LAB MANUAL

Computer Networks Lab

(CIC – 355)

B.Tech Programme
(CSE)

Maharaja Surajmal Institute of Technology
Affiliated: GGSIP University
C-4, Janak Puri, New Delhi - 110058

CONTENTS

Chapter 1

Introduction

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless. As computer networks have increased in number and size, moreover computer networks are used almost everywhere because of various benefits of computer networks, like file sharing, printer sharing, internet connection sharing, multi-player gaming, internet telephone services, entertainment etc. thus it is important to understand the basic concepts of computer networks. Packet Tracer is virtual networking simulation software developed by CISCO, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student can interact with various networking devices, by customizing the configurations, by turning them on and off etc. Packet Tracer is teaching and learning software and a tool, easy to work with, thus after working with virtual environment, a student gains lot of confidence, when it comes to working in real-time environment. We can track the path of a packet, when it moves from source to destination, and also learn and understand, how to troubleshoot a network, when a packet doesn't reach the destination. Packet Tracer can be used to learn concepts more clearly by creating different scenarios. Since Networking is all about imagination and it's difficult to track movement of packets in a real-time environment, thus various networking concepts can be explained by creating a virtual environment, showing the moment of packets, exactly as it would happen in real-time. Packet tracer can be used to understand the working of various networking devices, their use, what makes them different and their appropriate use in a designing a network. Packet tracer is a user friendly tool, with various options, where a user can customize and design a network. Various tests can be run, to understand various network failures and how to troubleshoot them in real-time. CISCO stands for commercial and industrial security corporation. CISCO is the global leader in IT and networking. CISCO primarily provides networking-related assistance for companies of all sizes and helps them to connect, interact, and collaborate. The CISCO packet tracker was developed by the CISCO Company. It is a type of tool that provides the simulator to practice simple and complex networks. The main purpose of the CISCO pocket tracker is to help the student for the purpose of learning hand on experience in networking. It also provides specific skills for CISCO technology. This tool cannot replace the router or switch because this software has some inbuilt protocol. The

interesting thing is that this device has not only the CISCO product but also it has some inbuilt networking support. This tool also facilitates some technical concepts like CCENT and CCNA, where the packet utilizes all the technical concepts and networking systems. This packet also helps the student to complete their assignment by working on their own or working with a team. It also helps the engineer to test their application before implementing them. Also, the engineers who work on network support can also deploy any changes also use the CISCO packet. First, the engineers test the changes they want to make. Then if all the changes worked perfectly, the packet proceeded toward deployment of the test. With the help of this packet tracker, it is very easier for all the engineers to add or remove any simulated network devices. We can perform these operations in two steps. One is drag and drop user interface, and another is the command line interface. The main purpose of CISCO Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop CISCO technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches.

Features of CISCO Packet Tracker

There are some features that are provided by the CISCO packet tracker. These are as follows:
CISCO packet tracker supports the multi-user system that allows any user to connect in different topologies across different computer networks. By using this feature, the teacher assigns different tasks to different students.
We can also remove the capabilities of the CISCO packet tracker with the help of an API. This feature is also provided by the CISCO packet tracker.
We can also remove the special features like accessibility, gaming, assessment delivery, and interaction with the real world from the CISCO packet tracker.
We can download this from the Netacad account for free of cost.
We can also simulate the configuration related to routers, and this can be accessed anywhere.
We can access this configuration with unlimited devices.
It also provides a self-placed and interactive environment.
The Enhanced Physical Mode transports you to a virtual lab where you can simulate cabling devices on a rack. Refresh key skills such as device placement (Rack & Stack), on-device power switching, device port-to-port cabling (including cable selection and management), troubleshooting, and more.
The Network Controller allows you a centralized dashboard to see the network's state, instantly discover and diagnose issues, and push configuration changes to all managed devices at once,

whether you use its Web GUI or its APIs. You may also use real-world programs on your computer to access the Network Controller and run your infrastructure automation scripts.

Workspace for CISCO Packet Tracer

1. Logical

The logical workspace shows the logical network topology that is built by the user. It displays the connecting, placing, and clustering of virtual network devices.

2. Physical

In the physical workspace, we can see the physical implementation of the logical network. It also shows how the network devices such as switches, routers, and hosts are connected in a real network topology.

Modes

There are two types of modes-:

Real-time Mode: The devices in a network behave as real devices do and look similar to real devices.

Simulation Mode: In this mode, a student can see and control time intervals, to learn how to troubleshoot network failures

Networking Devices

There are various networking devices which can be used to create different networking lab scenarios. E.g. Routers, Switches, Hubs, Wireless Devices, Connections, End Devices, WAN Emulation, Custom Made Devices, Multi-user Connection, Personal Computer, Laptops, Servers, Printers, IP Phones, VOIP Devices, Analog-Phones, TVs, Wireless-Tablets, PDAs, Wireless End Devices, Wired End Devices etc.

Connections

Various types of cables which can be used to connect various networking devices in a packet tracer are Console cable, Copper straight-through cable, Copper Cross-over Cable, Fiber Cable, Phone Cable, Coaxial Cable, Serial DTE, Serial DCE, and Octal Cable. While connecting various cables to connect various networking devices, it is important to know which type of cable to use and to which port the cable should be connected to a particular networking device. Most of the times we deal with a pc, switch and a router, thus it’s important to know what type of cable can be used to connect these devices On a PC, we can add a module based on the requirement, enable firewall rules, assign IPV4 and IPV6 address, default-gateway and subnet mask to an interface. We can also create a dial-up connection and use the terminal software to access the CLI of a router using console cable. We can run various diagnostics tests using

Command Prompt; also we can use Web Browser, Wireless connection, VPN, Traffic Generator, MIBBrowser, Cisco Ip Communicator, Email, PPPoE Dialler, Text Editor.

Devices	Cables
PC to PC	Cross-Over Cable
PC to Router	Cross-Over Cable
PC to Switch	Straight Cable
Switch to Router	Straight Cable
Router to Router	Serial Cable

We can also use the following services on a server HTTP, DHCP, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, FIREWALL, IPV6 FIREWALL, and test these services from the client machine. Packet tracer has a user friendly CLI mode, where a user can type different commands to configure various network devices. It is important to know which mode a student is using, what the commands to be used in that mode are and how to navigate between different modes of a networking device.

Simple Scenario: Let's take a simple scenario by connecting a PC to a Router using a cross-over cable. If it is a brand new router then it needs to be connected using a console cable and configured using terminal software. These are the basic modes of a router, which are recognized by the symbols shown in the table below. A user needs to know which mode he is in, what are the various commands that he can type in that mode and how to navigate between different modes of a router. If a user is not sure of what are the commands to be typed in any mode, then he can type the "?" Symbol to get help, or the list of commands to be typed in that mode.

Mode	Symbol
User Mode	Router>
Privilege Mode	Router#
Global Configuration Mode	Router(config)#
Interface Configuration Mode	Router(config-if)#
Line Configuration Mode	Router(config-line)#

A user can access the CLI-Mode of a router either by using a terminal software, for first time configuration, when a PC is connected to a Router, using a console cable or by using telnet/ssh/putty etc. when it is connected using a cross-over cable. Following basic commands can be typed on any router to assign an IP address on an Ethernet and serial interface.

Router Commands:

```
Router>enable
Router# configure terminal
Router(config)# interface FastEthernet0/0
Router(config)# ip address 192.168.1.0 255.255.255.0
Router(config)# no shutdown
Router(config)# interface serial0/1/0
Router(config)# ip address 172.115.1.0 255.255.0.0
Router(config)# no shutdown
```

Benefits of Using a Packet Tracer

Packet tracer provides network simulation and visualization. It can be used to enhance and improve the practical knowledge of computer networking principles among students. Moreover, students can design mini-projects with solutions with more innovation and creativity. As with other tools, students are able to understand the use of different networking protocols but they are not able to understand the application of these protocols in the real networks, thus packet tracer can be used to design and configure a network, and understand the application of various protocols. As students can't access different networking devices, because of the cost, also devices may be damaged and further, movement of packets from source to destination can't be seen in a real-time, thus by using packet tracer, students can access the virtual network devices any time and no damage can be caused to devices, moreover the movement of packets can be shown by simulations.

Chapter 2

Lab Requirements

Software Requirements	Turbo C Operating Systems- Windows 10
Hardware Requirements	Intel Core™ 10700 CPU2.90 Ghz, i7 10th Generation, 8 GB DDR4 RAM, 1 TB HDD, LAN Card (10/100 Mbps)

Chapter 3

Marking Scheme for the Practical Exam

There will be two practical exams in each semester.

- Internal Practical Exam
- External Practical Exam

Internal Practical Exam:

It is taken by the concerned Faculty member of the batch.

Marking Scheme:

Total Marks: 40

Division of 40 marks is as follows:

1. Regularity: 30
    - Weekly performance in the lab
    - Attendance
    - File
2. Viva Voce: 10

NOTE: For the regularity, marks are awarded to the student out of 10 for each experiment performed in the lab and at the end the average marks are giving out of 30.

External Practical Exam:

It is taken by the concerned faculty member of the batch and by an external examiner. In this exam student needs to perform the experiment allotted at the time of the examination, a sheet will be given to the student in which some details asked by the examiner needs to be written and at last viva will be taken by the external examiner.

Marking Scheme:

Total Marks: 60

Division of 60 marks is as follows:

a. Evaluation of the answer sheet 20
b. Viva Voice 15
c. Experiment performance 15

d. File submitted 10

NOTE:

- Internal marks + External marks = Total marks given to the students
  (40 marks) + (60 marks) = (100 marks)
- Experiments given to perform can be from any section of the lab.

Computer Networks Lab (CIC-355)

List of Experiments

1. Introduction to Networking Simulation Tools: Wireshark, Cisco Packet Tracer.	**CO1**
2. Installation of Cisco Packet Tracer and creating different topologies (star, ring and hybrid) in Cisco packet tracer.	**CO2**
3. To understand the operation of TELNET by accessing the router in server room from a PC in IT office.	**CO5**
4. To implement an IP Addressing Scheme and Subnetting in small networks using Cisco Packet Tracer.	**CO4**
5. To implement the static routing using Cisco Packet Tracer.	**CO3**
6. To implement the DHCP onto the Network Topology using Cisco Packet Tracer.	**CO3**
7. To implement the DNS, Email Services in the Network using Cisco Packet Tracer.	**CO5**
8. To implement the Dynamic Routing Protocols: RIP, IGRP using Cisco Packet Tracer.	**CO3**
9. To construct multiple router networks and implement the EIGRP Protocol.	**CO3**
10. To implement the Network Address Resolution (NAT) using Cisco Packet Tracer.	**CO5**
Value Added Programs	
1. To study about various network connecting devices and wires used for their interconnection.	**CO2**
2. Create a Straight cable and Crossover cable using RJ45 connector.	**CO2**
3. To study about the configuration of Inter connection between different networks by using Cisco Packet Tracer.	**CO2**
4. Introduction to Discrete Event Simulation tools NS2 , NS3 and installation of Ns3.	**CO1**

Viva Voice Questions

1. Explain, what is Network?
2. What is a Link?
3. What is a node?
4. What is a gateway or Router?
5. What is point-point link?
6. What is Multiple Access?
7. What are the criteria necessary for an effective and efficient network?
8. Name the factors that affect the performance of the network?
9. Name the factors that affect the reliability of the network?
10. Name the factors that affect the security of the network?
11. What is Protocol?
12. What are the key elements of protocols?
13. What are the key design issues of a computer Network?
14. Define Bandwidth and Latency?
15. Define Routing?
16. What is a peer-peer process?
17. When a switch is said to be congested?
18. Define the terms Unicasting, Multicasting and Broadcasting?
19. Name the categories of Multiplexing?
20. List the layers of OSI
21. Which layers are network support layers?
22. Which layers are user support layers?
23. Which layer links the network support layers and user support layers?
24. What are the concerns of the Physical Layer?
25. What are the responsibilities of Data Link Layer?
26. What are the responsibilities of Network Layer?
27. What are the different link types used to build a computer network?
28. What are the categories of Transmission media?
29. What are the types of errors?
30. What is subnet?
31. Difference between the communication and transmission.
32. What are the possible ways of data exchange?
33. What is meant by Hubs?
34. What is meant by Bridges?
35. Definitions of Firewall?
36. What is the Difference between HUB and SWITCH?
37. Difference between Physical Address and Logical Address?
38. What is PING Utility?
39. What do u mean by Gateway?
40. What is meant by Base band and Broadband Transmission?

Experiment No. 1

AIM: Introduction to Network Simulation Tools- Wireshark, CISCO Packet Tracer, NS3.

A network simulator is a tool or software program that allows for analyzing the relationships between different components connected in the network. In computer networking, "network simulation" (not "stimulation") refers to the process of creating a model or imitation of a computer network in a controlled virtual environment. This simulation allows you to study and analyze how the network behaves under different conditions and scenarios without the need for physical hardware or affecting an actual network.

Different Network stimulation tools are as follows-:

Wireshark- Wireshark is an open-source network protocol analyzer used for real-time monitoring and analysis of data packets on computer networks. Its features include packet capture from various sources, real-time analysis, packet inspection, filtering, support for numerous protocols, decoding, statistics, color coding, protocol hierarchy display, export options, scripting and automation capabilities, and customization. It is a cross-platform tool, widely utilized by network administrators, security professionals, and developers to diagnose network issues, troubleshoot problems, ensure network security, and gain insights into network communication.

Cisco Packet Tracer- Cisco Packet Tracer is a network simulation tool developed by Cisco for learning and practicing networking concepts. It offers features like network device simulation, support for various protocols, realistic packet analysis, collaborative learning, and an interactive interface. It's widely used in education, especially within Cisco Networking Academy courses, for hands-on learning and assessments. Packet Tracer is cross-platform and has an active user community, making it a valuable resource for students and network professionals to gain practical experience in networking without the need for physical hardware.

NS-3- Network Simulator 3 or NS-3, is an open-source network simulation framework. Its modular design supports the simulation of a wide range of networking protocols and realistic network scenarios, including wireless and mobility aspects. Users can visualize simulation results, and it is cross-platform and integrates with Python for scripting. NS-3 is actively developed and has a supportive community. It's widely used in research and education for in-depth network analysis, experimentation, and teaching networking concepts.

In conclusion, these tools collectively offer a comprehensive suite for computer network professionals and learners. Cisco Packet Tracer aids in understanding networking fundamentals, NS-3 facilitates advanced research and experimentation, while Wireshark provides the means to diagnose and secure networks effectively. Together, they empower individuals and organizations to thrive in the dynamic world of computer networking.

Experiment No.2

Aim-: Installation of Cisco Packet Tracer and creating different topologies (star, ring and hybrid) in Cisco packet tracer.

Theory-:

To install Cisco Packet Tracer on Windows in four steps, follow these instructions:

Step 1: Download Packet Tracer

Visit the Cisco Networking Academy's Packet Tracer download page: https://www.netacad.com/courses/packet-tracer

Sign in with your Cisco Networking Academy account or create one if you don't have an account.

Accept the terms and conditions.

Download the latest version of Cisco Packet Tracer for Windows.

Step 2: Install Packet Tracer

Locate the downloaded installation file (usually a .exe file) and double-click it to run the installer.

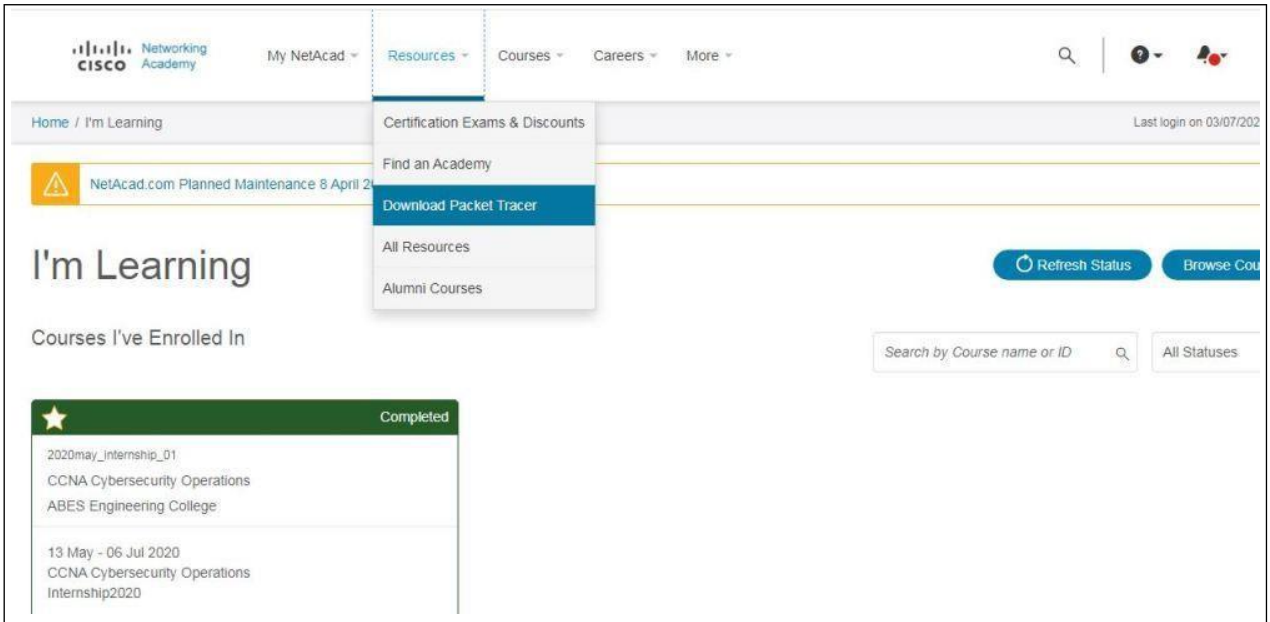
Follow the on-screen instructions to install Packet Tracer.

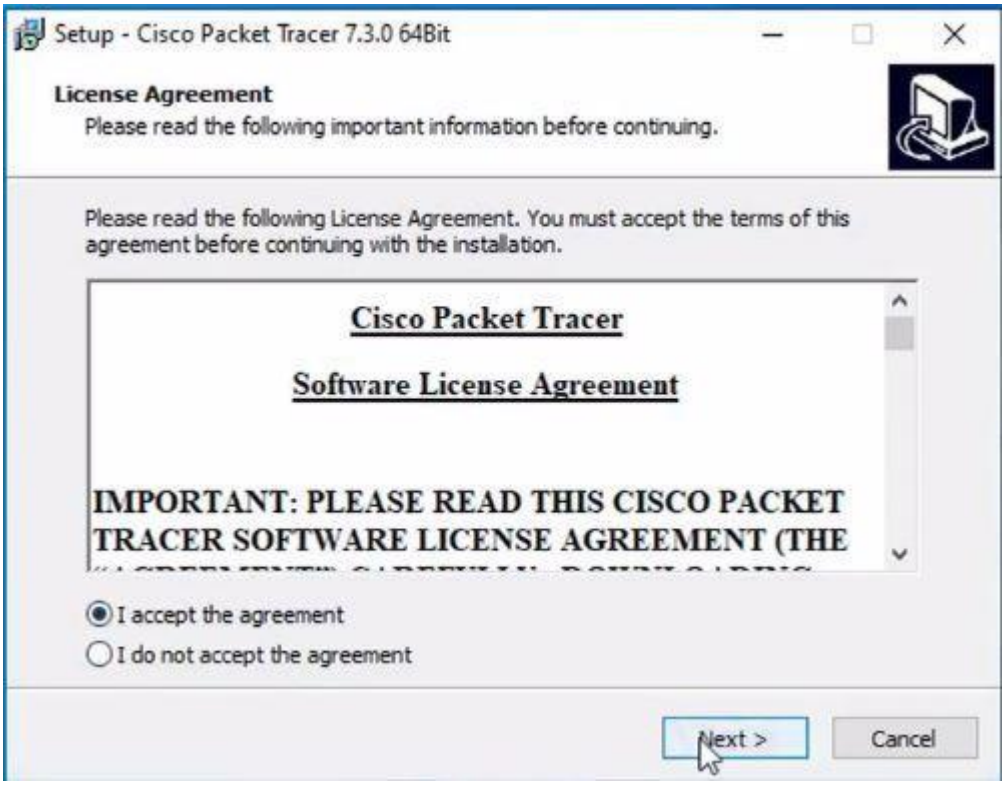
During the installation, you may be prompted to agree to the End-User License Agreement (EULA). Accept it to continue.

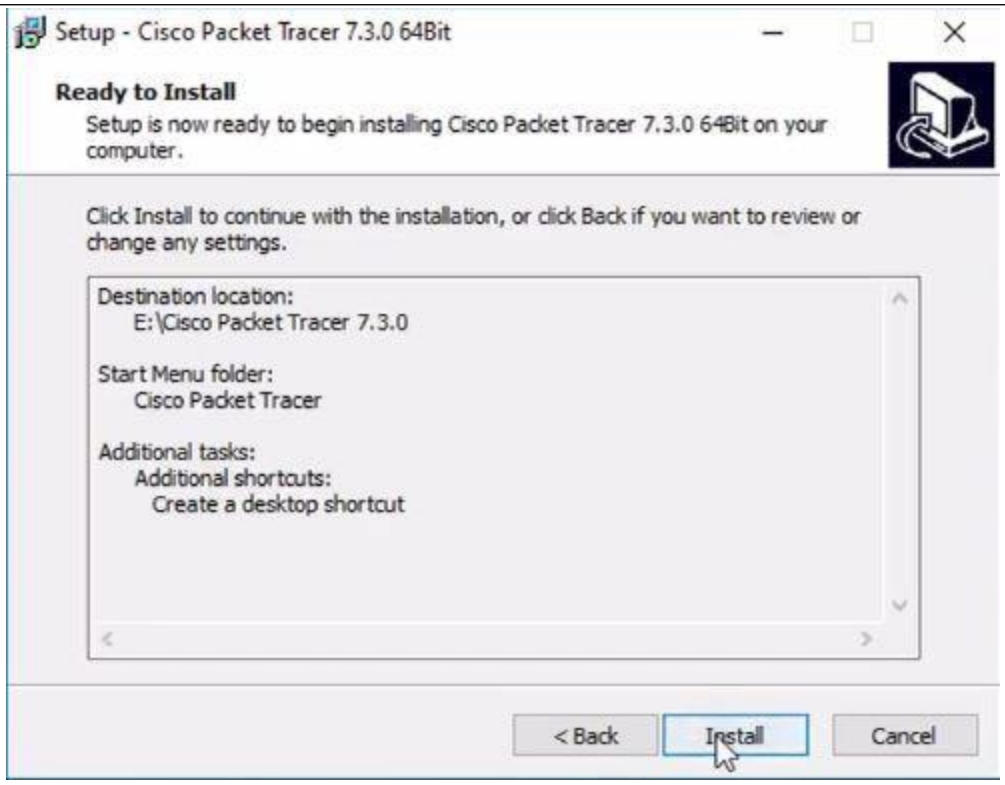
Choose the installation location and follow any other setup prompts.

Step 3: Launch Packet Tracer

After the installation is complete, you can launch Packet Tracer from the Start menu or desktop shortcut.


Networking Academy
My NetAcad
Resources
Courses
Careers
More
Home / I'm Learning
Last login on 03/07/202
Certification Exams & Discounts
Find an Academy
Download Packet Tracer
All Resources
Alumni Courses
NetAcad.com Planned Maintenance 8 April
I'm Learning
Refresh Status
Browse Cou
Courses I've Enrolled In
Search by Course name or ID
All Statuses
Completed
2020may_internship_01
CCNA Cybersecurity Operations
ABES Engineering College
13 May - 06 Jul 2020
CCNA Cybersecurity Operations
Internship2020

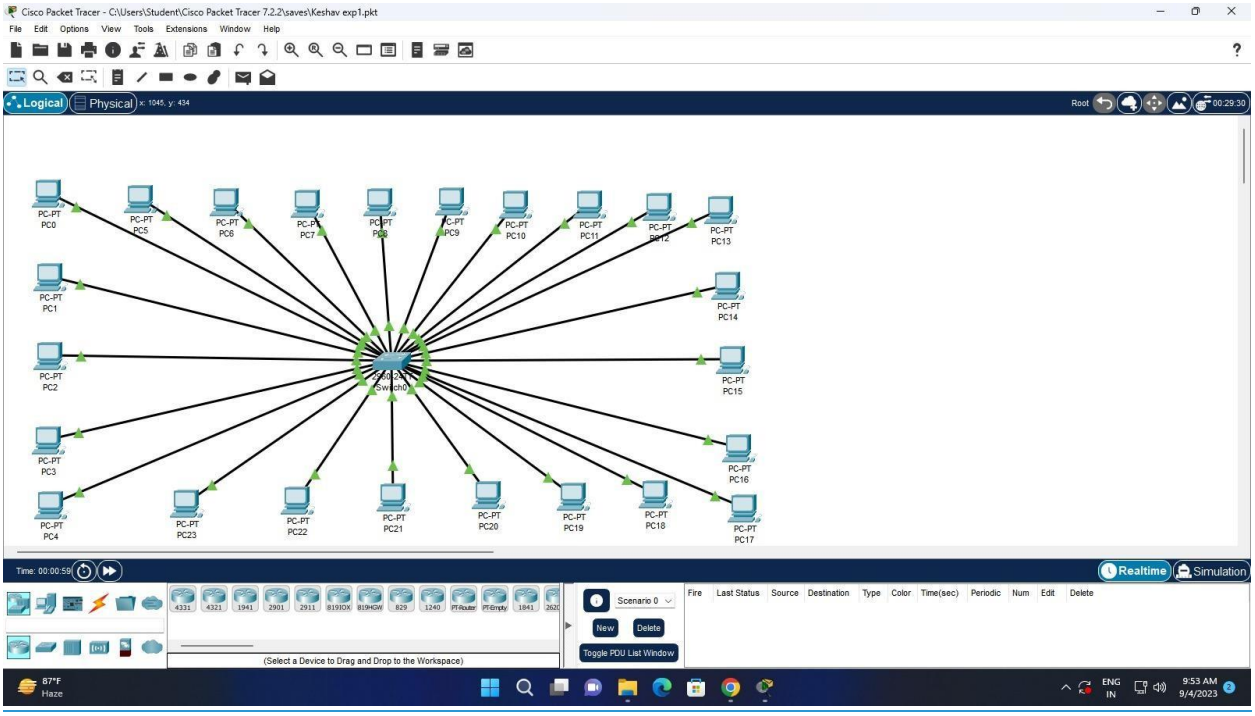

Setup - Cisco Packet Tracer 7.3.0 64Bit
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Cisco Packet Tracer
Software License Agreement
IMPORTANT: PLEASE READ THIS CISCO PACKET TRACER SOFTWARE LICENSE AGREEMENT (THE
I accept the agreement
I do not accept the agreement
Next >
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Ready to Install
Setup is now ready to begin installing Cisco Packet Tracer 7.3.0 64Bit on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
E:\Cisco Packet Tracer 7.3.0
Start Menu folder:
Cisco Packet Tracer
Additional tasks:
Additional shortcuts:
Create a desktop shortcut
< Back
Install
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Completing the Cisco Packet Tracer 7.3.0 64Bit Setup Wizard
Setup has finished installing Cisco Packet Tracer 7.3.0 64Bit on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch Cisco Packet Tracer
Finish

Creating different Topologies:

1) Star Topology- A star topology is a type of network topology in which all devices (such as computers, printers, or other networked devices) are connected to a central hub or switch. Each device on the network has a dedicated connection to the central hub, and data traffic typically flows through the hub when devices communicate with each other.



Advantages of Star Topology:

Centralized Management: The central hub or switch makes it easy to manage and monitor the network. Network administrators can easily add, remove, or troubleshoot devices from a central location.

High Reliability: If one cable or device fails, it typically doesn't affect the rest of the network. Other devices can continue to function without disruption.

Scalability: It's relatively easy to add new devices to a star network without affecting the existing network structure. You can simply connect a new device to the central hub.

Isolation: Problems or traffic from one device are less likely to affect other devices in the network due to the isolated connections.

Ease of Troubleshooting: When an issue arises, it's often easier to identify and resolve in a star topology because of the centralized layout.

Disadvantages of Star Topology:

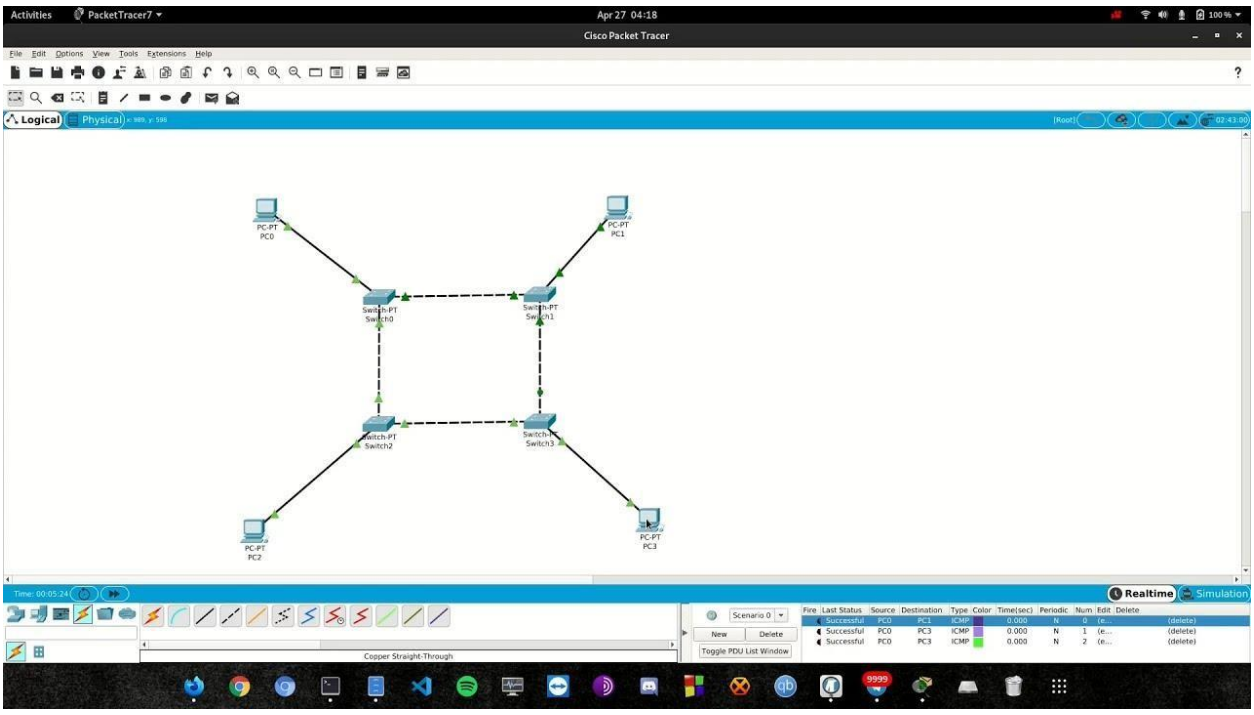
Single Point of Failure: The central hub or switch is a single point of failure. If it fails, the entire network can become inaccessible. Redundancy measures (backup hubs) can be costly to implement.

Cost: Implementing a star topology can be more expensive than other topologies, especially as the network grows, due to the need for multiple cables and a central hub/switch.

Cabling Complexity: Star topologies often require a significant amount of cabling, especially in larger networks. Managing and organizing these cables can be challenging.

Limited Scalability: While it's relatively easy to add devices, there can be limitations to the number of devices that can be connected to a single central hub before performance starts to degrade.

2) Ring Topology- A ring topology is a type of network topology in which each device is connected to exactly two other devices, forming a closed-loop or ring-like structure. Data travels in a unidirectional or bidirectional manner around the ring until it reaches its destination. In a bidirectional ring, data can travel in both directions, while in a unidirectional ring, data travels in only one direction.



Advantages:

Reliability: Ring topologies are highly reliable due to the presence of redundancy. If one link or device fails, data can still find an alternative path to reach its destination.

Deterministic: The deterministic nature of ring topologies can be an advantage in certain applications where strict timing or sequencing is required.

Equal Access: In a bidirectional ring, all devices have equal access to the network and share the transmission load evenly.

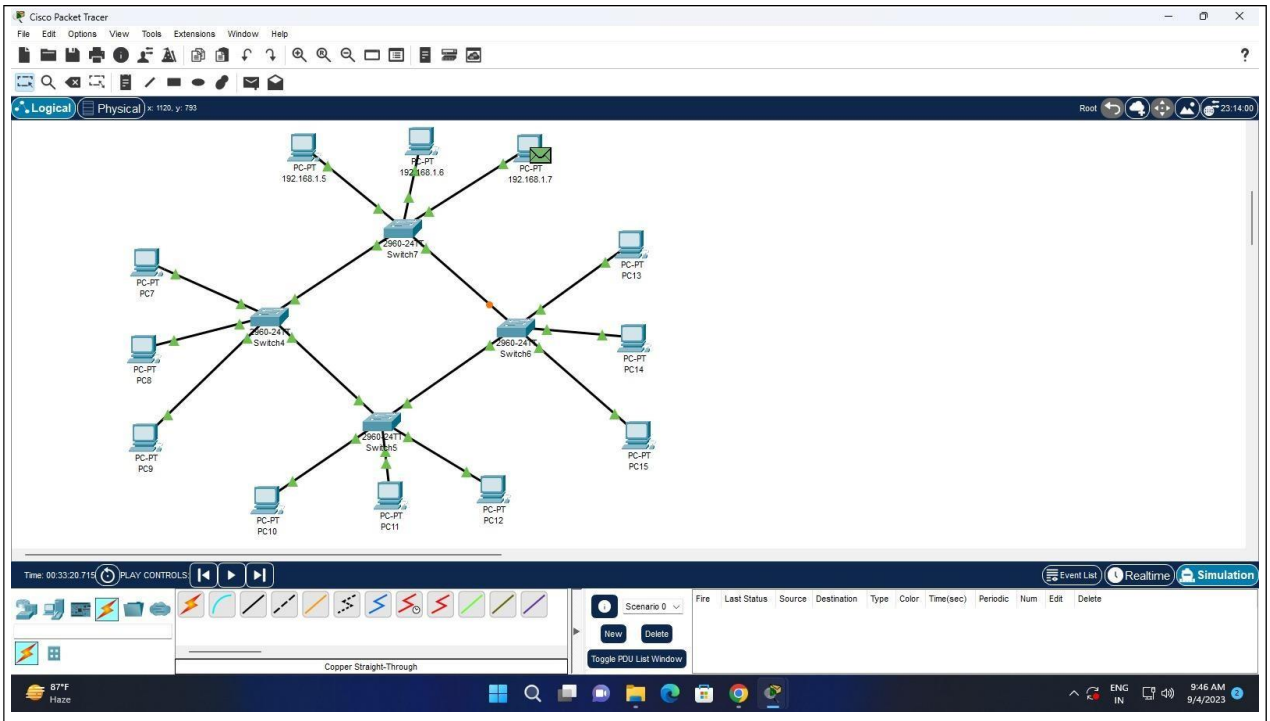
Disadvantages:

Cost: Ring topologies can be expensive to set up and maintain due to the need for additional cabling and devices.

Failure Handling: While they offer redundancy, diagnosing and repairing a failure in a ring topology can be complex and time-consuming.

Limited Scalability: Expanding a ring network can be challenging because adding new devices may require the entire network to be temporarily disconnected and reconfigured.

3) Hybrid Topology- A hybrid topology is a type of network topology that combines two or more different basic topologies to create a more complex and flexible network infrastructure. This approach is often used to leverage the advantages of multiple topologies while mitigating their respective disadvantages. Hybrid topologies can be customized to meet the specific needs of an organization or network environment.



Advantages of Hybrid Topology:

Flexibility: Hybrid topologies can be tailored to specific network requirements. Organizations can use the combination of topologies that best suit their needs.

Scalability: Hybrid topologies can often be expanded and scaled up more easily than single topologies, allowing for the addition of new devices or segments.

Reliability: By integrating redundant paths and elements, hybrid topologies can offer enhanced fault tolerance and reliability. A failure in one segment may not disrupt the entire network.

Performance: Hybrid topologies can provide optimized performance for different segments of the network. For example, high-performance star segments can be combined with fault-tolerant ring segments.

Isolation: Different segments of the network can be isolated from each other, which can be useful for security or management purposes.

Disadvantages of Hybrid Topology:

Complexity: Hybrid topologies can be more complex to design, implement, and manage than single topologies, which may increase the cost and administrative overhead.

Cost: Integrating multiple topologies may require additional hardware and cabling, leading to increased costs.

Maintenance: Troubleshooting and maintaining a hybrid topology can be more challenging due to its complexity.

Compatibility: Care must be taken to ensure that the different topologies within the hybrid network are compatible and can effectively communicate with each other.

Experiment No. 3

AIM: To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

Telnet, developed in 1969, is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. Telnet stands for Teletype Network, but it can also be used as a verb; 'to telnet' is to establish a connection using the Telnet protocol.

Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.

Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines. Telnet is a protocol by which you can remotely login into remote devices to make changes in the configuration of that device. The aim of this article is to give you a quick guide about how you can enable telnet on a switch.

Procedure:

- Open the CISCO Packet tracer software
- Drag and drop 1 pc and 1 laptop using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router
- Type CLI's for the router
- Make and verify the connections from any pc to the server by providing correct password; in command prompt of PC.
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Input Details for TELNET

Router 0	PC0	PC1
IP Address : 192.168.0.1 Gate way : -	IP Address : 192.168.0.2 Gate way: 192.168.0.1	IP Address : 192.168.0.3 Gate way: 192.168.0.2

ROUTER CLI:

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Router(config)#line vty 0 4
Router(config-line)#password sai123
```

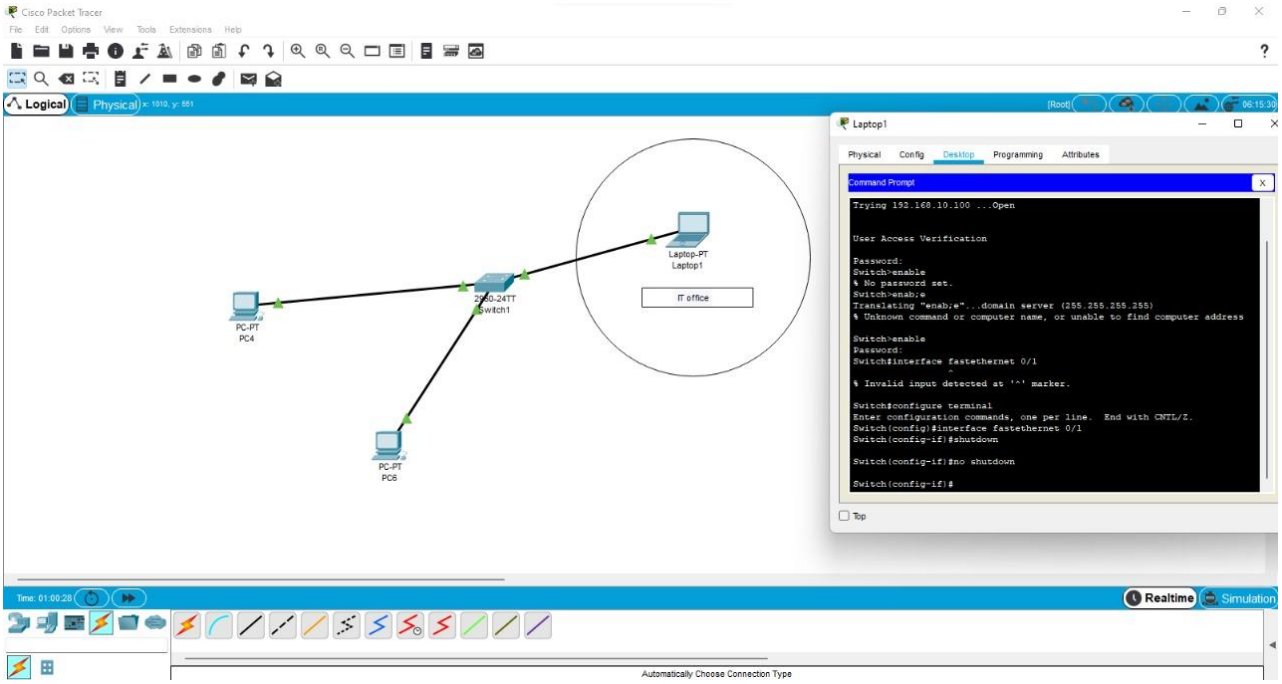
Router(config-line)#login local

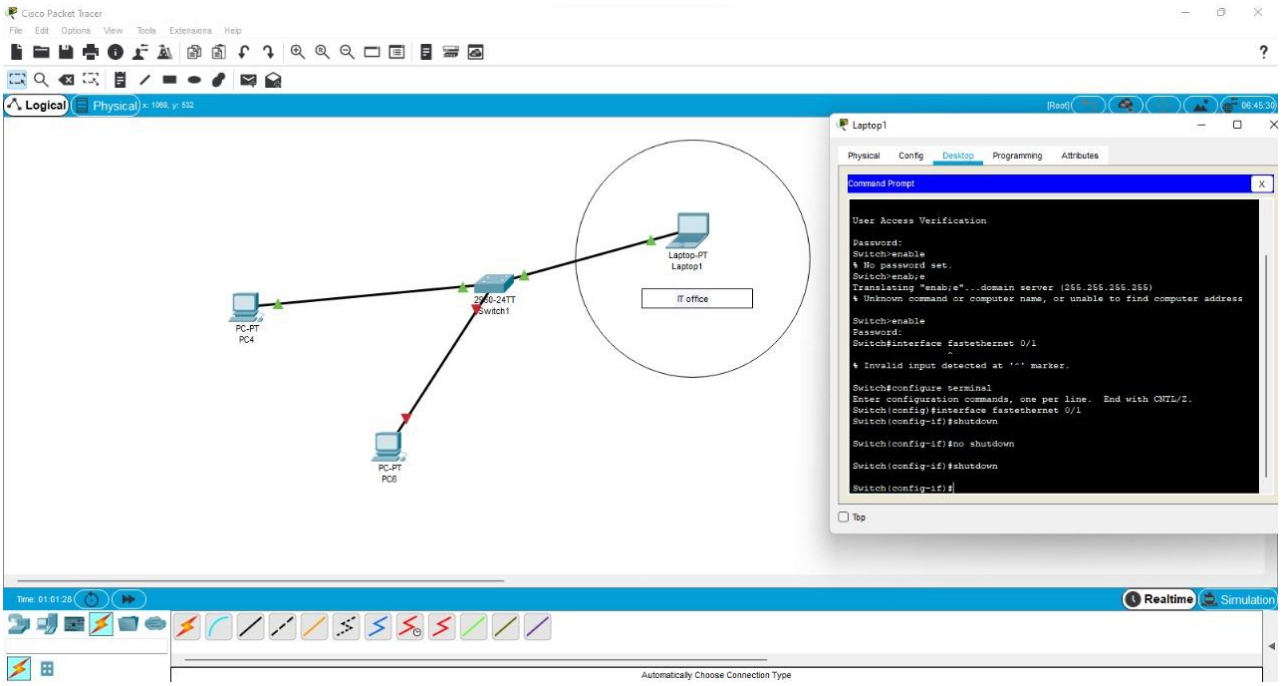
Router(config-line)#exit

Router(config)#username sai privilege 4 password sai123

Router(config)#exit

OUTPUT:





PINGING FROM PC0 TO SERVER USING TELENET:

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=255

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 192.168.0.1

Trying 192.168.0.1 ...Open User Access Verification

Username: **sai**

Password: **<type the password---sai123(invisible)>**

Router#show ip route ***(now router can be accessed from pc0)***

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0 L 192.168.0.1/32 is directly connected, GigabitEthernet0/0 Router#

Result: Thus, verified the operation of TELNET and accessed the router from PCs.

Experiment No.4

AIM: To implement an IP Addressing Scheme and Subnetting in small networks using Cisco Packet Tracer.

A subnet, or sub-network, is a part of a larger network. Subnet is a logical part of IP-: The Internet Protocol (IP) is the method for transmitting data from one computer to another over the Internet network .Each computer or host on the internet, has at least one IP Address as a unique identifier.

PROCEDURE:

1. First open the cisco packet tracer desktop and select the devices listed here (PC, Switch, PT-switch, Router, PT-Router).
2. Configure the router :

- Drag and drop a router onto the workspace.
- Double-click the router to open the configuration window.
- Click the interfaces tab.
- For each interface that will connect to a subnet, click the edit button.
- Enter the IP address of router on that subnet.
- Subnet Mask: enter the subnet mask for the subnet.
- Click ok to save your changes.

3. Configure the devices on each subnet.

- For each device on a subnet, double-click the device to open the configuration window.
- Click the desktop tab.
- Open the IP configuration window, enter the following :-

- Enter an IP address.
- Enter the subnet mask.

- Click OK to save your changes.

4. Verify the configuration :

- Ping each device on the network from another device to verify that they can communicate with each other.
- To configure the router , you would :-

1) Drag and drop a router onto the workspace.
2) Double-click the router to open the configuration window.
3) Click the interface tab.
4) For the first interface, click the edit button.
5) In the IP configuration section , enter the following :

- IP address : 192.168.1.1
- Subnet Mask : 255.255.255.0

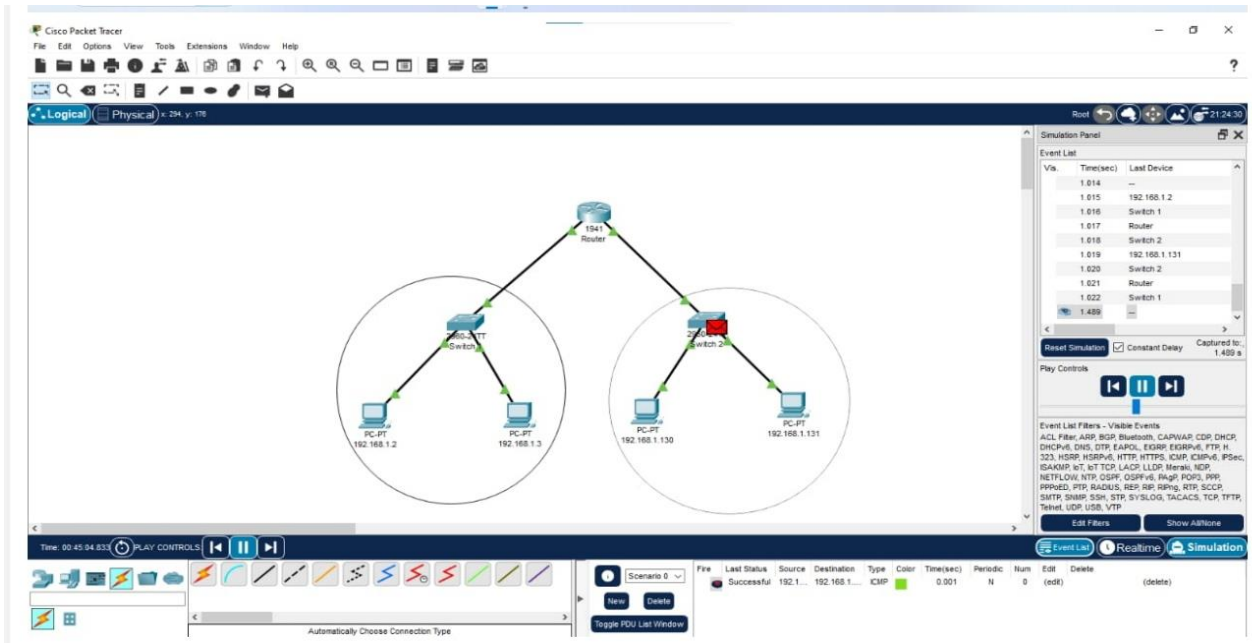
6) Click OK to save your changes.

➢ To configure the devices on each subnet , you would :

1. For each device on the first subnet, double click the device to open the configuration window.
2. Click the desktop tab.
3. In the IP configuration window, enter the following.

- IP address: An IP address between 192.168.1.2 and 192.168.1.126
- Subnet mask : 255.255.255.0

4. Click OK to save your changes.
5. For each device on the second subnet, double-click the device to open the configuration window.
6. Click the desktop tab.
7. Click the IP configuration button and enter the IP address between 192.168.2.130 and 192.168.2.254
8. Click OK to save your changes.


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
1941 Router
Switch 1
Switch 2
PC-PT 192.168.1.2
PC-PT 192.168.1.3
PC-PT 192.168.1.130
PC-PT 192.168.1.131
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type

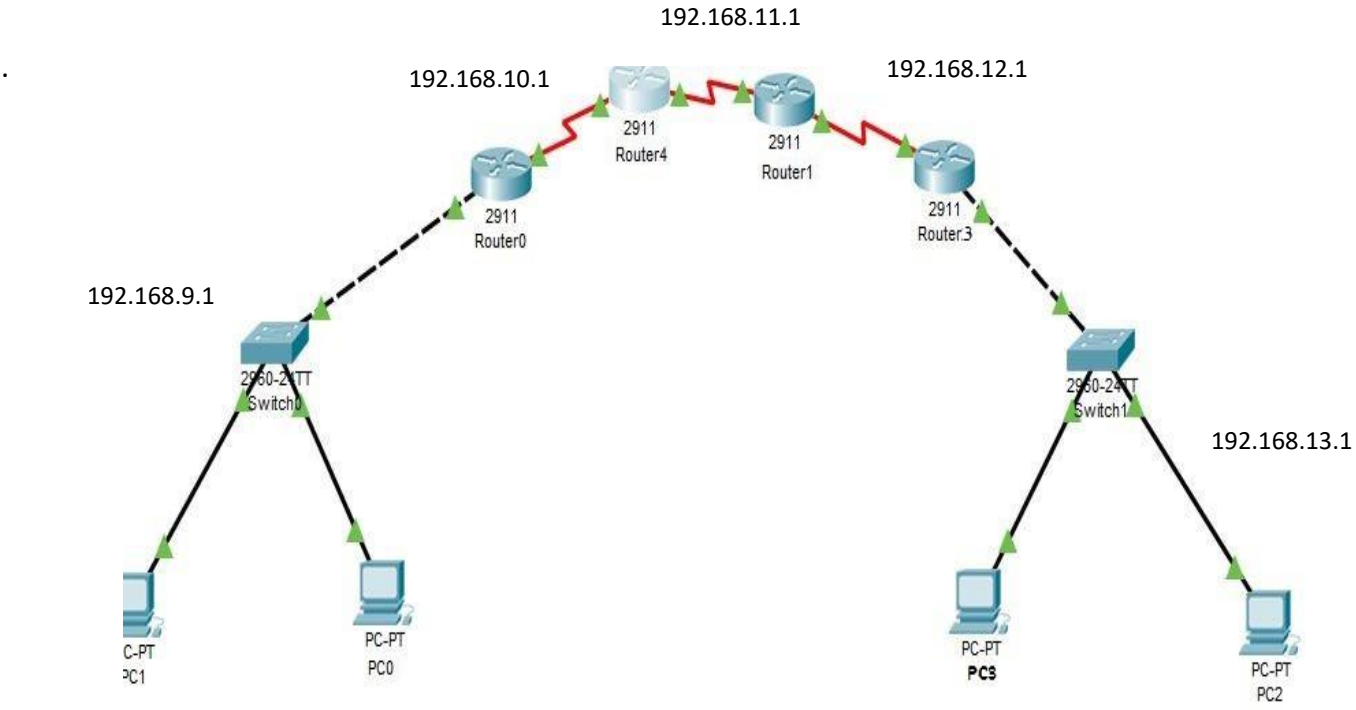
Experiment No. 5

AIM: To implement the static routing using Cisco Packet Tracer.

NETWORK TOPOLOGY FOR INTER LAN:

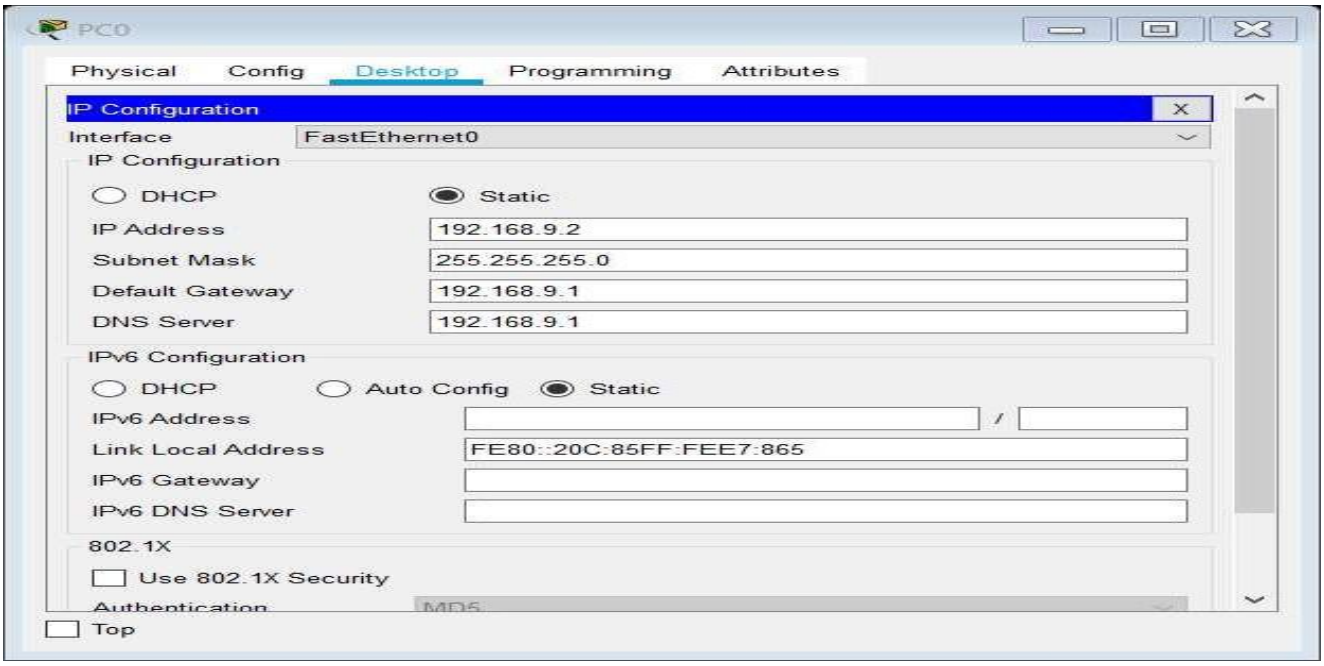
Here, four different networks will be formed by using required Routers, Switches and PCs, these all the devices interconnected by using suitable connecting network cables.

First network at left end, have two PCs, PC0 and PC1, connected with a switch which further connected to Router0 that have network ID as 192.168.9.1. Router0 next connected to Router4 and have the network ID 192.168.10.1; Router4 connected with Router1 and have the network ID 192.168.11.1. In the same way network ID between Router1 and Router3 is 192.168.12.1. At the extreme right end the nework that is connected with Router3 is having two PCs connected via a switch have the network ID 192.168.13.1.

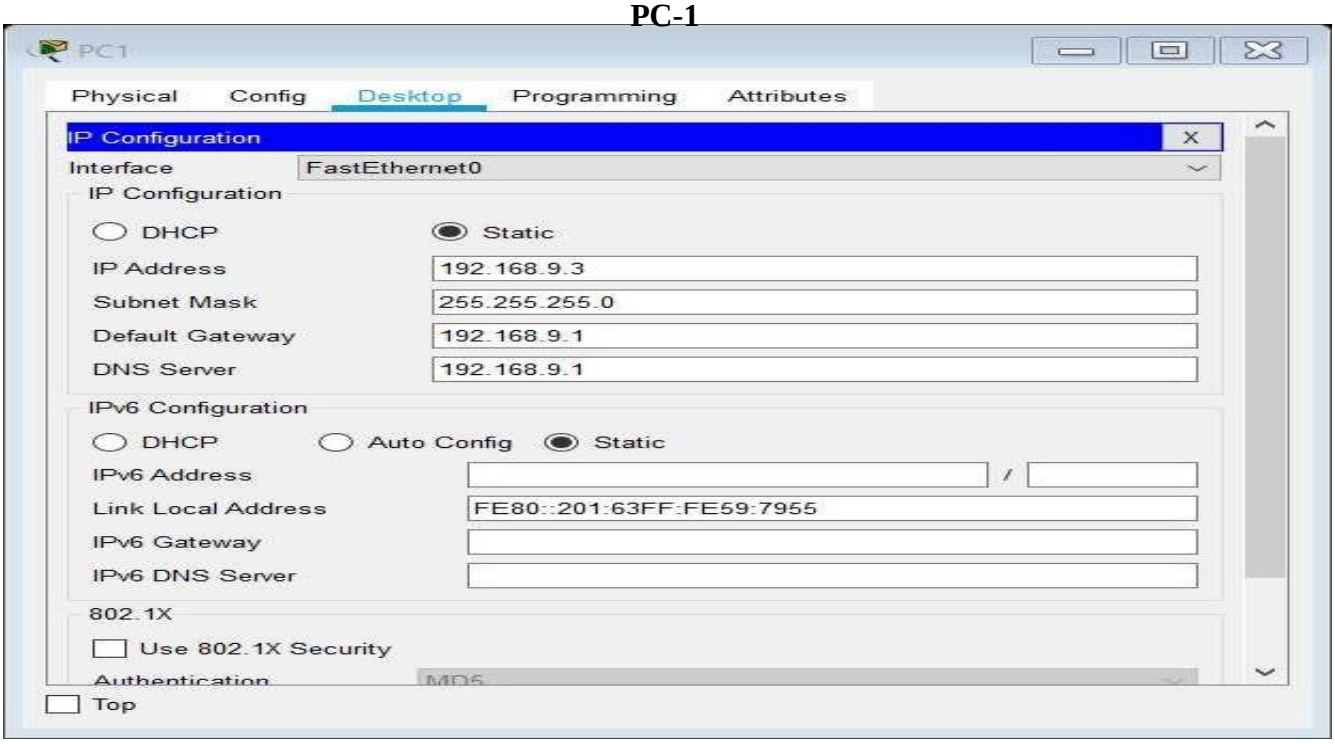


CONFIGURATION OF IP AND SUBNET MASK AT PC SIDE

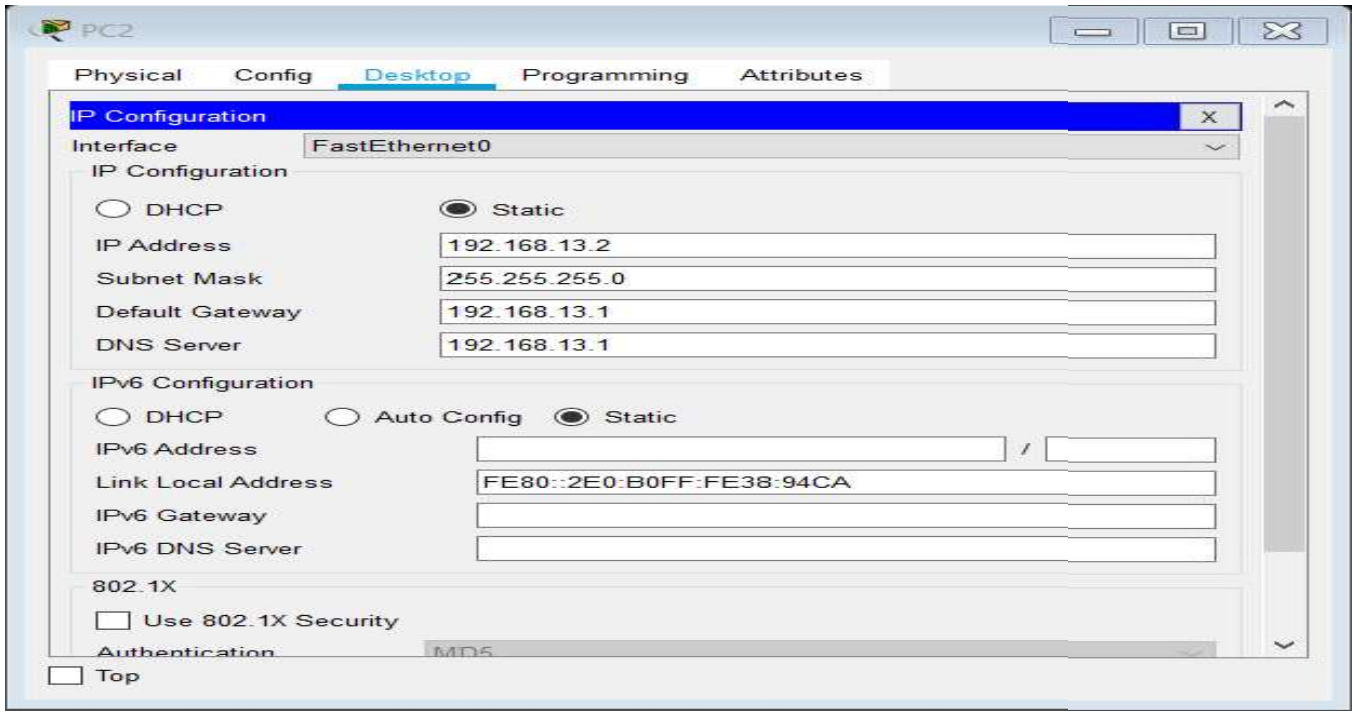
PC-0

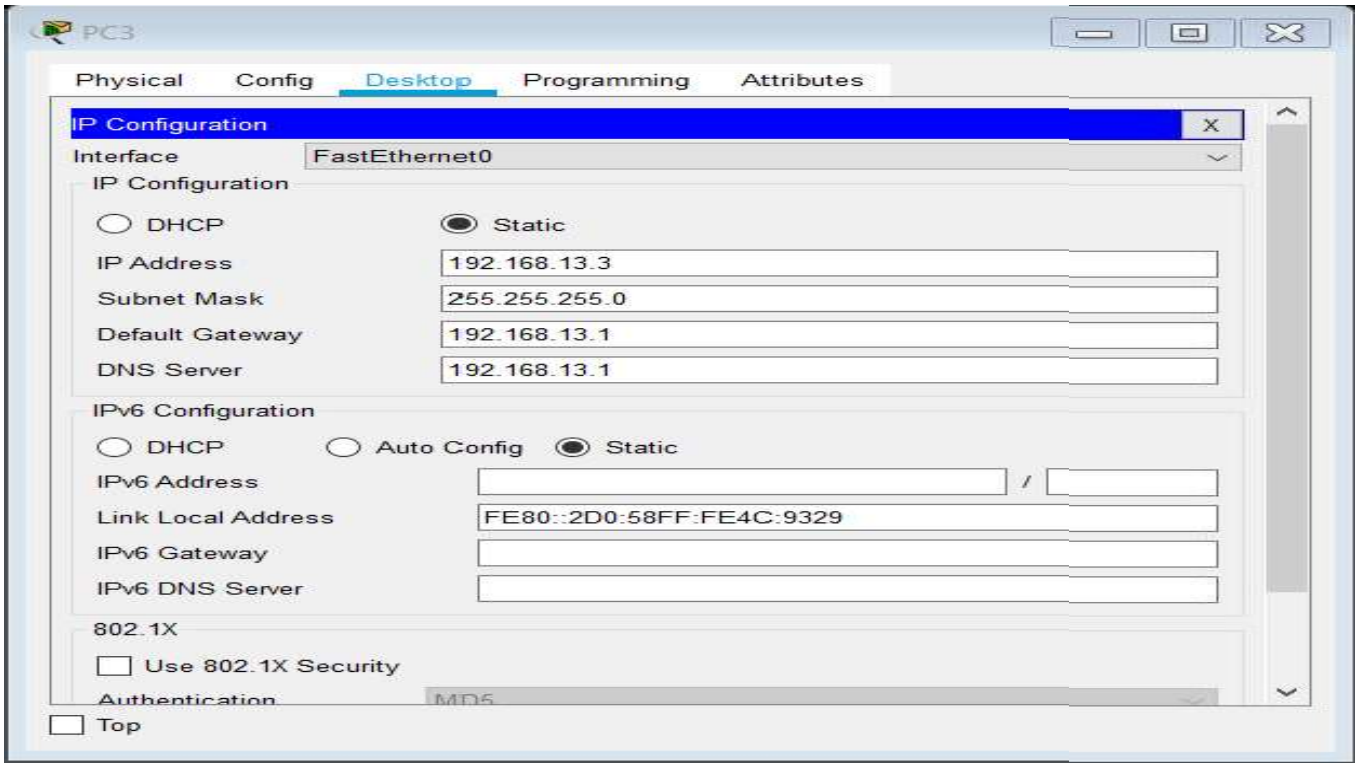


PC-1

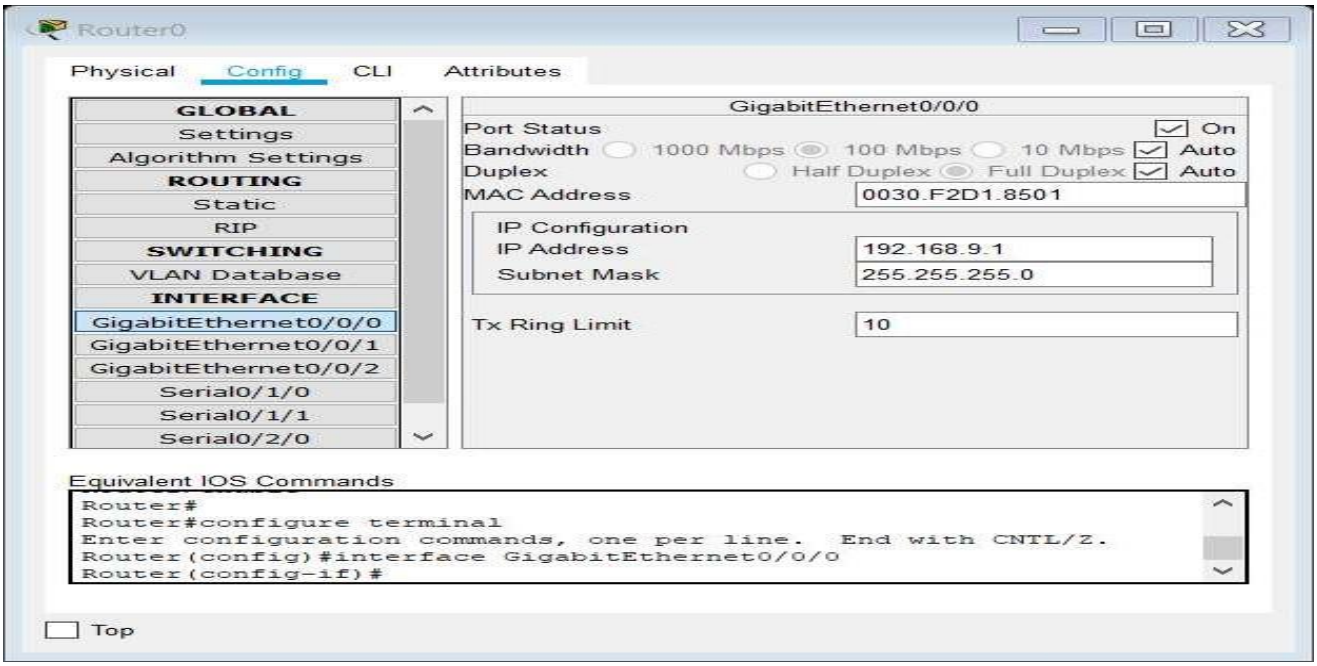


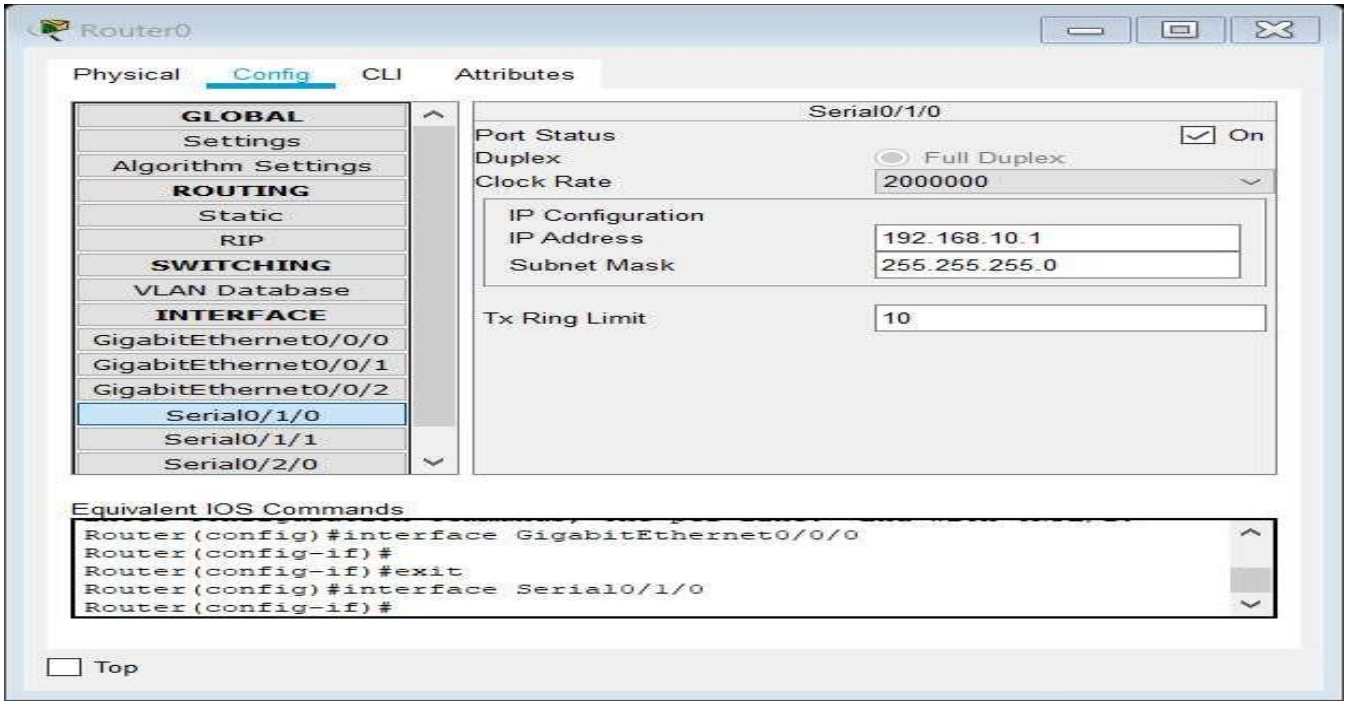
PC-2


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.13.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.13.1
DNS Server
192.168.13.1
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2E0:B0FF:FE38:94CA
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.13.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.13.1
DNS Server
192.168.13.1
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:58FF:FE4C:9329
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top

CONFIGURATION OF IP AND SUBNET MASK AT ROUTER

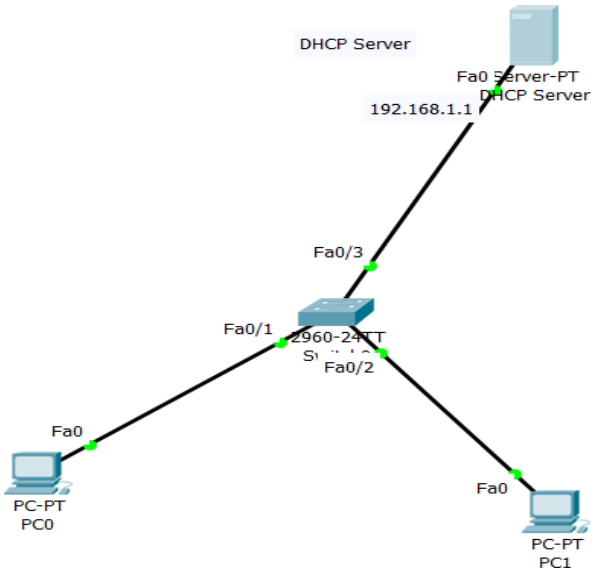


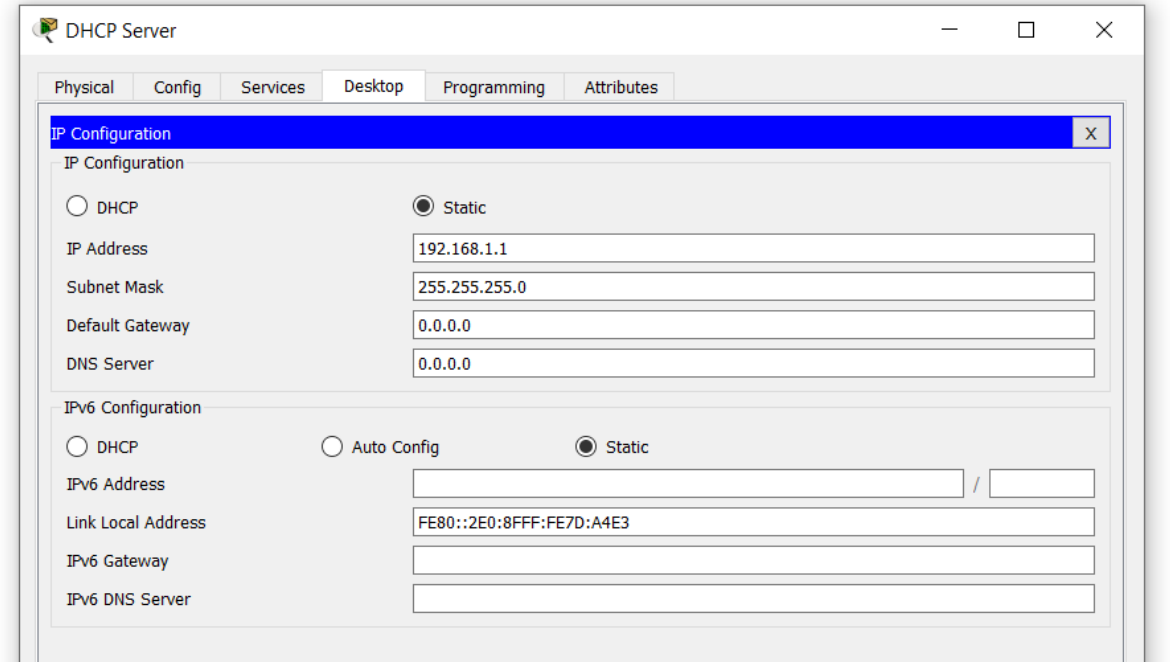


Experiment No. 6

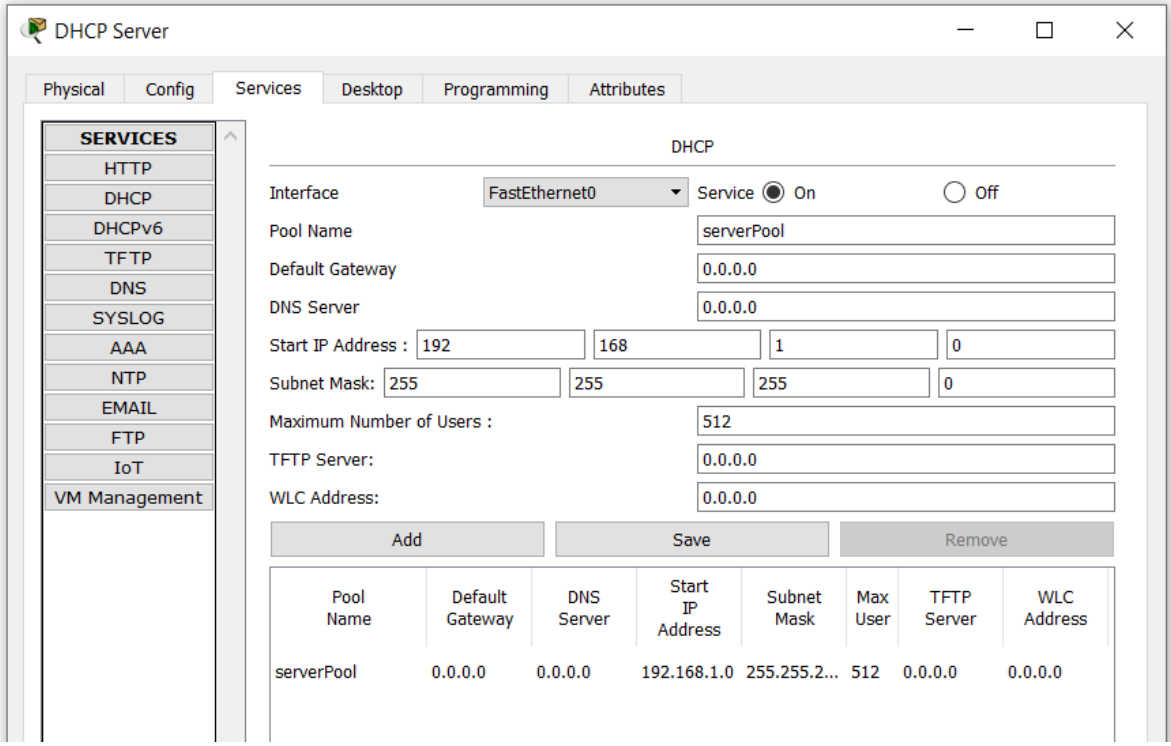
AIM-: To implement the DHCP onto the Network Topology using Cisco Packet Tracer.

DHCP Server:- The DHCP (Dynamic Host Configuration Protocol) is a network protocol used to assign IP automatically to the systems with the help of a machine called DHCP server.A DHCP Server allows computers to request an IP address and networking parameters automatically. If you do not have a DHCP Server to configure IP addresses automatically to the PCs then you need to assign a static or manual IP address on the Computers. So in simple words, we can say that DHCP Server is only used for assigning the IP addresses to the Systemsautomatically.

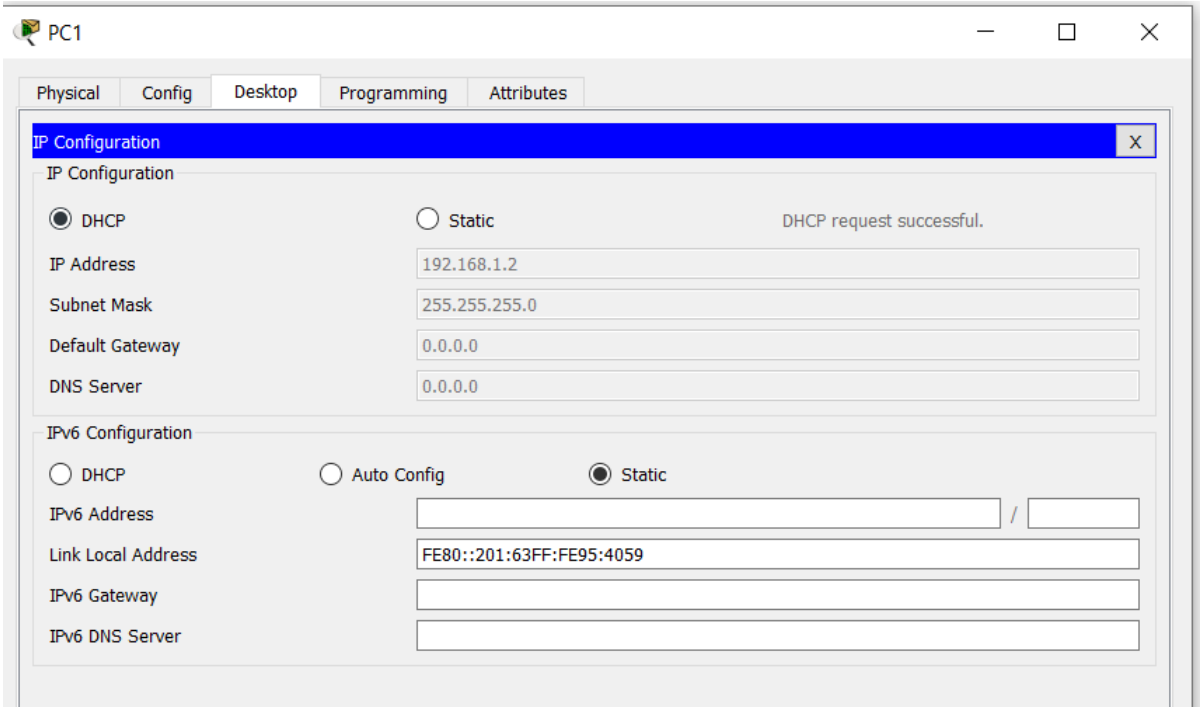




Configuration of DHCP Server



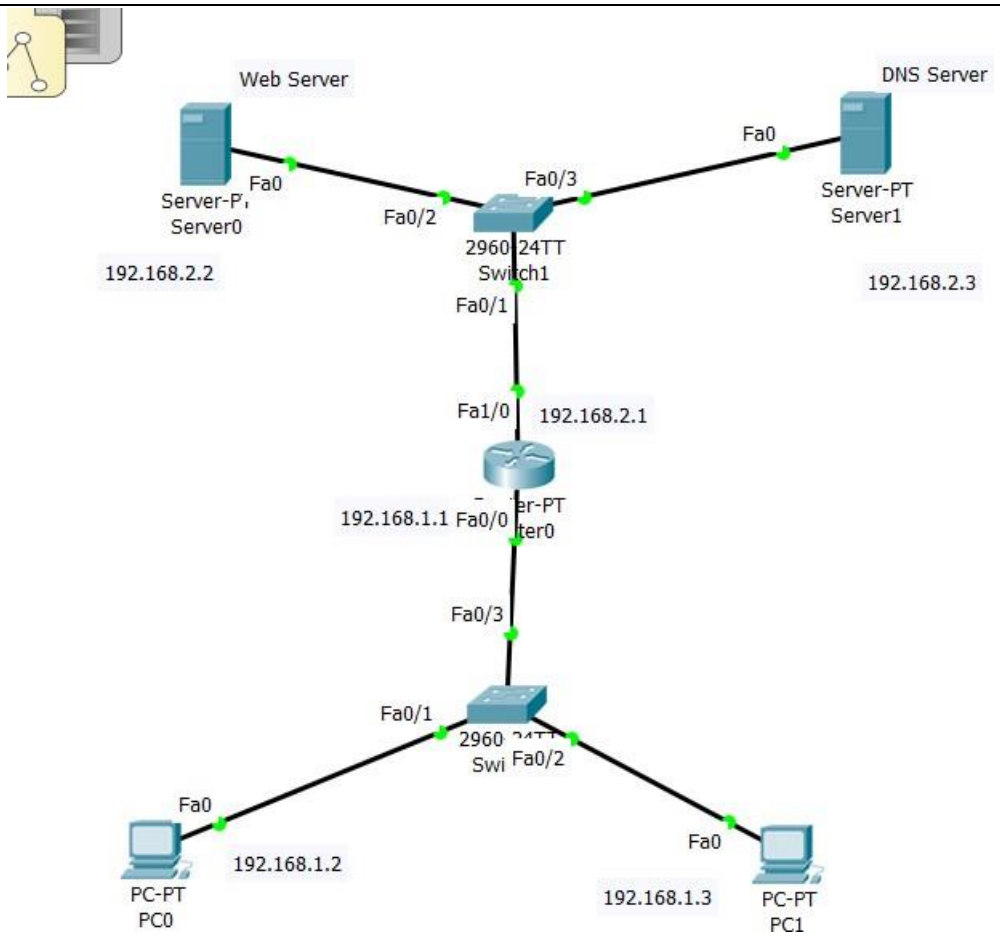
Assign IP address to the PC


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:63FF:FE95:4059
IPv6 Gateway
IPv6 DNS Server

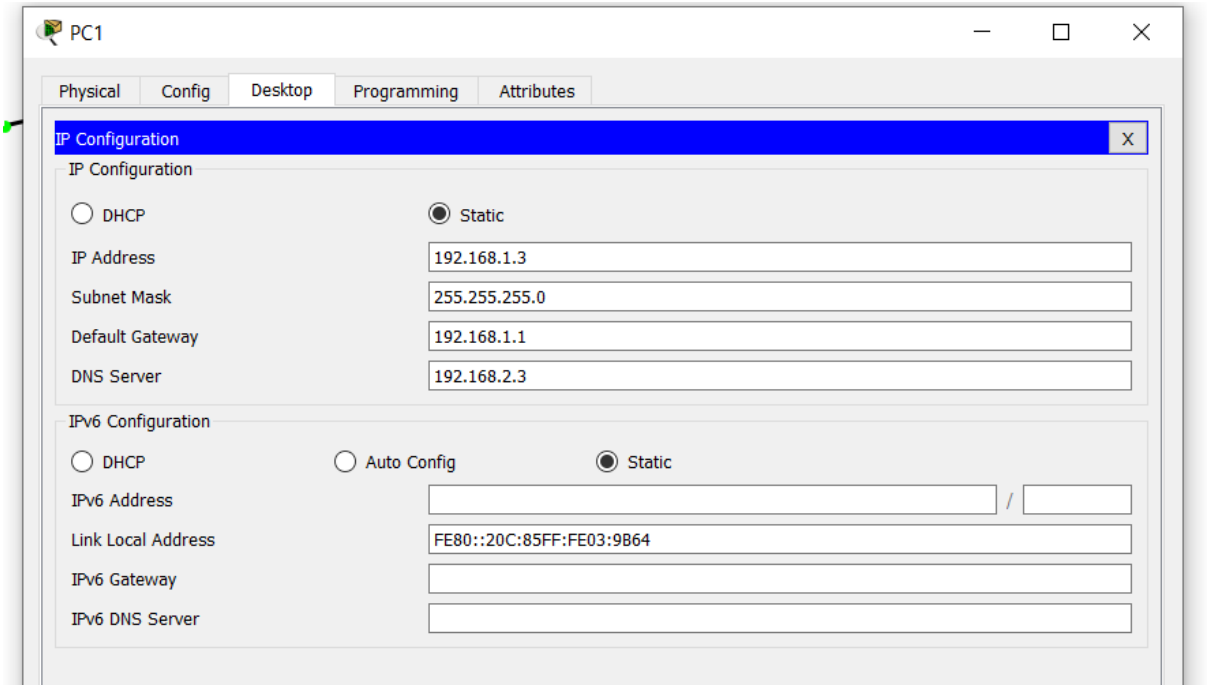
Experiment No. 7

AIM-: To implement the DNS, Email Services in the Network using Cisco Packet Tracer.

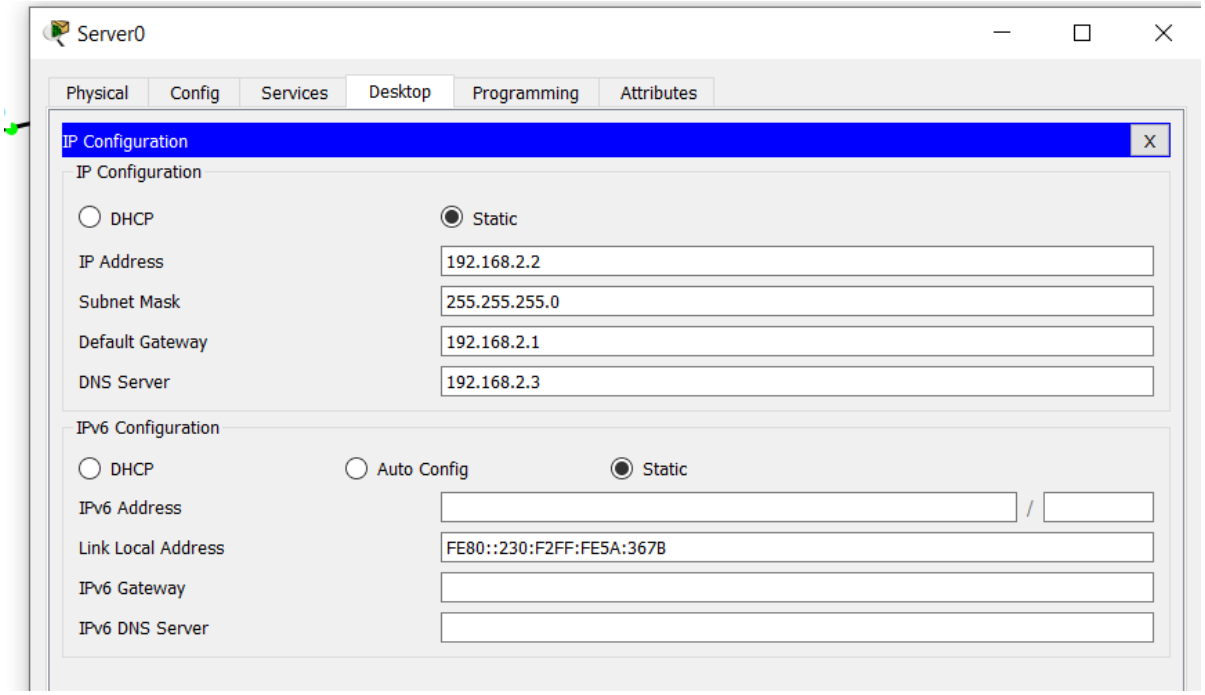
A Domain Name Service (DNS) server resolves host names into IP addresses. Although we can access a network host using its IP address, DNS makes it easier by allowing us use domain names which are easier to remember. For example its much easier to access google website by typing http://www.google.com as compared to typing http://208.117.229.214. In either case, we'll access google website, but using domain name is obviously easier. Now, before any host can use a DNS service, we must configure a DNS server first. For example, when you type the URL http://www.google.com in your browser, the host will querythe DNS server for the IP address of http://www.google.com. The DNS server will resolve http://www.google.com into an IP address then answer back the host with the IP address. An HTTP server is a web server. It stores web resources that can be accessed by a web client. Your PC's browser (a web client) requests for web resources from a web server overthe internet. Web resources are files such as text and images that the server will give to the client on request.

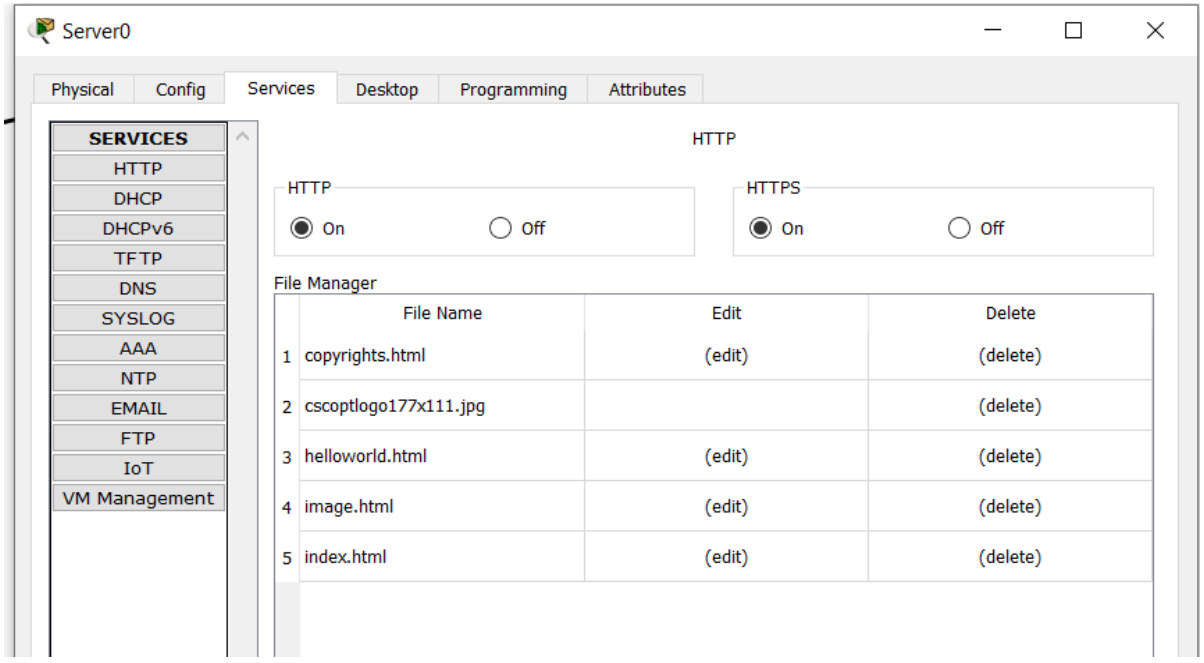


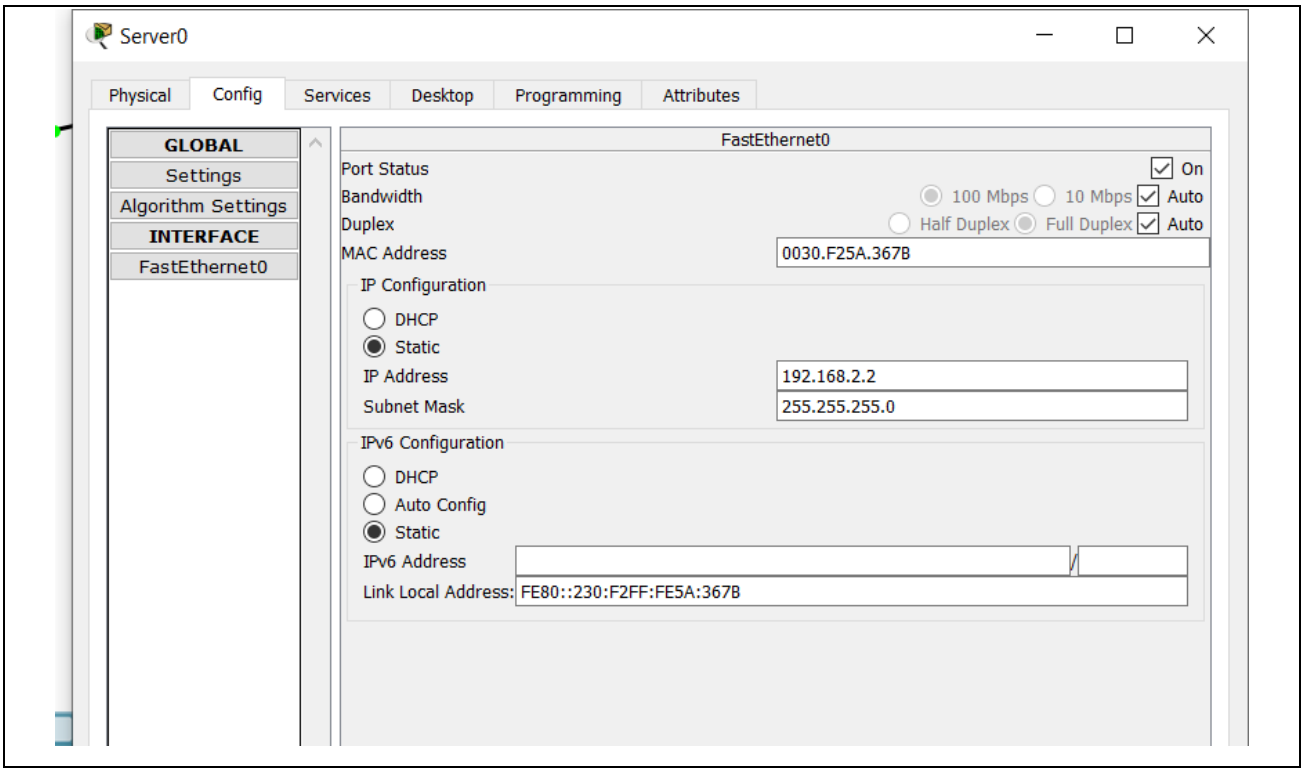
Configuration of PC



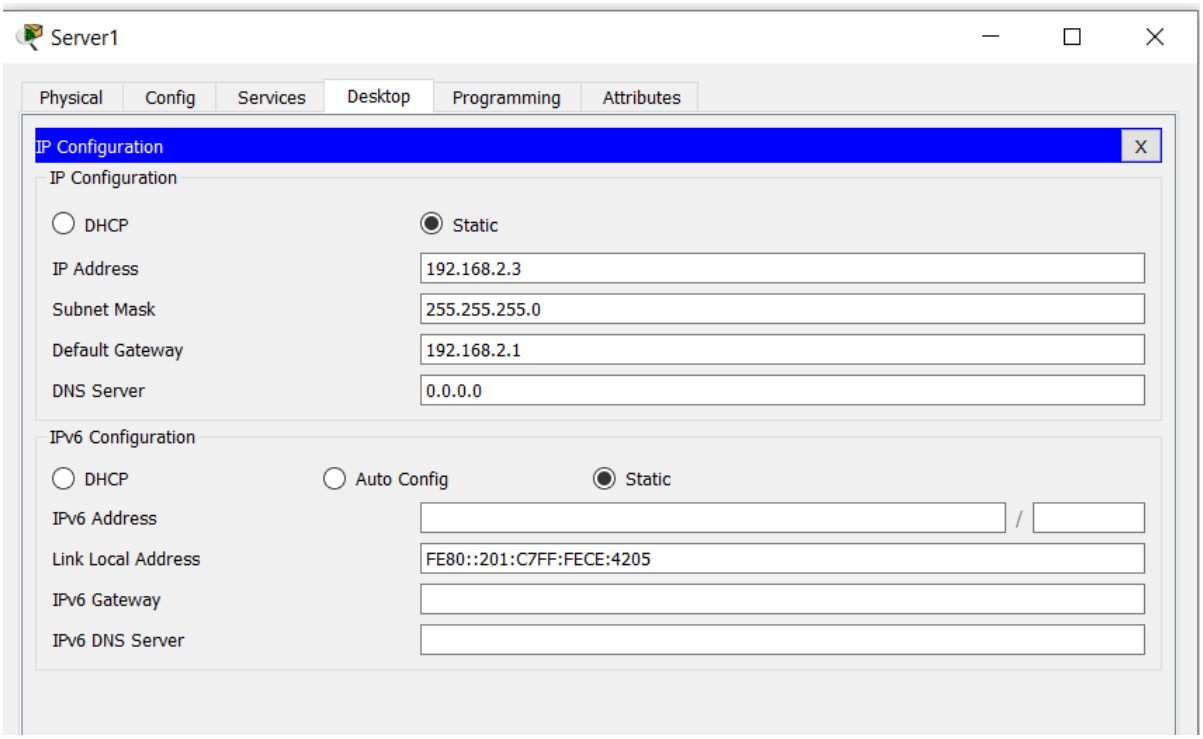
Configuration of Web Server

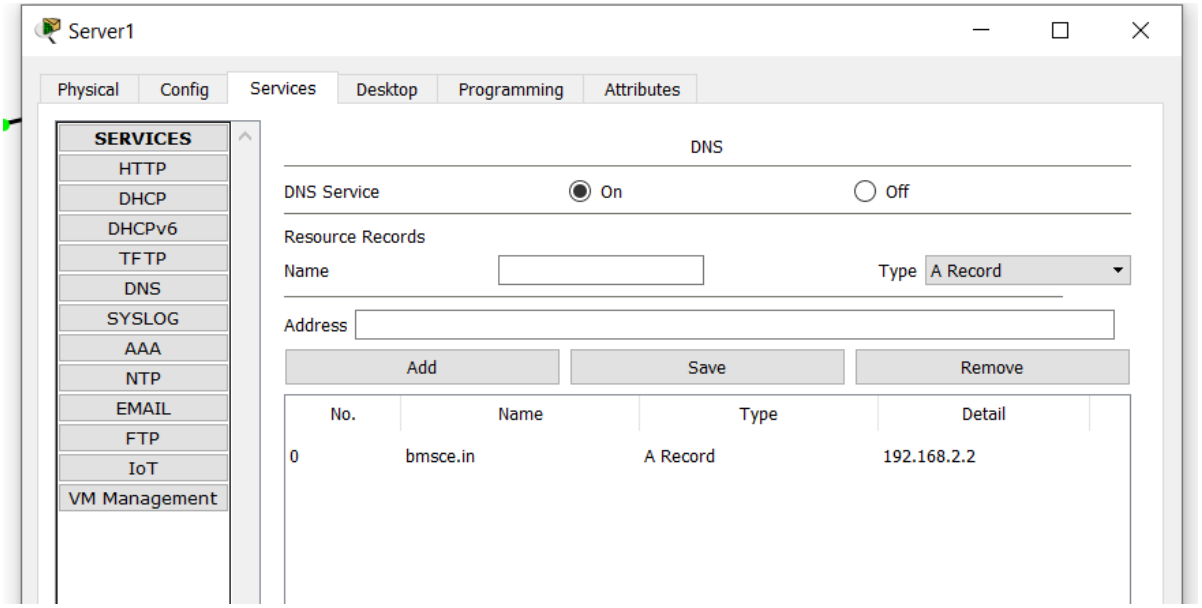





Server0
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0030.F25A.367B
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address:
FE80::230:F2FF:FE5A:367B

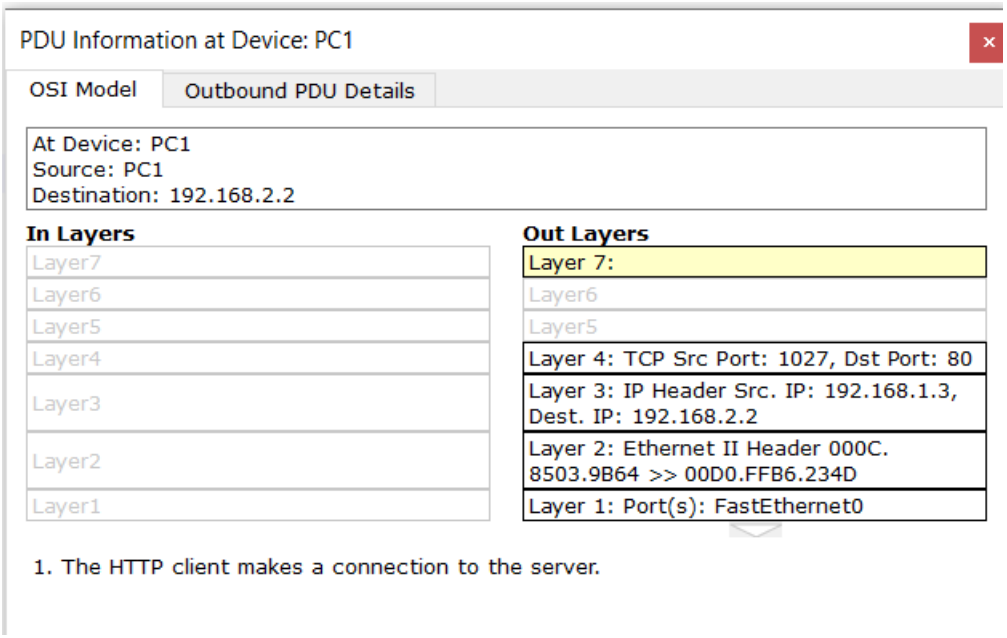
Configuration of DNS Server



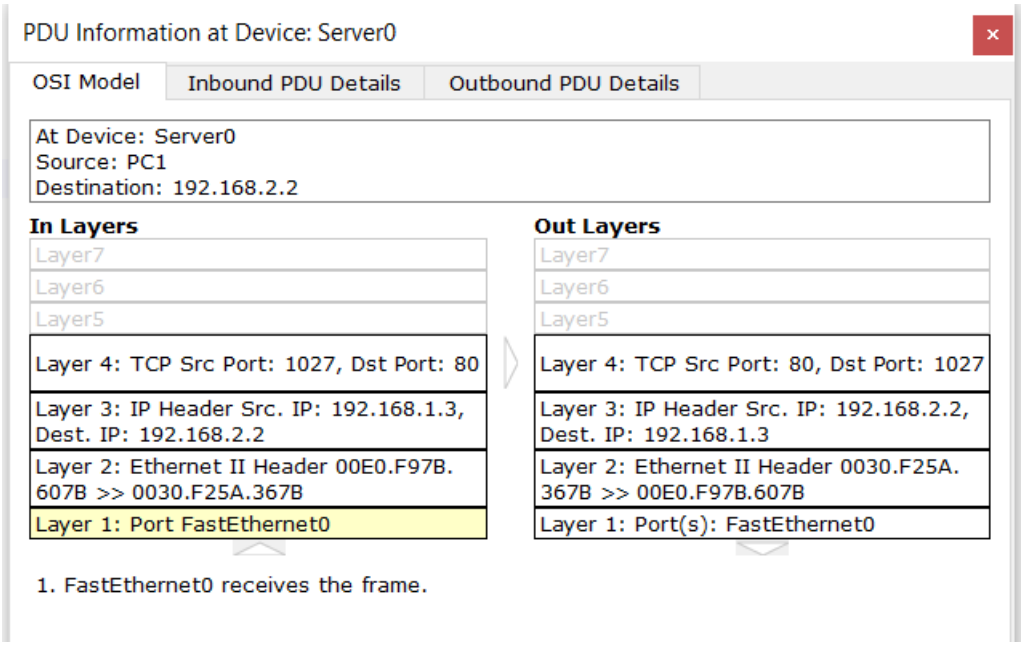


Demo of TCP and HTTP using Cisco packet tracer

Use Simulation Mode Select the PC with IP Address 192.168.1.3 . Click on the webBrowser and type 192.168.2.2 . Show the Demo of TCP by right clicking on the Envelop. Note down the values at every Layer.

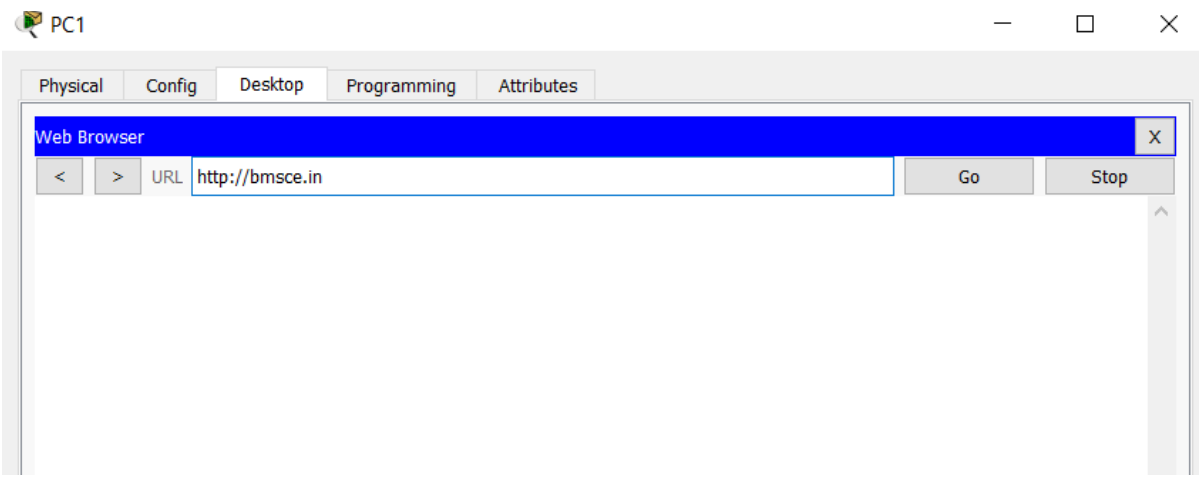


PDU information at Web server

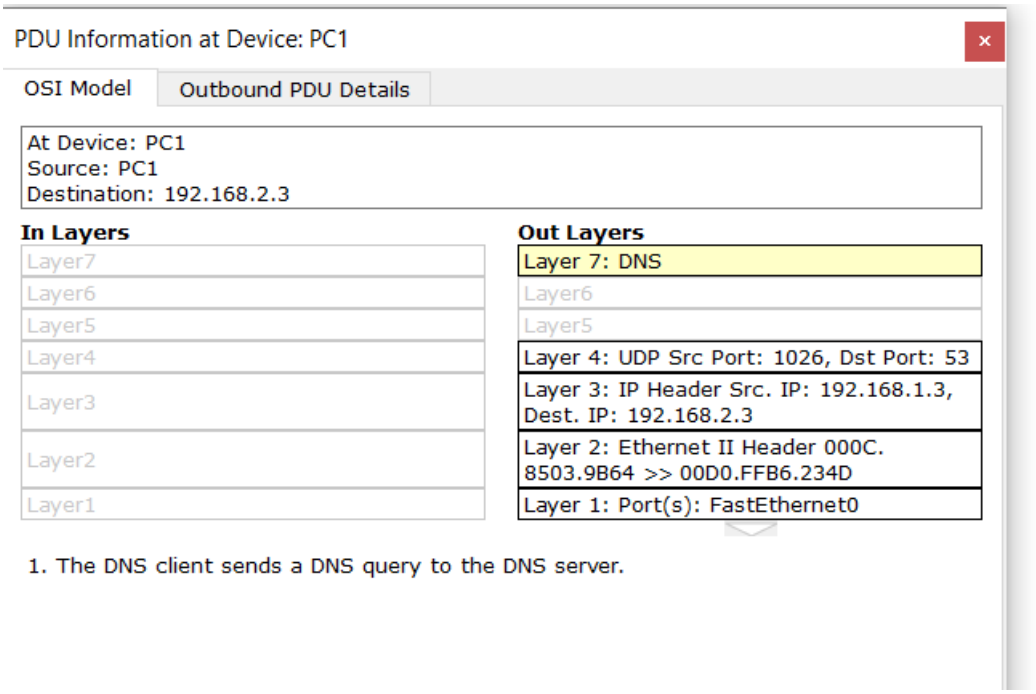


Demo of UDP with DNS

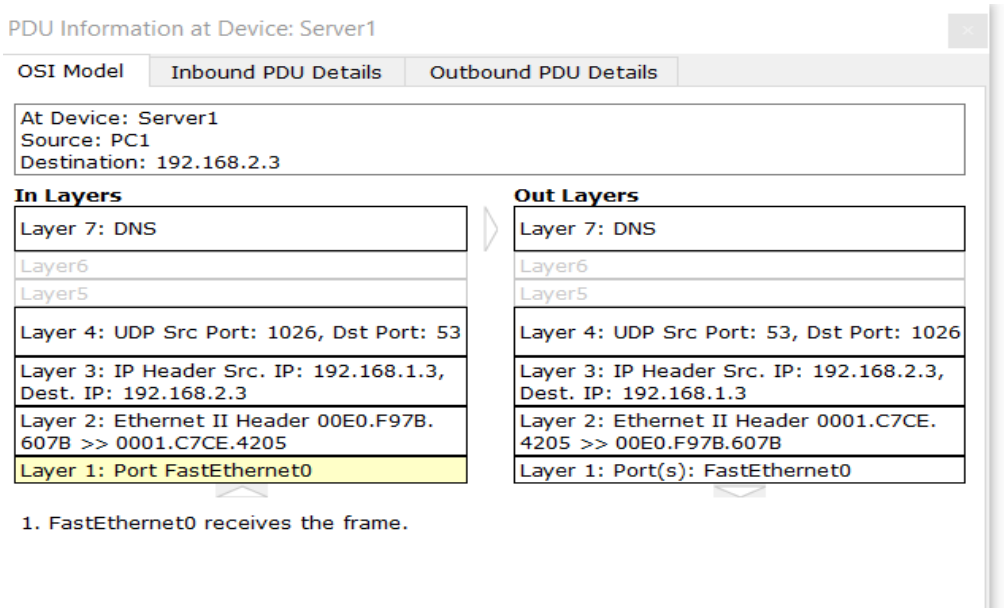
At the same PC in Simulation mode select web Browser and type bmsce.in



Show the demo of UDP with DNS



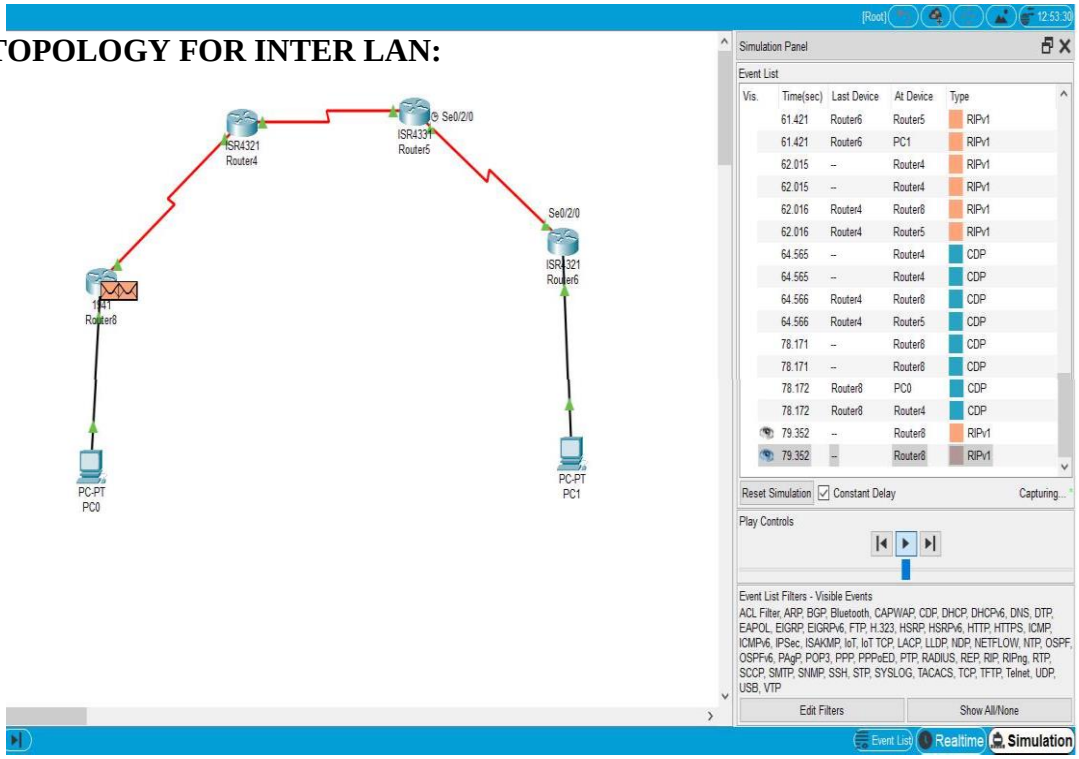
At the DNS Server



Experiment No. 8

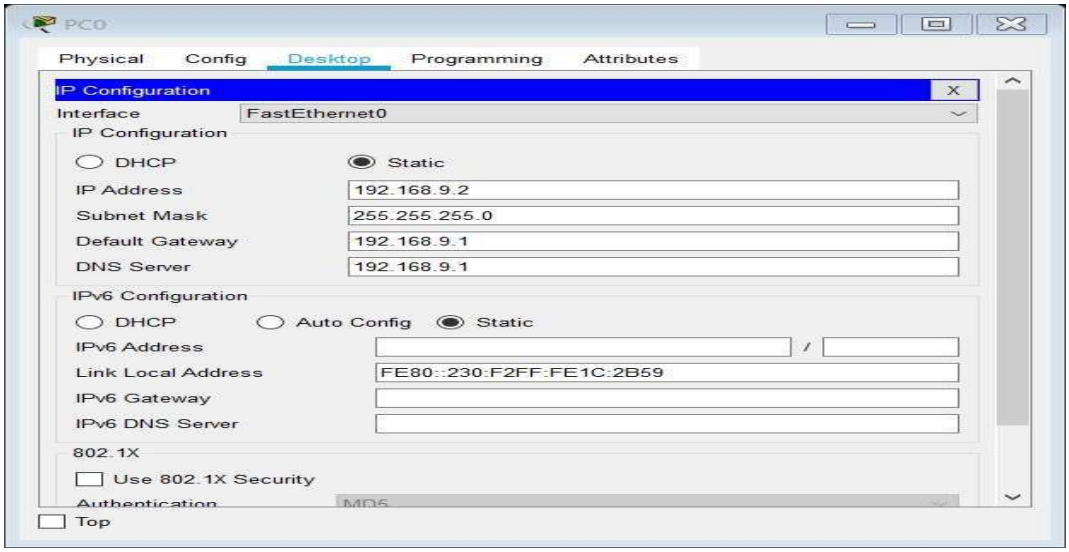
AIM: To study about the configuration of distance vector RIP routing protocol by using Cisco Packet Tracer.

NETWORK TOPOLOGY FOR INTER LAN:

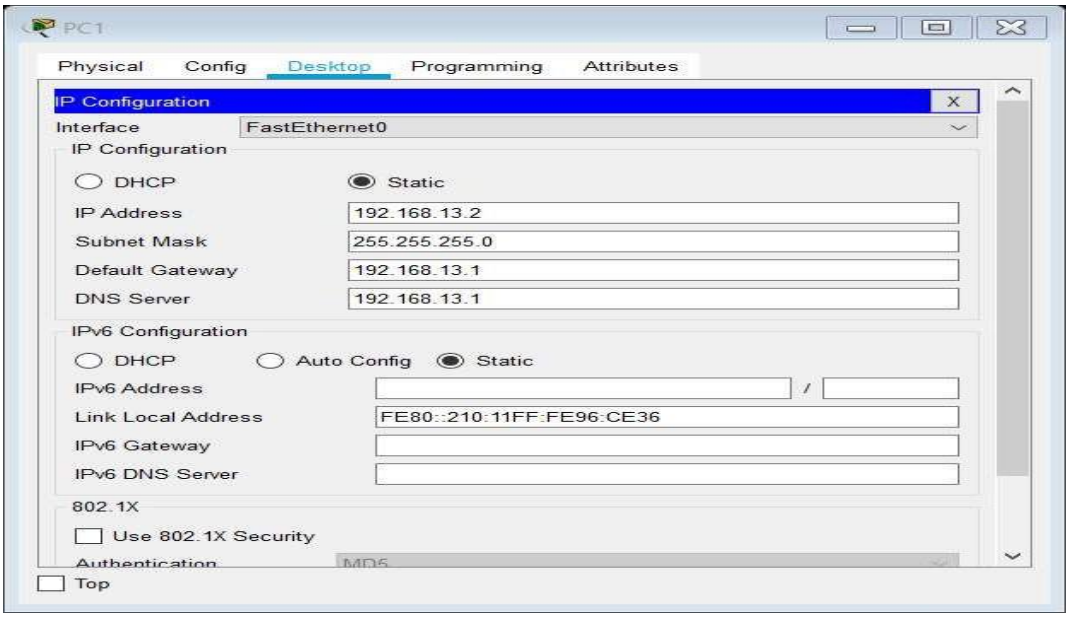


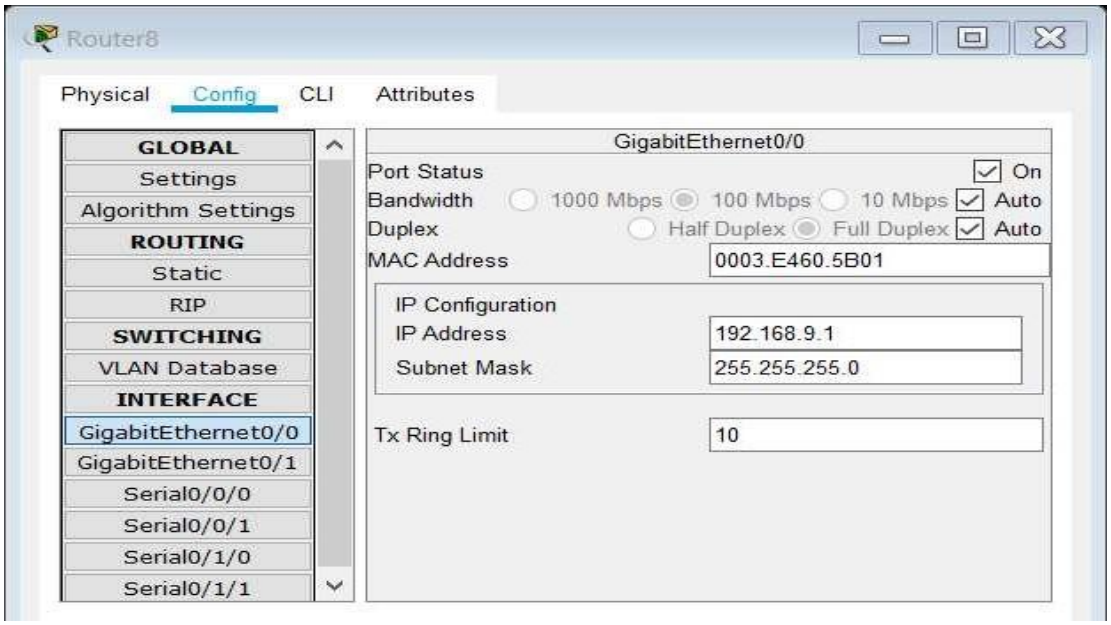
CONFIGURATION OF IP AND SUBNET MASK AT PC:

PC-0:

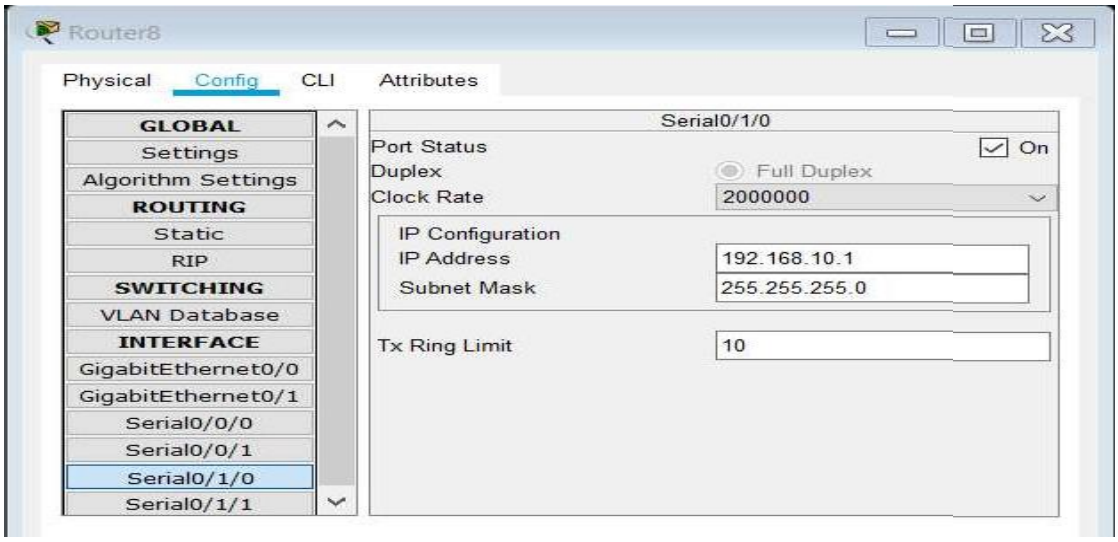


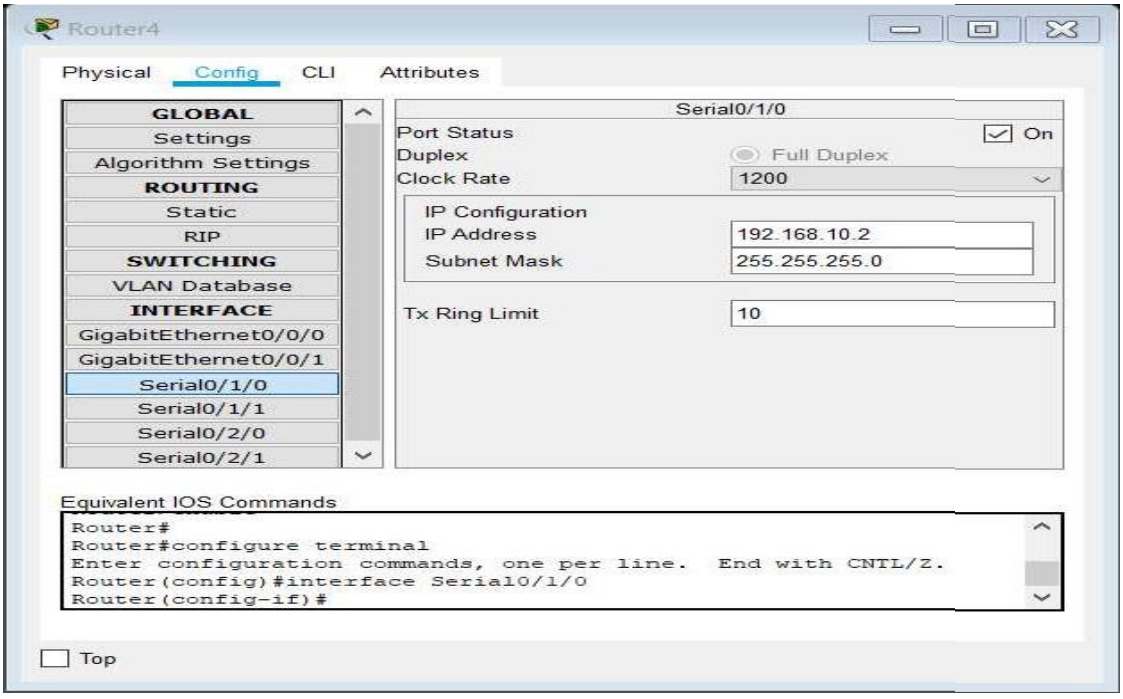
PC-1:


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.13.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.13.1
DNS Server
192.168.13.1
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::210:11FF:FE96:CE36
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top

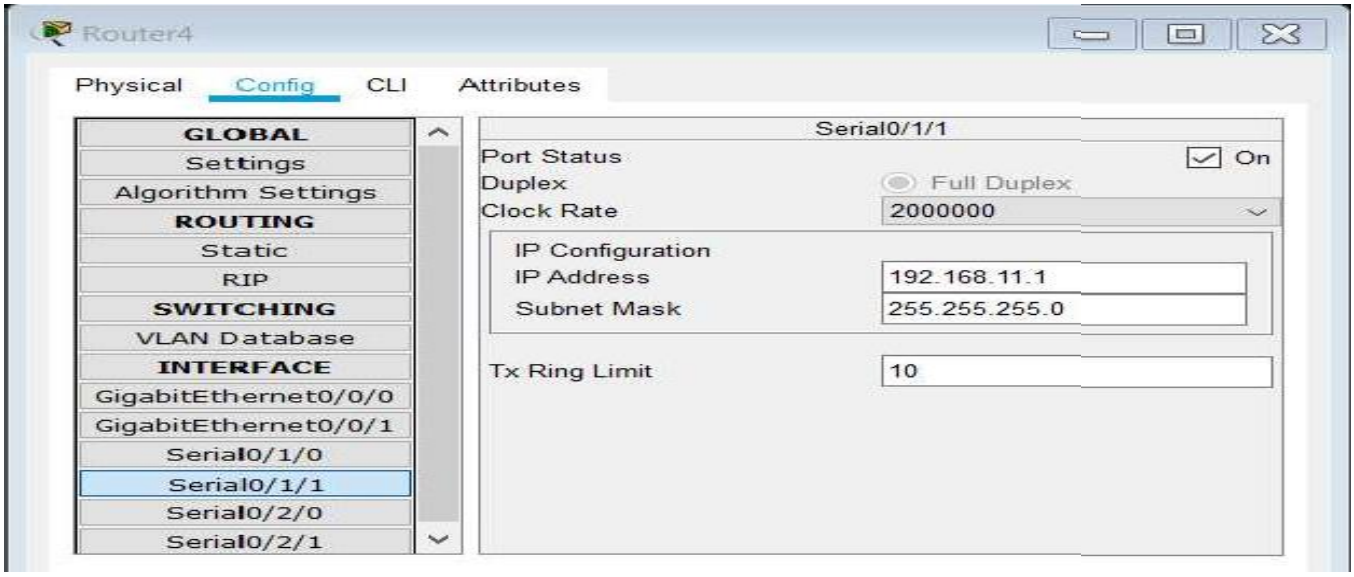

Router8
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0003.E460.5B01
IP Configuration
IP Address
192.168.9.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

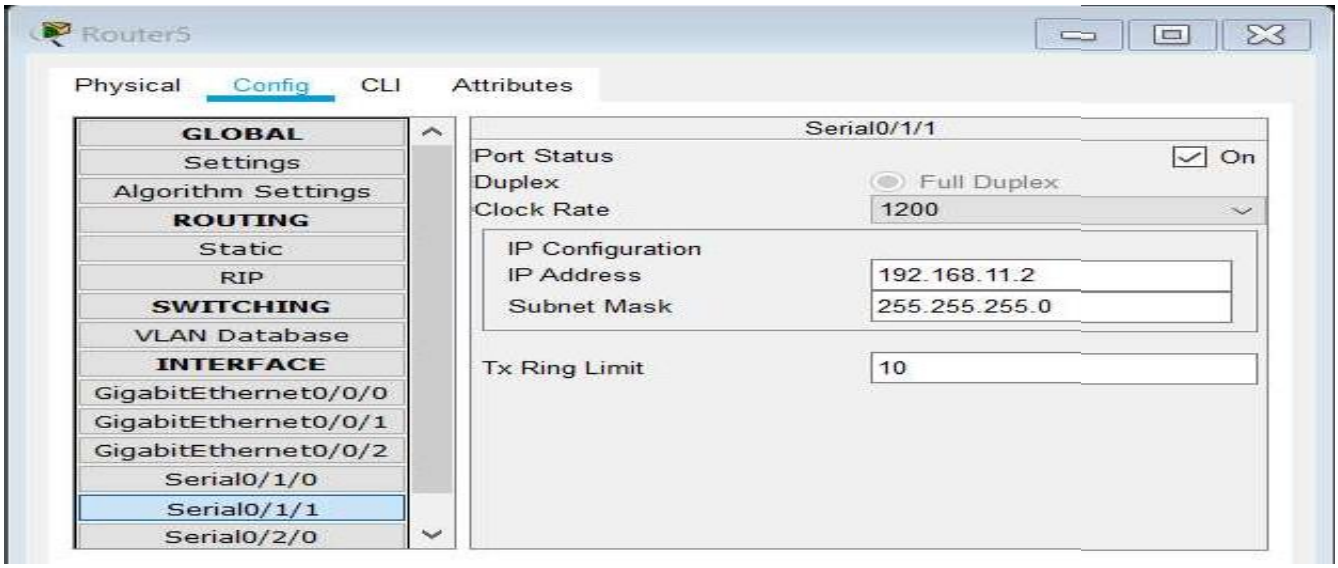
ROUTER8 (Serial 0/1/0)



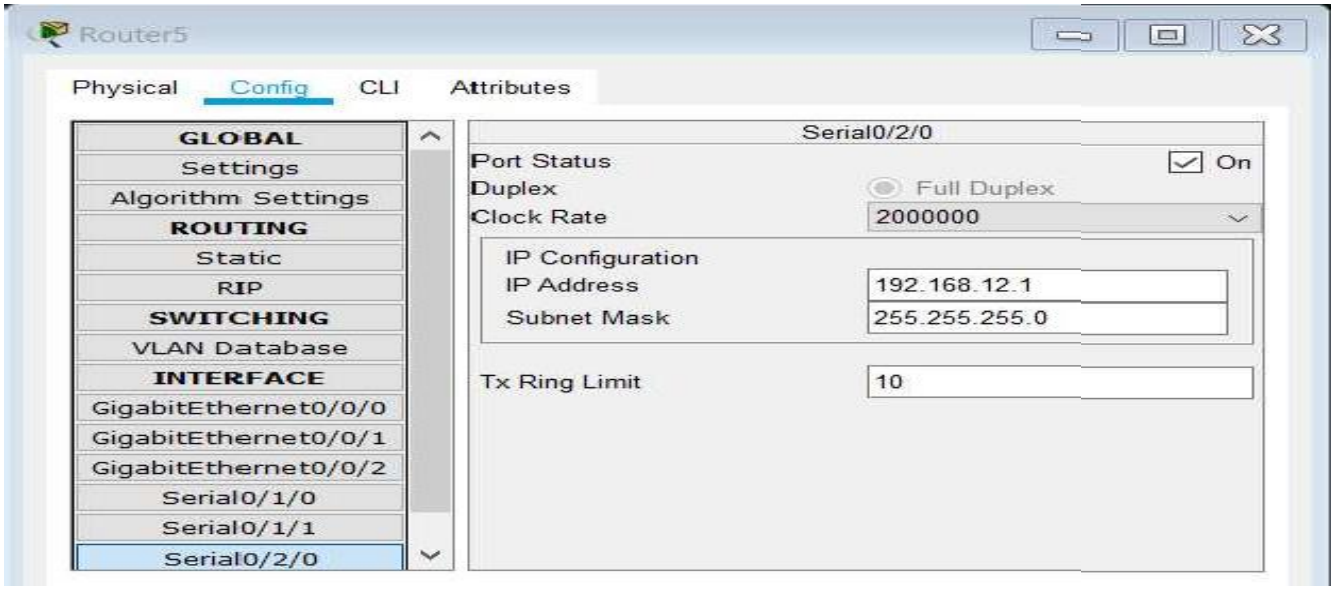


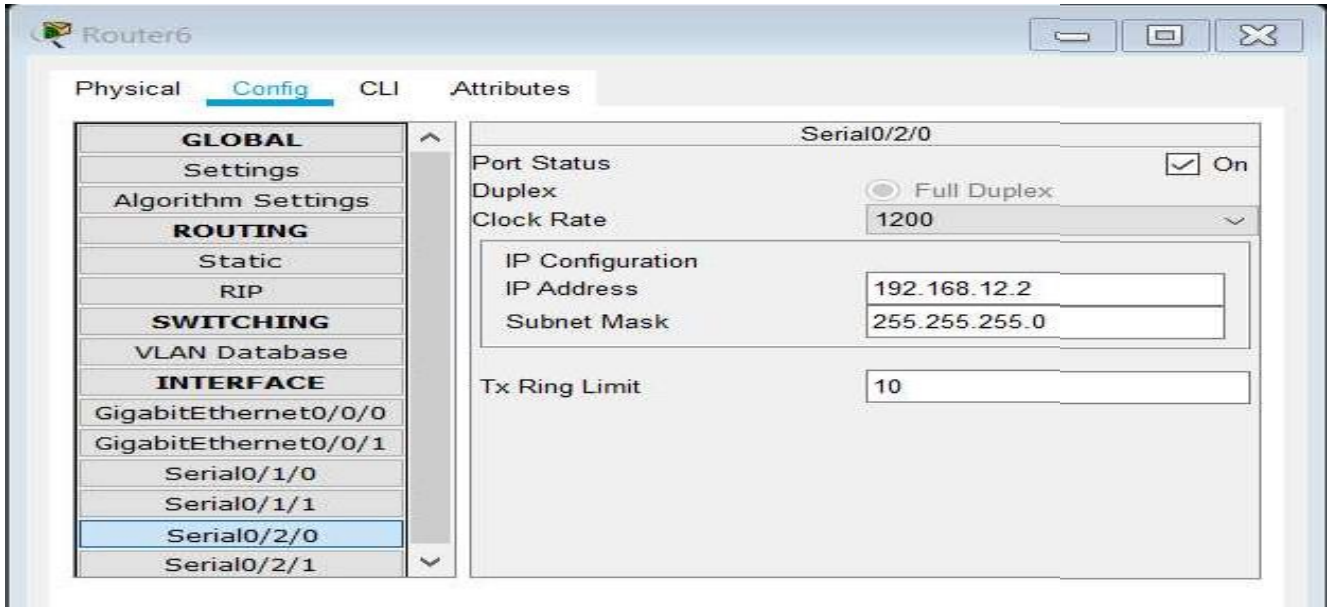
ROUTER4 (Serial 0/1/1)



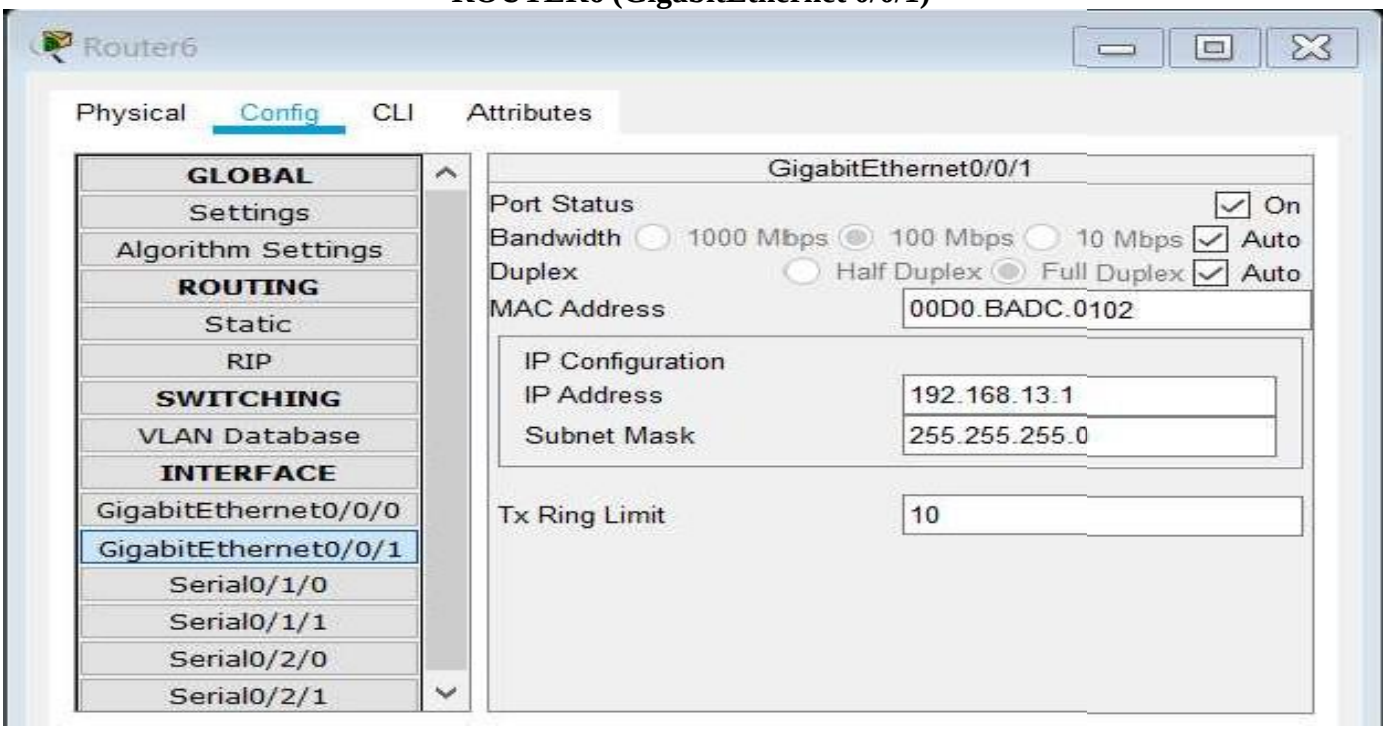


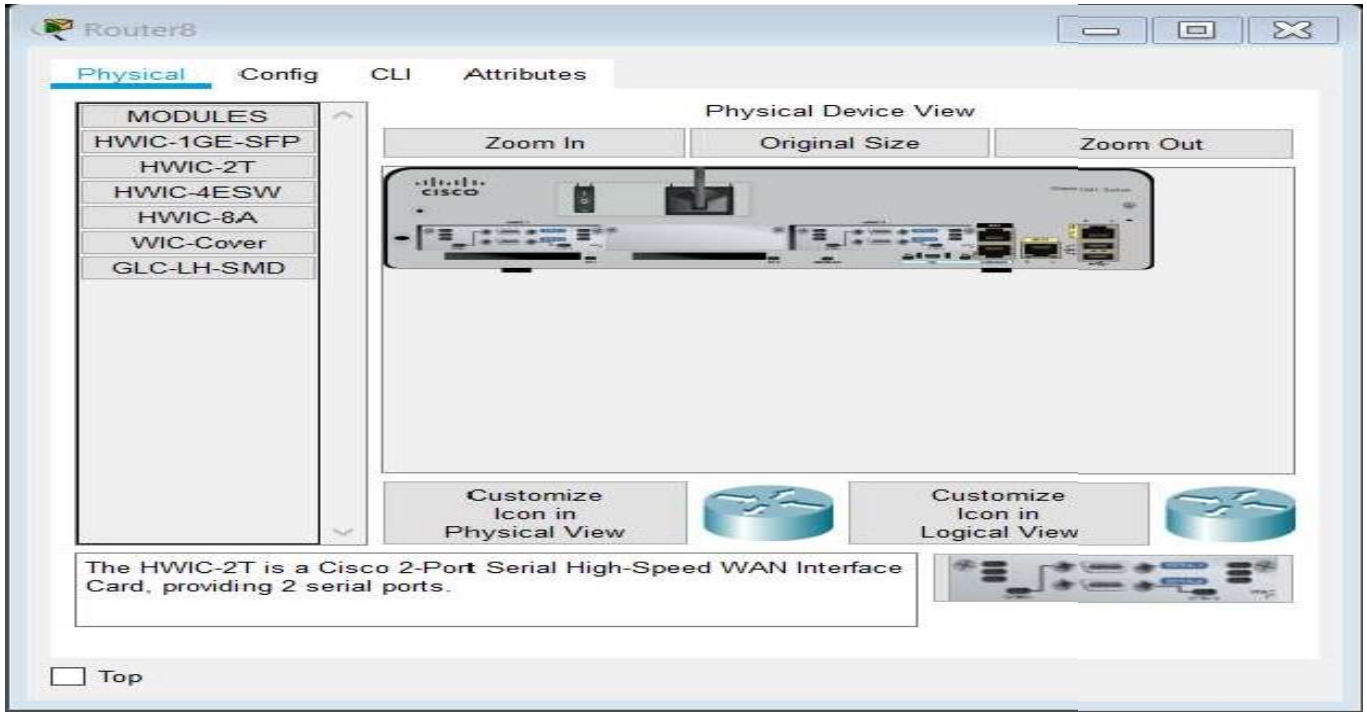
ROUTER5 (Serial 0/2/0)



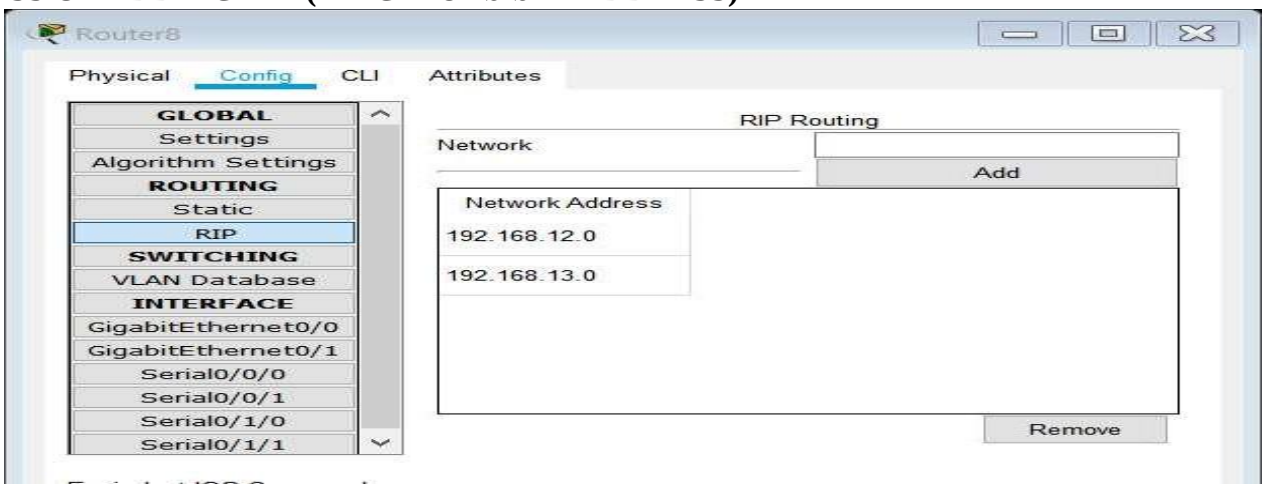


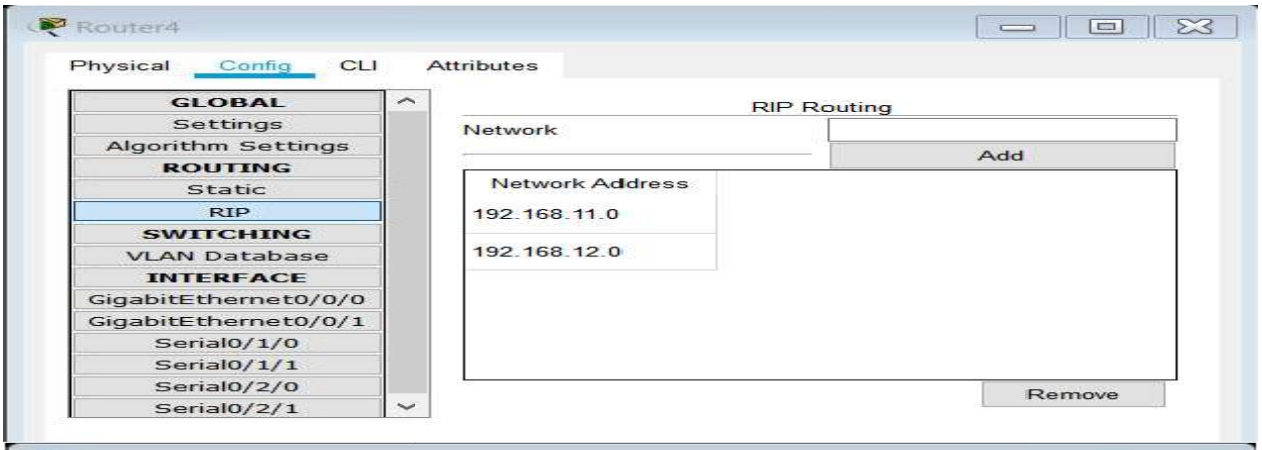
ROUTER6 (GigabitEthernet 0/0/1)

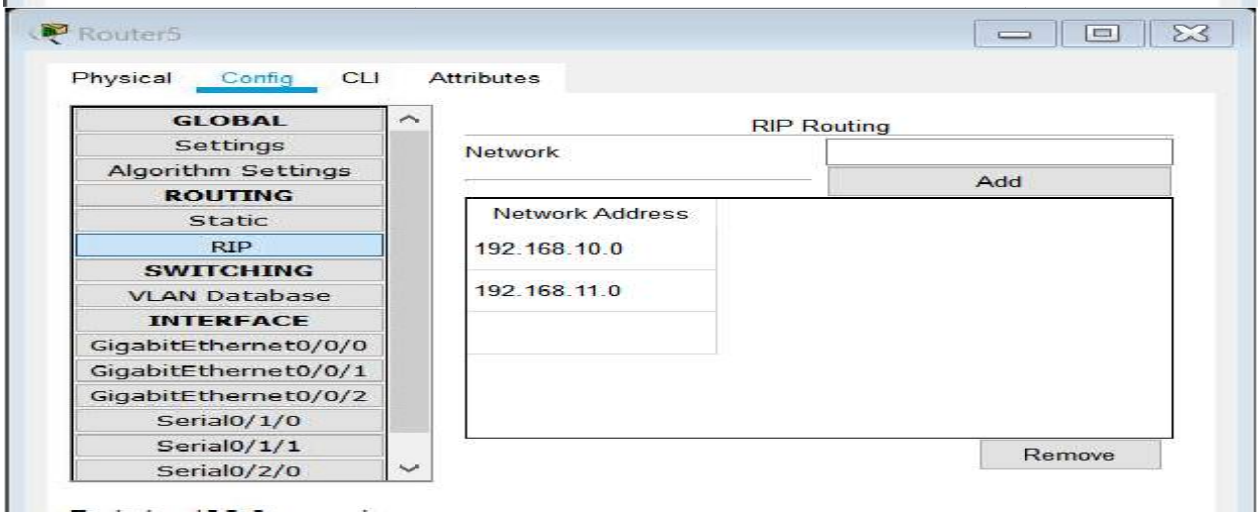


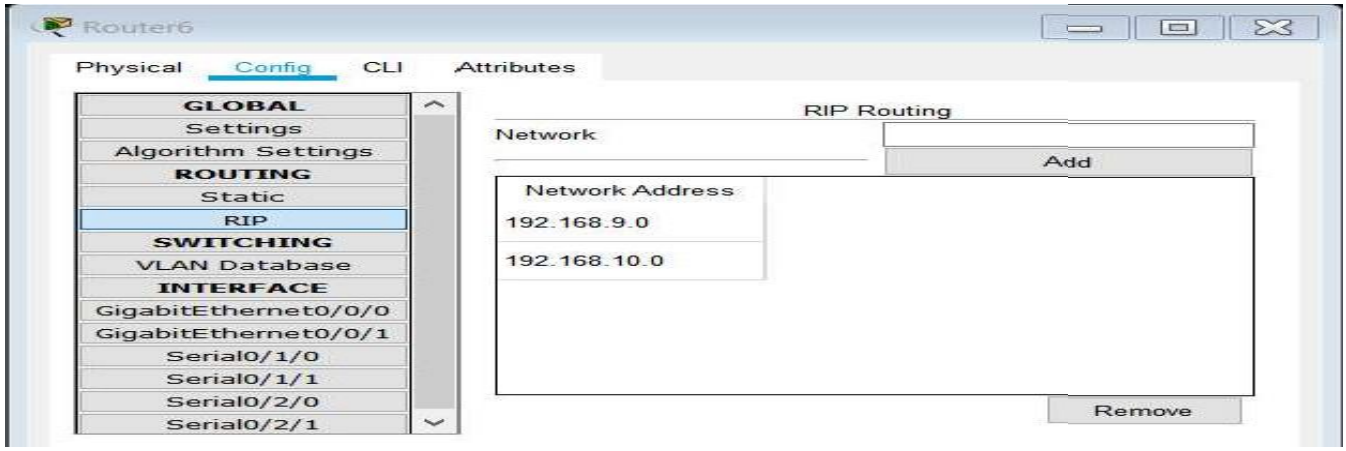


PROCESS OF ADDING RIP (NEIGHBORS'S IP ADDRESS)

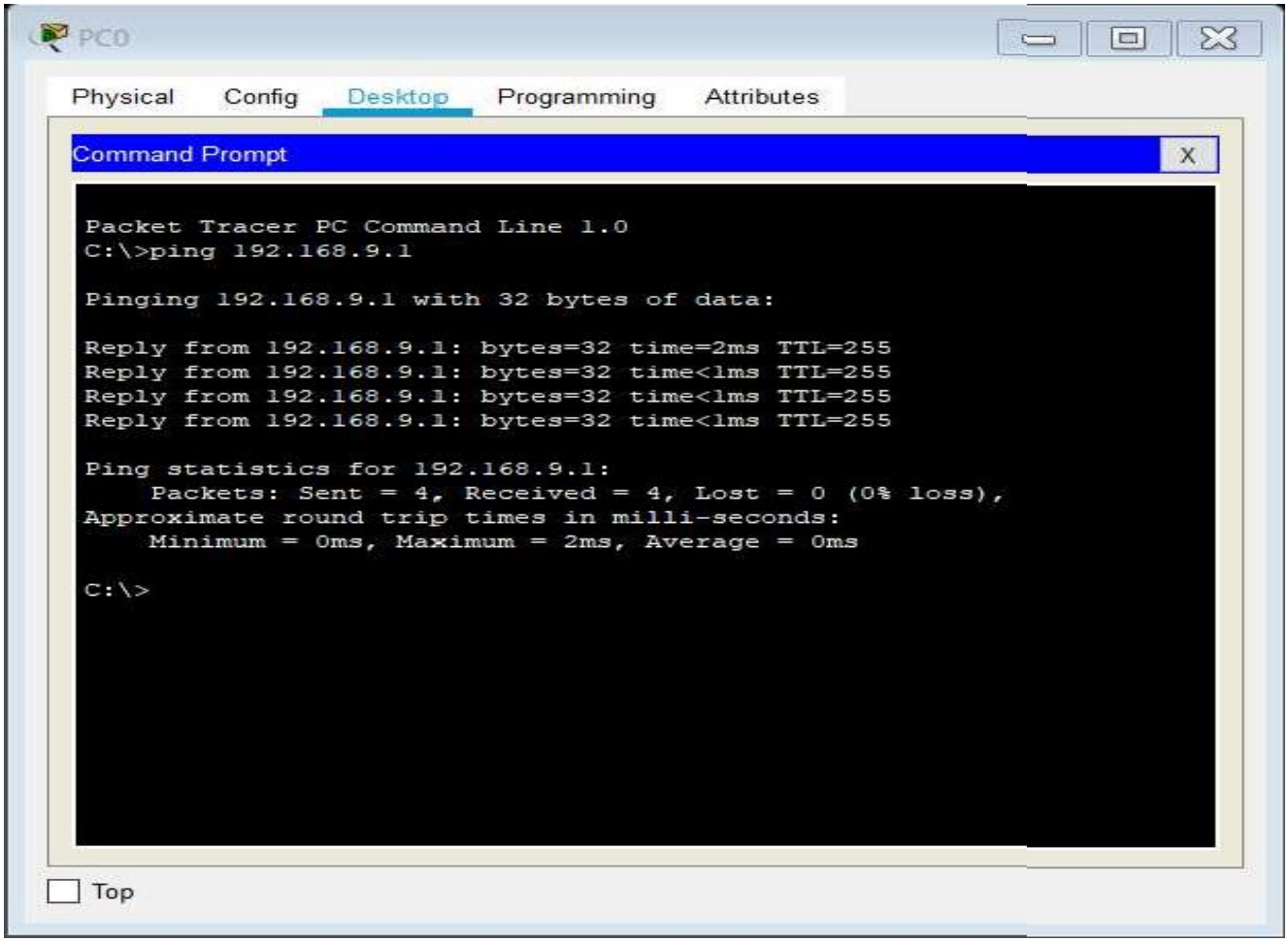








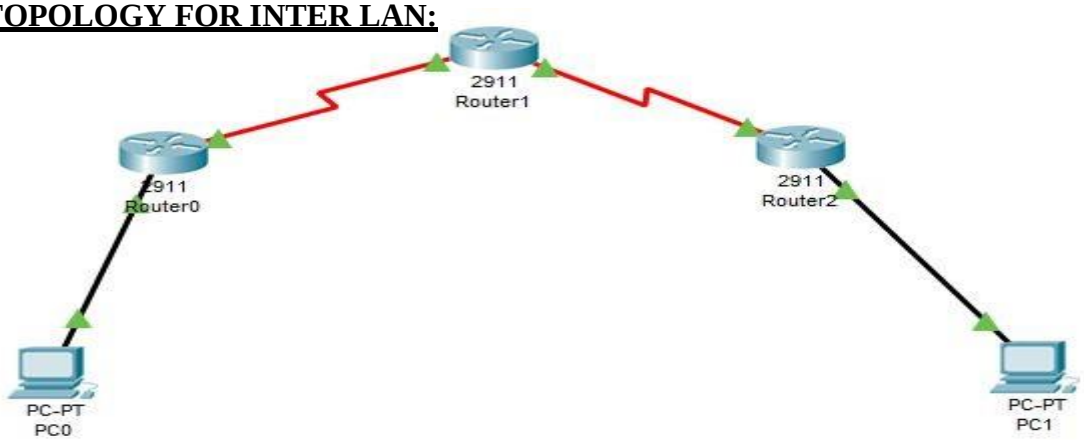
Using Ping command:



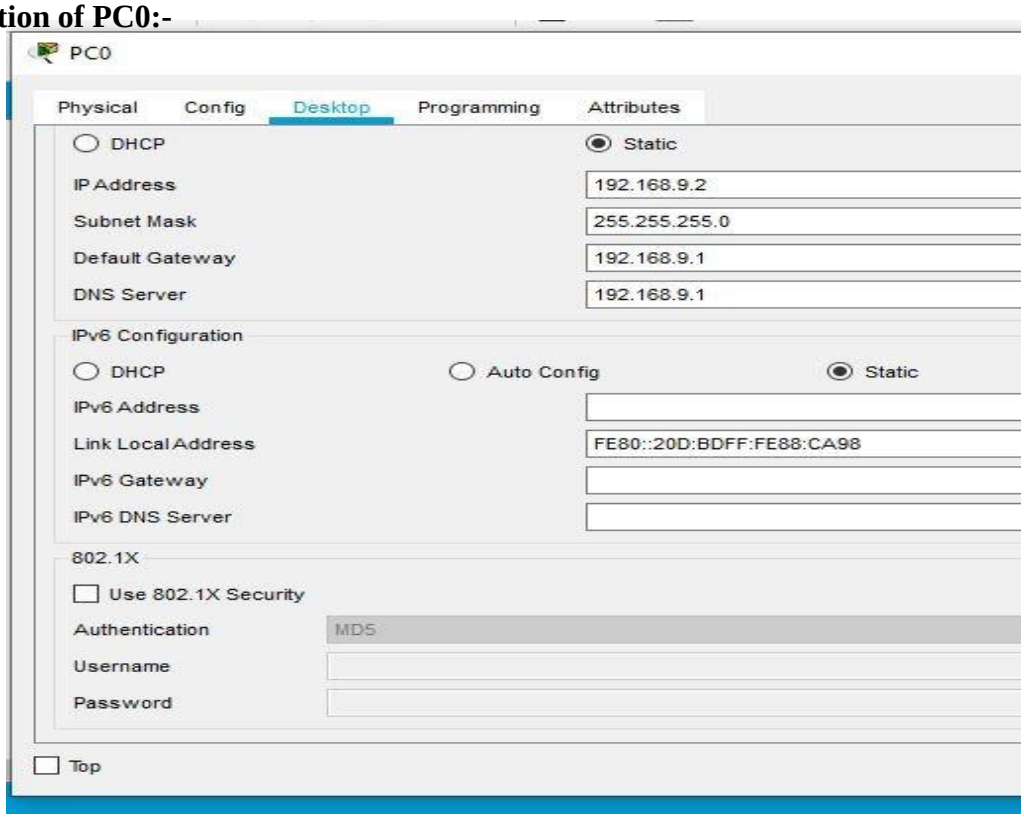
Experiment No. 9

AIM: To construct multiple router networks and implement the EIGRP Protocol.

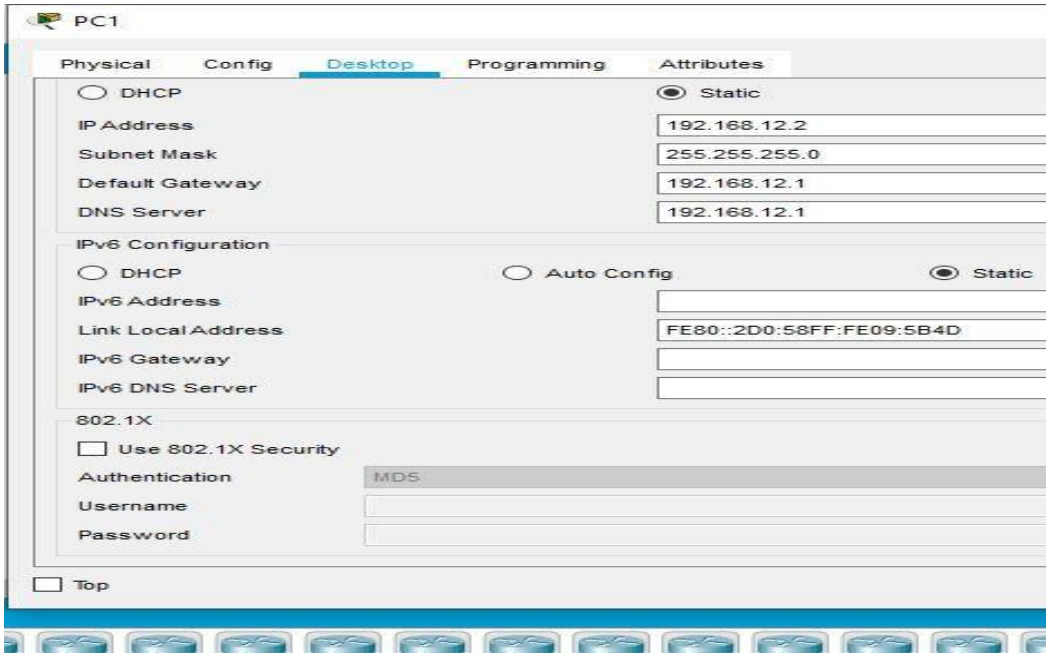
NETWORK TOPOLOGY FOR INTER LAN:



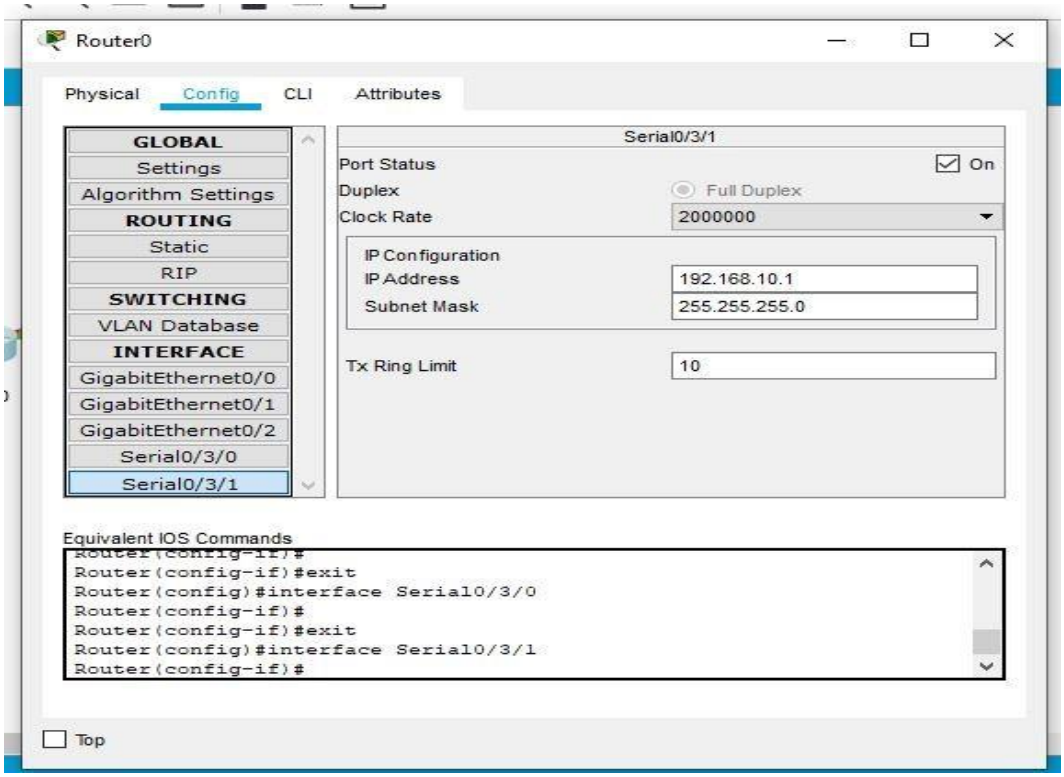
Configuration of PC0:-



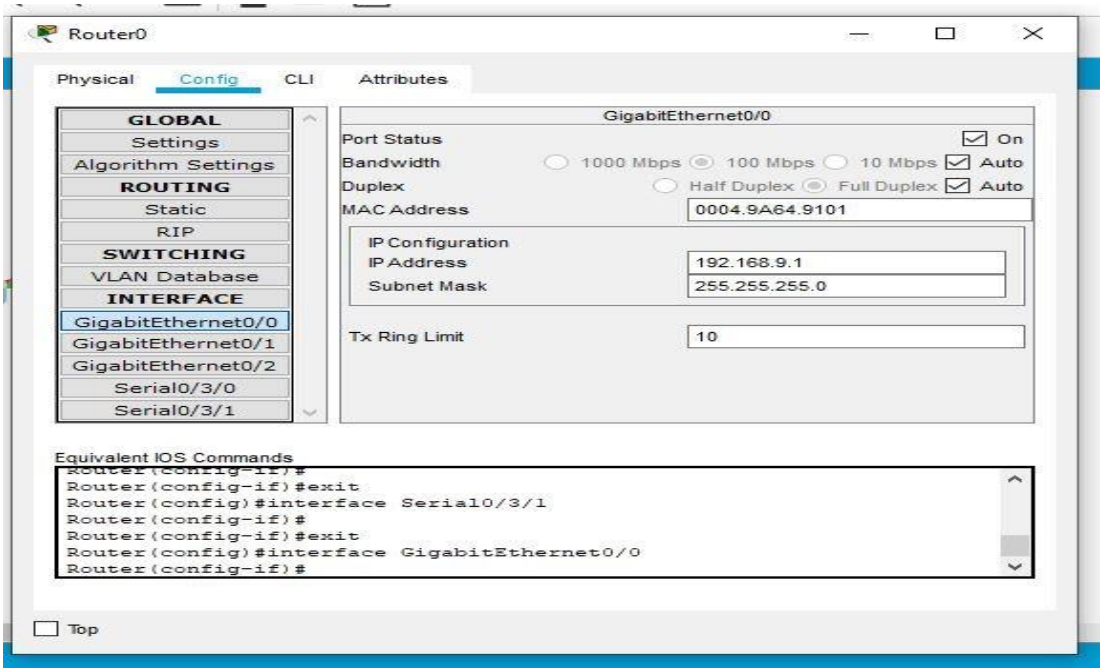
Configuration of PC1:-



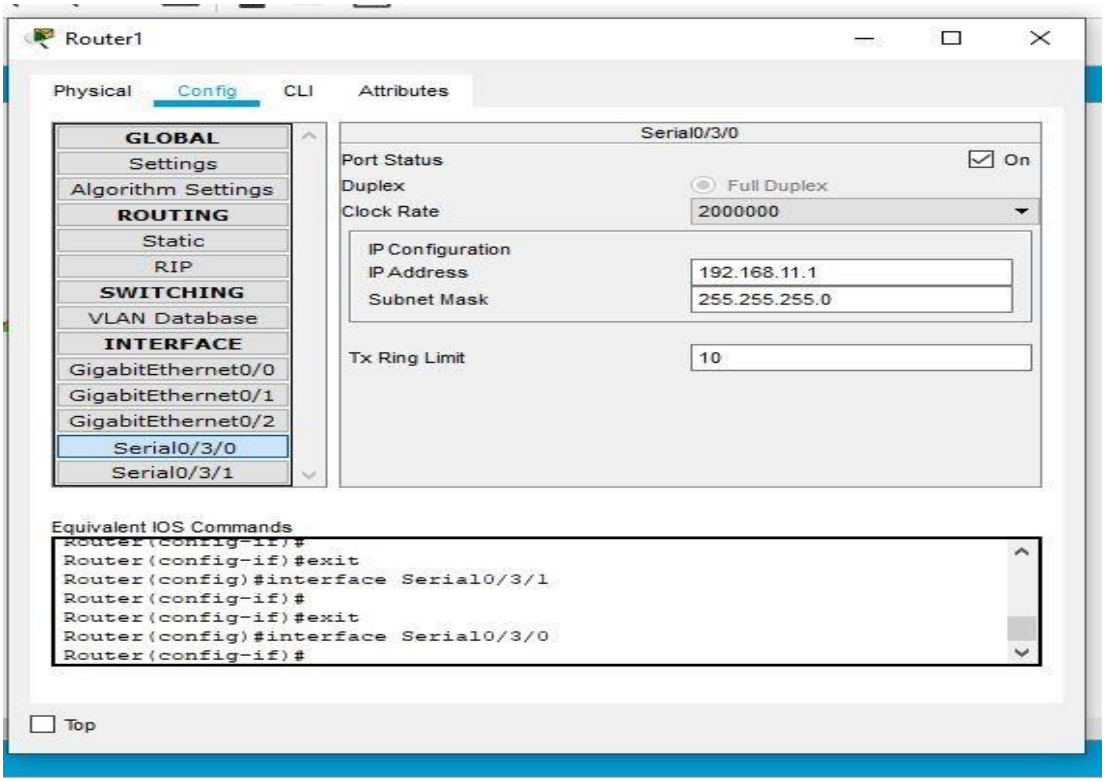
Configuration of Router 0(Serial 0/3/1):-



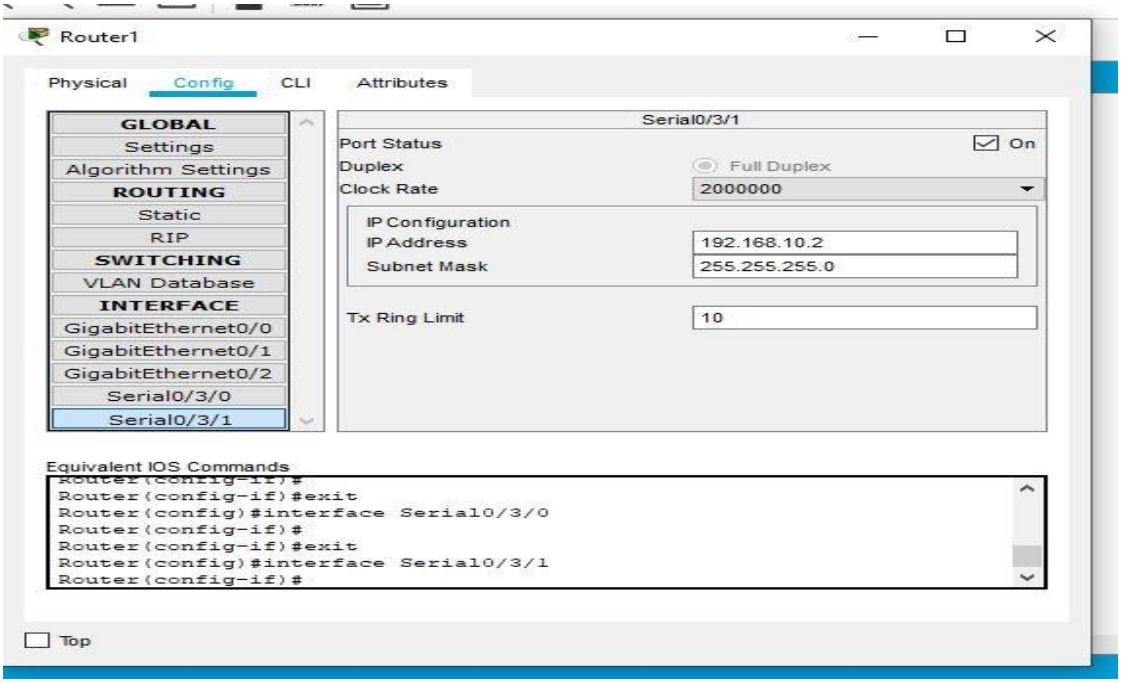
Configuration of Router 0 (GigabitEthernet 0/0):-



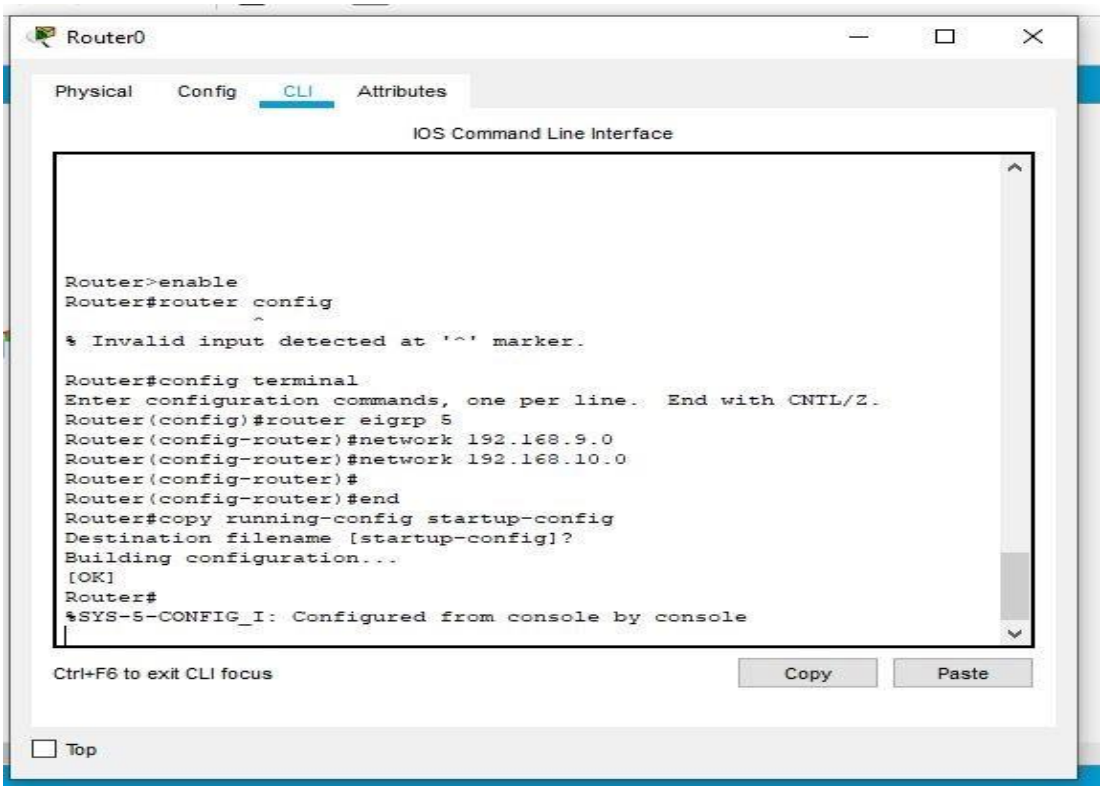
Configuration of Router 1(Serial 0/3/0):-



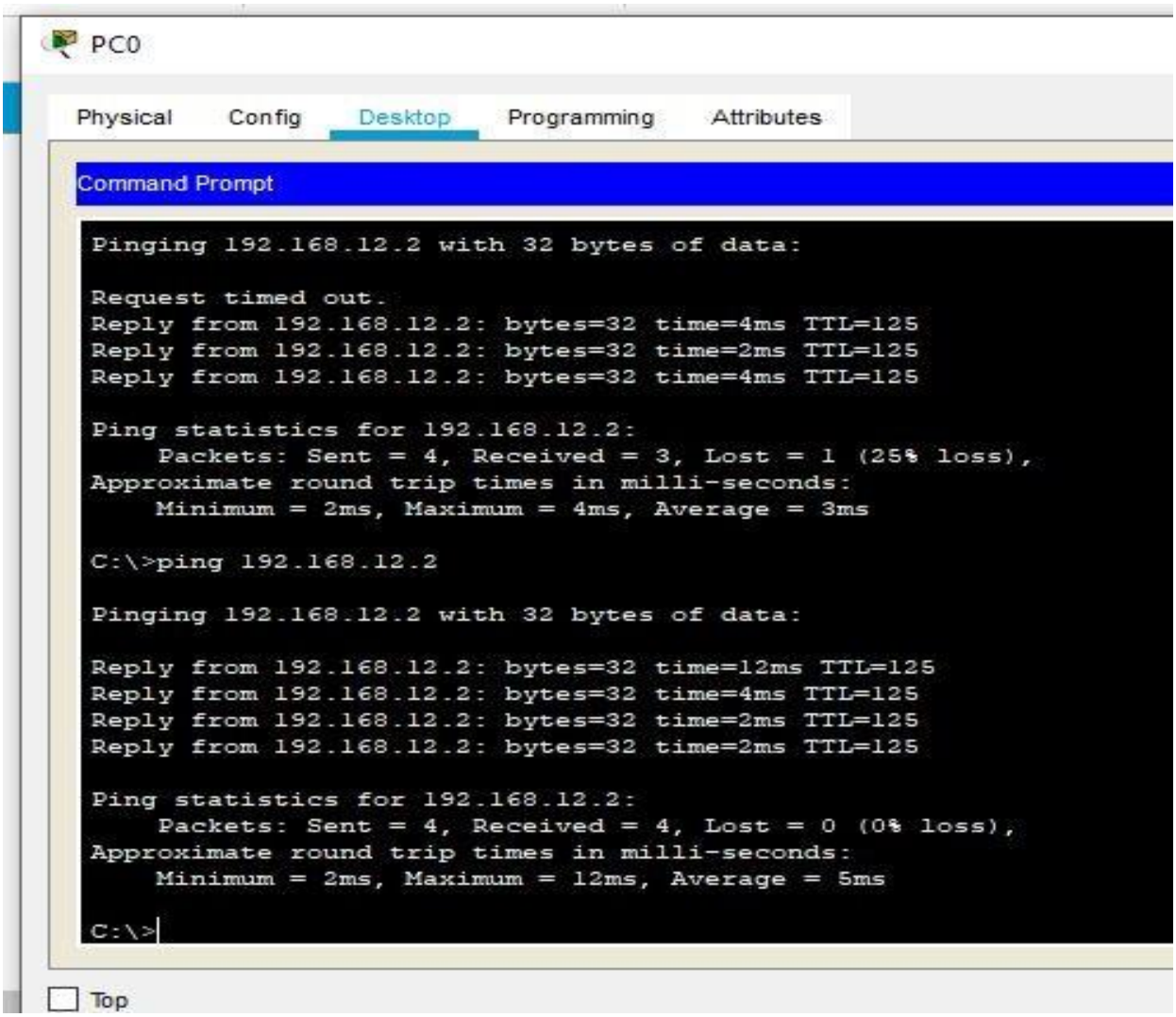
Configuration of Router 1(Serial 0/3/1):-



Router 0 CLI configuration:-



TERMINAL OUTPUT-:



Experiment No. 10

Aim-: To implement the Network Address Resolution (NAT) using Cisco Packet Tracer.

For a computer to communicate with the Internet as a whole, it must have an IP address. Usingthe IPv4 system, these are unique, 32-bit numbers that are broken up into four different binaryoctets. It doesn't matter whether it's a server, or a computer, or an Xbox. If it doesn't have an IP address, it's not getting online.

But, there simply isn't enough IP addresses to go around to give each host their own address. So, in order to make better use of the extremely limited address space available, we use Network Address Translation.

Network Address Translation allows a single device to sit between a local area network and the Internet, and forward traffic to the appropriate host. You probably know this as your router.The advantage of this is multiple computers can share the same IP public address.

This single device (usually a router, switch, or hardware firewall) modifies IP packet headerson the fly, ensuring that the contents of the packet get to the intended destination. However, itcomes with a downside, as it becomes exponentially harder for hosts outside the local networkto communicate with servers that are located behind the router.

There are multiple ways in which Network Address Translation can work, with the three of themost common being Dynamic NAT, Static NAT, and Overloading.

1. Dynamic NAT

With Dynamic NAT, a router will maintain a list of public IP addresses. When a host behind the network needs to transmit or receive, the router will select one of the public IP addresses that is not currently in use, and forward any packets accordingly. As a result, this means a host's IP address can change at any given moment.

But crucially, it means a large pool of hosts can share a significantly smaller pool of IP addresses. This was vital, given the impending exhaustion of the available pool of IPv4 addresses.

2. Overloading (PAT)

A common way of performing network address translation is through something called 'Overloading', where multiple internal IP addresses are mapped to a single public IP address. This is done by giving each internal host a corresponding port. For instance, suppose you'vegot three computers on an internal network, and a public IP address of 212.18.123.123. Eachof those internal computers could theoretically be accessible via 212.18.123.123:2001,212.18.123.123:2002 and 212.18.123.123:2003.

This is commonly known as Port Address Translation (PAT), Single-Address NAT, and port-level multiplexed NAT.

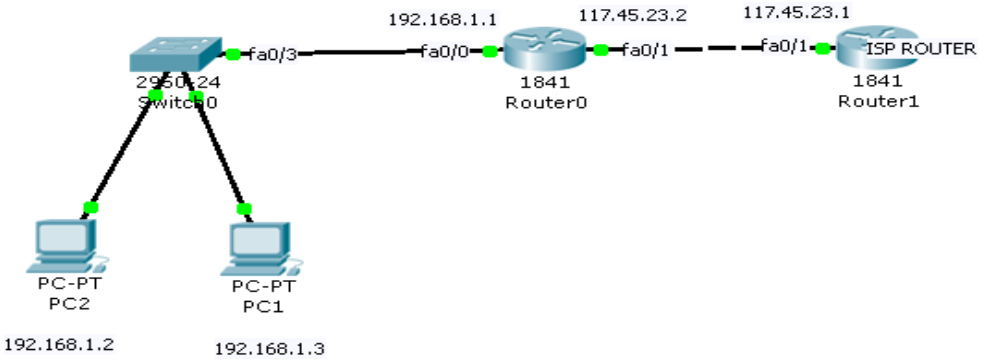
3. Static NAT

Finally, let's talk about Static NAT.

Internal networks, like your home or office network, do not use the same IP addressing systemthat's used on the public Internet. Any networked device effectively has two IP addresses. Thefirst is a private one, and that's only reachable from within that network. The second is the onethat's externally accessible.

Static NAT makes it possible to create a direct, one-to-one link between a private IP address and a static, public IP address.

Dynamic Network Address Translation



Step 1: Draw the topology as shown below

Configure the devices with the IP address as shown in above figure.

Step 2: Configure the router 0 as below

Clock on Router 0

Select CLI

Execute the following commands-:

Router>enable

Router#configureterminal

Router(config)#interface fastethernet 0/0

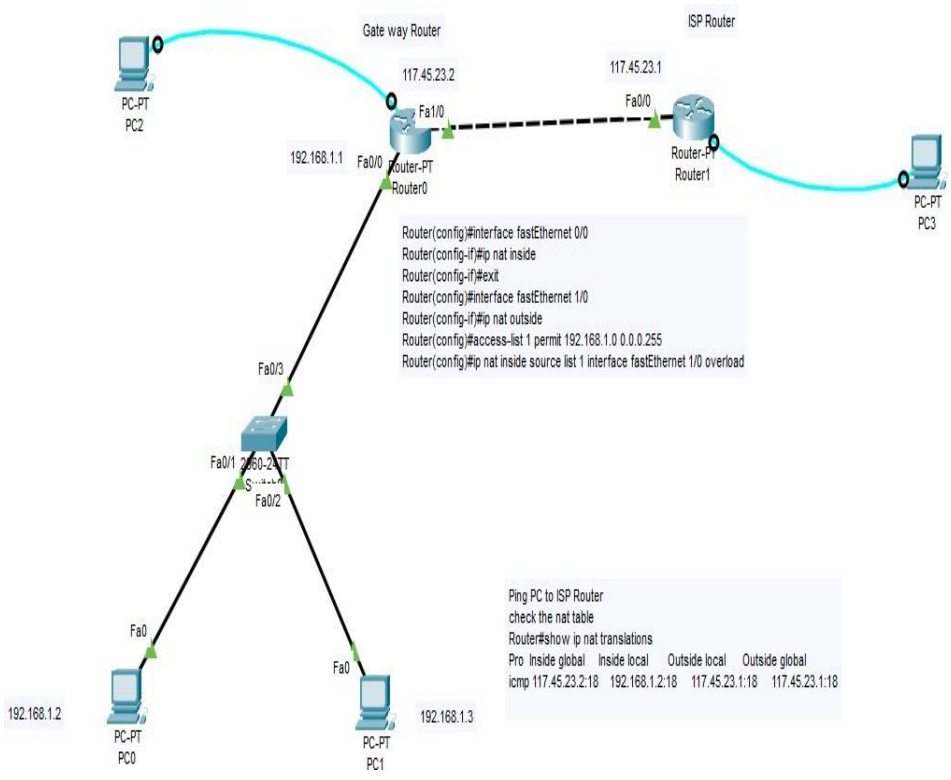
Router(config)#ip nat inside

Router(config)#interface fastethernet 0/1Router(config)#ip nat outside

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#ip nat pool public-ips 117.45.23.2 117.45.23.5 netmask 255.255.255.0

Router(config)#ip nat inside source list 1 pool public-ips overload



Step 1: Design the network as shown in the figure.

Step 2: To configure the routers use the Console.

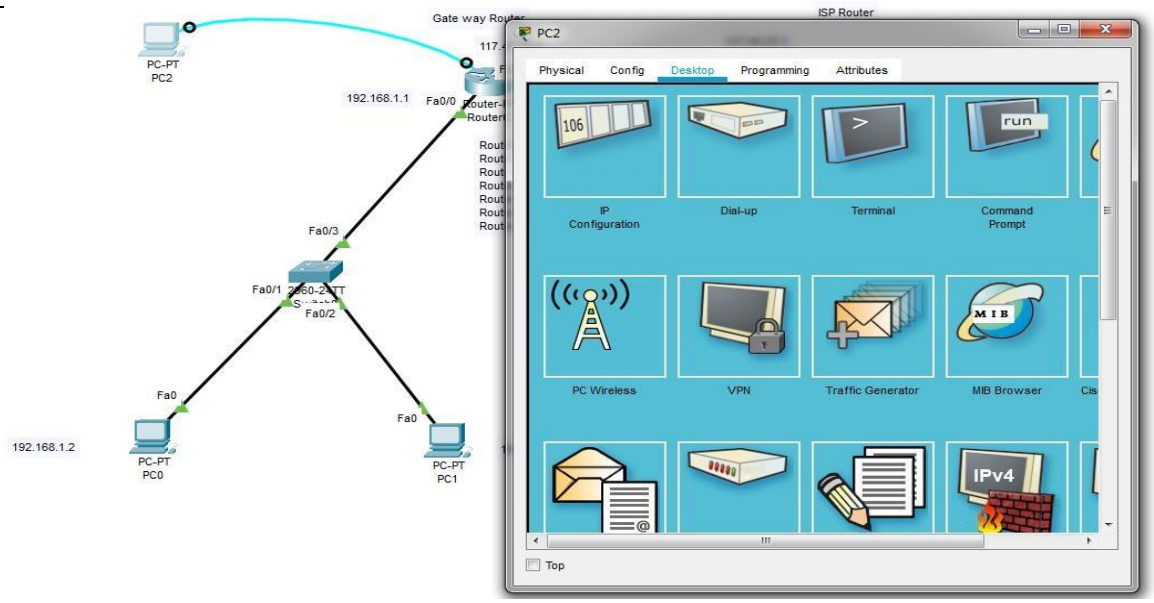
<u>Procedure to Configure the Router Using Console</u>

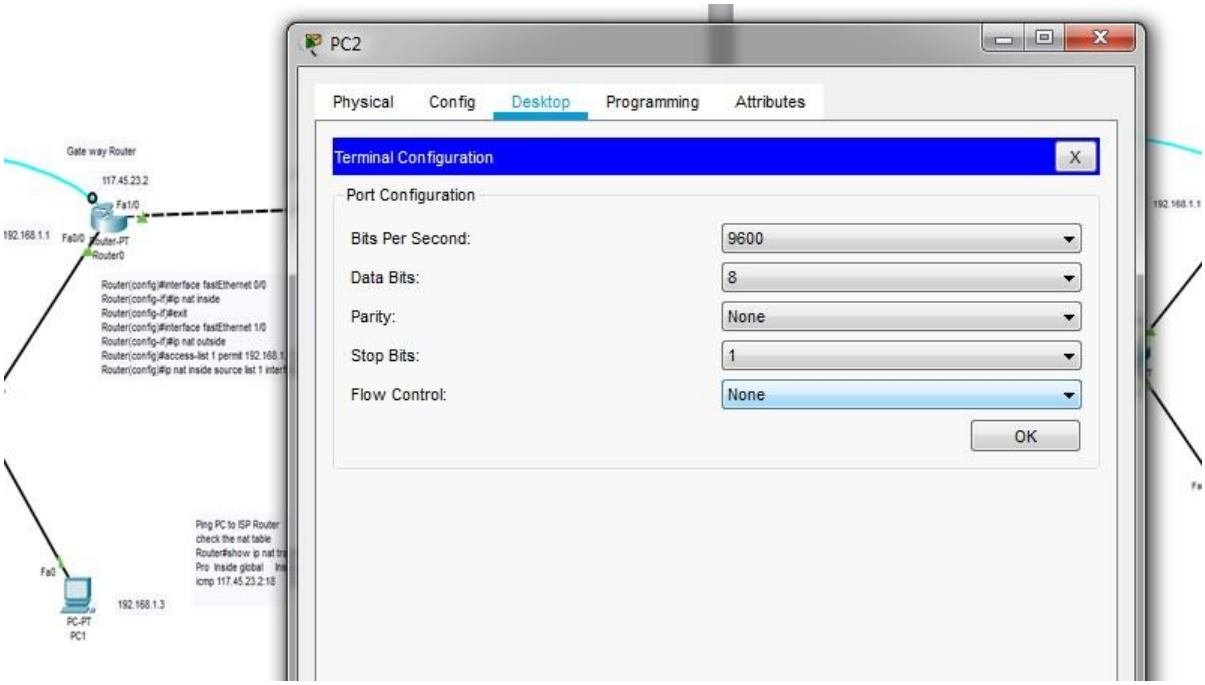
Connect PC and Router using Console Cable.

PC using RS232C and Router to Console Port.

Click on PC

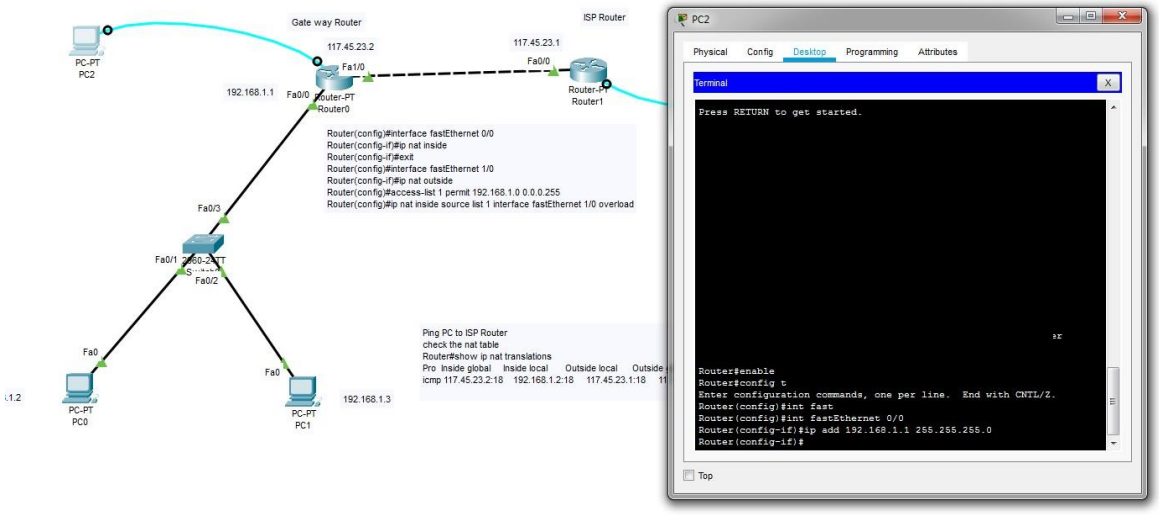
Select Terminal. Click OK. Now the PC will be used to configure the Router.





Step 3: configure two ports fast0/0 and fast1/0

Step 4: Configure Default Gateway of Router – Gateway Router

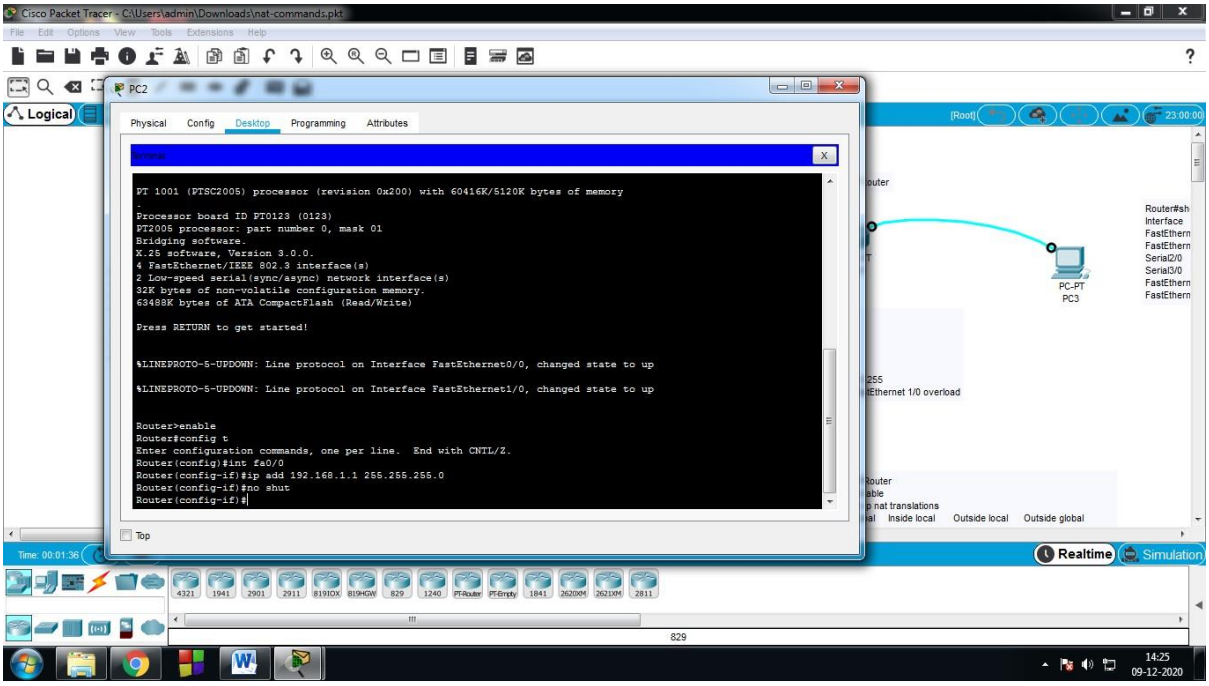


Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int fa0/0

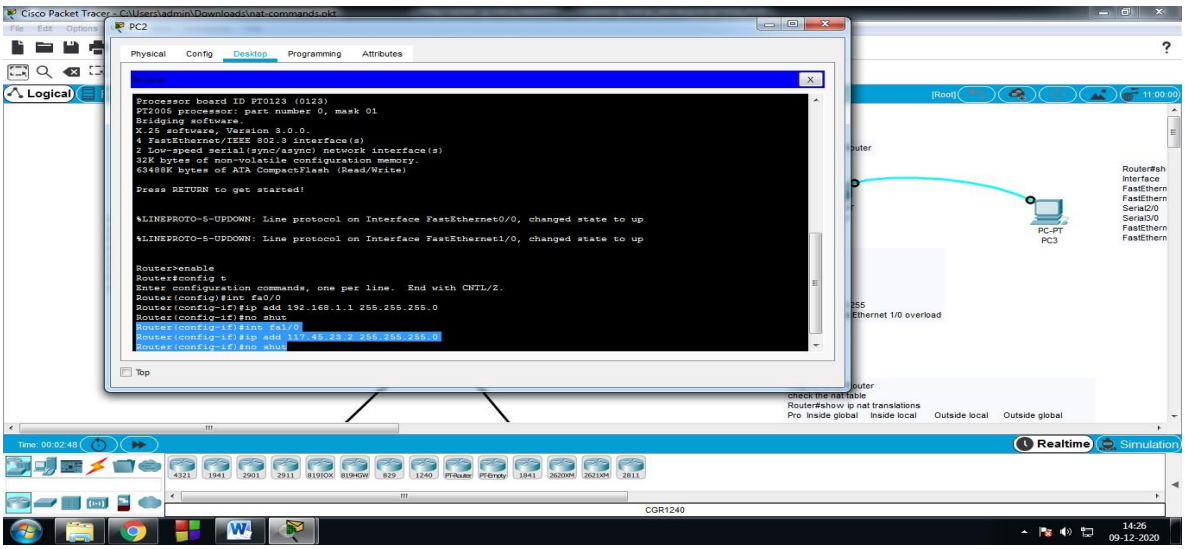
Router(config-if)#ip add 192.168.1.1 255.255.255.0Router(config-if)#no shut



Router#enable Router#config t

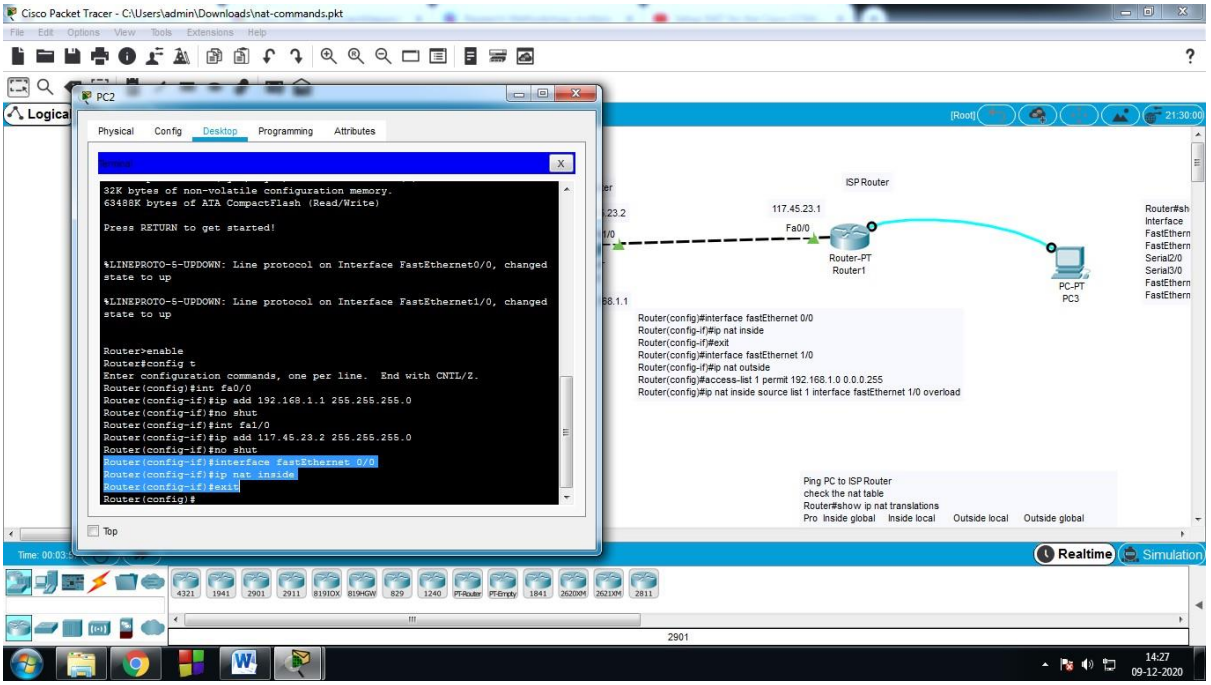
Enter configuration commands, one per line. End with CNTL/Z.Router(config)#int fa1/0

Router(config-if)#ip add 117.45.23.2 255.255.255.0Router(config-if)#no shut



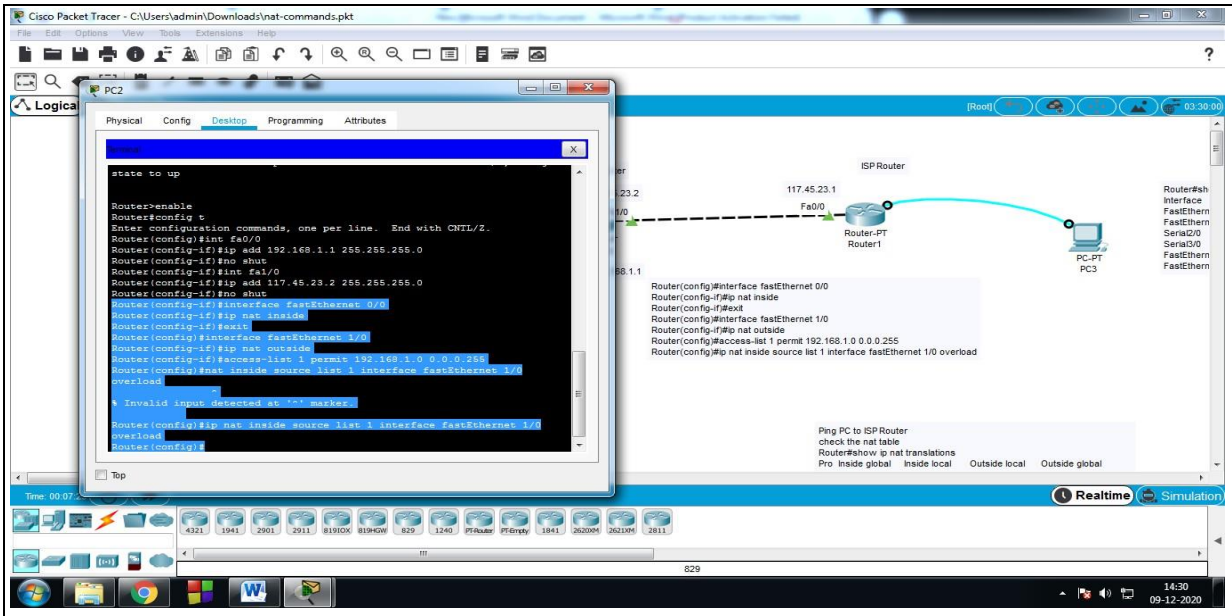
Step 5: configure NATing at Gate way Router

Router(config-if)#interface fastEthernet 0/0Router(config-if)#ip nat inside Router(config-if)#exit



Router(config-if)#interface fastEthernet 0/0Router(config-if)#ip nat inside Router(config-if)#exit Router(config)#interface fastEthernet 1/0 Router(config-if)#ip nat outside

Router(config-if)#access-list 1 permit 192.168.1.0 0.0.0.255 Router(config)#ip nat inside source list 1 interface fastEthernet 1/0 overloadRouter(config)#



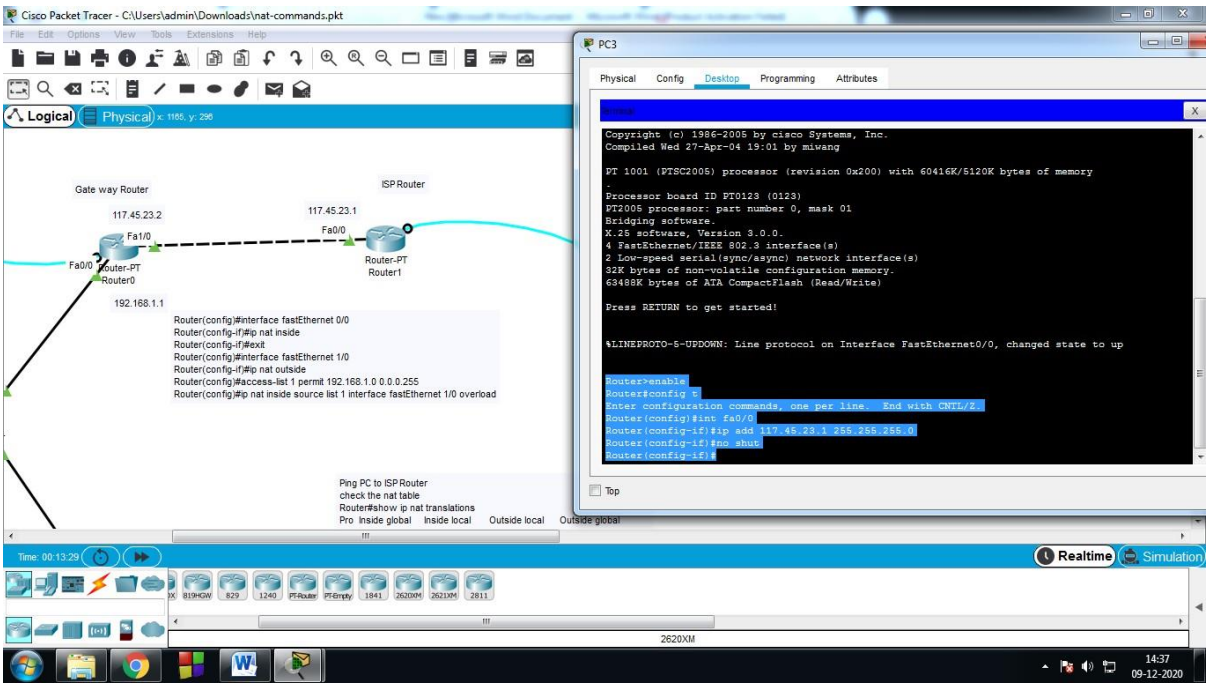
Step 7: Click on PC3 and configure the ports fast0/0

Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z.Router(config)#int fa0/0

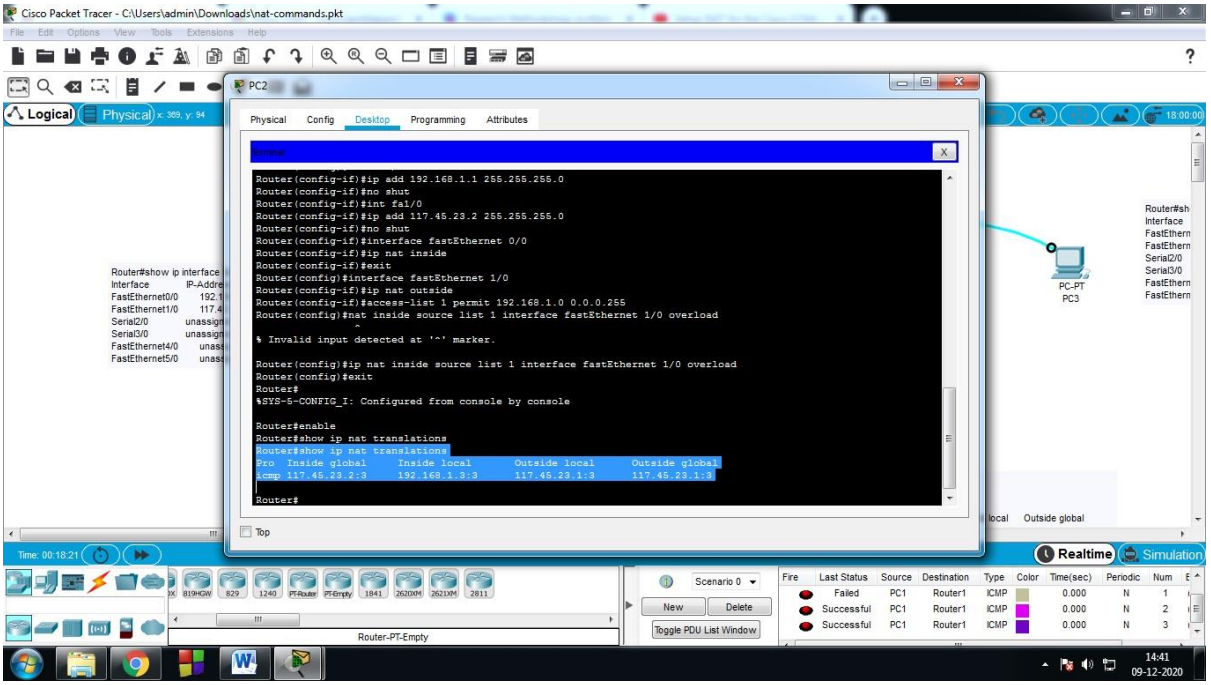
Router(config-if)#ip add 117.45.23.1 255.255.255.0Router(config-if)#no shut

Router(config-if)#



Step 8: Ping PC to ISP Router and check the nat tableRouter#enable

Router#show ip nat translations



Experiment No 1

Aim: To study about various network connecting devices and wires used for their interconnection.

Theory:

Types of network connecting devices:

Hub.
Switch.
Router.
Bridge.
Gateway.
Repeater.
Access Point.

HUB:- A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

SWITCH:- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device

ROUTER:- A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

BRIDGE:-Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

GATEWAY:-A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

REPEATER:- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

ACCESS POINT:-While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Types of Cables:

Console cable: Also known as Cisco cables, rollover cables and management cables — are designed for a specific purpose. They connect Cisco networking devices to terminals or PCs for configuration. Typically, the Cisco end will connect via RJ45, and the terminal end will conclude in a serial connection.

Copper through: When you connect two devices of different types together, you use a straight through cable. When you connect two devices of the same type together, you use a crossover cable. All Pg. 6 cables are straight through if you insert a network device between two devices of the same kind.

Coaxial cable: Sometimes known as coax cable, is an electrical cable which transmits radio frequency (RF) signals from one point to another.

DCE AND DTE cables: With the DCE cable, (red zigzag with clock) the side you click first will be the DCE, the second will be DTE. With the DTE cable (red zigzag no clock) the side you click first will be DTE, the second will be DCE.

Experiment No 2

Aim-: Create a Straight cable and Crossover cable using RJ45 connector.

Theory-:

1. Cut into the plastic sheath about 1 inch (2.5 cm) from the end of the cut cable. The crimping toolhas a razor blade that will do the trick with practice.

2. Unwind and pair the similar colors.

3. Pinch the wires between your fingers and straighten them out as shown. The color order is important to get correct.

4. Use scissors to make a straight cut across the 8 wires to shorten them to 1/2 Inch (1.3 cm) fromthe cut sleeve to the end of the wires.

5. Carefully push all 8 unstripped colored wires into the connector. Note the position of the blueplastic sleeve. Also note how the wires go all the way to the end.

6. A view from the top. All the wires are all the way in. There are no short wires.

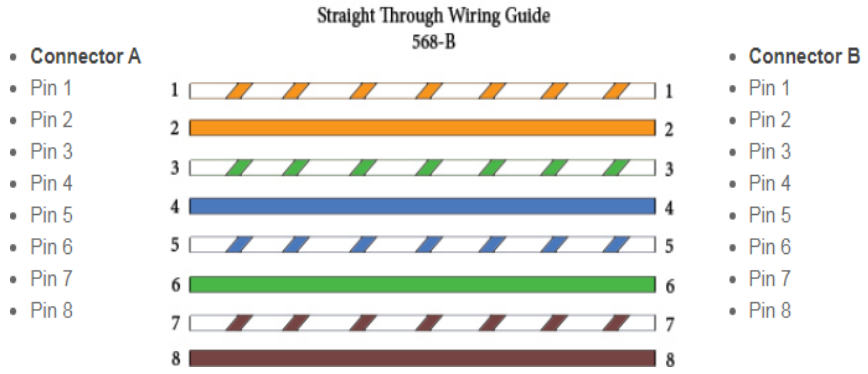
CRIMPING THE CABLE: Carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

For a standard "Straight Through" cable, repeat all steps and wire color order on the other end of cable. For a cross-over cable, the other end will have a different color order.

The Ethernet cables for connectivity in most office and home environments rely on twisted wire pairs within an overall cable - Cat 5, Cat 6 and Cat 7 all used this format. Twisting the wires together enables the currents to balance, i.e. in one wire the current is moving in one direction and in the other wire of the pair the current is going in the other, enabling the overall fields around the twisted pair to cancel.

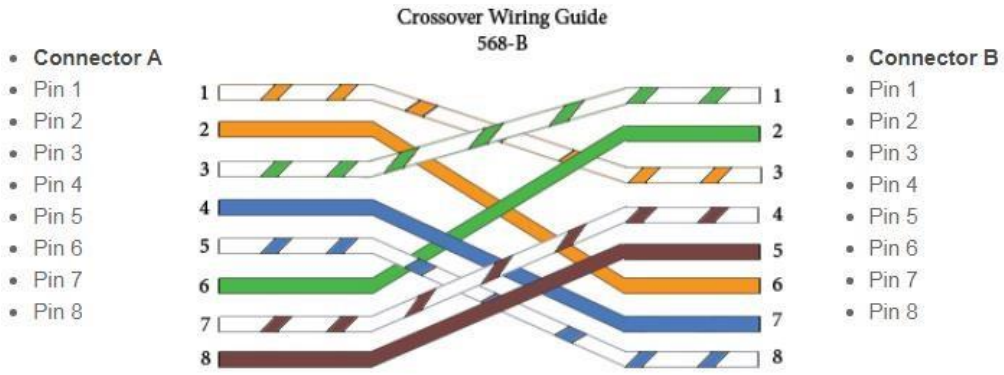
Straight-Through Wired Cables

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words, Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2, etc. Straight-Through wired cables are most commonly used to connect a host to a client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers, and other network client devices to the router switch or hub (the host device in this instance).



Crossover Wired Cables

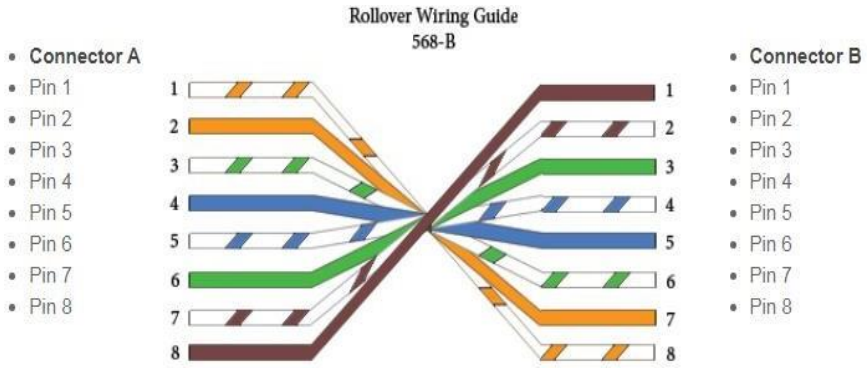
Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable). Using the 568-B standard as an example below, you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B, etc. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connectinga router to a router. Note: While in the past, when connecting two host devices directly, a crossover cable was required. Nowadays, most devices have auto-sensing technology that detects the cable anddevice and crosses pairs when needed.



Rollover Wired Cables

Rollover wired cables, most commonly called rollover cables, have opposite Pin assignments on each end of the cable or, in other words, it is "rolled over." Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollovercables, sometimes referred to as Yost cables are most commonly used to

connect to a device's console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.



Cat 5

Alternatively known as an Ethernet cable or LAN cable, a Cat 5 or category 5 is a network cable that consists of four twisted pairs of copper wire terminated by an RJ-45 connector. The picture shows anexample of a Cat 5 cable. Cat 5 cable is used in home and business networks, providing data transmission speeds of up to 100 MB per second. The maximum recommended length of a Cat 5 cable is 100 meters. Exceeding this length without the aid of a bridge or other network device could cause network issues, including data packet loss and data transmission speed degradation.

Cat 6

Cat 6 or Category 6 is a network cabling that consists of four twisted pair wires, has a data rate of 10,000 Mbps, and is used in Ethernet and Gigabit Ethernet.

Cat 7

Cat 7 or Category 7 is network cabling that consists of four twisted pair wires, transmits data at a rate of up to 10000 Mbps, and is used in Ethernet and Gigabit Ethernet.

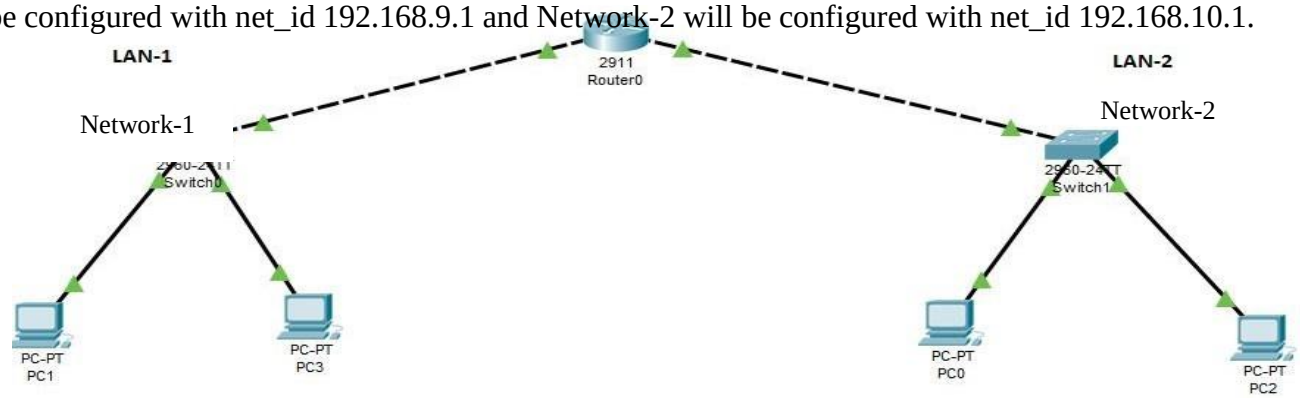
Experiment No 3

AIM: To study about the configuration of Inter connection between different networks by using Cisco Packet Tracer.

NETWORK TOPOLOGY FOR INTER LAN:

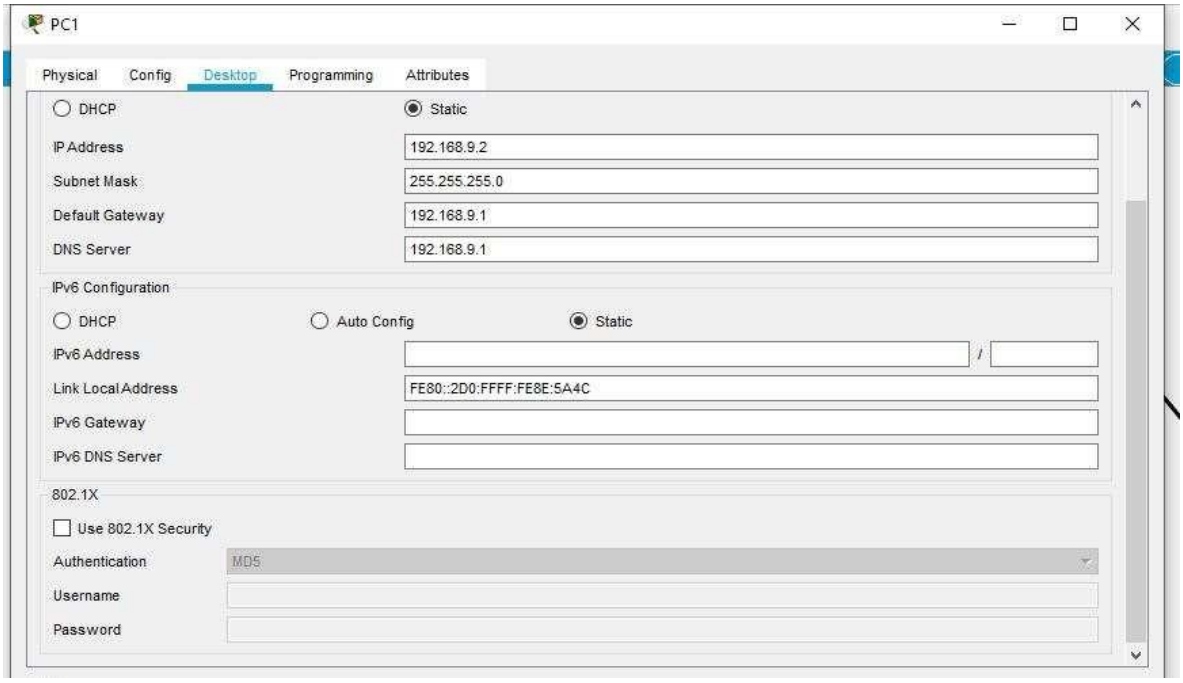
Here, two different LANs will be formed by using required Switches and PCs and after connecting all the devices of a Network by using suitable connecting wires, both networks are interconnected by using a Router.

Network-1 will have two PCs, PC1 and PC3, connected with a switch and Network-2 will have PC0 and PC2 connected with another switch. Router0 will be used to interconnect both Network-1 and Network-2. Network-1 will be configured with net_id 192.168.9.1 and Network-2 will be configured with net_id 192.168.10.1.

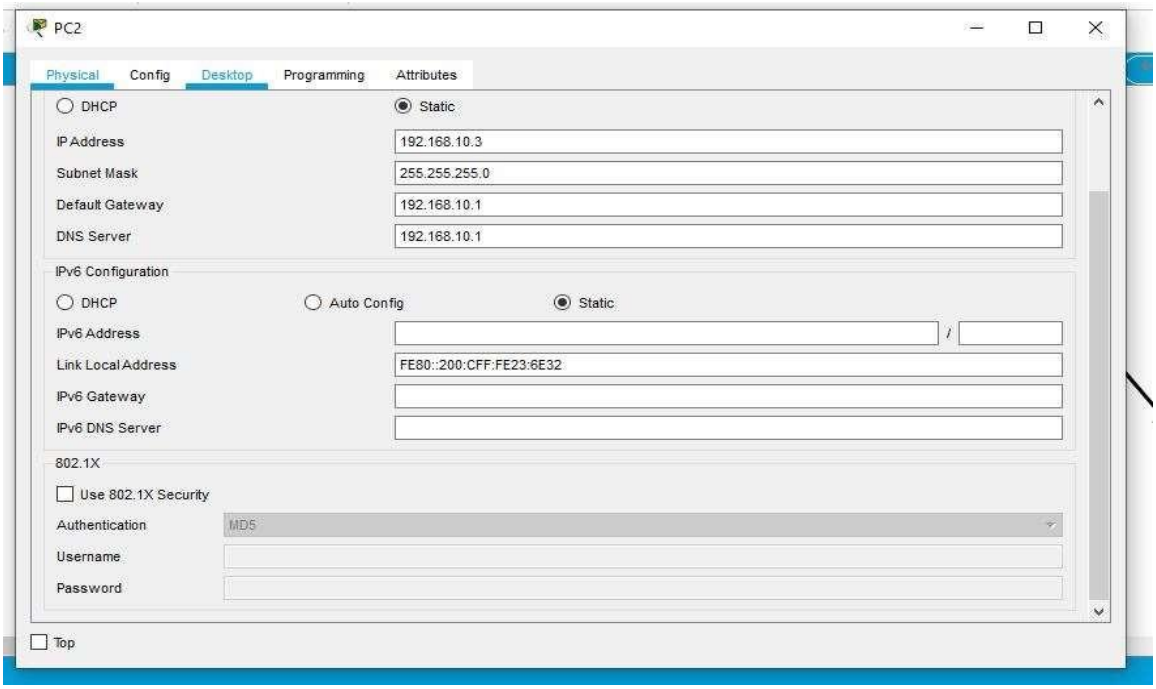


Configuration of IP, subnet mask, default gateway and DNS at PC side:

PC-1:



PC-2:



CONFIGURATION OF IP AND SUBNET MASK AT ROUTER:

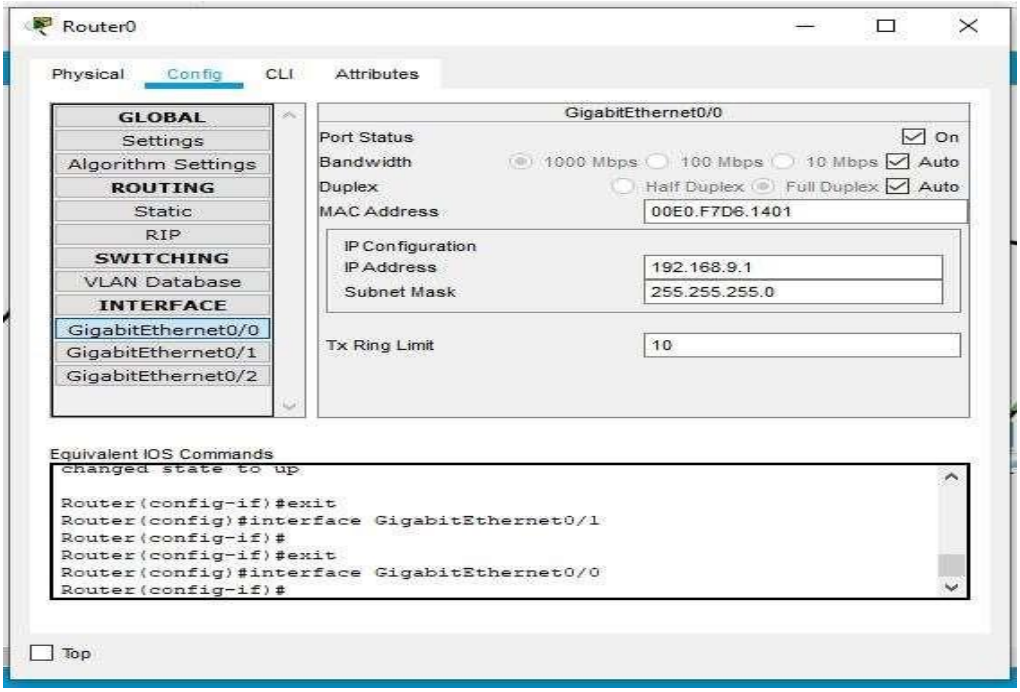
As Router0 is used to interconnect both the Networks, gigabit interfaces 0/0 and 0/1 will be used to connect Network-1 and Network-2 respectively. So, gigabit interface 0/0 of Router0 need to be configured to communicate with network 192.168.9.1 and gigabit interface 0/1 with network 192.168.10.1.

Following Commands can be used to configure an interface:

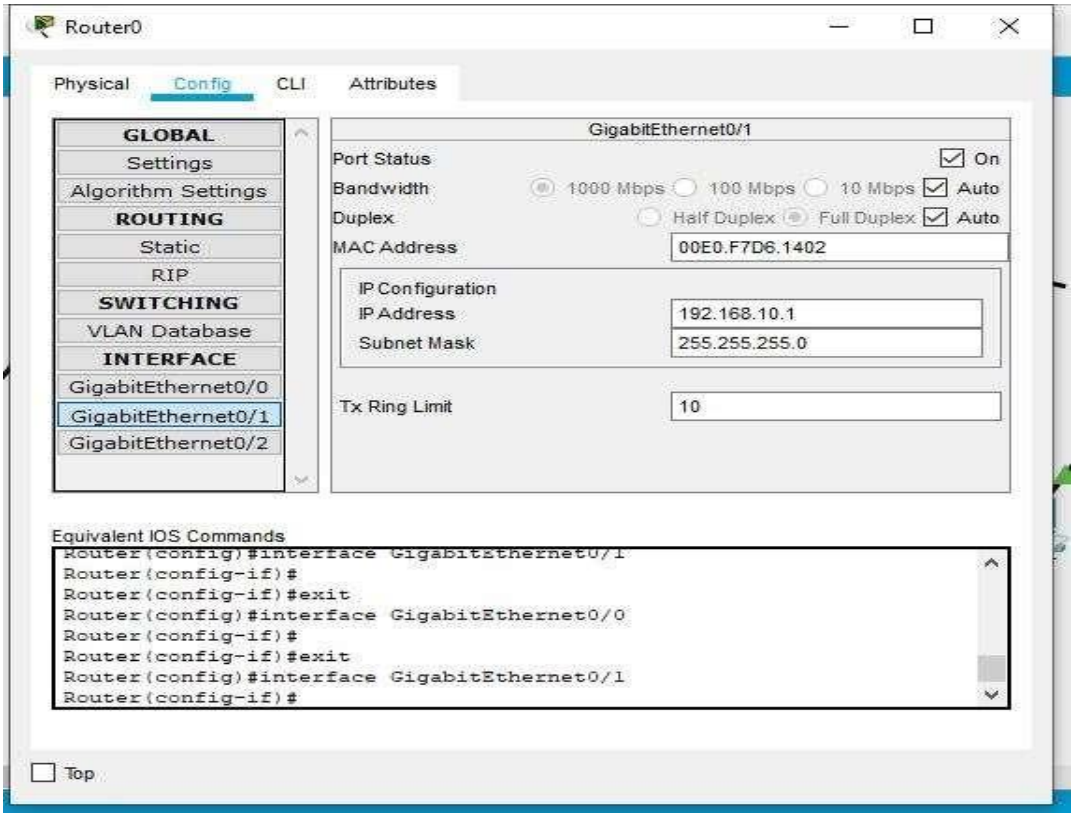
Router#conf terminal
Router(config)#interf
ace GigabitEthernet
0/0
Router(config-if)#ip address
10.1.1.1 255.255.255.0
Router(config-if)# no
shutdown
Router(config-if)#exit

Value Added Program

GigabitEthernet 0/0 interface Configuration



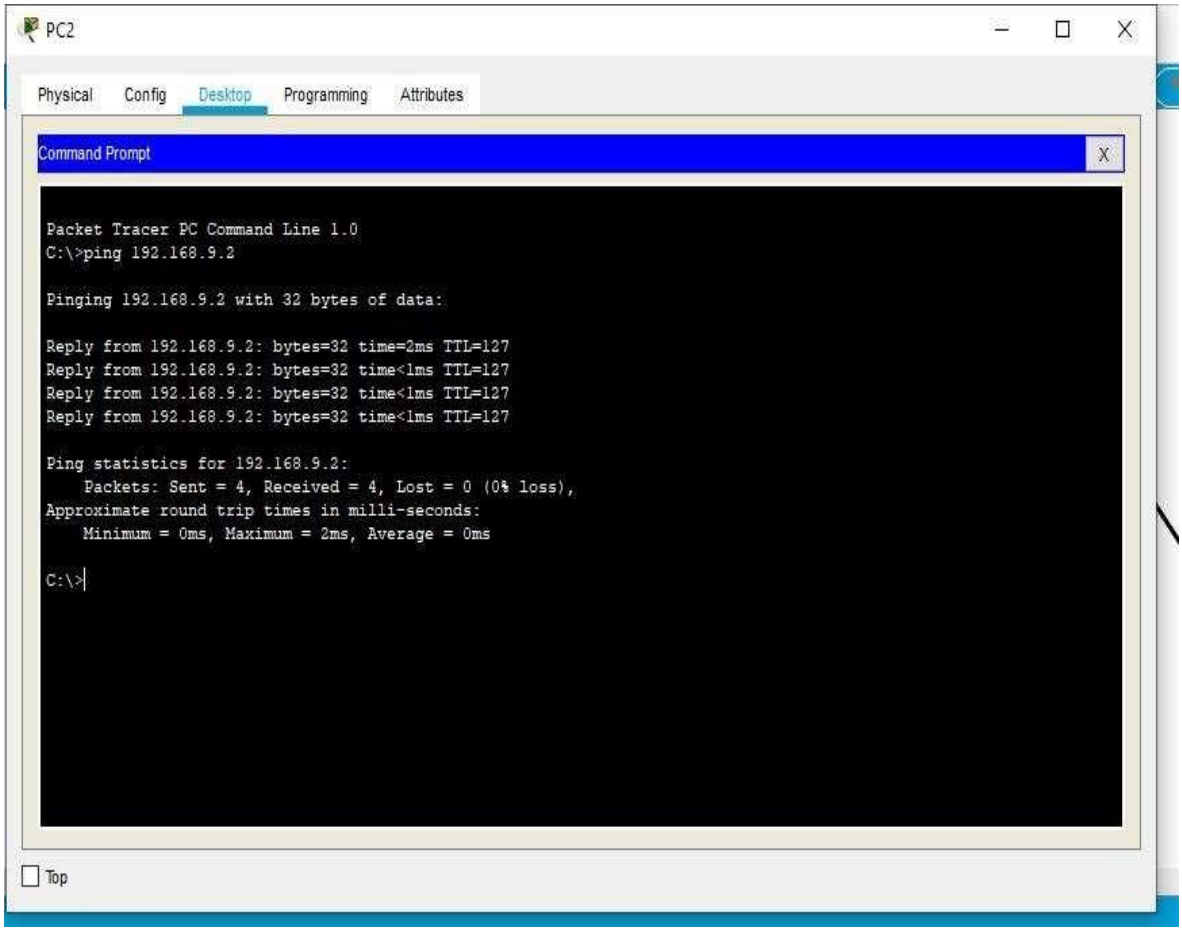
GigabitEthernet 0/1 interface Configuration



After the completion of configuration of IP on at both the interfaces of Router0, PING (Packet Inetr Net Groper) will be used to check the connectivity between networks. PING uses the Internet Control Message Protocol (ICMP) to communicate with other devices on the network.

The syntaxis:

ping *ip-address*

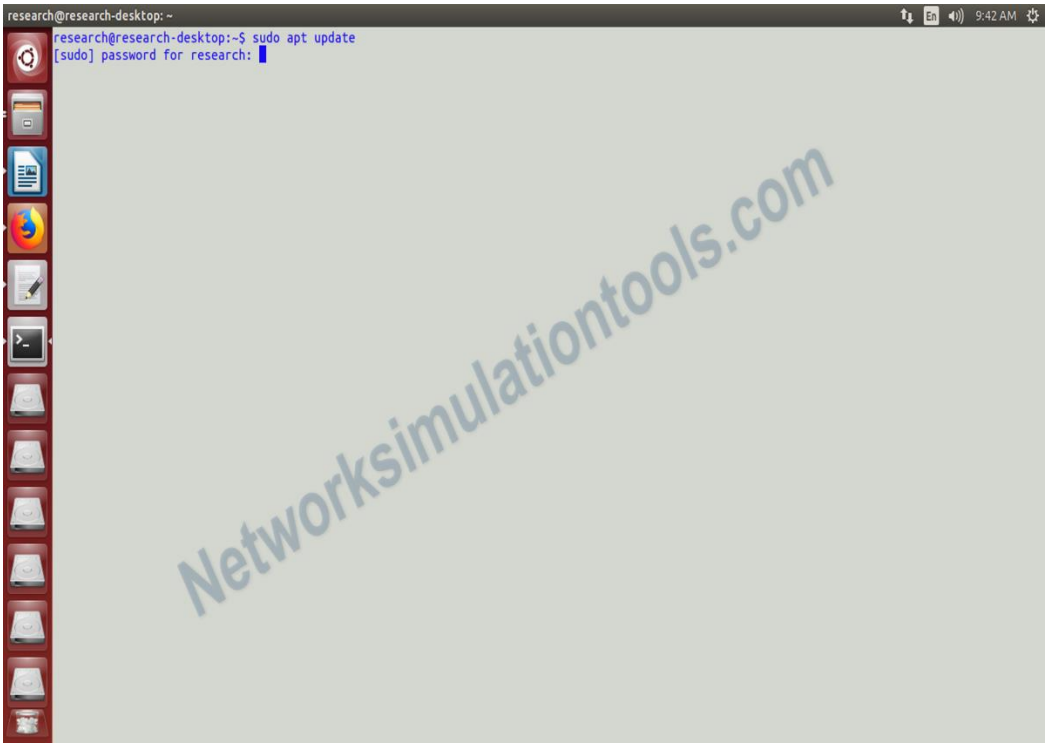


Experiment No 4

Aim-: Introduction to Discrete Event Simulation tools NS2, NS3 and installation of NS3.

Step 1-: Update libraries

Initially, open the terminal by press ctrl+alt+T buttons or search from the installed software list., update the system related libraries for the further new updated software installations, by using the commands sudo apt update and sudo apt upgrade



Step 2-: Install the supported packages

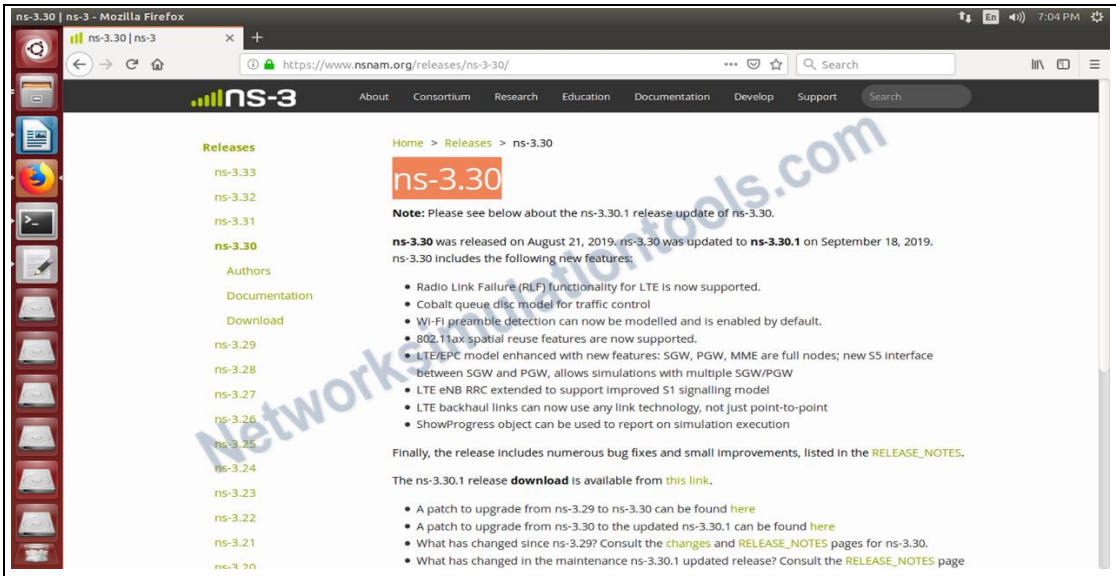
Next install the supported packages for the new NS3 installation. For the supported package installation we use the following command.

sudo apt-get install build-essential autoconf automake libxmu-dev python-pygoocanvas python-pygraphviz cvs mercurial bzr git cmake p7zip-full python-matplotlib python-tk python-dev python-kiwi python-gnome2 python-gnome2-desktop-dev python-rsvg qt4-dev-tools qt4-qmake qt4-qmake qt4-default gnuplot-x11 wireshark

Step 3-: Download the ns3 package

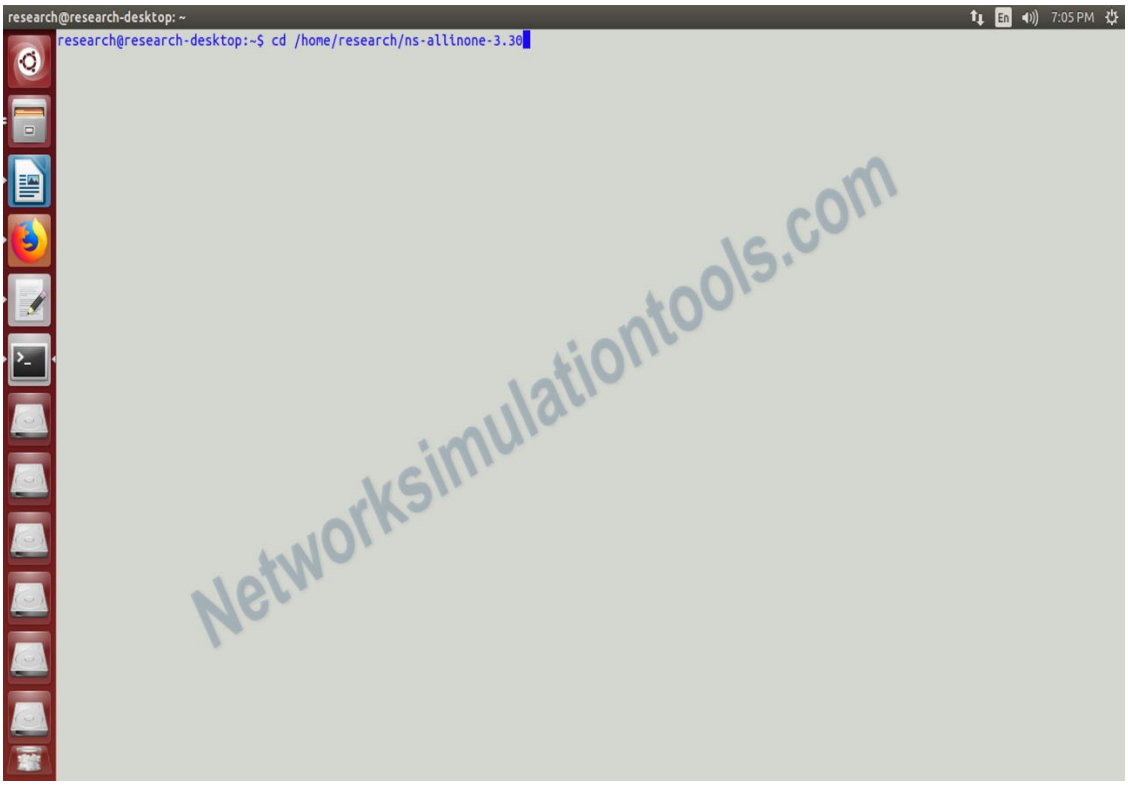
Download the ns3 package from https://www.nsnam.org, the downloaded file looks like ns-allinone-3.30.tar.bz2.

To unzip the Right click over the above file and extract it to the folder (/home/username/). Most preferred place to install is to put it in the home folder.



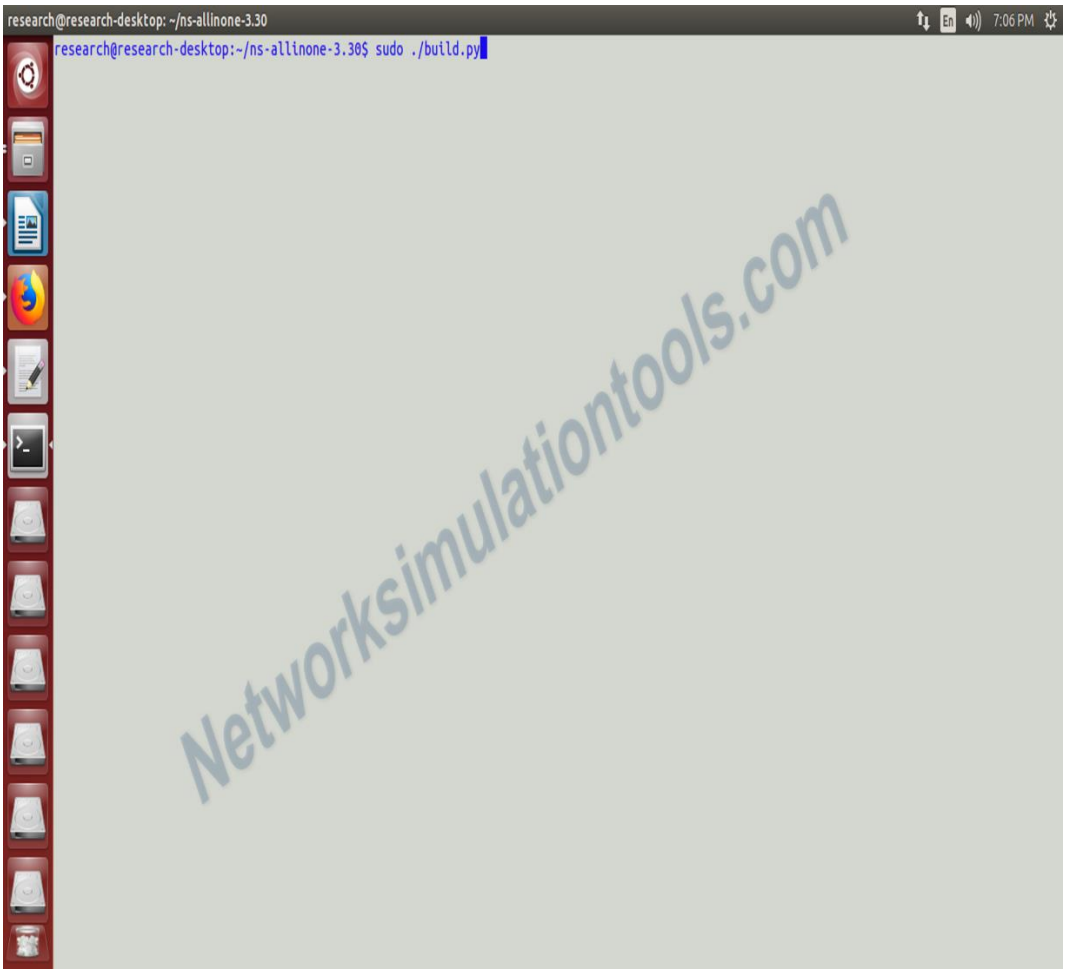
Step 4-: Build the NS-3 Package

For build the Ns3 package, we perform the process of change the location by using the command, cd ns-allinone-3.30/ and also build the package by using the command ./build.py



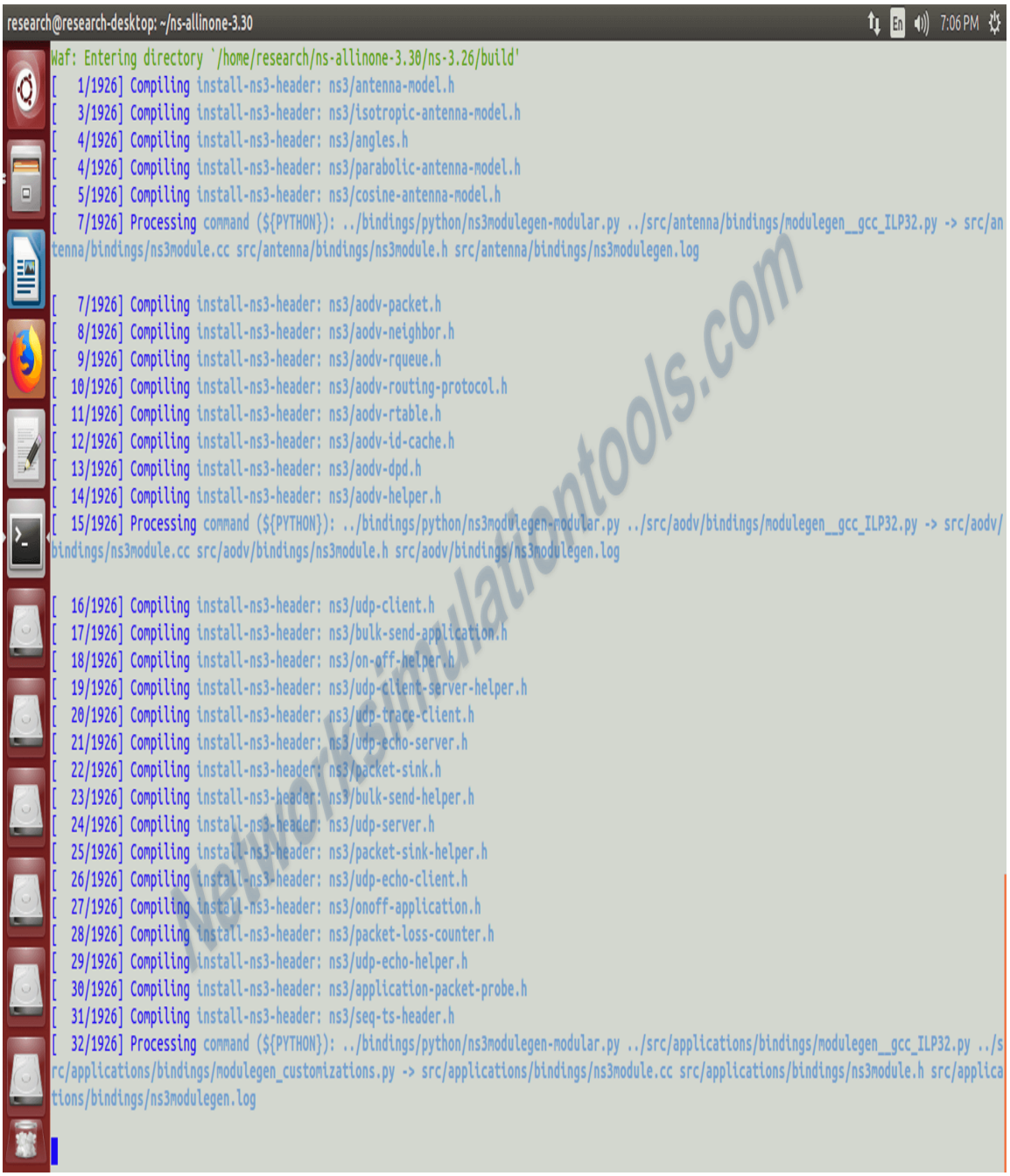
Step 5-: Build processing

We perform the project development of change the location by using the command of step 6.



Step 6-: Command building

By using the command, cd ns-allinone-3.30/ and also build the package by using the command ./build.py



Step 7-: Command Building Result

Let we look for Command Building Result in NS3 to build the package by using the command ./build.py