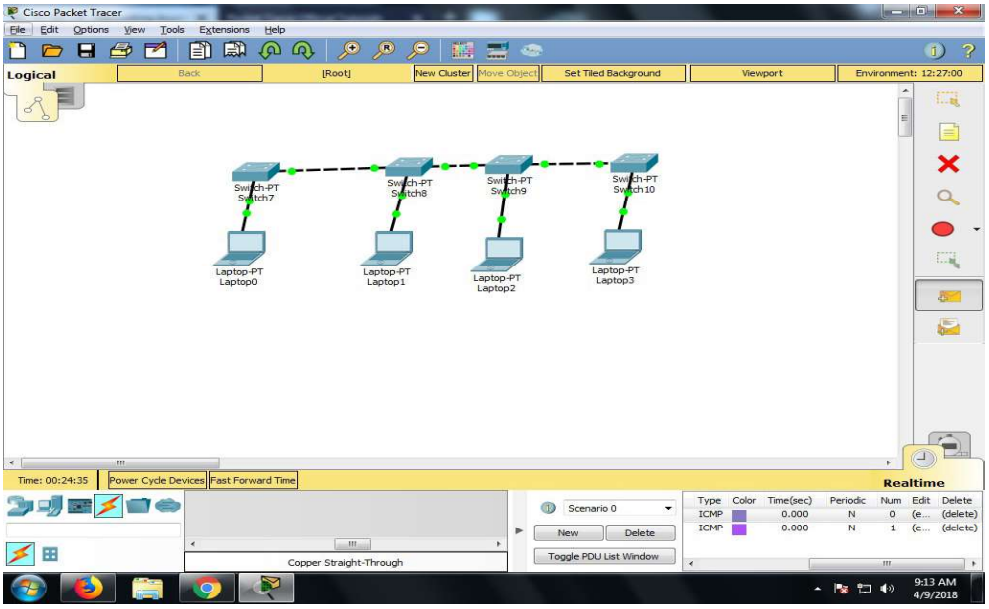


Fig 6: Network devices connected in Bus topology

POST EXPERIMENT QUESTIONS:

Q1. How Repeaters are different form Hubs?

Q2. Mention the different types of network switches and the layer where they are used?

LAB EXPERIMENT 6

OBJECTIVE: Configure network topology to implement VLANs with trunking using Packet Tracer software.

BRIEF DESCRIPTION: the objective is to design and implement a network topology that includes VLANs (Virtual Local Area Networks) using the Packet Tracer software. VLANs allow the logical segmentation of a network, enabling different groups of devices to be grouped together even if they are physically connected to the same switch. Trunking, on the other hand, is used to carry multiple VLAN traffic across a single network link.

STEPS FOR HANDLING NETWORK :

1. Launch Packet Tracer: Start the Packet Tracer software on your computer.
2. Create the network topology: Build the network topology by dragging and dropping the required devices from the device list onto the workspace. Include switches, routers, and PCs as needed.
3. Connect the devices: Connect the devices using appropriate cables. Use Ethernet cables to connect PCs to switches and switches to routers.
4. Configure VLANs: Access the switch's configuration interface by double-clicking on it. Navigate to the VLAN configuration section and create the required VLANs. Assign VLAN IDs and names to each VLAN.
5. Assign ports to VLANs: Assign switch ports to specific VLANs. Determine which ports belong to which VLANs and configure them accordingly. For access ports, assign a single VLAN. For trunk ports, configure them to allow traffic from multiple VLANs.
6. Configure trunking: Identify the trunk links between switches. Access the switch's configuration interface and configure the trunk ports. Enable trunking and specify the allowed VLANs on the trunk links.
7. Verify configurations: Verify that the VLANs and trunking configurations are correctly applied. Check the status of the VLANs and trunk ports to ensure they are active and operational.
8. Test connectivity: Test the connectivity between devices within the VLANs. Ping devices in the same VLAN to ensure communication is successful. Ping devices in different VLANs to verify VLAN isolation.

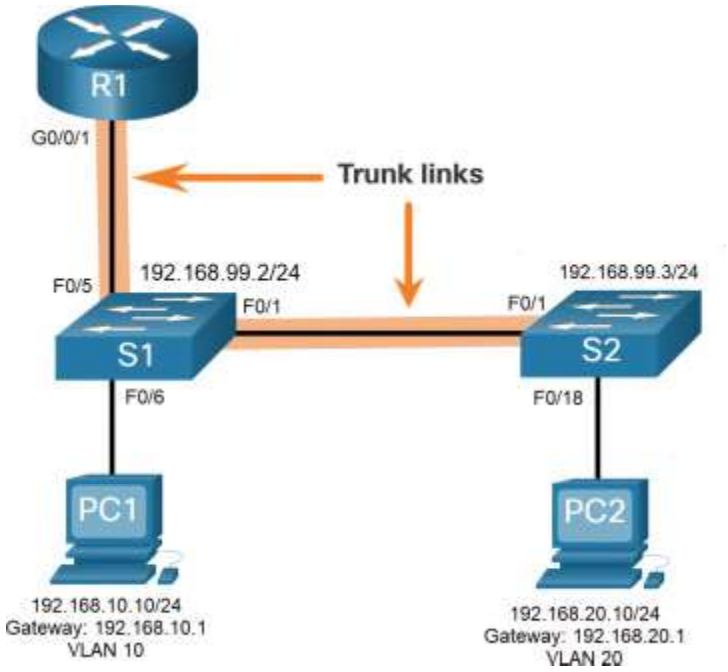
9. Troubleshoot and refine: If there are any connectivity issues or misconfigurations, troubleshoot and refine the configurations. Check VLAN assignments, trunk configurations, and port settings to resolve any problems.
10. Document the configuration: Document the VLAN and trunking configurations for future reference. Include details such as VLAN IDs, names, assigned ports, and trunk configurations.
11. Monitor and maintain: Monitor the network to ensure VLANs and trunking continue to function as expected. Regularly review the configurations and make any necessary adjustments or updates.

PRE EXPERIMENT QUESTIONS:

Q1 What is a VLAN (Virtual Local Area Network), and what are its benefits in a network environment?

Q2 How does VLAN trunking allow for the implementation of VLANs across multiple switches?

EXPRIMENT SETUP : Design topology in packet tracer



In Figure the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.

To route between VLANs, the R1 GigabitEthernet 0/0/1 interface is logically divided into three subinterfaces, as shown in Table. The below table also shows the three VLANs that will be configured on the switches.

G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

Table : Subinterface VLAN IP Address

Step 1 : S1 VLAN and Trunking Configuration

Step 2 : S2 VLAN and Trunking Configuration

Step 3 : R1 Subinterface Configuration

Step 4 : Verify Connectivity Between PC1 and PC2

Step 5 : Router-on-a-Stick Inter-VLAN Routing Verification

POST EXPERIMENT QUESTIONS:

Q1 How can you configure a router to support VLANs and enable communication between different VLANs in Packet Tracer?

Q2 What tools and commands are available in Packet Tracer for monitoring and troubleshooting VLAN-related issues?

LAB EXPERIMENT 7

OBJECTIVE : Configure and implementation of a router within Network using Packet Tracer.

BRIEF DESCRIPTION : In this experiment, participants will learn how to configure a router and connect it to other devices within a network. They will gain hands-on experience in setting up IP addresses, configuring routing protocols, and establishing communication between different networks.

STEPS FOR HANDLING NETWORK HARDWARE:

1. Launch Packet Tracer: Open the Packet Tracer application on your computer.
2. Set up the network topology: Create the network topology by adding devices such as PCs, switches, and the router onto the workspace. Connect the devices using appropriate network cables.
3. Configure IP addresses: Assign IP addresses to each device in the network, including the PCs and the router. Ensure that the IP addresses are within the same subnet.
4. Configure router interfaces: Access the router's configuration interface by double-clicking on it. Configure the IP addresses of the router's interfaces, usually the FastEthernet or GigabitEthernet ports, that connect to other devices in the network.
5. Configure default gateway: Specify the default gateway IP address on the PCs in the network. This should be the IP address of the router interface that connects to the LAN.
6. Verify connectivity: Use the built-in tools in Packet Tracer, such as the Ping or Traceroute commands, to verify connectivity between devices in the network. Test connectivity between the PCs and between the PCs and the router.
7. Test routing functionality: Send network traffic between different subnets connected to the router to ensure that the routing functionality is working correctly. Verify that the router can forward packets between different networks.
8. Implement security measures (optional): Depending on your network requirements, you may want to configure security features such as access control lists (ACLs), firewall rules, or VPN settings on the router.
9. Monitor and troubleshoot: Continuously monitor the network for any issues or errors. If any connectivity or routing problems occur, use Packet Tracer's debugging tools, such as examining routing tables or interface statuses, to troubleshoot and resolve the issues.

10. Document the configuration: Document the router's configuration settings, including IP addresses, routing protocols, and any security measures implemented. This documentation will serve as a reference for future troubleshooting or network expansion.

PRE EXPERIMENT QUESTIONS:

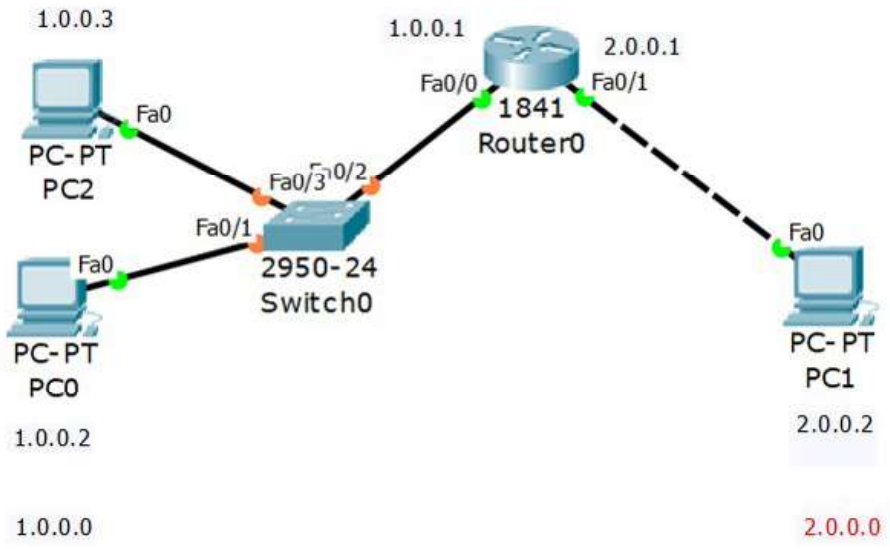
Q1 What is the purpose of a router in a network?

Q2 What are the key components of a router and their functions?

Q3 How does a router differ from a switch in terms of functionality?

Q4 What is the role of routing protocols in a router, and how do they facilitate communication between networks?

EXPRIMENT SETUP :



Configuration on Router:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#host satish
satish(config)#int fa0/0
satish(config-if)#ip address 1.0.0.1 255.0.0.0

satish(config-if)#no shut

satish(config-if)#exit
satish(config)#int fa0/1
satish(config-if)#ip add 2.0.0.1 255.0.0.0
satish(config-if)#no shut
```

POST EXPERIMENT QUESTIONS:

Q1 How do you secure a router's configuration in Packet Tracer, and what are some best practices for router security?

Q2 Explain the concept of network address translation (NAT) and how it can be configured in a router using Packet Tracer.

LAB EXPERIMENT 8

OBJECTIVE : Configure network topology and implement static routing using Packet Tracer Software.

BRIEF DESCRIPTION : In this experiment, the objective is to design and configure a network topology using Packet Tracer software. The network will consist of multiple devices such as routers, switches, and PCs, connected in a specific arrangement. The experiment will focus on implementing static routing within the network. Static routing involves manually configuring the routing tables on the routers, specifying the next hop for each destination network. This allows for explicit control over the network traffic flow.

STEPS FOR HANDLING NETWORK :

1. Design the Network Topology:
    - Identify the devices required for your network, such as routers, switches, and PCs.
    - Determine the logical layout of your network, including the IP addressing scheme for each subnet.
    - Use Packet Tracer's device palette to drag and drop the necessary devices onto the workspace.
    - Connect the devices using appropriate cables and configure their interfaces with IP addresses.
2. Configure IP Addresses:
    - Access the CLI (Command Line Interface) of each device (e.g., router or PC) in Packet Tracer.
    - Configure the IP addresses for the interfaces of each device according to the logical layout you designed.
    - Use the "ip address" command followed by the desired IP address and subnet mask to assign IP addresses to the interfaces.
3. Enable Routing:
    - Determine the routing protocol or method you want to use (in this case, static routing).
    - Access the CLI of each router in Packet Tracer.
    - Configure static routes on each router to direct traffic to the appropriate destination networks.

- Use the "ip route" command followed by the destination network address, subnet mask, and next-hop router's IP address to configure static routes.

4. Verify Connectivity:
    - Use Packet Tracer's simulation mode to test network connectivity.
    - Ping from one device to another to verify that the static routes are correctly configured.
    - Ensure that the ICMP (Internet Control Message Protocol) traffic is allowed through any firewalls or security features on the devices.
5. Monitor and Troubleshoot:
    - Monitor the network for any issues or errors.
    - If any connectivity or routing problems arise, use Packet Tracer's logging and debugging features to troubleshoot.
    - Check the routing tables on each router to ensure that the correct static routes are present.
6. Document the Configuration:
    - Document the network topology, including the IP addresses assigned to each device and the configured static routes.
    - Take screenshots or export the configuration files from Packet Tracer for reference purposes.

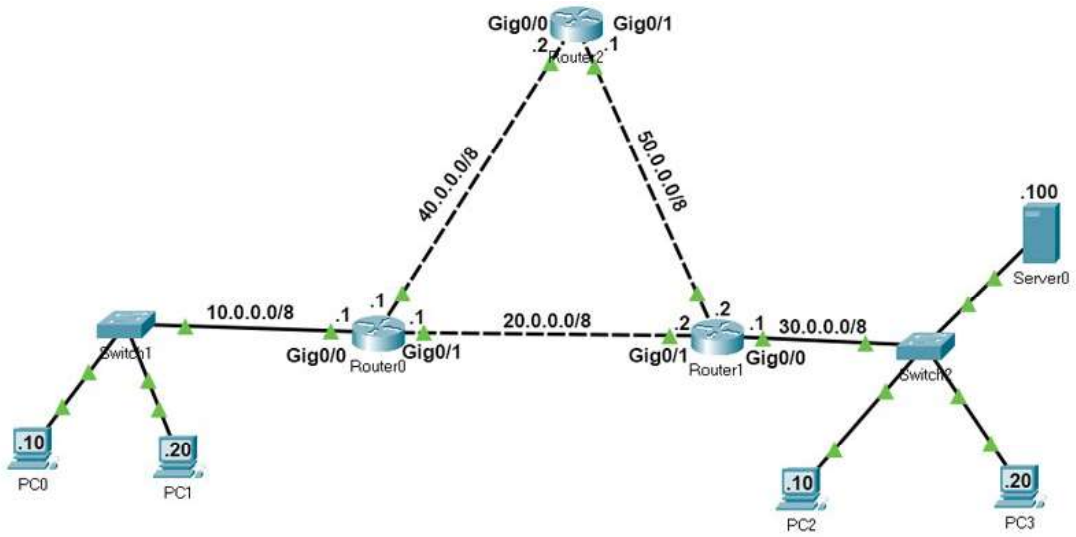
PRE EXPERIMENT QUESTIONS:

Q1 Explain the process of configuring static routes in Packet Tracer.

Q2 How can you verify the successful implementation of static routes in Packet Tracer?

Q3 What are some common issues that can occur when configuring network topology and implementing static routing, and how would you troubleshoot them?

EXPRIMENT SETUP : Design network topology



In this lab, each network has two routes to reach. We will configure one route as the main route and another route as the backup route. If the link bandwidth of all routes is the same, we use the route that has the least number of routers as the main route. If the link bandwidth and the number of routers are the same, we can use any route as the main route and another route as the backup route.

If we specify two routes for the same destination, the router automatically selects the best route for the destination and adds the route to the routing table. If you manually want to select a route that the router should add to the routing table, you have to set the AD value of the route lower than other routes. For example, if you use the following commands to create two static routes for network 30.0.0/8, the route will place the first route to the routing table.

```
#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10
#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20
```

Creating, adding, verifying static routes :

Routers automatically learn their connected networks. We only need to add routes for the networks that are not available on the router's interfaces. For example, network 10.0.0.0/8, 20.0.0.0/8 and 40.0.0.0/8 are directly connected to Router0. Thus, we don't need to configure routes for these networks. Network 30.0.0.0/8 and network 50.0.0.0/8 are not available on Router0. We have to create and add routes only for these networks.

The following table lists the connected networks of each router.

Router	Available networks on local interfaces	Networks available on other routers' interfaces
Router0	10.0.0.0/8, 20.0.0.0/8, 40.0.0.0/8	30.0.0.0/8, 50.0.0.0/8
Router1	20.0.0.0/8, 30.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 40.0.0.0/8
Router2	40.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 20.0.0.0/8, 30.0.0.0/8

Router1 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 10.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 40.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#exit
Router#show ip route static
S 10.0.0.0/8 [10/0] via 20.0.0.1
S 40.0.0.0/8 [10/0] via 20.0.0.1
Router#
```

Router2 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 40.0.0.1
Router(config)#ip route 30.0.0.0 255.0.0.0 50.0.0.2
Router(config)#exit
Router#show ip route static
S 10.0.0.0/8 [1/0] via 40.0.0.1
S 30.0.0.0/8 [1/0] via 50.0.0.2
Router#
```

POST EXPERIMENT QUESTIONS:

Q1 Explain the concept of default routes and how they can be configured in Packet Tracer.

Q2 How does packet forwarding occur in a network with static routing, and how can you visualize this process in Packet Tracer?

Q3 Describe a scenario where you would choose to implement static routing instead of a dynamic routing protocol, and explain your reasoning.

LAB EXPERIMENT 9

OBJECTIVE : Configure network topology and implement dynamic routing protocol such as RIP, OSPF etc. using Packet Tracer.

BRIEF DESCRIPTION : In this experiment, the objective is to simulate and configure a network topology using Packet Tracer, a network simulation tool. The focus is on implementing dynamic routing protocols like RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) within the network.

STEPS FOR HANDLING NETWORK :

1. Understand the Experiment Requirements:
    - Read and familiarize yourself with the experiment guidelines, objectives, and requirements.
    - Ensure you have a clear understanding of the network topology and the dynamic routing protocol to be implemented (RIP, OSPF, etc.).
    - Take note of any specific configurations or settings mentioned in the experiment instructions.
2. Launch Packet Tracer:
    - Open Packet Tracer on your computer.
    - If required, create a new project or load the existing project provided for the experiment.
3. Design the Network Topology:
    - Use the Packet Tracer workspace to design the network topology based on the experiment requirements.
    - Place the required devices such as routers, switches, and PCs onto the workspace.
    - Connect the devices using appropriate network cables to establish the desired network connectivity.
4. Configure IP Addresses:
    - Assign IP addresses to the interfaces of the devices in the network.
    - Ensure that each device has a unique IP address within the same network segment.
    - Verify the connectivity between devices using basic connectivity tests or the "ping" command.

5. Implement Dynamic Routing Protocol:
    - Choose the dynamic routing protocol to be implemented (RIP, OSPF, etc.).
    - Configure the routers to enable the chosen routing protocol on their interfaces.
    - Set up the necessary parameters for the routing protocol, such as network addresses, timers, and authentication if required.
6. Verify Routing Protocol Functionality:
    - Check the routing tables on the routers to ensure that they have learned the network routes correctly.
    - Use commands like "show ip route" or "show ip ospf database" to verify the routing information.
    - Perform connectivity tests between devices to verify that routing is functioning as expected.
7. Test Network Resilience and Adaptability:
    - Introduce changes to the network topology, such as adding or removing links or devices.
    - Observe how the dynamic routing protocol adapts to the changes and updates the routing tables accordingly.
    - Verify that devices can still communicate and that the routing protocol successfully adjusts to the network changes.
8. Document and Analyze Results:
    - Record the configurations made, including IP addresses, routing protocol settings, and any additional configurations.
    - Document the observed behavior of the network, including any issues or unexpected outcomes.
    - Analyze the results to ensure that the network topology is functioning correctly and the dynamic routing protocol is operating as intended.
9. Troubleshooting (if necessary):
    - If any issues arise during the experiment, troubleshoot the network to identify and resolve the problems.
    - Use debugging tools, log files, and relevant commands to investigate and troubleshoot the network connectivity or routing issues.
10. Finalize the Experiment:

- Summarize the experiment results and findings in a report or as instructed by the experiment guidelines.
- Review the configurations, documentation, and analysis to ensure accuracy and completeness.

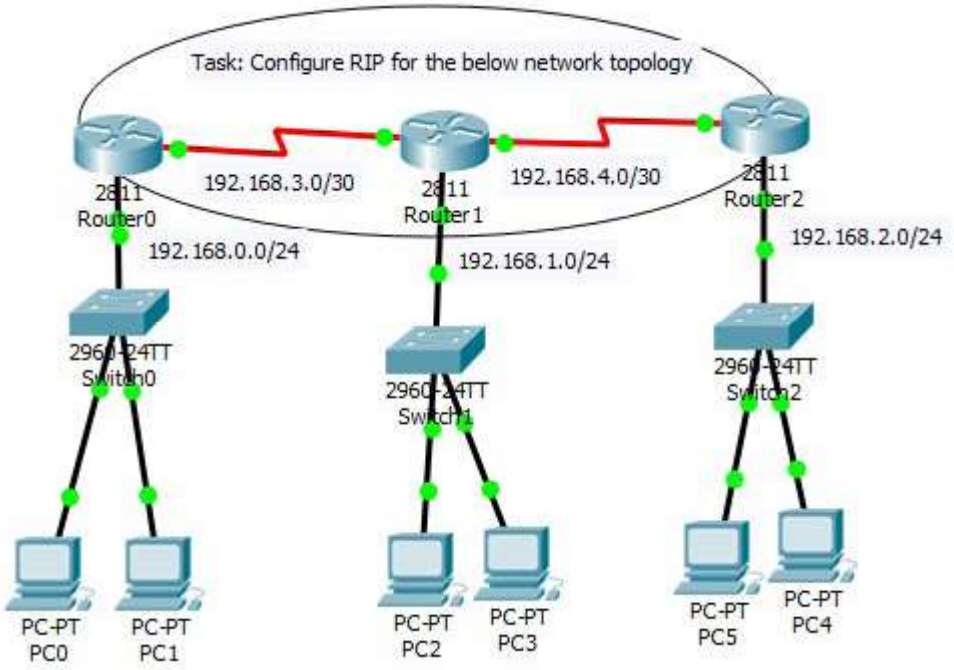
PRE EXPERIMENT QUESTIONS:

Q1 What is the purpose of implementing a dynamic routing protocol in a network?

Q2 Explain the concept of routing and why it is essential for communication between networks.

Q3 What are the key differences between static routing and dynamic routing protocols?

EXPRIMENT SETUP : Design network topology



Router0 Configuration :

```
Router>en
Router#conf t
Router(config)#hostname Router0
Router0(config)#int s0/3/0
Router0(config-if)#ip add 192.168.3.1 255.255.255.252
```

```
Router0(config-if)#no shut
Router0(config-if)#desc connection to Router1
Router0(config-if)#int f0/0
Router0(config-if)#ip add 192.168.0.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#desc connection to LAN
Router0(config-if)#exit
Router0(config)#router RIP
Router0(config-router)#netw 192.168.0.0
Router0(config-router)#netw 192.168.3.0
Router0(config-router)#no auto
Router0(config-router)#exit
Router0(config)#exit
Router0#copy run start
```

Router1 Configuration :

```
Router>en
Router#conf t
Router(config)#hostname Router1
Router1(config)#int s0/3/0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip add 192.168.3.2 255.255.255.252
Router1(config-if)#no shut
Router1(config-if)#desc connection to Router0
Router1(config-if)#int s0/2/0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip add 192.168.4.1 255.255.255.252
Router1(config-if)#no shut
Router1(config-if)#desc connection to Router2
Router1(config-if)#int f0/0
Router1(config-if)#ip add 192.168.1.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#desc connection to LAN
Router1(config-if)#exit
Router1(config)#router RIP
Router1(config-router)#netw 192.168.1.0
Router1(config-router)#netw 192.168.3.0
Router1(config-router)#netw 192.168.4.0
Router1(config-router)#no auto
Router1(config-router)#exit
Router1(config)#exit
Router1#copy run start
```

Router2 Configuration :

```
Router>en
Router#conf t
Router(config)#hostname Router0
Router2(config)#int s0/3/0
Router2(config-if)#ip add 192.168.4.2 255.255.255.252
Router2(config-if)#no shut
Router2(config-if)#desc connection to Router1
Router2(config-if)#int f0/0
Router2(config-if)#ip add 192.168.2.1 255.255.255.0
Router2(config-if)#no shut
Router2(config-if)#desc connection to LAN
Router2(config-if)#exit
```

```
Router2(config)#router RIP
Router2(config-router)#netw 192.168.4.0
Router2(config-router)#netw 192.168.2.0
Router2(config-router)#no auto
Router2(config-router)#exit
Router2(config)#exit
Router2#copy run start
```

POST EXPERIMENT QUESTIONS:

Q1 How can you prioritize specific routes or control the routing behavior in a dynamic routing protocol configuration in Packet Tracer?

Q2 Describe a scenario where you encountered a complex network topology with multiple routers and implemented a dynamic routing protocol successfully. Explain the steps you took and the challenges you faced.

LAB EXPERIMENT 10

OBJECTIVE : Configure a network and implement remote login of router and Management using Packet Trace

BRIEF DESCRIPTION : The objective of this experiment is to set up a network using Packet Tracer and configure remote login access to a router for management purposes. This experiment focuses on enabling secure remote access to the router using protocols such as SSH (Secure Shell) and Telnet. Additionally, it involves configuring management features like SNMP (Simple Network Management Protocol) to monitor and manage the network devices remotely.

STEPS FOR HANDLING NETWORK :

1. Design the network topology: Start by designing the network topology using Packet Tracer. Determine the number and types of devices required, such as routers, switches, and PCs. Connect the devices appropriately to create the desired network structure.
2. Configure router interfaces: Access the router's CLI (Command Line Interface) in Packet Tracer. Configure the IP addresses and subnet masks on the router's interfaces to enable communication with other devices in the network.
3. Enable remote login protocols: In the router's CLI, enable remote login protocols such as Telnet or SSH (Secure Shell). This will allow you to remotely access and manage the router from other devices.
4. Configure access credentials: Set up username and password authentication for remote login. Create a username and password combination to ensure secure access to the router.
5. Configure IP addressing on PCs: Set the IP addresses on the PCs connected to the network. Ensure that the PCs are on the same subnet as the router interfaces to establish communication.
6. Test remote login: From one of the PCs, open a terminal or command prompt and attempt to remotely log in to the router using Telnet or SSH. Use the router's IP address and the configured username and password. Verify that remote login is successful and that you can access the router's CLI remotely.
7. Implement remote management features: Utilize Packet Tracer's remote management features to perform various tasks on the router, such as configuring routing protocols, setting up VLANs, or implementing access control lists (ACLs). Use the appropriate commands in the router's CLI to configure and manage these features.

8. Test remote management functionality: After configuring specific features on the router, test their functionality remotely. Verify that the changes made through remote management are properly implemented and functional.
9. Monitor and troubleshoot: Utilize Packet Tracer's monitoring tools, such as the device console, to monitor the router's status, logs, and debug information. Use these tools to troubleshoot any connectivity issues, configuration errors, or other problems that may arise.
10. Document the configuration: Document the entire network configuration, including the router's remote login settings, management features, and any additional configurations made. This documentation will serve as a reference for future maintenance, troubleshooting, or replication of the network setup.

PRE EXPERIMENT QUESTIONS :

Q1 What is the purpose of remote login and management in network configuration?

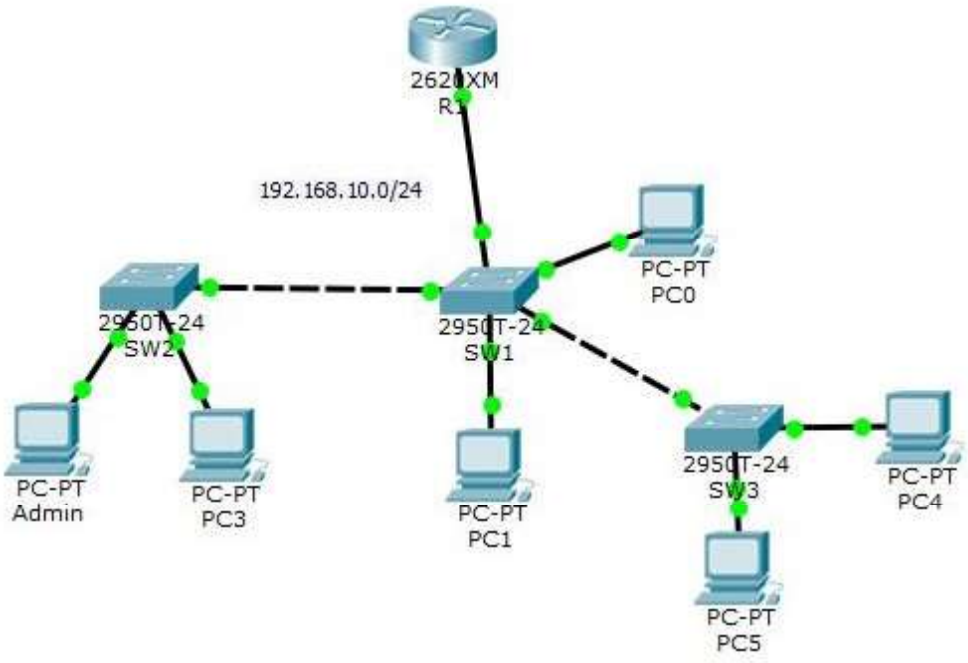
Q2 Explain the concept of remote login and how it enables access to a router from a remote location.

Q3 What are the different protocols commonly used for remote login and management of routers?

Q4 Describe the steps involved in configuring a network using Packet Tracer.

Q5 How do you enable remote login functionality on a router in Packet Tracer?

EXPRIMENT SETUP :



Enable Telnet and SSH on Cisco Router

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0
R1(config-line)#password Pass123
R1(config-line)#login
R1(config-line)#logging synchronous 
R1(config-line)#exec-timeout 40
R1(config-line)#motd banner $Admin Access Only$
R1(config-line)#exit
R1(config)#
```

- The "**line vty**" command enable the telnet and the "**0″** is just let a single line or session to the router. If you need more session simultaneously, you must type "**line vty 0 10**".
- The "**password**" command set the "**Pass123**" as a password for telnet. You can set your own password.
- The "**login**" command authenticate and ask you the password of telnet. If you type "**no login**" command, the telnet never authenticates for the password which is not a good practice in a real network environment.

- The "**logging synchronous**" command stops any message output from splitting your typing.
- The "**exec-timeout"** command just sets the time-out limit on the line from the default to "**40″** minutes.
- The **motd-banner** forces a banner message to appear when logging in.

```
R1(config)#enable password Password
R1(config)#exit
```

POST EXPERIMENT QUESTIONS:

Q1 How do you enable secure remote login using protocols like SSH (Secure Shell) in Packet Tracer?

Q2 What are the advantages of using secure remote login protocols compared to unsecured protocols like Telnet?

LAB EXPERIMENT 11

OBJECTIVE : Configure DHCP Server in the Network using packet tracer software.

BRIEF DESCRIPTION : The objective of this experiment is to configure a DHCP (Dynamic Host Configuration Protocol) server in a network using the Packet Tracer software. DHCP allows for automatic and centralized IP address assignment to network devices, simplifying network administration and reducing the chances of address conflicts.

STEPS FOR HANDLING NETWORK :

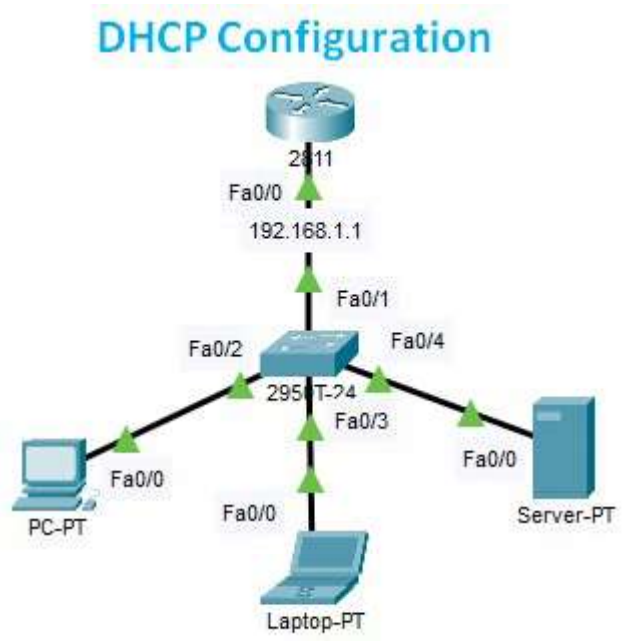
1. Launch Packet Tracer: Open the Packet Tracer software on your computer.
2. Create the Network Topology: Set up the network topology by adding the necessary devices such as routers, switches, and PCs. Connect them appropriately using Ethernet cables.
3. Configure IP addresses: Assign IP addresses to each device in the network manually or using a static IP address assignment.
4. Add and Configure DHCP Server: Select a router or a dedicated server device in the network where you want to configure the DHCP server. Right-click on the device and select "Config" to enter the device's configuration mode.
5. Access Global Configuration Mode: In the device configuration mode, enter the global configuration mode by typing the command "enable" and then "configure terminal" to access the router's or server's global configuration settings.
6. Enable DHCP Service: Type the command "service dhcp" to enable the DHCP service on the device.
7. Configure DHCP Pool: Define a DHCP pool by typing the command "ip dhcp pool [pool name]" and press Enter. Replace [pool name] with a name of your choice for the pool.
8. Set IP Address Range: Specify the range of IP addresses that the DHCP server can assign to devices in the network. Use the command "network [network address] [subnet mask]" to define the network address and subnet mask for the pool. For example, "network 192.168.1.0 255.255.255.0".
9. Configure Default Gateway: Set the default gateway for the devices in the network by using the command "default-router [gateway IP address]". Specify the IP address of the default gateway or router that provides access to other networks.

10. Set DNS Server: Specify the DNS (Domain Name System) server address that will be provided to the devices by using the command "dns-server [DNS server IP address]". Enter the IP address of the DNS server that devices should use for name resolution.
11. Set Lease Duration: Define the lease duration for IP addresses assigned by the DHCP server using the command "lease [duration]". Specify the desired duration in hours, days, or other time units. For example, "lease 24".
12. Exit Configuration Mode: Once you have completed the DHCP server configuration, exit the device configuration mode by typing the command "exit" until you return to the user mode.
13. Save Configuration: Save the configuration changes by typing the command "copy running-config startup-config" to ensure that the configuration is persistent even after restarting the network simulation.
14. Test DHCP Configuration: Start the simulation in Packet Tracer and verify that the DHCP server is functioning correctly by checking if the devices connected to the network are assigned IP addresses automatically.

PRE EXPERIMENT QUESTIONS:

1. What information does a DHCP server provide to client devices in a network?
2. How do you assign and configure IP address ranges for DHCP clients using Packet Tracer?
3. Explain the process of configuring lease durations for IP addresses assigned by the DHCP server in Packet Tracer.
4. What are some additional DHCP options that can be configured in Packet Tracer, such as default gateway, DNS servers, and domain name?

EXPRIMENT SETUP :



POST EXPERIMENT QUESTIONS :

1. How do you monitor and analyze the DHCP server's performance and utilization in Packet Tracer?
2. Explain the concept of DHCP relay and how it can be configured in Packet Tracer to support DHCP requests across multiple networks.
3. How can you configure reservations or static IP assignments for specific devices in a DHCP server using Packet Tracer?

This lab manual has been prepared by

Prof. Hansraj
(hansraj@ggnindia.dronacharya.info)

Crosschecked By
HOD CSE

Please spare some time to provide your valuable feedback