Computer Networks Lab

Practical File

Faculty Name: Ms. Sakshi Goel

Student's Name:Parv Kumra
Roll No.: 02414812721

Semester: 5

Group: 5 CST1

Maharaja Agrasen Institute of Technology

Sector – 22, Rohini, New Delhi - 110085

Department of Computer Science and Engineering

Rubrics for Lab Assessment

Rubrics		0	1	2	3
		Missing	**Inadequate**	**Needs Improvement**	**Adequate**
R1	Is able to identify the problem to be solved and define the objectives of the experiment.	No mention is made of the problem to be solved.	An attempt is made to identify the problem to be solved but it is described in a confusing manner, objectives are not relevant, objectives contain technical/ conceptual errors or objectives are not measurable.	The problem to be solved is described but there are minor omissions or vague details. Objectives are conceptually correct and measurable but may be incomplete in scope or have linguistic errors.	The problem to be solved is clearly stated. Objectives are complete, specific, concise, and measurable. They are written using correct technical terminology and are free from linguistic errors.
R2	Is able to design a reliable experiment that solves the problem.	The experiment does not solve the problem.	The experiment attempts to solve the problem but due to the nature of the design the data will not lead to a reliable solution.	The experiment attempts to solve the problem but due to the nature of the design there is a moderate chance the data will not lead to a reliable solution.	The experiment solves the problem and has a high likelihood of producing data that will lead to a reliable solution.
R3	Is able to communicate the details of an experimental procedure clearly and completely.	Diagrams are missing and/or experimental procedure is missing or extremely vague.	Diagrams are present but unclear and/or experimental procedure is present but important details are missing.	Diagrams and/or experimental procedure are present but with minor omissions or vague details.	Diagrams and/or experimental procedure are clear and complete.
R4	Is able to record and represent data in a meaningful way.	Data are either absent or incomprehensible.	Some important data are absent or incomprehensible.	All important data are present, but recorded in a way that requires some effort to comprehend.	All important data are present, organized and recorded clearly.
R5	Is able to make a judgment about the results of the experiment.	No discussion is presented about the results of the experiment .	A judgment is made about the results, but it is not reasonable or coherent.	An acceptable judgment is made about the result, but the reasoning is flawed or incomplete.	An acceptable judgment is made about the result, with clear reasoning. The effects of assumptions and experimental uncertainties are considered.

INDEX

Name:Parv Kumra

Enrolment Number: 02414812721

Branch: Computer Science and Technology

Group: 5 CST1

S No.	*Experiment name*	*Date of performing*	*Date of checking*	*R1*	*R2*	*R3*	*R4*	*R5*	*Signature*

EXPERIMENT – 1

AIM: Introduction to Network Simulation Tools : Wireshark and ciscoPacket Tracer.

THEORY:

Simulation

A simulation imitates the operation of real world processes or systems withthe use of models. The model represents the key behaviours and characteristics of the selected process or system while the simulation represents how the model evolves under different conditions over time.

Types of Simulation

- Discrete Models – Changes to the system occur at specific times
  - Division of Property Management trouble calls
  - Acquisition or construction business processes
  - A manufacturing system with parts entering and leaving at specifictimes
- Continuous Models – The state of the system changes continuously over time
  - A reservoir as water flows in and out
  - Chilled water or steam distribution
- Mixed Models – Contains both discrete and continuous elements
  - A refinery with continuously changing pressure inside vessels anddiscreetly occurring shutdowns
  - Chilled water distribution including plant shutdowns

Network Simulation

Network simulation is a technique whereby a software program replicates the behavior of a real network. This is achieved by calculating the interactions between the different network entities such as routers, switches, nodes, accesspoints, links, etc. Most simulators use discrete event simulation in which the modeling of systems in which state variables change at discrete points in time.

Network Simulator

A network simulator is a software program that can predict the performance of a computer network or a wireless communication network. In simulators, the computer network is modeled with devices, links, applications, etc., and the network performance is reported.

Types of Network Simulators

- Network Simulator version 2 (NS-2)
- Ns3
- Netkit
- Marionnet
- JSIM (Java-based Simulation)
- OPNET
- QualNet
- The open-source simulators are Marrionet, Netkit, NS2, JSIM
- The commercial simulators are OPNET and QualNet

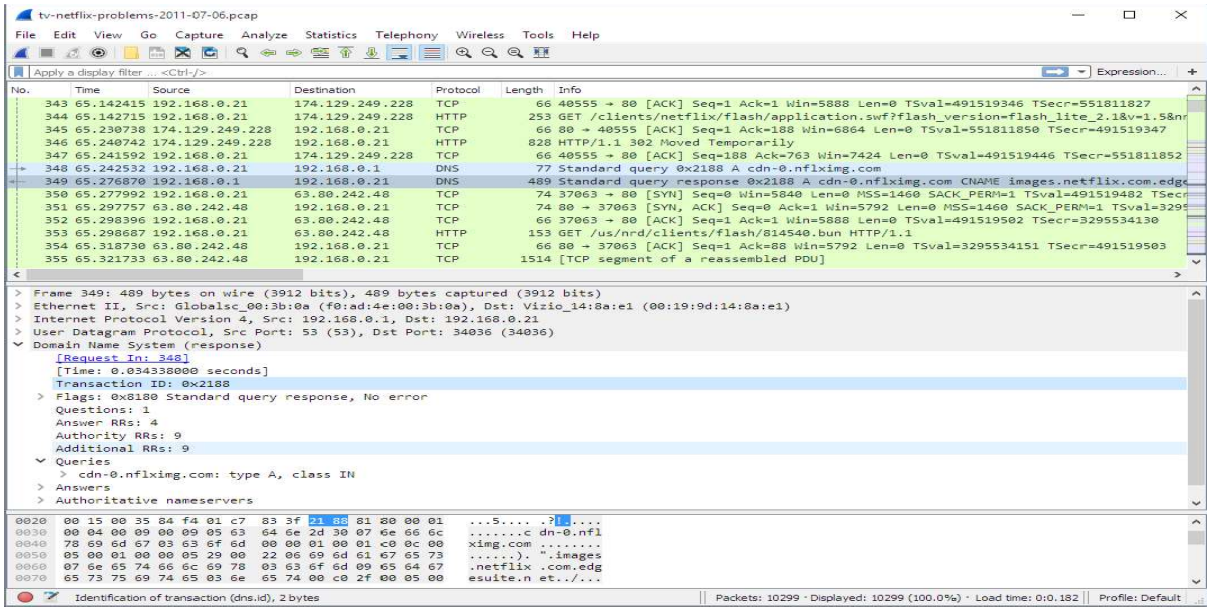
Applications of Network Simulators

- 5G-NR capacity, throughput and latency analysis
- Network R & D (More than 70% of all Network Research paper reference anetwork simulator)
- Defense applications such as HF / UHF / VHF Radio based MANET
- Radios, Tactical data links etc.
- IOT, VANET simulations
- UAV network/drone swarm communication simulation
- Machine Learning: Testing ML algorithms for optimizing network parameters,generating synthetic data training ML algorithms on networks
- Education: Online courses, Lab experimentation, and R & D. Most universitiesuse a network simulator for teaching / R & D since it is too expensive to buy hardware equipment

Wireshark

- Wireshark is the world's foremost network protocol analyzer. It lets you seewhat's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.

- Wireshark is cross-platform, using the Qt widget toolkit in current releases toimplement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unixlike operating systems, and Microsoft Windows.



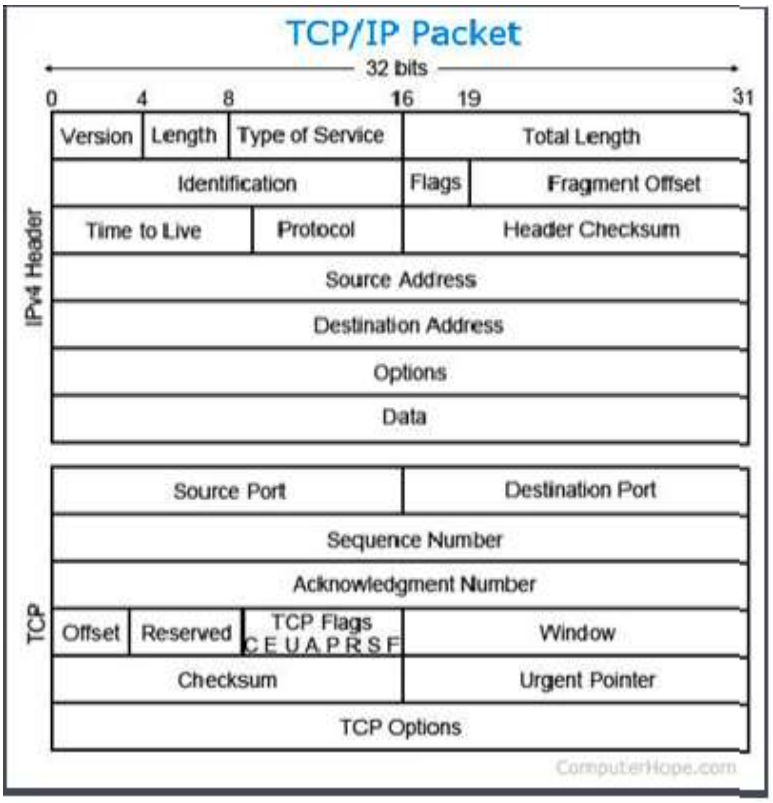
Packets

A packet is a small unit of data that is used for the transmission of information across a network. They allow data to be broken down into manageable chunksfor efficient transmission, routing, and error detection and correction. It typically consists of two main parts: a header and a payload.

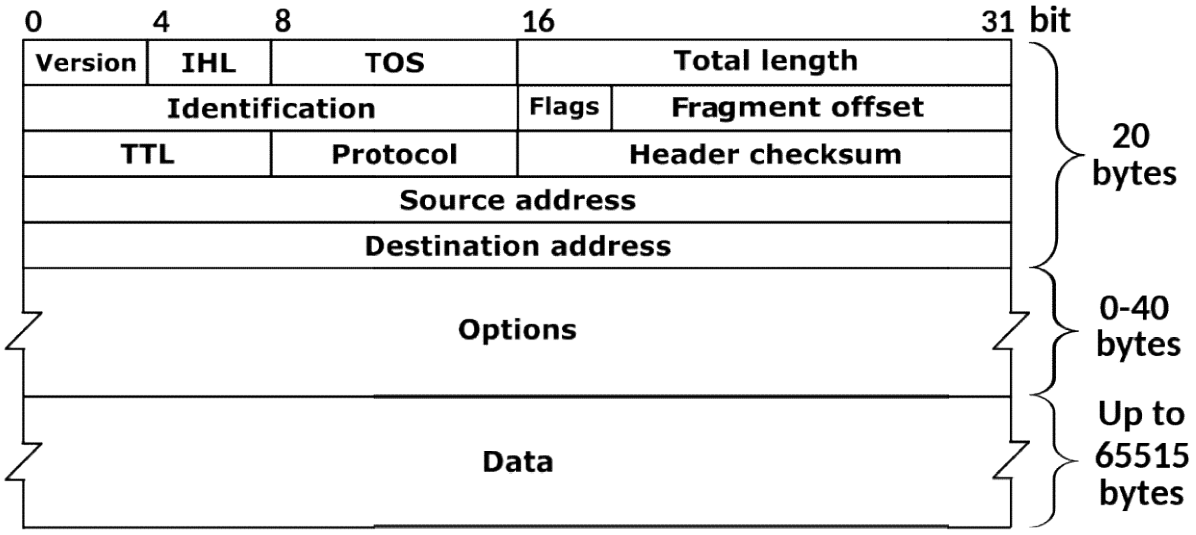
Header: The header contains control information essential for routing and managing the packet as it travels through the network. This information includes source and destination addresses, packet sequence numbers, error-checking data, and other metadata.

Payload: The payload contains the actual data that is being transmitted, such as a part of a file, an email message, or any other information. The size and format of the payload can vary depending on the network protocol being used.

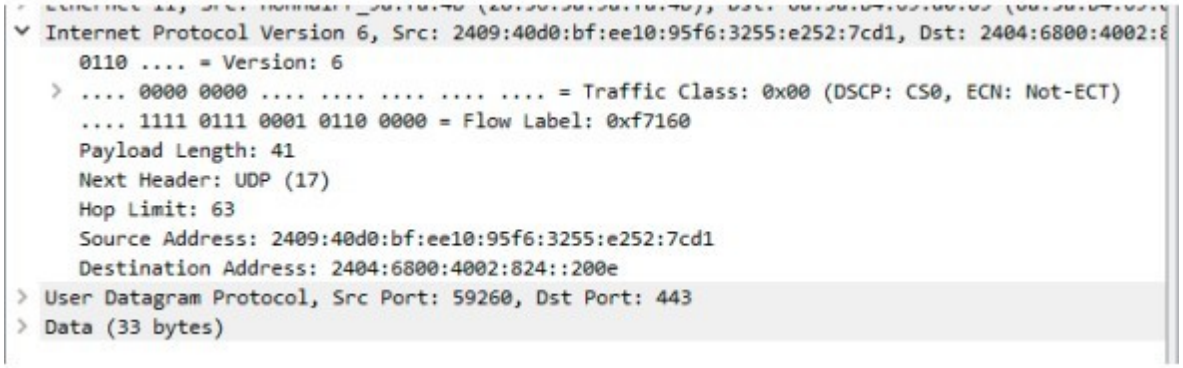
Packet Structure



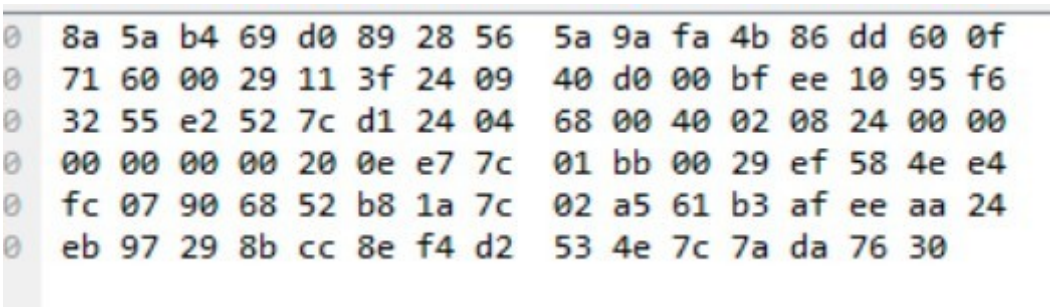
IPV4 Header Format



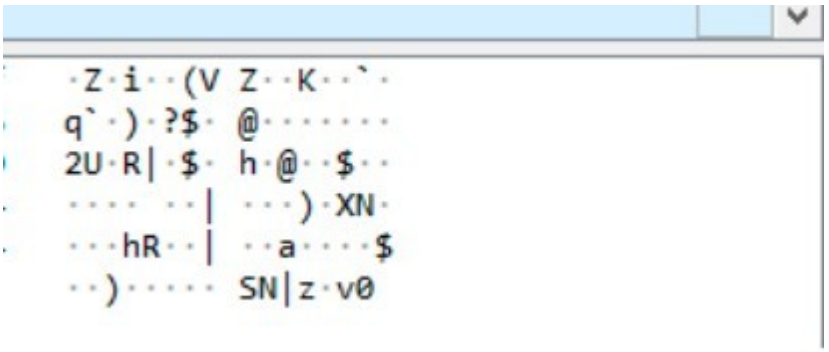
Ipv4 header of a packet captured by Wireshark



Converted Hex Code of Ipv4 header



Hexcode converted to ASCII Hexdump



Color Coding

Green: Green packets usually represent TCP ACK (acknowledgment) packets.These are used to acknowledge the receipt of data packets in a TCP connection.

Light Blue: Light blue packets typically represent DNS (Domain Name System)traffic. DNS packets are used to resolve domain names to IP addresses.

Red: Red packets indicate potential issues or errors in the network traffic. These can include TCP retransmissions, checksum errors, or other anomalies.

Yellow: Yellow packets often represent ICMP (Internet Control Message Protocol) traffic. ICMP is used for network diagnostics, error reporting, andother control functions.

Black: Black packets represent TCP resets, which are used to abruptlyterminate a TCP connection.

Gray: Gray packets are packets that do not fit into any of the predefined color categories. They can include various types of network traffic that don't fall intothe common protocol categories.

Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation and visualisation tool developed by Cisco Systems. It is widely used in the field of networking and is especially popular among students, instructors, and professionals who want tolearn, practice, and teach various networking concepts. Packet Tracer allows users to create and configure virtual networks, experiment with network topologies, and simulate network behaviour.

Purpose

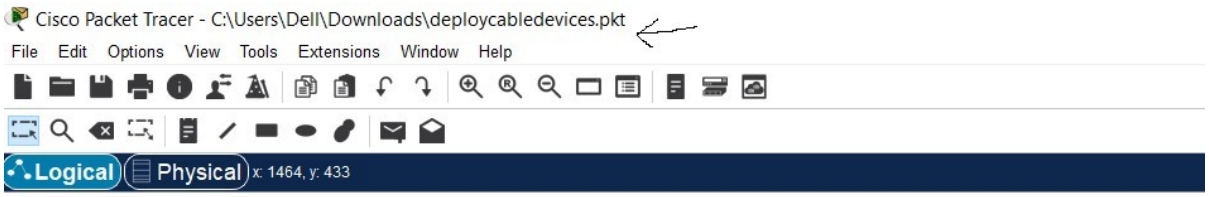
Cisco Packet Tracer is primarily designed for educational purposes, offering asafe and controlled environment for learning about computer networks, routing, switching, and network device configurations. It's commonly used in networking courses and certification programs, such as Cisco's CCNA and CCNP.

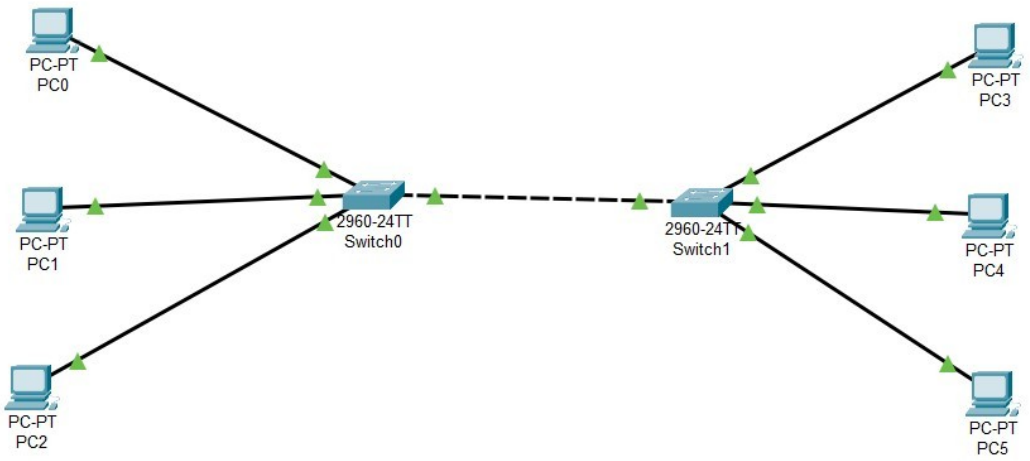
Simulation Capabilities

Packet Tracer can simulate various network devices, including routers, switches, PCs, servers, and more. Users can create network topologies by dragging and dropping these devices onto a virtual canvas and connecting them using cables. It also simulates the behavior of these devices and the flowof data packets through the network.

Features

- **Device Support**: Packet Tracer includes a wide range of Cisco devices andmodules, allowing users to build complex network designs.
- **Protocols**: It supports various networking protocols, including TCP/IP, DHCP,NAT, OSPF, EIGRP, and more.
- **Visualisation**: Users can visualise the flow of data packets, examine deviceconfigurations, and monitor network performance.
- **Activity Wizard**: Instructors can create custom network scenarios andactivities to assess students' understanding of networking concepts.





EXPERIMENT – 2

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

THEORY:

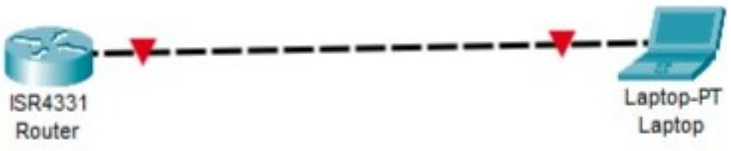
Telnet is a network protocol that allows you to establish a text-based communication session with another computer or device over a network, typically the Internet or a local area network (LAN). It enables you to connect to a remote host and interact with it through a command-line interface.

Here are some key points about Telnet:

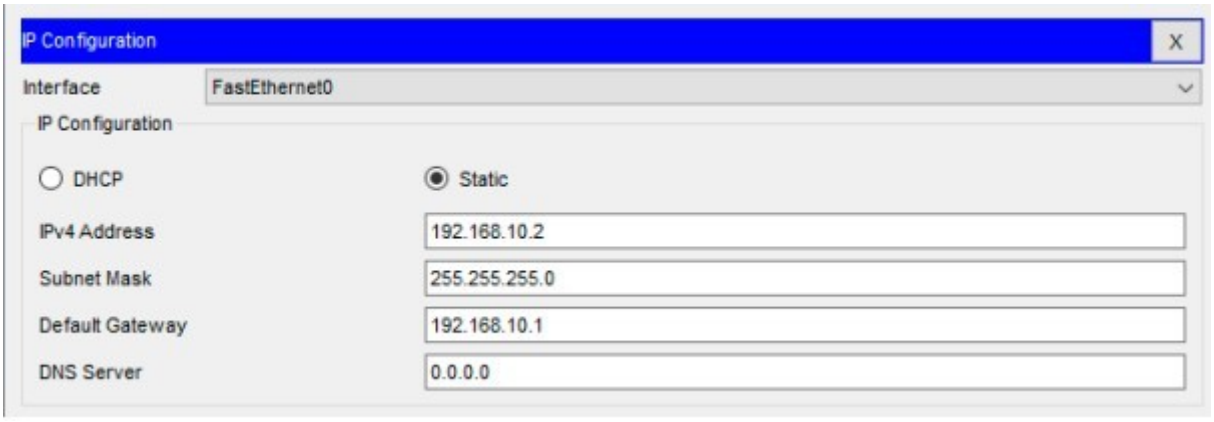
- **Text-Based Communication**: Telnet sessions are text-based, meaning thatyou communicate with the remote host by sending and receiving text commands and responses.
- **Port Number**: Telnet typically uses port number 23 for communication, though it can be configured to use other ports as well.
- **Remote Access**: Telnet provides a way to remotely access and manage servers, routers, switches, and other networked devices. It allows you to log into a remote system and run commands on it as if you were physically present.
- **Insecure**: Telnet is considered insecure because it transmits data, including usernames and passwords, in plain text over the network. This makes it vulnerable to eavesdropping and interception by malicious actors. For this reason, it is generally recommended to use more secure alternatives like SSH(Secure Shell) for remote access.

Procedure

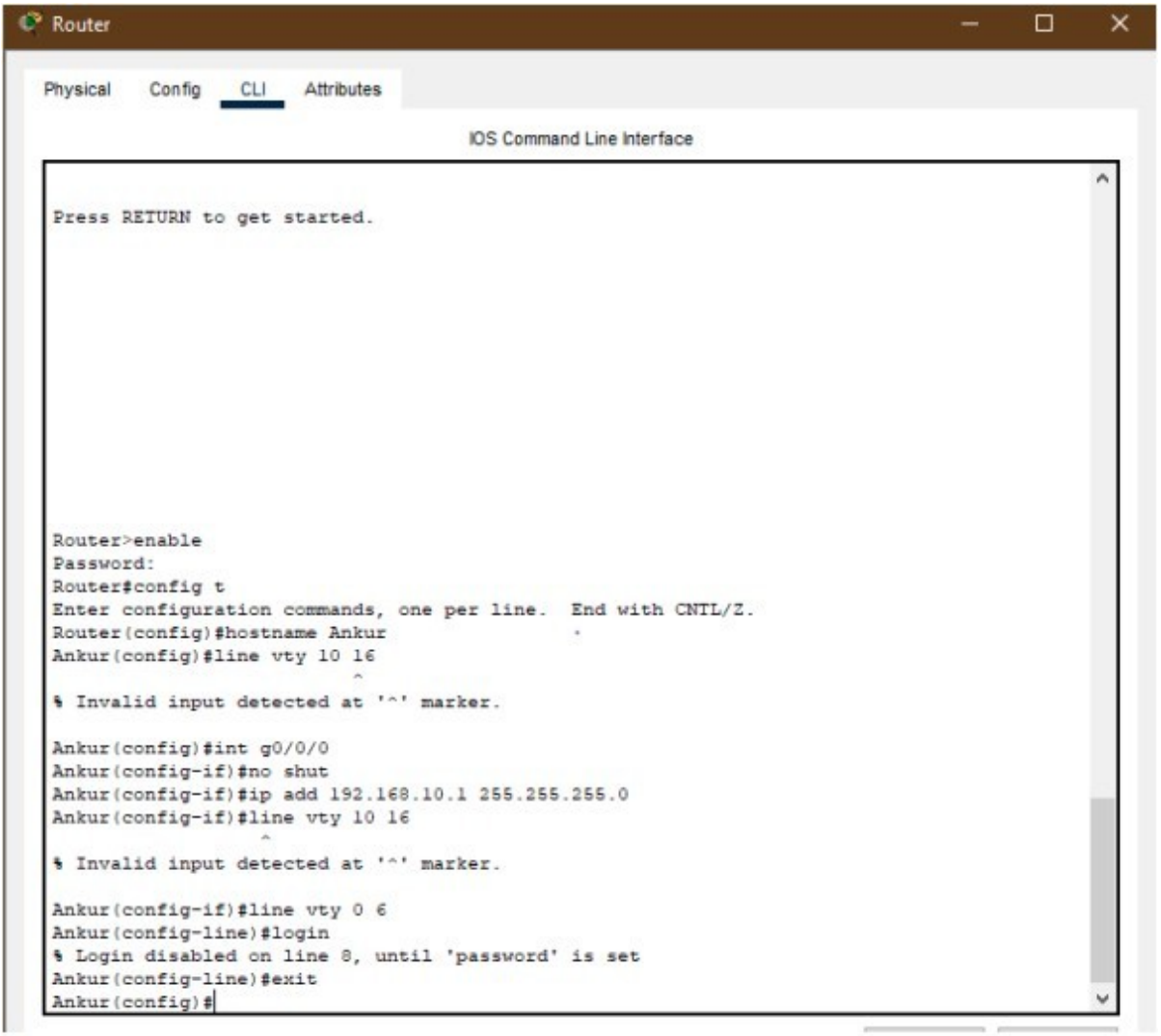
1. **Connecting router to end device**



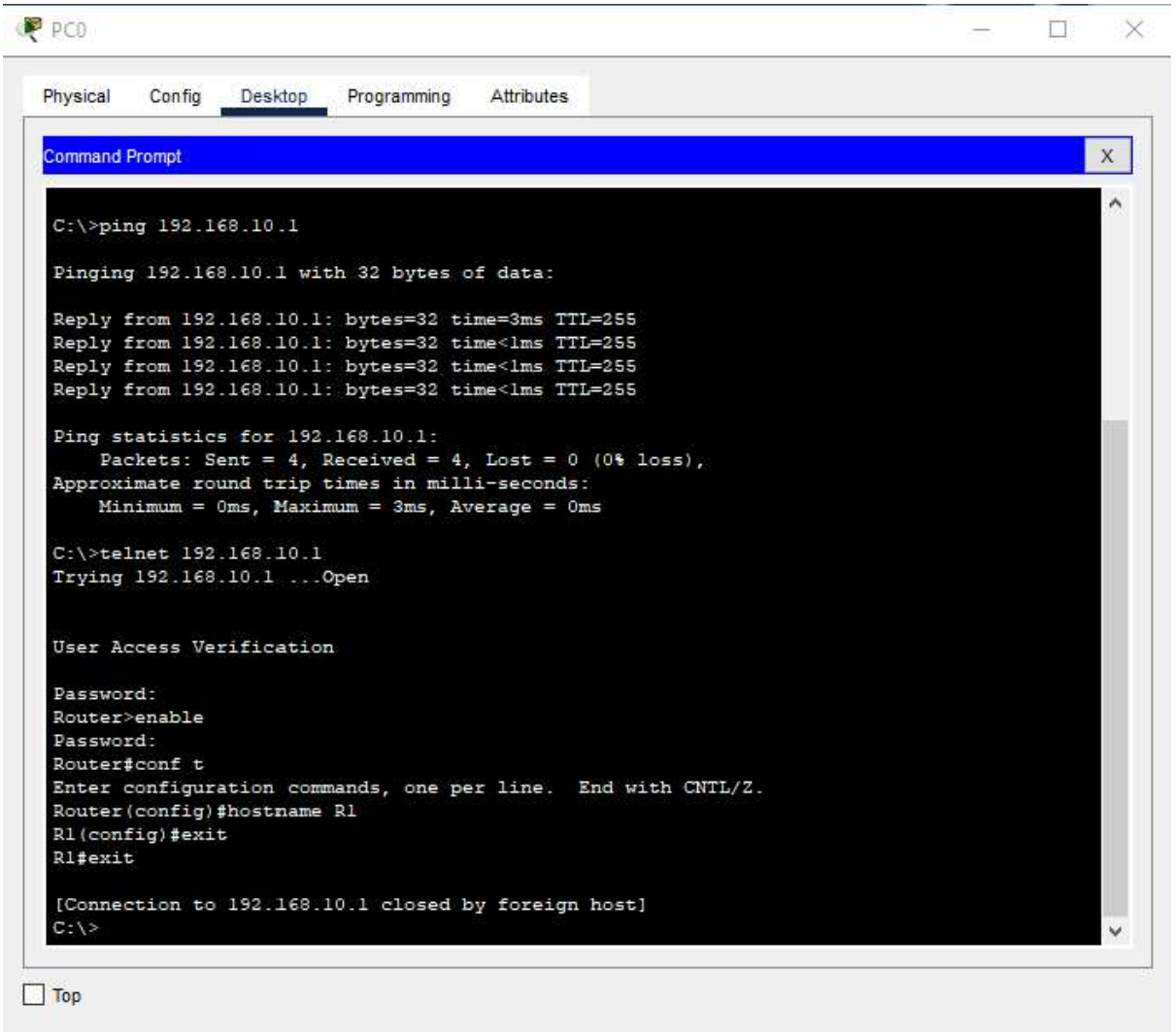
2. Setting the IP and Subnet mask to End Device



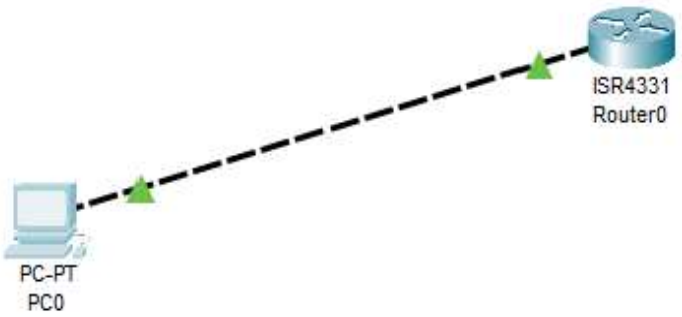
3. Setting up the configuration of the Router



4. Accessing the router using endpoint



5. The Connection is successfully Established



EXPERIMENT – 3

AIM: To implement IP Addressing Scheme and Subnetting in small networks using CiscoPacket Tracer.

THEORY:

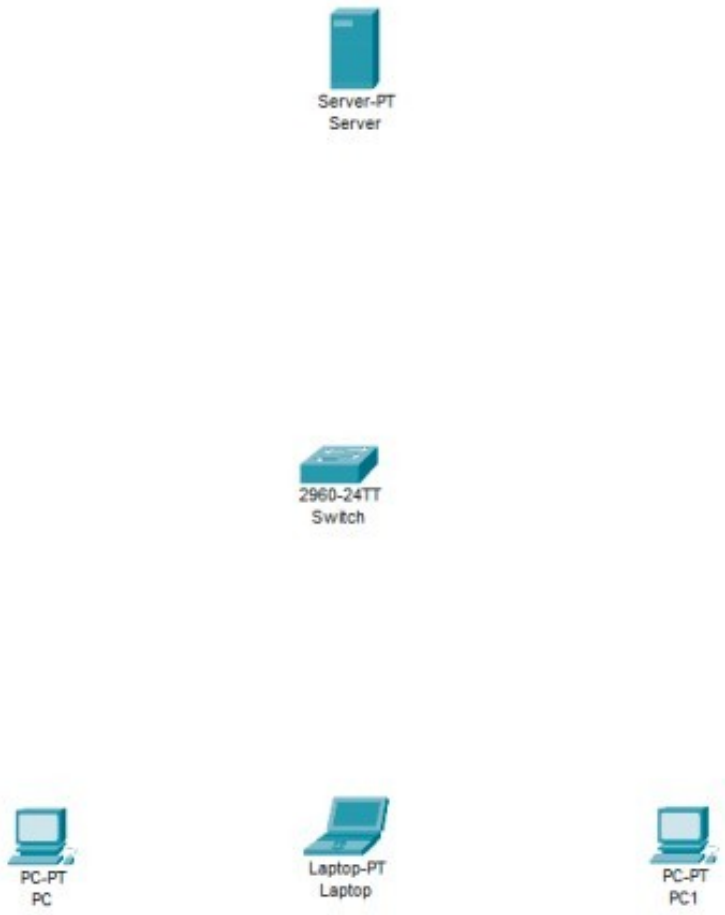
DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol usedin TCP/IP networks to automatically assign IP addresses and configuration information to devices on a network. DHCP is commonly used in homes and businesses to simplify the process of connecting devices to a network.

Here's how DHCP works:

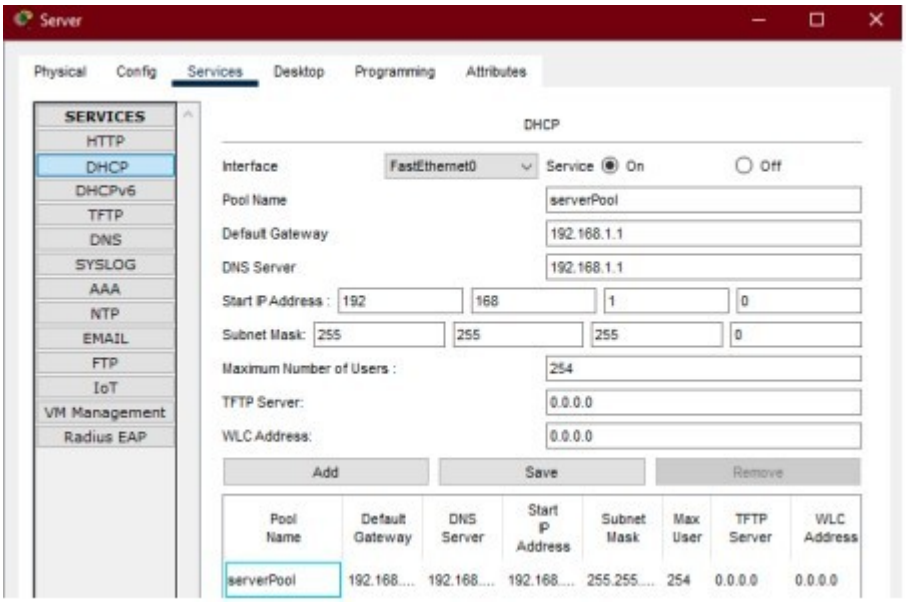
- **Request for IP Address**: When a device, such as a computer or smartphone,connects to a network (usually via Ethernet or Wi-Fi), it sends out a DHCP request to the network.
- **DHCP Server**: A DHCP server on the network receives the request. The serveris responsible for managing a pool of available IP addresses.
- **IP Assignment**: The DHCP server selects an available IP address from its pooland assigns it to the requesting device. This ensures that each device on the network has a unique IP address, which is crucial for proper communication.
- **Configuration Information**: Along with the IP address, the DHCP server can also provide other configuration information to the device, such as the subnet mask, default gateway (router), DNS (Domain Name System) server addresses,and more. This information is essential for the device to communicate effectively on the network.
- **Lease Time**: DHCP assignments are typically temporary and come with a leasetime. After a specified period, the device must renew its lease with the DHCP server. This allows network administrators to manage and reconfigure the network more easily.

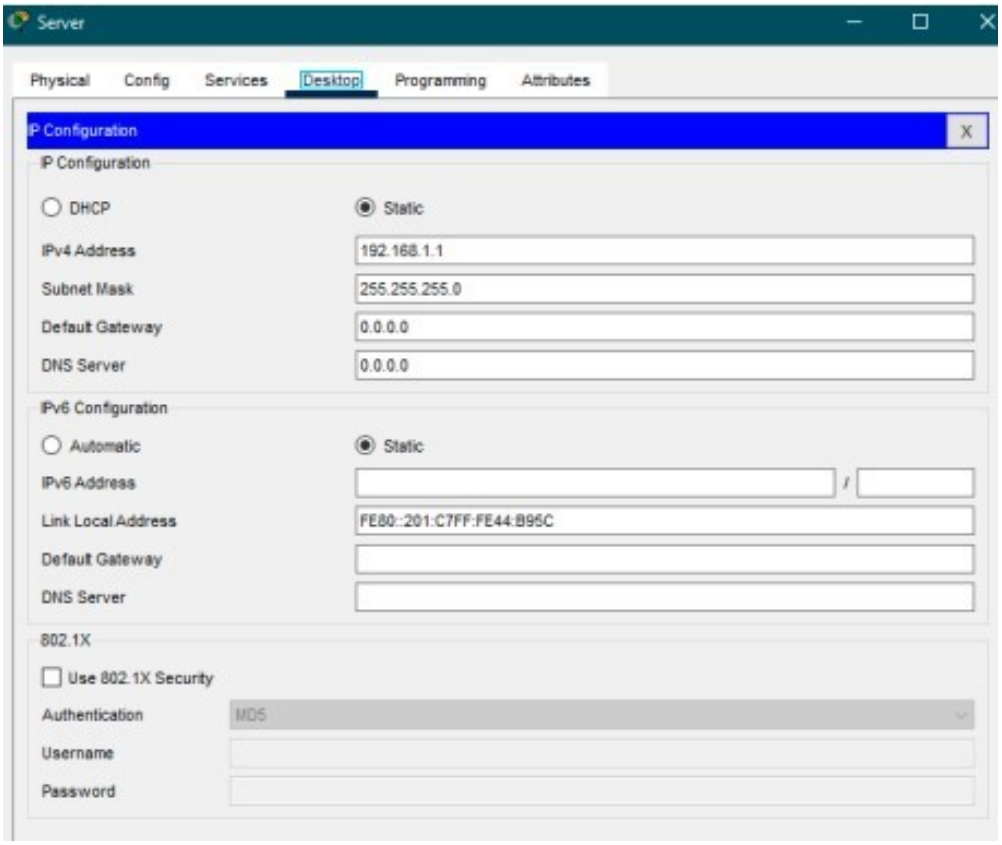
Procedure

1. **Connect server switch and Endpoints**

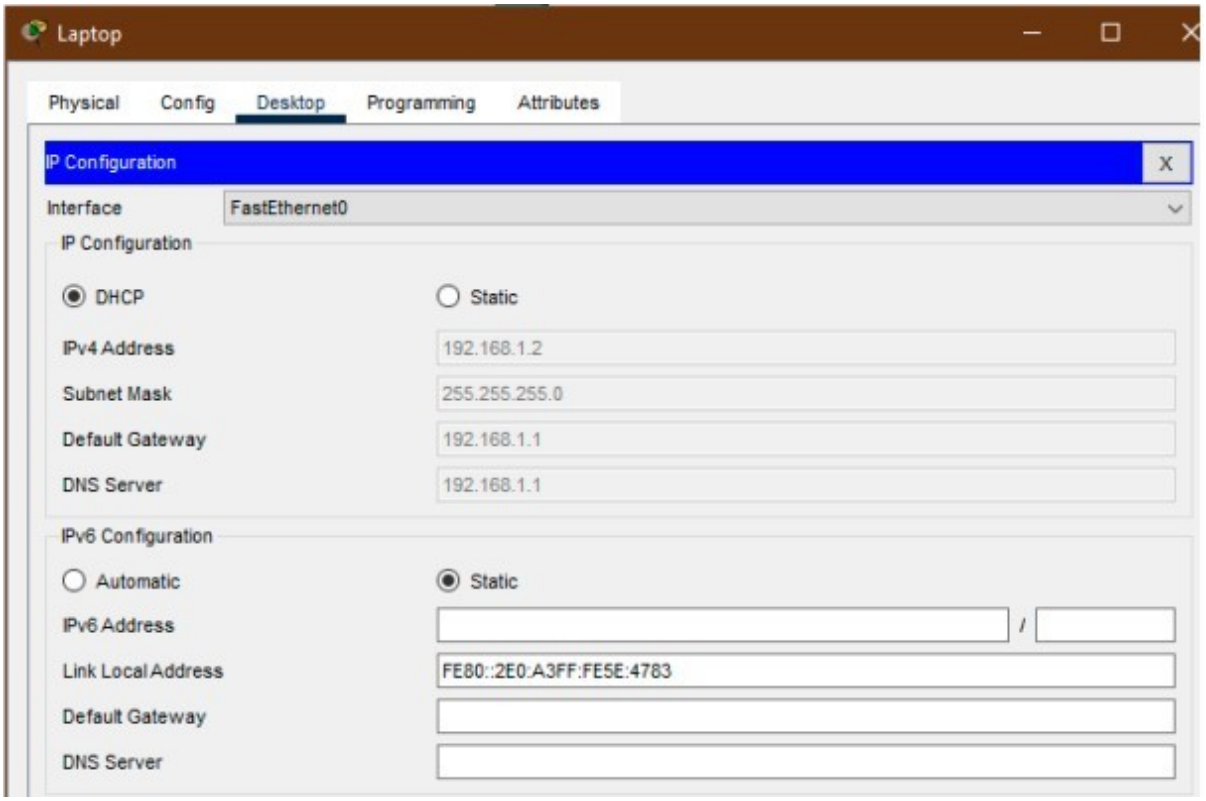


2. **Set IP configuration and DHCP Services on Server**

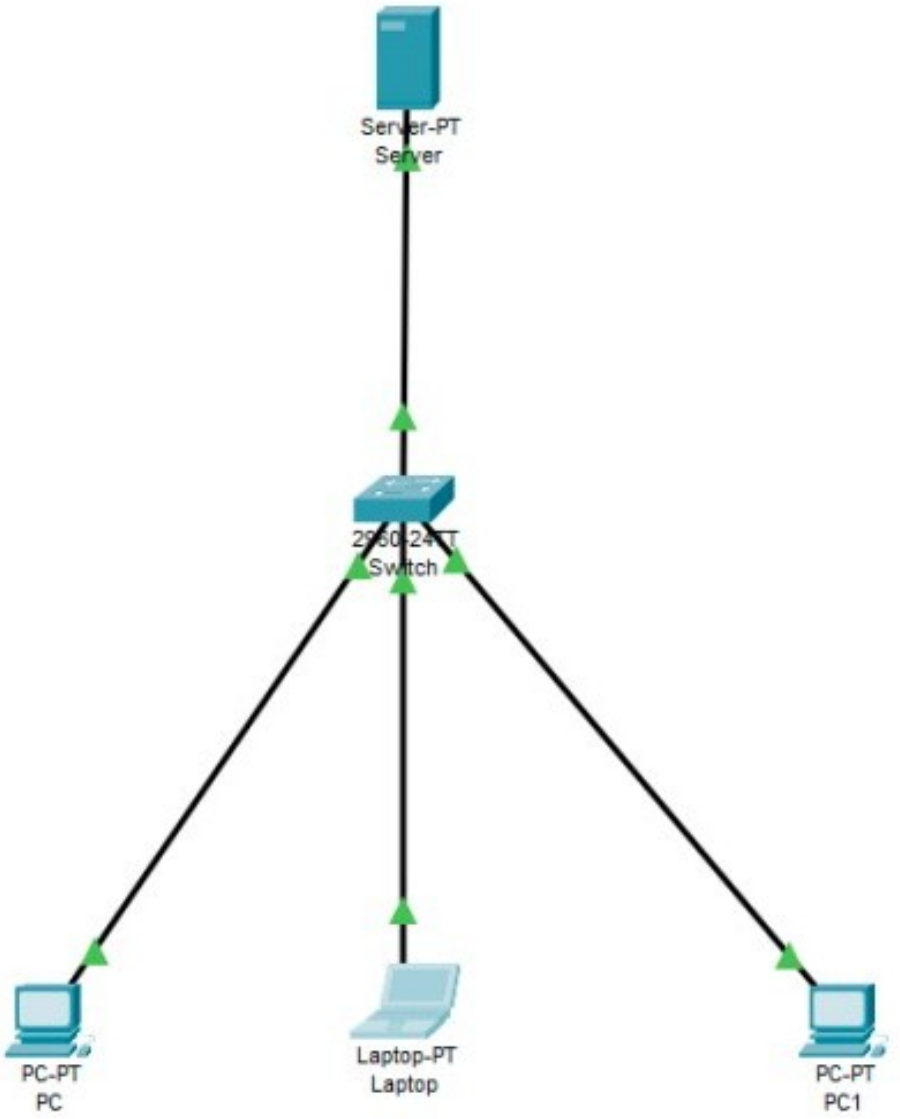




3. Set up the IP Configuration of all Endpoints



4. **Connect all the server, switch and Endpoints**



EXPERIMENT –4

AIM: To implement Static Routing using Cisco Packet Tracer.

THEORY:

Defination of Routing

Routing is the process of directing data packets between devices or networks in a computer network. It involves determining the most efficient path for data to travel from the source to the destination, ensuring effective communication across interconnected devices. This process is essential for enabling data exchange and communication within networks.

Types of Routing

Routing is a process that is performed by layer 3 (or network layer) devices inorder to deliver the packet by choosing an optimal path from one network toanother. There are 3 types of routing:

1. **Static Routing:** Static routing is a process in which we have to manuallyadd routes to the routing table.
2. **Default Routing:** This is the method where the router is configured to send all packets toward a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.
3. **Dynamic Routing:** Dynamic routing makes automatic adjustments of theroutes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down.

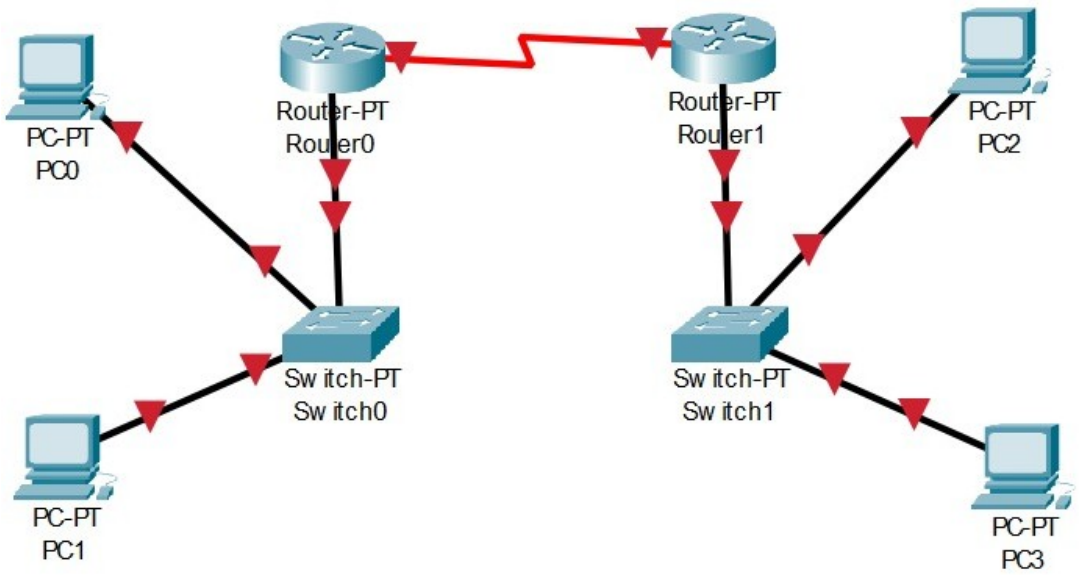
Terms used in implementation

When implementing static routing, there are several key terms and conceptsthat are commonly used. Here are some of the important terms:

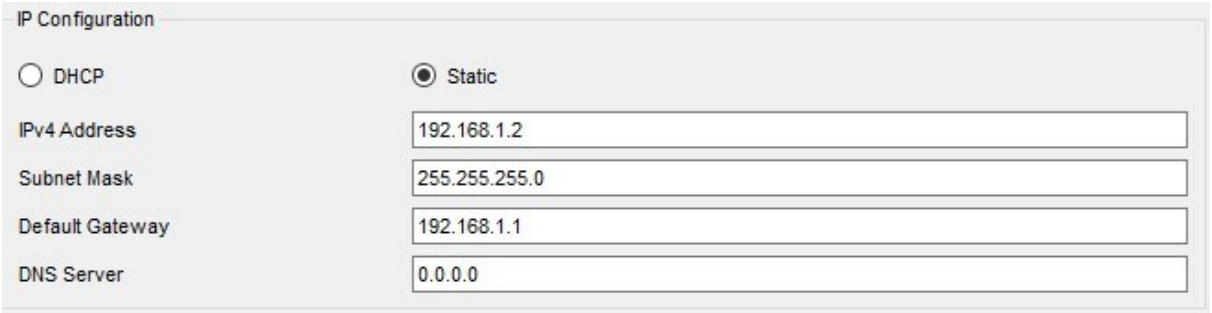
- **Routing Table:** A data structure stored in a router that contains information about available routes and their associated metrics orcosts.
- **Route:** A specific path or sequence of network nodes (like routers or switches) that data packets follow from the source to the destination.
- **Destination Address:** The address indicating where a data packet isintended to go. In IP networks, this is an IP address.
- **Next-Hop Address:** The address of the next device (usually a router) inthe path to the destination.
- **Default Route (Gateway of Last Resort):** A special type of static routethat is used when there is no specific route in the routing table for a destination.

PROCEDURE :

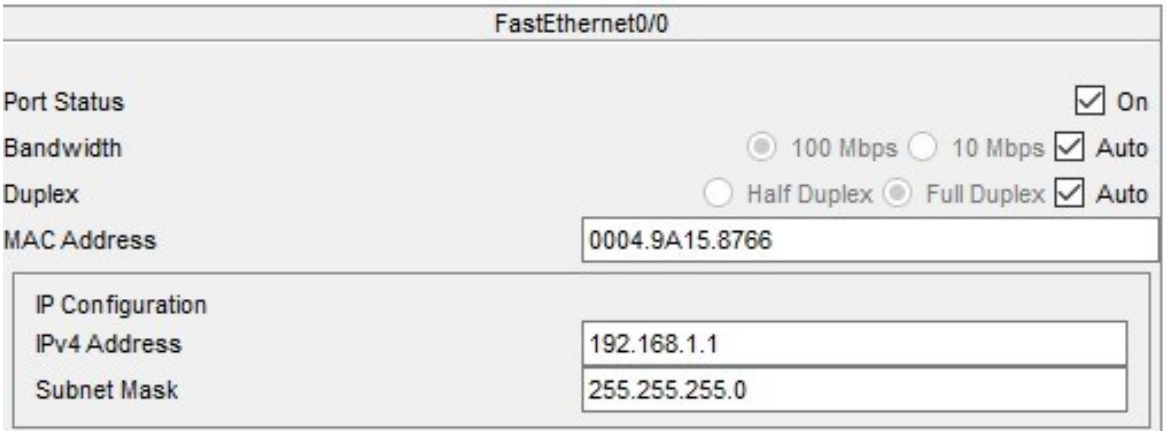
1. **Make the following connection on Cisco Packet Tracer**

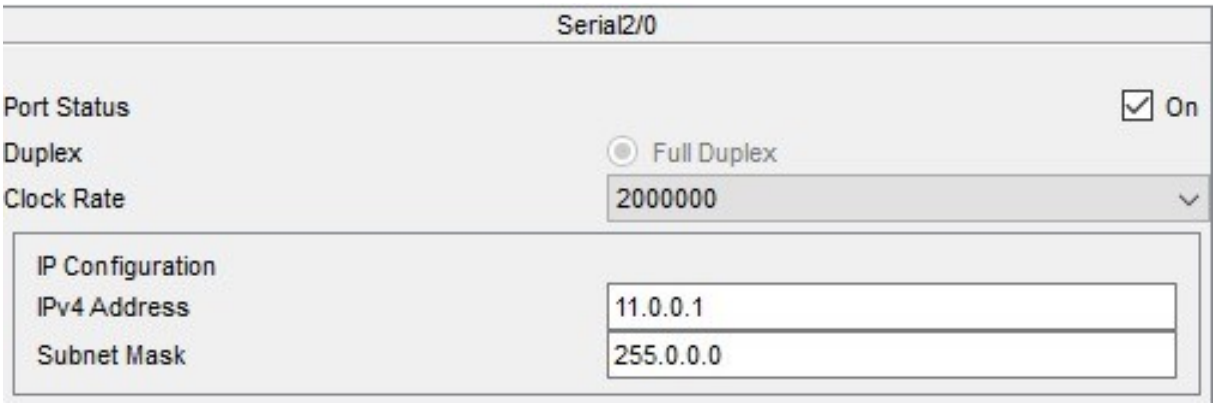


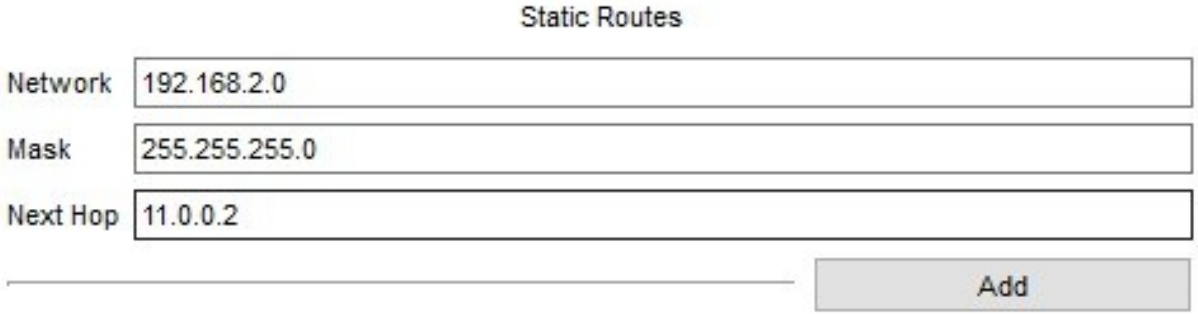
2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shownbelow)**



3. **Configure router with IP address and subnet mask.**







4. **Verifying the network by pinging the IP address of any PC.**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=15ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 9ms

C:\>
```

EXPERIMENT –5

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

THEORY:

DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol usedin TCP/IP networks to automatically assign IP addresses and configuration information to devices on a network. DHCP is commonly used in homes and businesses to simplify the process of connecting devices to a network.

Here's how DHCP works:

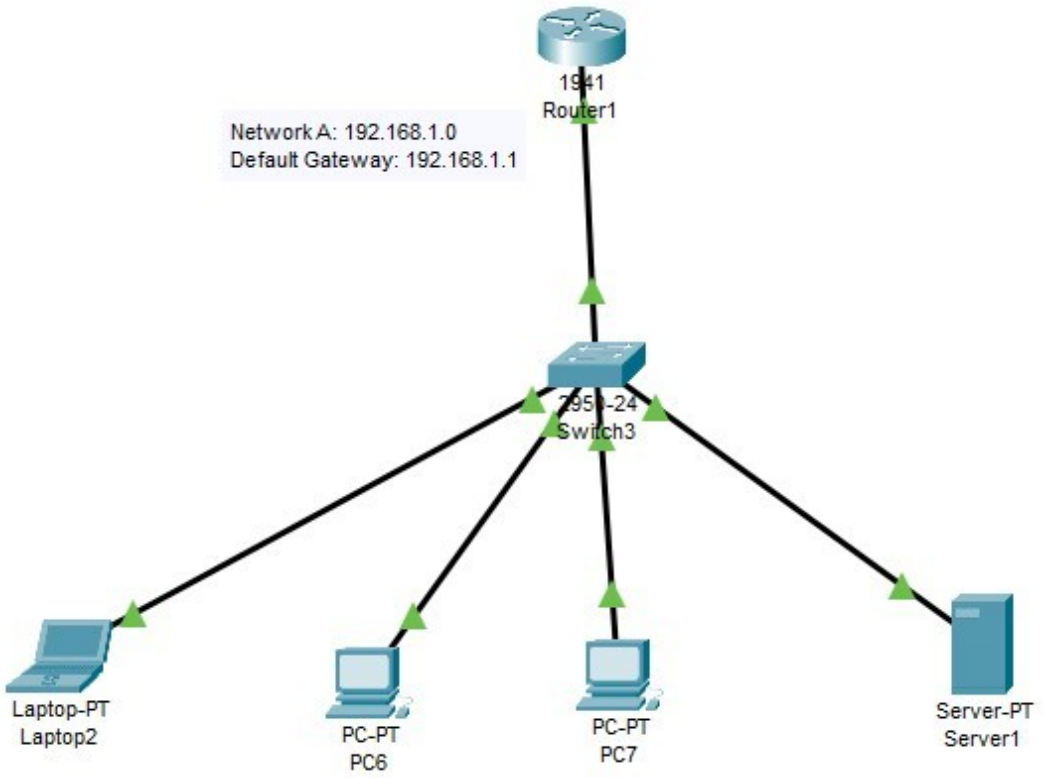
- **Request for IP Address**: When a device, such as a computer or smartphone,connects to a network (usually via Ethernet or Wi-Fi), itsends out a DHCP request to the network.
- **DHCP Server**: A DHCP server on the network receives the request. Theserveris responsible for managing a pool of available IP addresses.
- **IP Assignment**: The DHCP server selects an available IP address fromits pooland assigns it to the requesting device. This ensures that eachdevice on the network has a unique IP address, which is crucial for proper communication.
- **Configuration Information**: Along with the IP address, the DHCP server can also provide other configuration information to the device, such as the subnetmask, default gateway (router), DNS (Domain Name System) server addresses,and more. This information is essential for thedevice to communicate effectively on the network.
- **Lease Time**: DHCP assignments are typically temporary and come witha leasetime. After a specified period, the device must renew its lease with the DHCP server. This allows network administrators to manage and reconfigure the network more easily.

The use of DHCP greatly simplifies network management because it eliminates the need to manually assign and configure IP addresses for each device on the network.Instead, devices can connect to the network and obtain the necessary network settings automatically. DHCP is an integral part of most modern networks and is

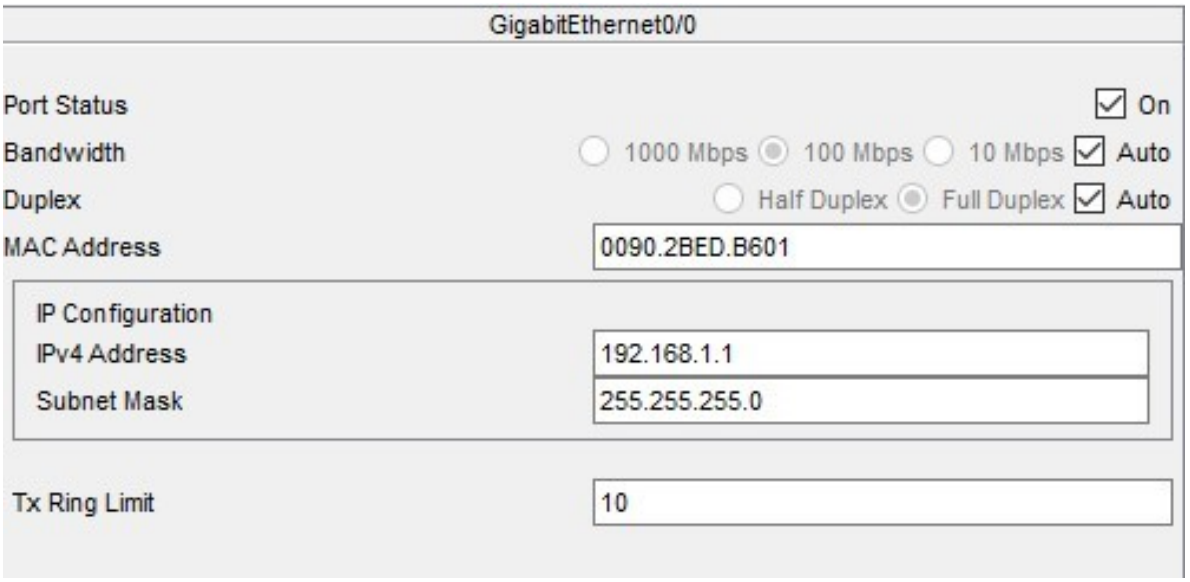
essential for the efficient and scalable management of IP addresses in both small andlarge network environments.

Procedure:

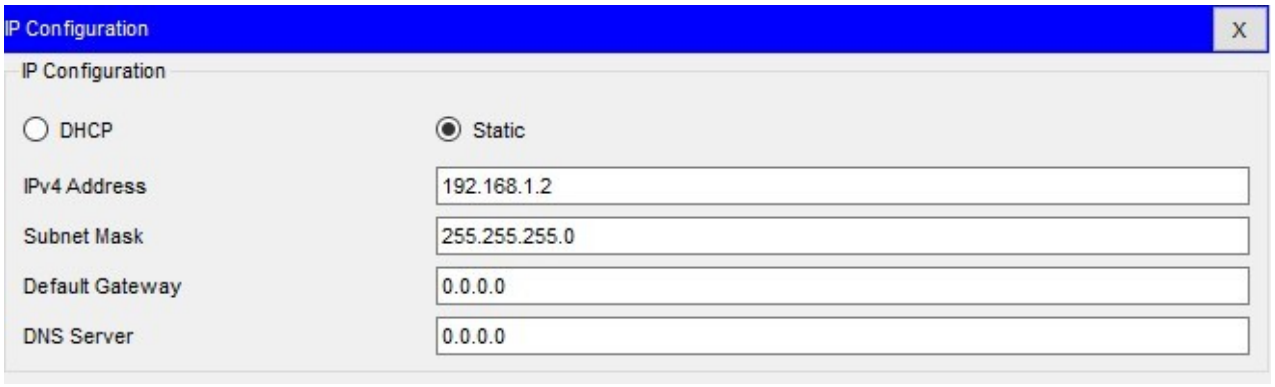
1. **Connect server switch and Endpoints**

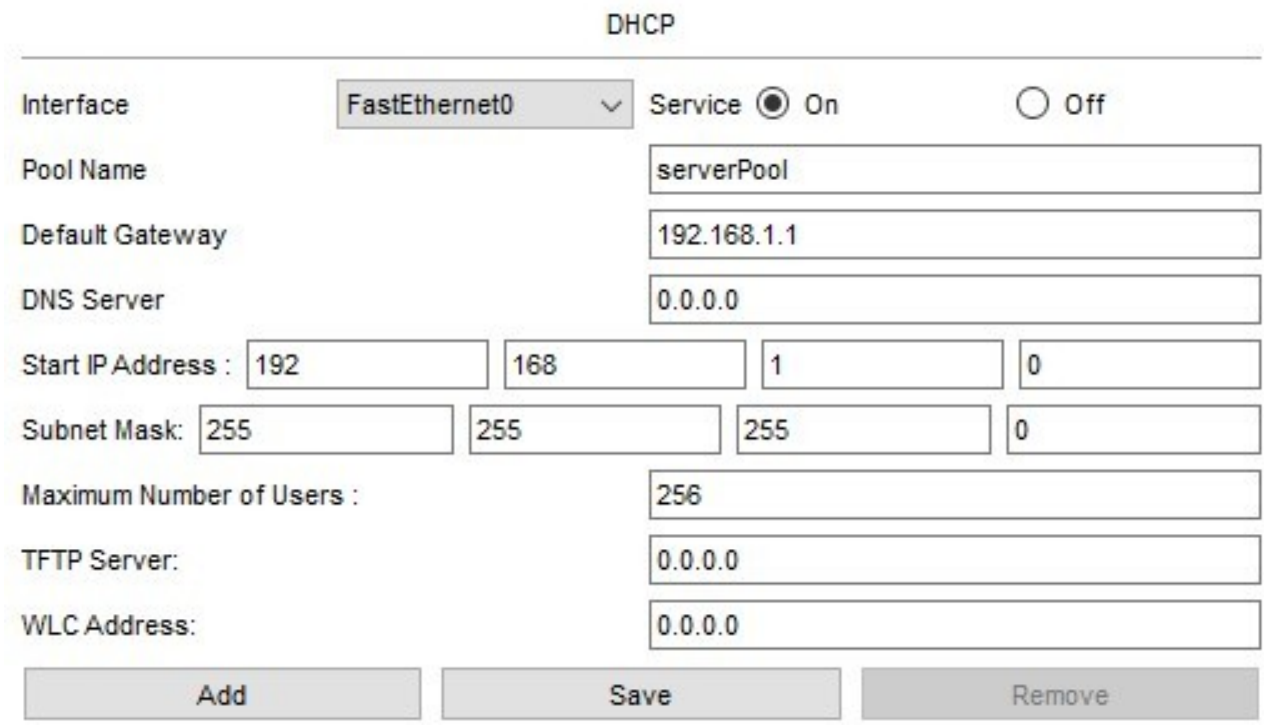


2. **Setting the IP and Subnet mask to Router Device**

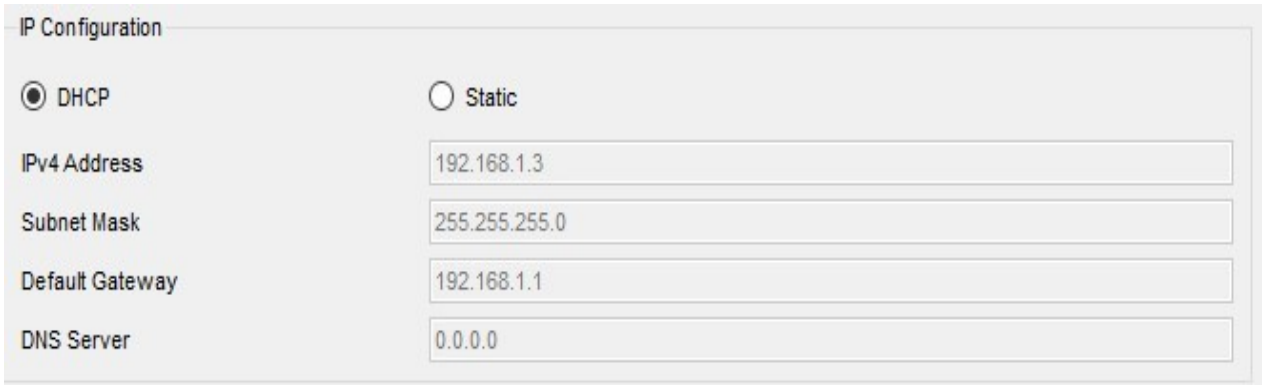


3. Setting up the configuration of the Server

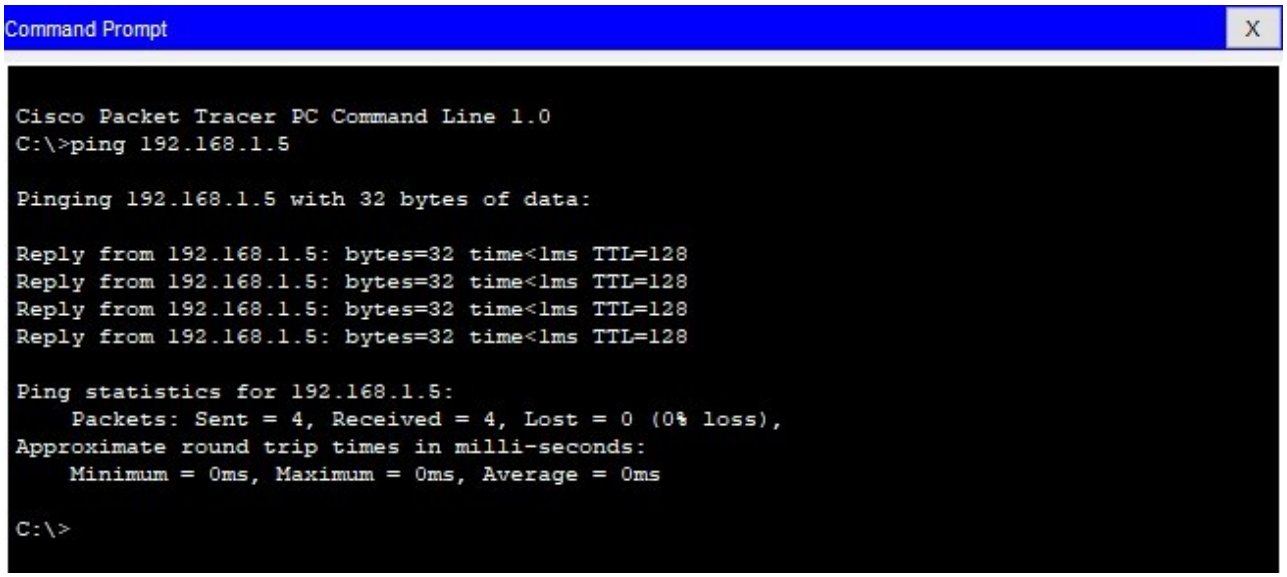




4. Giving IP Address to end devices



5. Verifying the connection by two end devices



EXPERIMENT – 6

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

DNS Servers

THEORY:

Domain Name System (DNS) is a hostname for **IP address** translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.

What is the Need of DNS?

Every host is identified by the IP address but remembering numbers is very difficult for people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

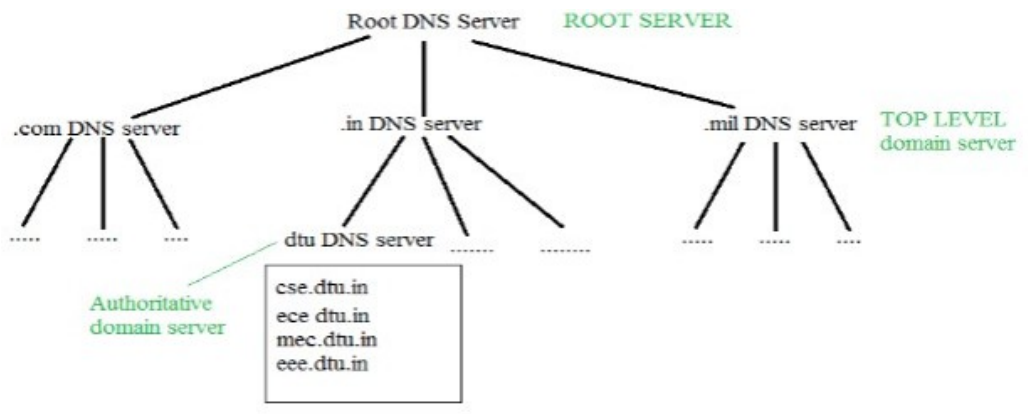
Types of Domain

There are various kinds of domain:

- **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
- **Country domain:** .in (India) .us .uk
- **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type

Organization of Domain

It is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delays for that to happen organization of the database is very important.



Email Service

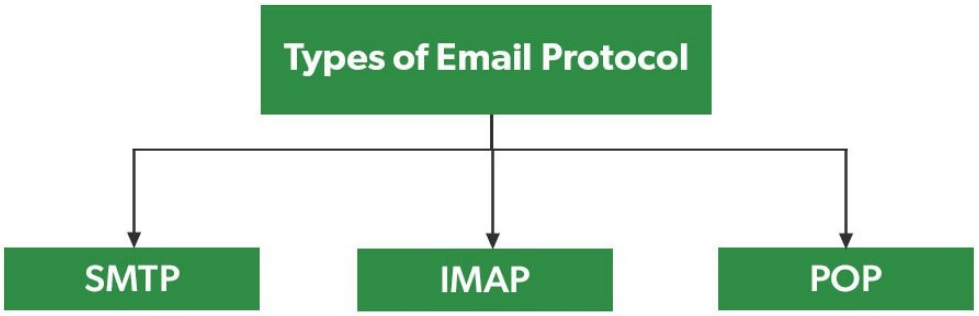
THEORY:

Email protocols are a collection of protocols that are used to send and receive emails properly. The email protocols provide the ability for the client to transmit the mail to or from the intended mail server. Email protocols are a set of commands for sharing mails between two computers. Email protocols establish communication between the sender and receiver for the transmission of email. Email forwarding includes components like two computers sending and receiving emails and the mail server. There are three basic types of email protocols.

Types of Email Protocols:

Three basic types of email protocols involved for sending and receiving mails are:

- SMTP
- POP3
- IMAP



SMTP (Simple Mail Transfer Protocol):

Simple Mail Transfer Protocol is used to send mails over the internet. SMTP is an application layer and connection-oriented protocol. SMTP is efficient and reliable for sending emails. SMTP uses TCP as the transport layer protocol. It handles the sending and receiving of messages between email servers over a TCP/IP network. This protocol along with sending emails also provides the feature of notification for incoming mails. When a sender sends an email then the sender's mail client sends it to the sender's mail server and then it is sent to the receiver mail server through

SMTP. SMTP commands are used to identify the sender and receiver email addresses along with the message to be sent.

Some of the SMTP commands are HELLO, MAIL FROM, RCPT TO, DATA, QUIT, VERIFY, SIZE, etc. SMTP sends an error message if the mail is not delivered to the receiver hence, reliable protocol.

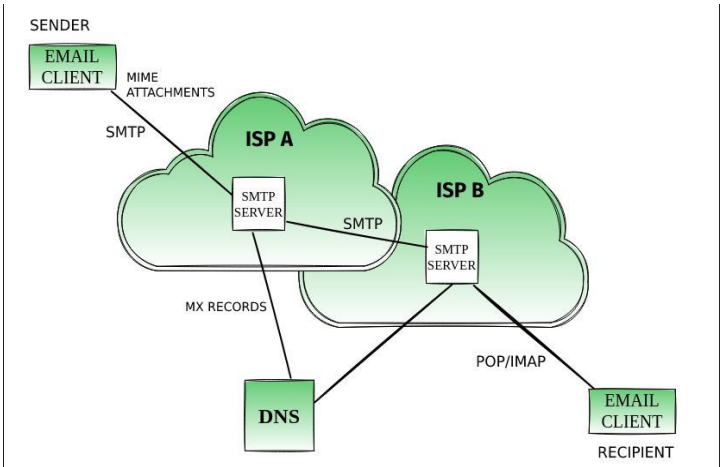
POP(Post Office Protocol):

Post Office Protocol is used to retrieve email for a single client. POP3 version is the current version of POP used. It is an application layer protocol. It allows to access mail offline and thus, needs less internet time. To access the message it has to be downloaded. POP allows only a single mailbox to be created on the mail server. POP does not allow search facilities

Some of the POP commands are LOG IN, STAT, LIST, RETR, DELE, RSET, and QUIT. For more details please refer to the POP Full-Form article.

IMAP(Internet Message Access Protocol):

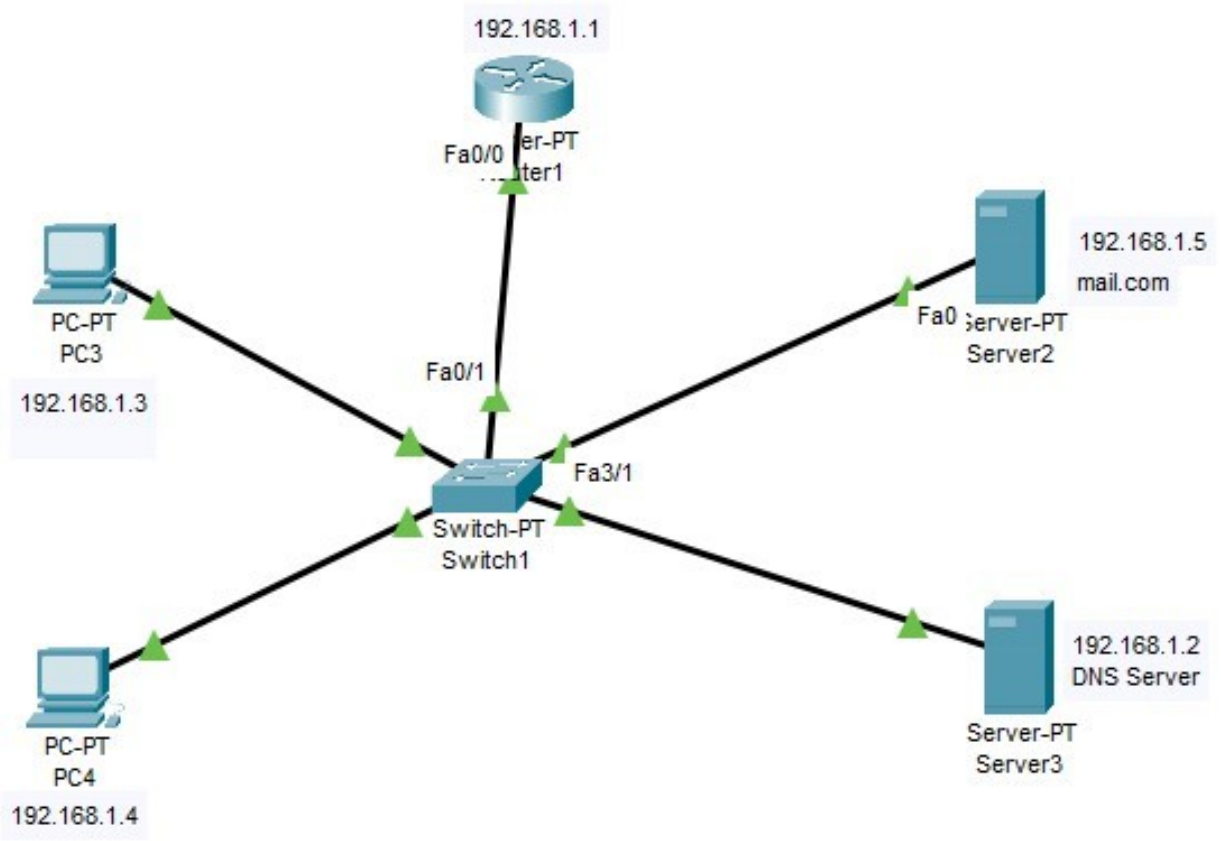
Internet Message Access Protocol is used to retrieve mails for multiple clients. There are several IMAP versions: IMAP, IMAP2, IMAP3, IMAP4, etc. IMAP is an application layer protocol. IMAP allows to access email without downloading them and also supports email download. The emails are maintained by the remote server. It enables all email operations such as creating, manipulating, delete the email without reading it. IMAP allows you to search emails. It allows multiple mailboxes to be created on multiple mail servers and allows concurrent access. Some of the IMAP commands are: IMAP_LOGIN, CREATE, DELETE, RENAME, SELECT, EXAMINE, and LOGOUT.



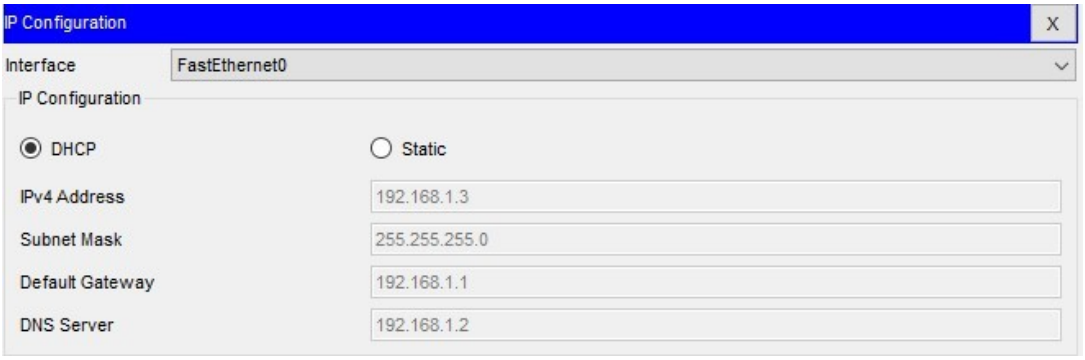
EMAIL PROTOCOLS

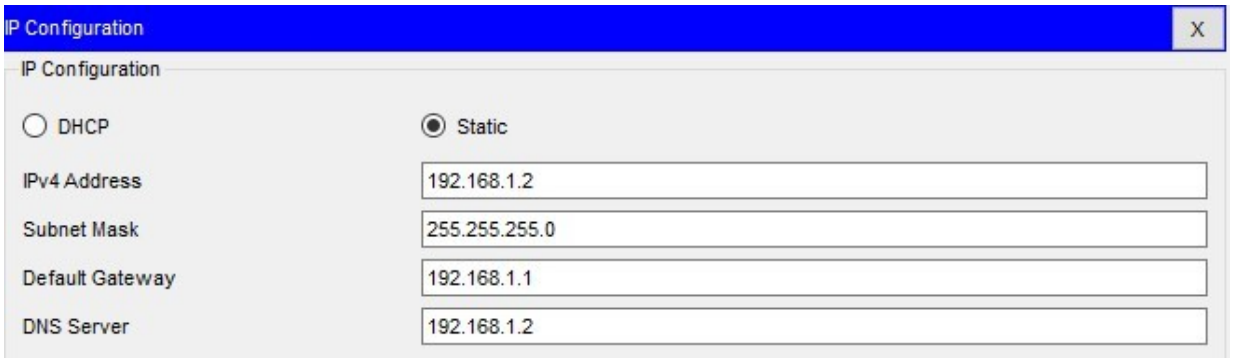
PROCEDURE:

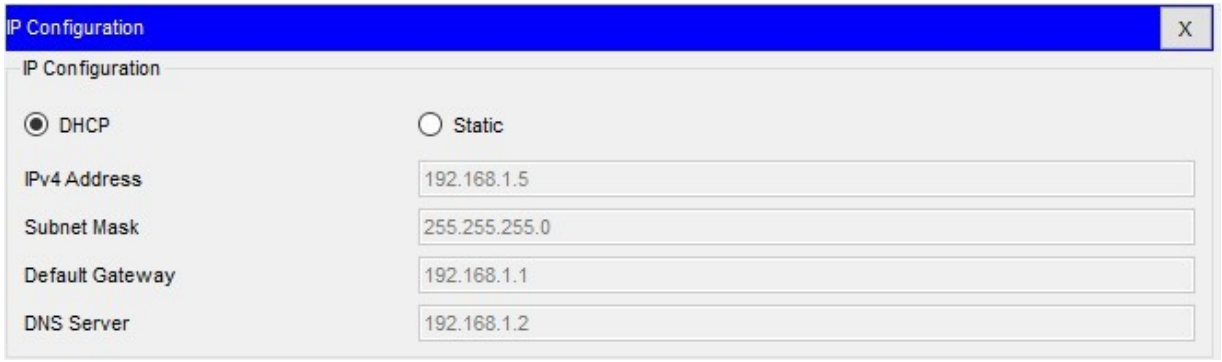
1. **Build the network topology**



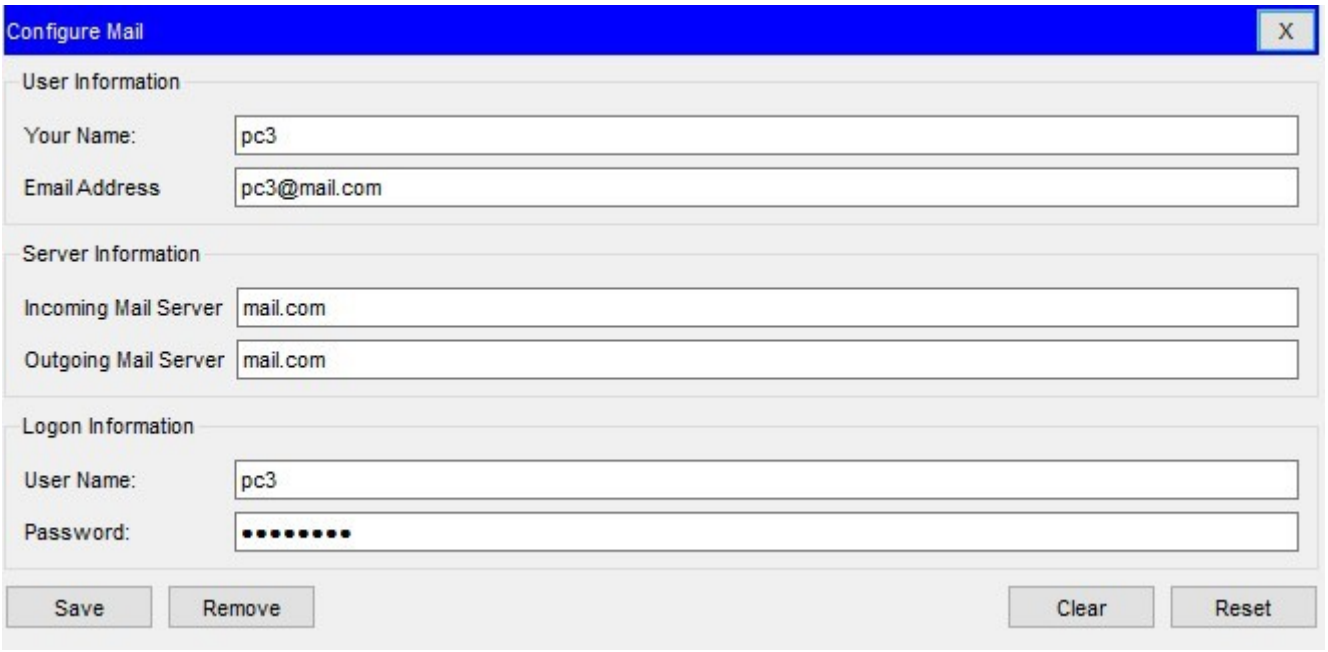
2. **Configure IP addresses on the PCs, DNS Server and the Mail Server.**

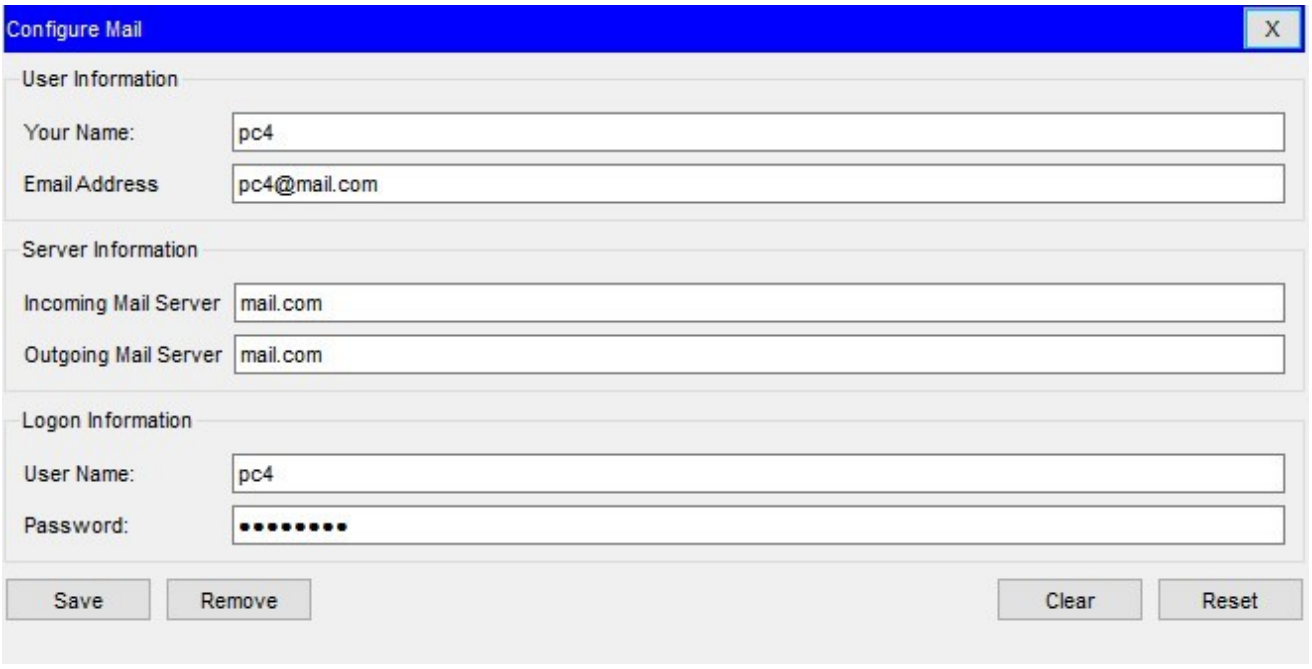




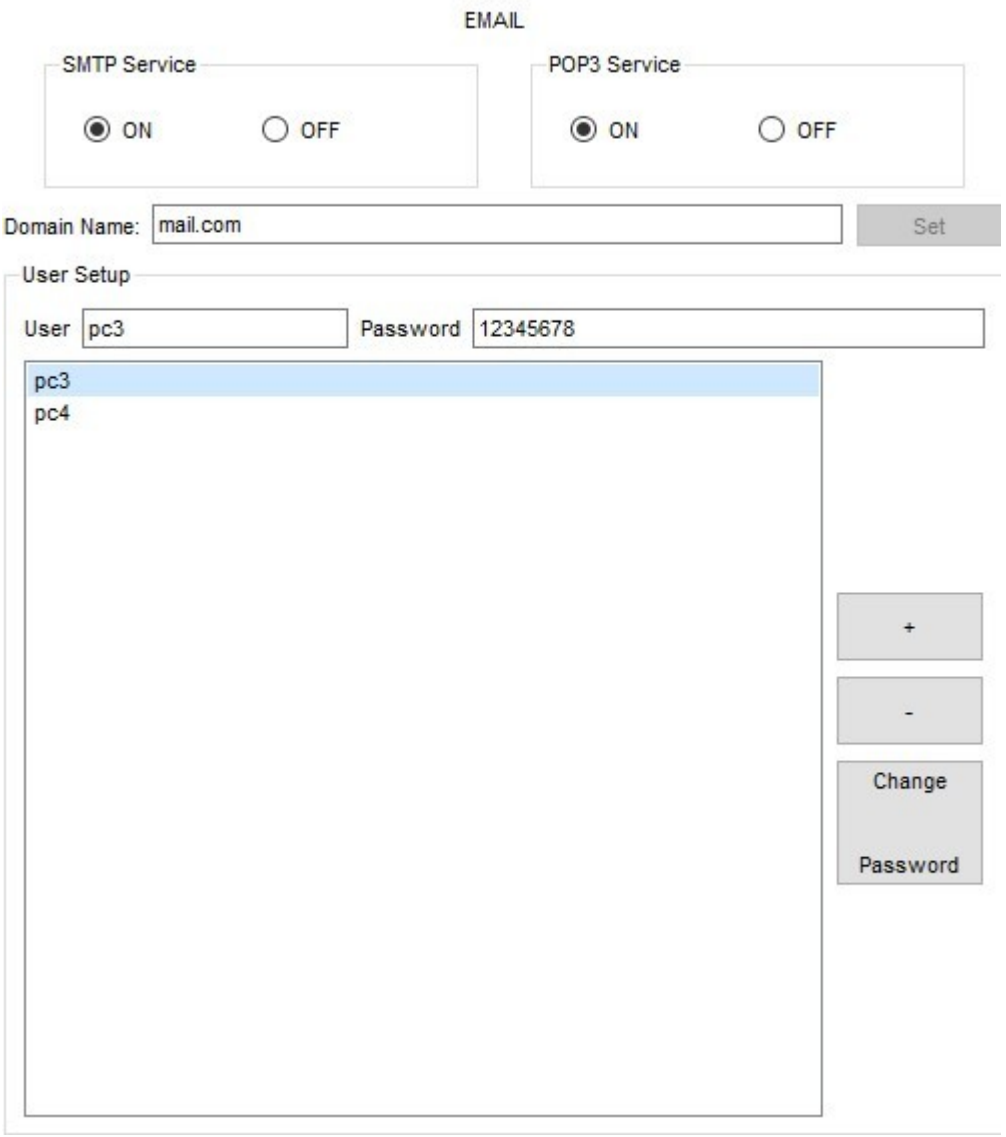


3. **Now configure mail clients on the PCs and mail service on the generic server.**

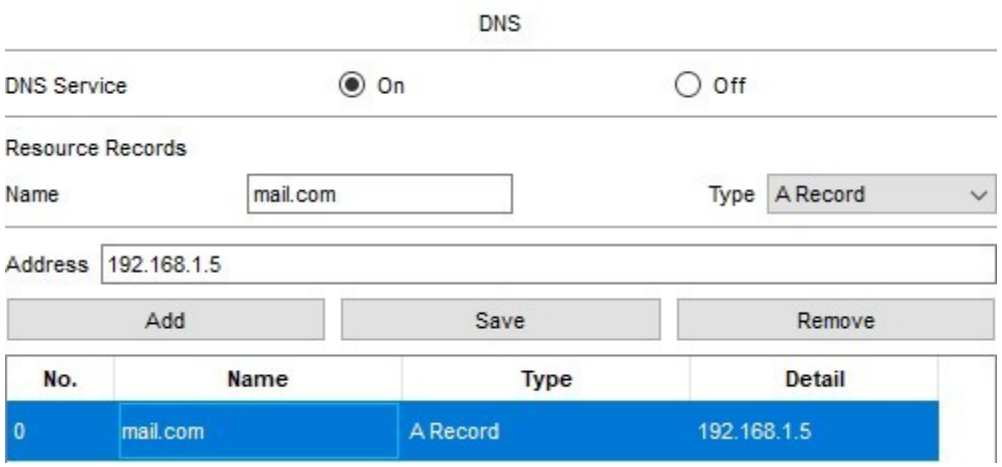




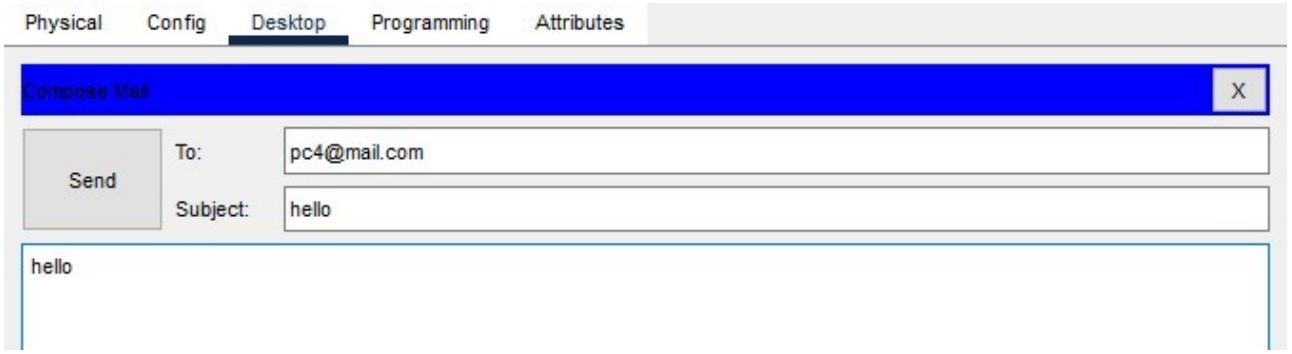
4. **Configure the email server.**

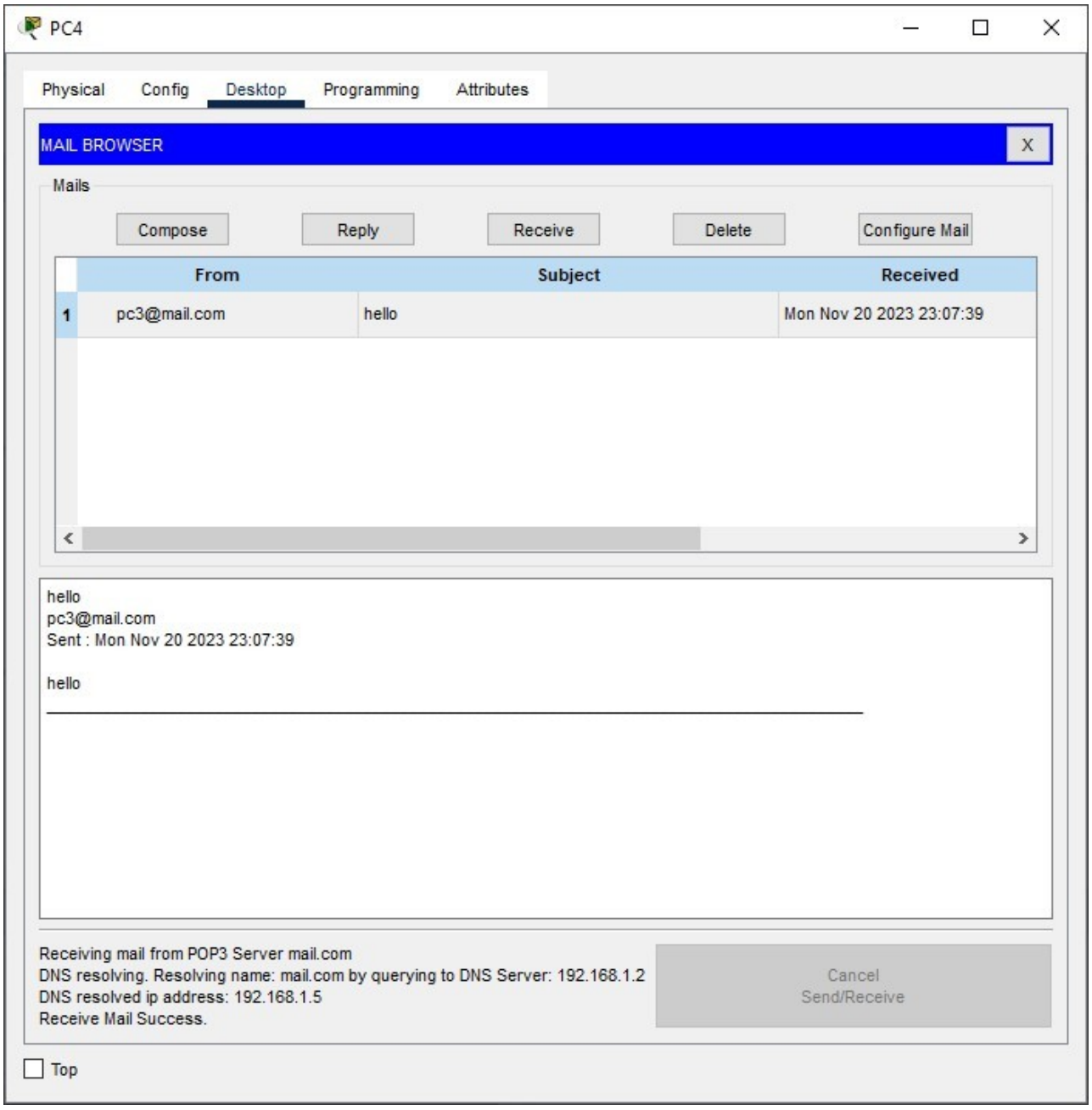


5. **configure a DNS server.**



6. **Lastly test the email service. Go to PC3 email client, compose an email and send its to PC4 email address (pc4@mail.com).**





EXPERIMENT 7

AIM: To implement the Dynamic Routing Protocols : RIP and IGRPusing Cisco Packet Tracer.

Routing Information Protocol

THEORY:

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reacha network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust routing information received from neighbor routers. Thisis also known as Routing on rumors.

RIP versions:

There are three versions of routing information protocol – **RIP Version1**, **RIPVersion2**, and **RIPng**.

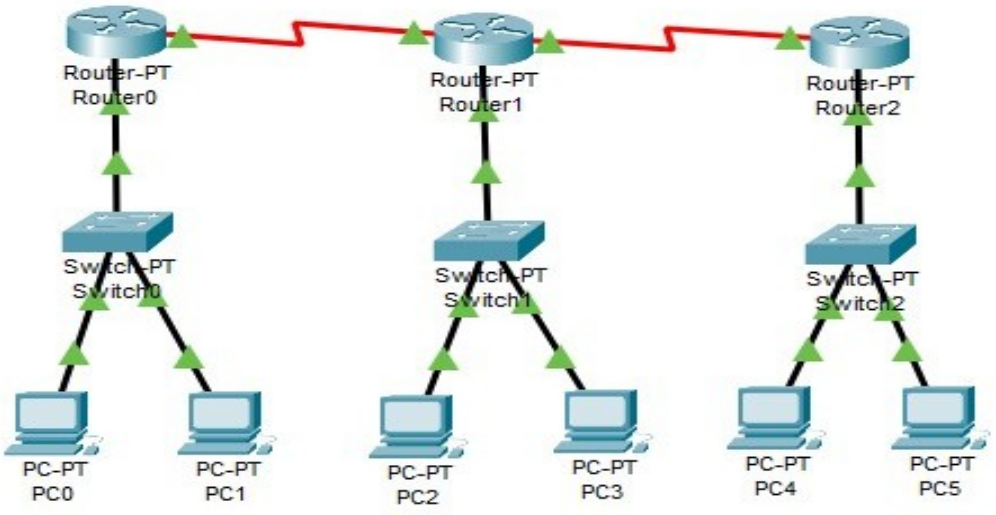
RIP v1	RIP v2	RIPng
Sends update as broadcast	Sends update asmulticast	Sends update asmulticast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run onIPv6 networks)
Doesn't support authentication of updatedmessages	Supports authenticationof RIPv2 update messages	–
Classful routing protocol	Classless protocolupdated supportsclassful	Classless updates aresent

RIP v1 is known as Classful Routing Protocol because it doesn't send information of subnet mask in its routing update.
RIP v2 is known as Classless Routing Protocol because it sends information of subnetmask in its routing update.

3. **Hold down timer:** This is the time for which the router waits for a neighbor router to respond. If the router isn't able to respond within a given time thenit is declared dead. It is 180 seconds by default.
4. **Flush time:** It is the time after which the entry of the route will be flushed if it doesn't respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds i.e time will be 180 + 60 = 240 seconds.

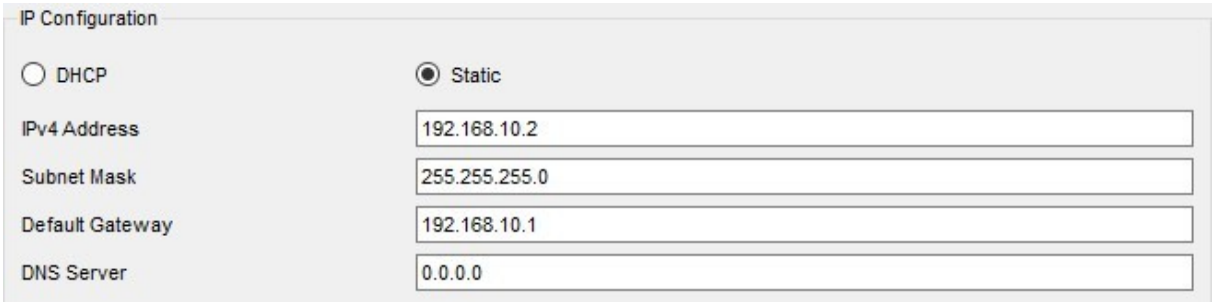
PROCEDURE :

1. *Make the following connection on Cisco Packet Tracer*



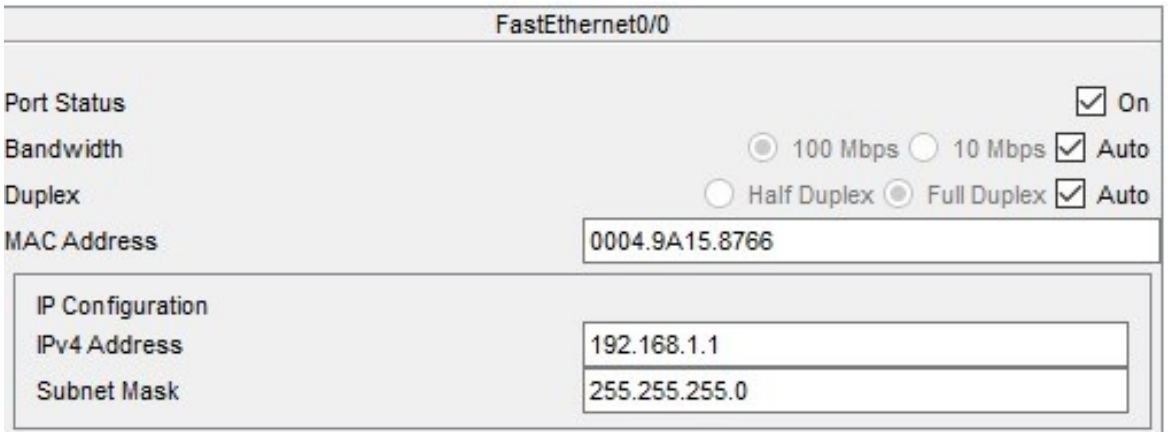
2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shownbelow)**

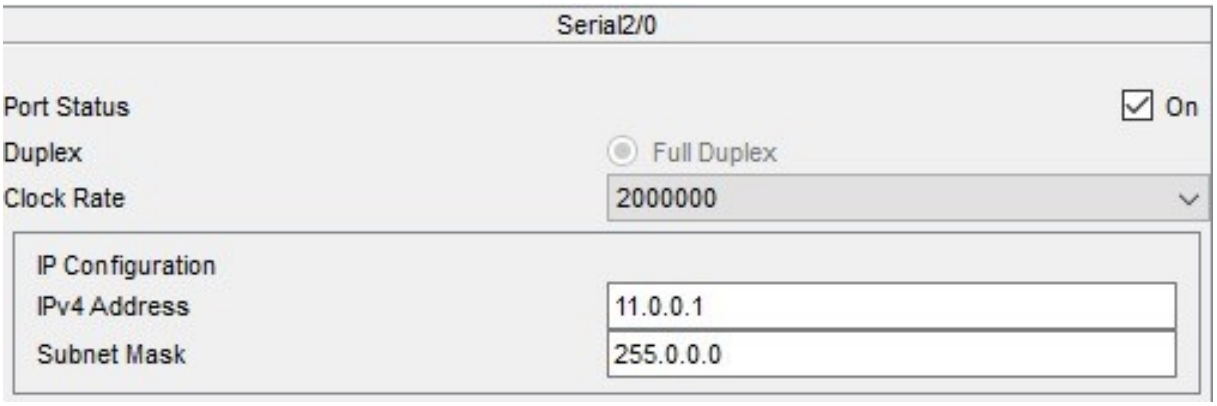
S.NO	Device	IPv4 Address	Subnet mask	Default Gateway
1.	PC0	192.168.10.2	255.255.255.0	192.168.10.1
2.	PC1	192.168.10.3	255.255.255.0	192.168.10.1
3.	PC2	192.168.20.2	255.255.255.0	192.168.20.1
4.	PC3	192.168.20.3	255.255.255.0	192.168.20.1
5.	PC4	192.168.30.2	255.255.255.0	192.168.30.1
6.	PC5	192.168.30.3	255.255.255.0	192.168.30.1



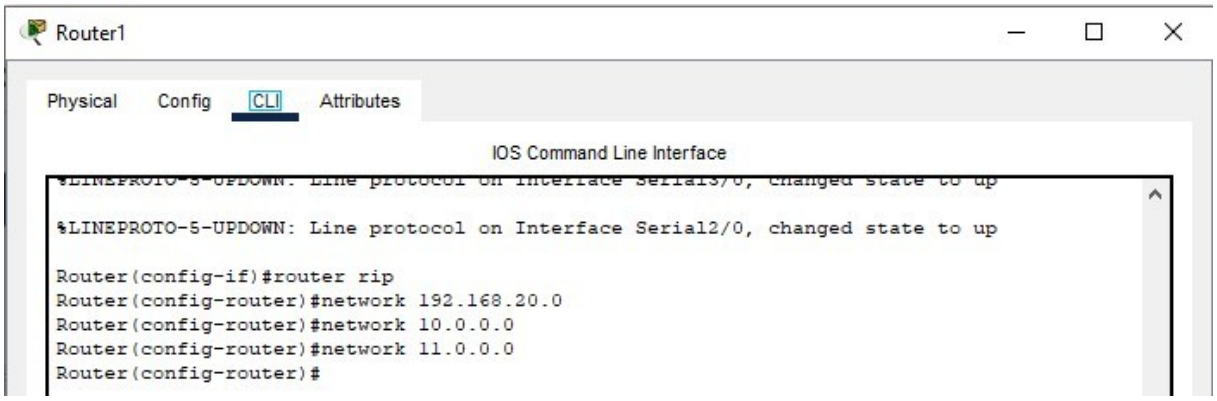
3. *Configure router with IP address and subnet mask.*

S.NO	Device	Interface	IPv4 Address	Subnet mask
1.	router0	FastEthernet0/0	192.168.10.1	255.255.255.0
		Serial2/0	10.0.0.1	255.0.0.0
2.	router1	FastEthernet0/0	192.168.20.1	255.255.255.0
		Serial2/0	10.0.0.2	255.0.0.0
		Serial3/0	11.0.0.1	255.0.0.0
3.	router2	FastEthernet0/0	192.168.30.1	255.255.255.0
		Serial2/0	11.0.0.2	255.0.0.0





4. **After configuring all of the devices we need to assign the routes to therouters.**



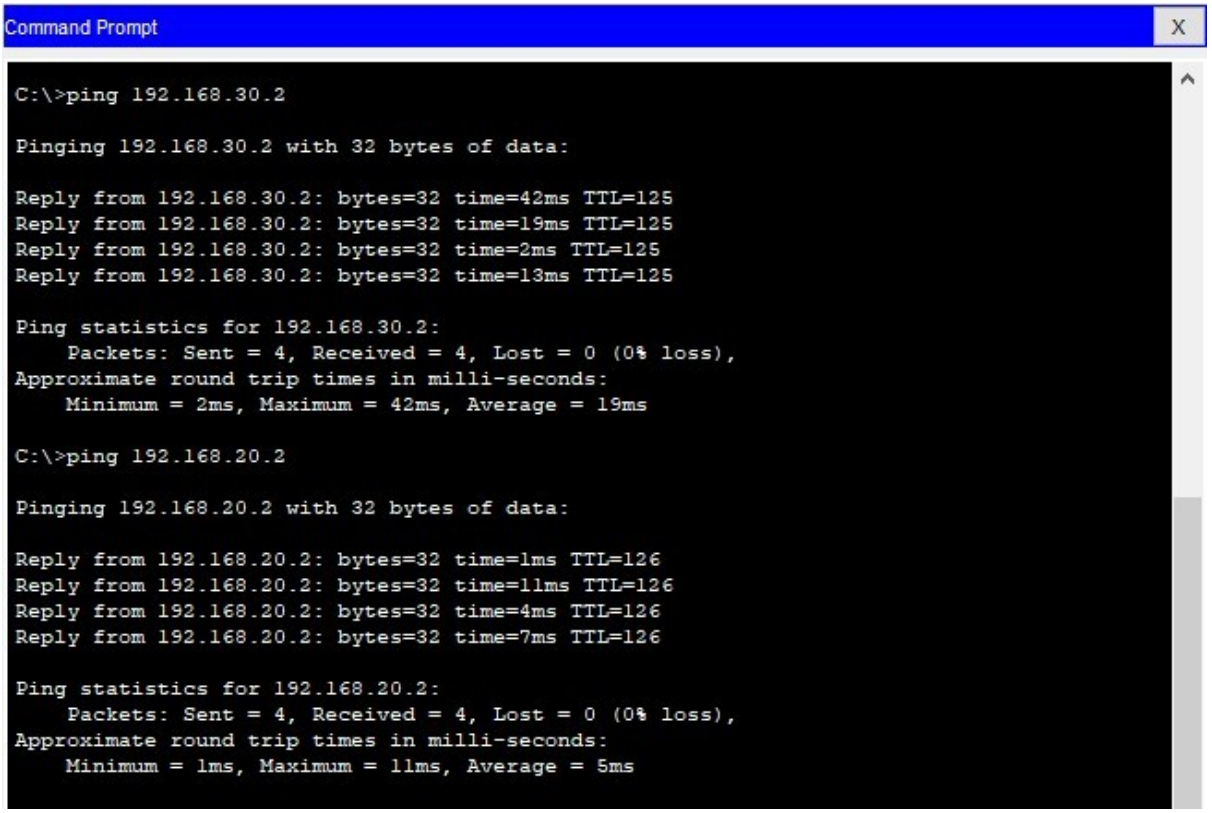

```
Router(config-if)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

Rotuter 0

```
Router(config-if)#router rip
Router(config-router)#network 192.168.30.0
Router(config-router)#network 11.0.0.0
Router(config-router)#
```

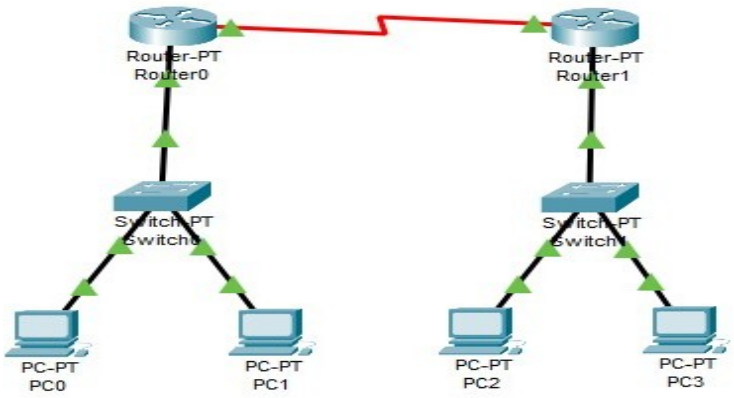
Router 2

5. **Verifying the network by pinging the IP address of any PC.**



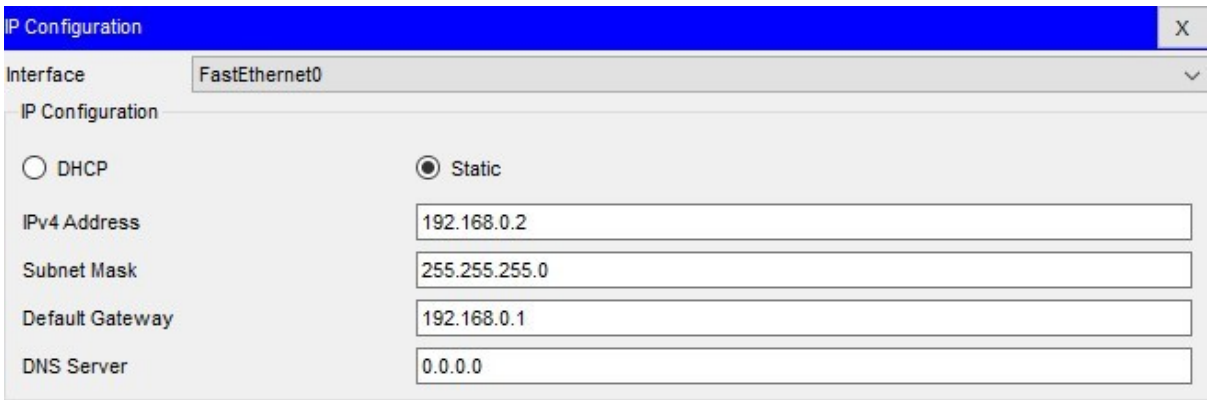
PROCEDURE :

1. *Make the following connection on Cisco Packet Tracer*

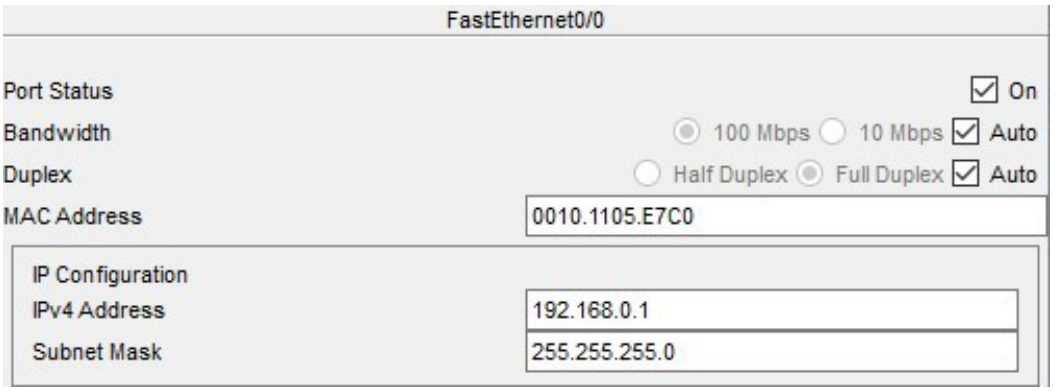


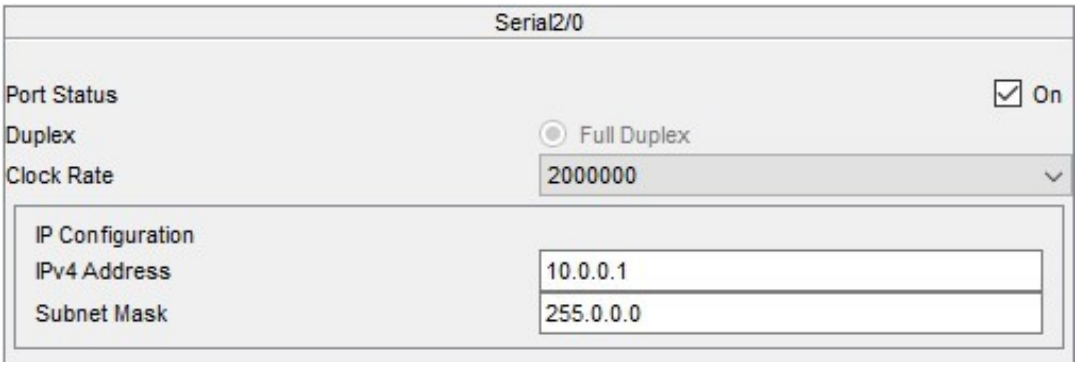
2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shownbelow)**

S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway
1.	pc0	192.168.0.2	255.255.255.0	192.168.0.1
2.	pc1	192.168.0.3	255.255.255.0	192.168.0.1
3.	pc2	172.168.0.2	255.255.255.0	172.168.0.1
4.	pc3	172.168.0.3	255.255.255.0	172.168.0.1



3. *Configure router with IP address and subnet mask.*





4. **After configuring all of the devices we need to assign the routes to therouters.**

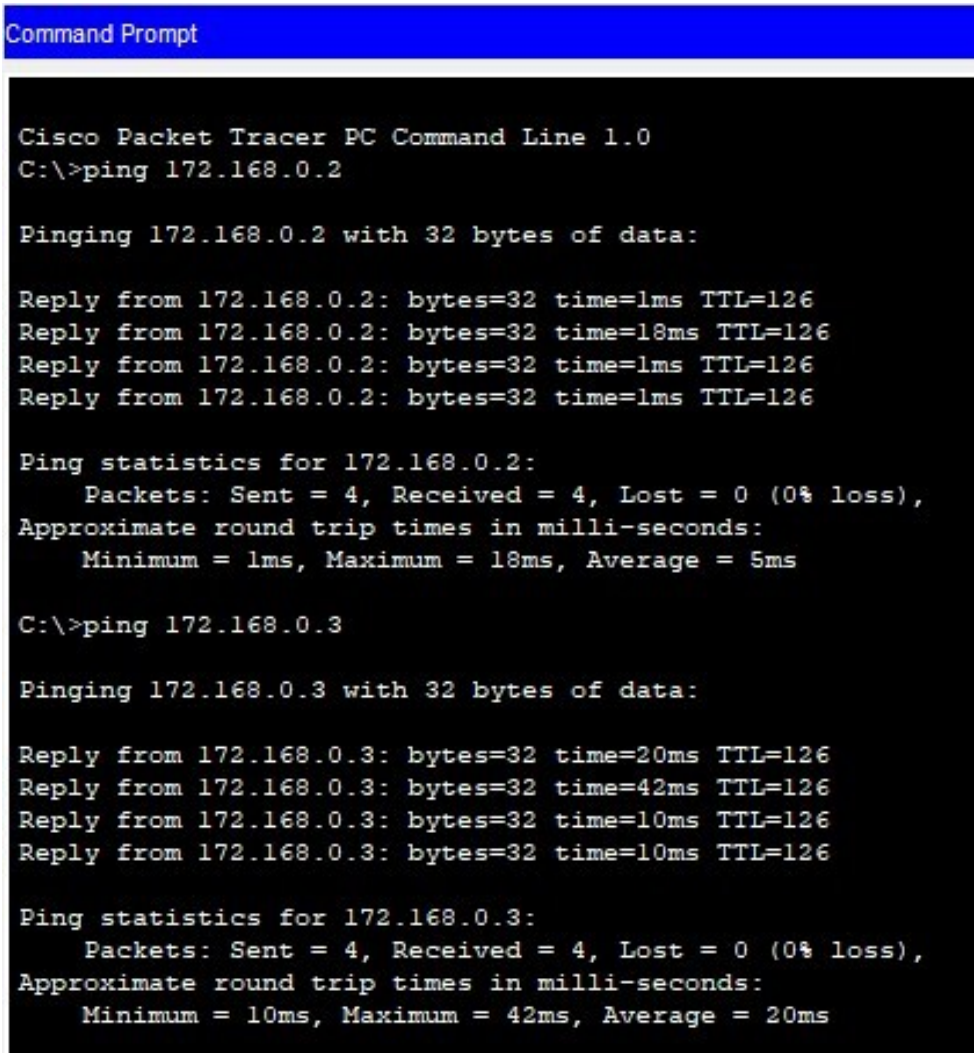
```
Router(config-if)#router  igrp 10
Router(config-router)#network 192.168.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

Router 0

```
Router(config-if)#router  igrp 10
Router(config-router)#network 172.168.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

Rotuter 1

5. **Verifying the network by pinging the IP address of any PC.**



EXPERIMENT8

AIM: To construct multiple router networks and implement the EIGRPProtocol.

THEORY:

Dynamic routing Protocol performs the same function as static routing Protocol does. In dynamic routing Protocol, if the destination is unreachable then another entry, in the routing table, to the same destination can be used. One of the routing protocols is EIGRP.

EIGRP:

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP. Administrative Distance for EIGRP are:-

EIGRP routes	AD values
Summary Routes	5
Internal Routes	90
external routes	170

It uses some messages to communicate with the neighbour devices that operateEIGRP. These are:-

1. **Hello message-**These messages are kept alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbour discovery/recovery, if there is any device operating EIGRP or ifany device(operating EIGRP) coming up again.

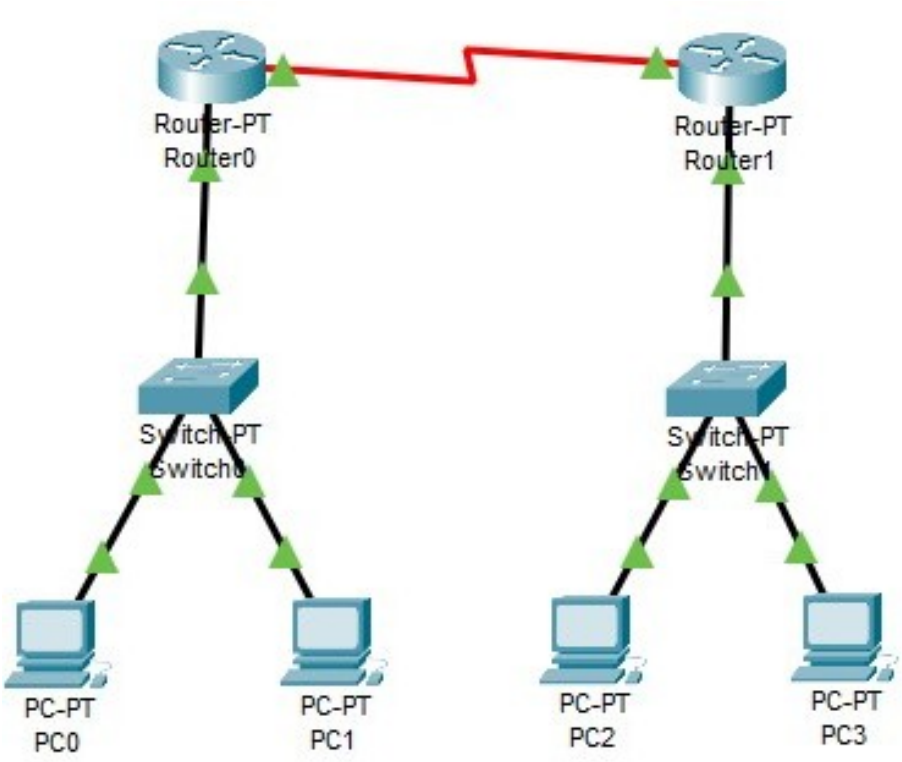
These messages are used for neighbor discovery if multicast at 224.0.0.10. Itcontains values like AS number, k values, etc.
These messages are used as acknowledgement when unicast. A hello with nodata is used as the acknowledgement.

2. **NULL update-**It is used to calculate SRTT(Smooth Round Trip Timer) andRTO(Retransmission Time Out).
   SRTT: The time is taken by a packet to reach the neighboring router and theacknowledgement of the packet to reach the local router.
   RTO: If a multicast fails then unicast is being sent to that router. RTO is the time for which the local router waits for an acknowledgement of the packet.
3. **Full Update –** After exchanging hello messages or after the neighbourship isformed, these messages are exchanged. This message contains all the best routes.
4. **Partial update-**These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all theroutes. These messages are multicast.
5. **Query message-**These messages are multicast when the device is declareddead and it has no routes to it in its topology table.
6. **Reply message –** These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
7. *Acknowledgement message*

   It is used to acknowledge EIGRP updates, queries, and replies. Acks are hellopackets that contain no data.

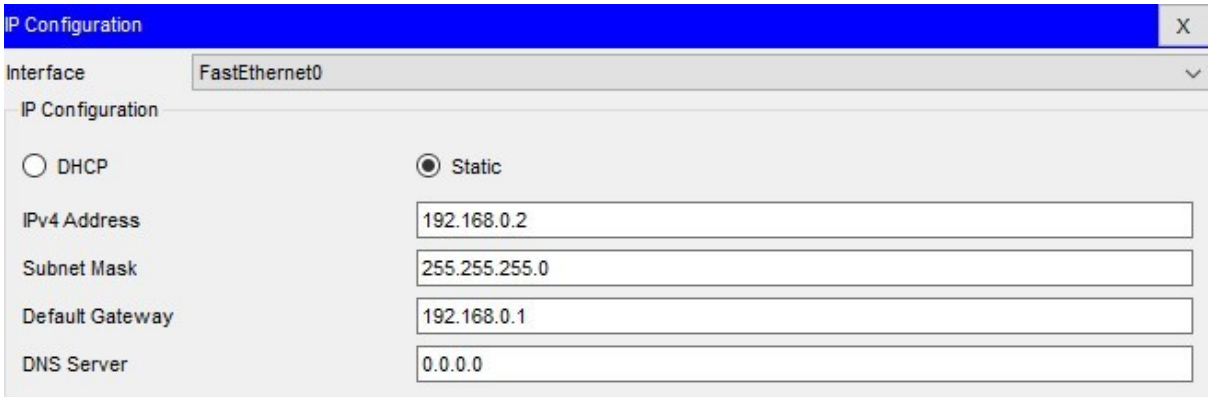
PROCEDURE :

1. *Make the following connection on Cisco Packet Tracer*



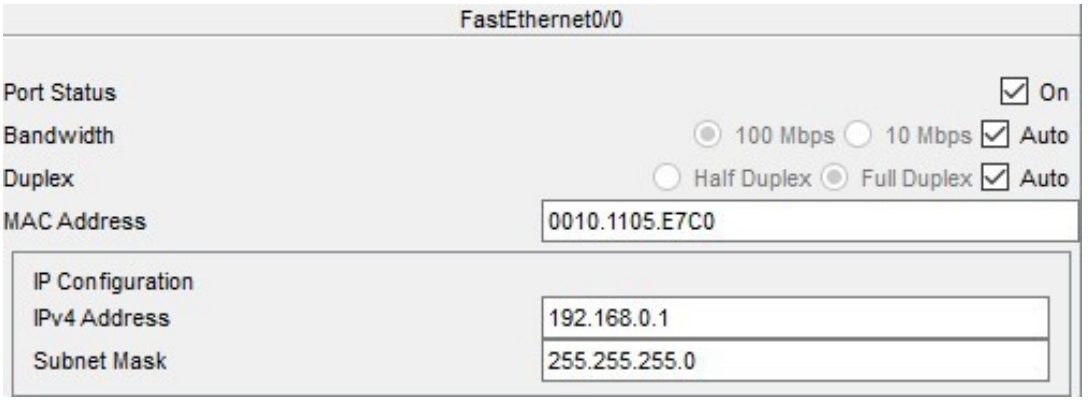
2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shownbelow)**

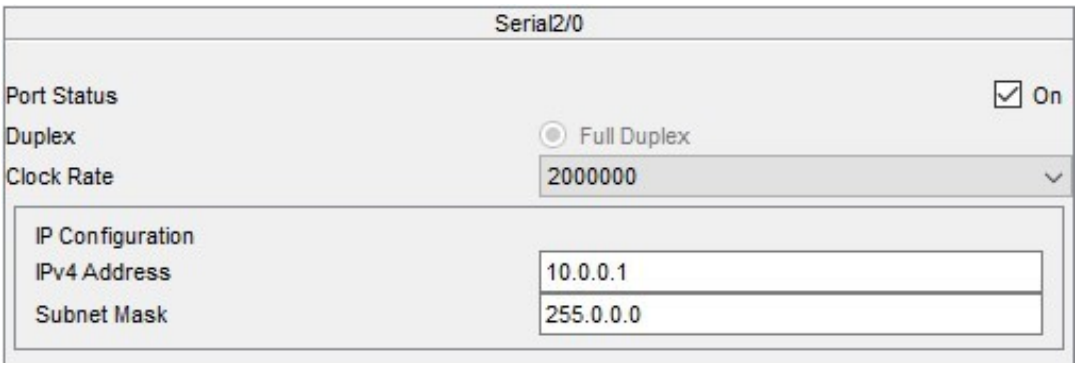
S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway
1.	pc0	192.168.0.2	255.255.255.0	192.168.0.1
2.	pc1	192.168.0.3	255.255.255.0	192.168.0.1
3.	pc2	172.168.0.2	255.255.255.0	172.168.0.1
4.	pc3	172.168.0.3	255.255.255.0	172.168.0.1



3. *Configure router with IP address and subnet mask.*

S.NO	Device	Interface	IPv4 Address	Subnet Mask
1.	router0	FastEthernet0/0	192.168.0.1	255.255.255.0
		Serial2/0	10.0.0.1	255.0.0.0
2.	router1	FastEthernet0/0	172.168.0.1	255.255.0.0
		Serial2/0	10.0.0.2	255.0.0.0





4. After configuring all of the devices we need to assign the routes to therouters.

IOS Command Line Interface

```
Router(config-if)#router eigrp 10
Router(config-router)#network 192.168.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.0.0.2 (Serial2/0) is up: new adjacency
```

Router 0

IOS Command Line Interface

```
Router(config-if)#router eigrp 10
Router(config-router)#network 172.168.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.0.0.1 (Serial2/0) is up: new adjacency
```

Rotuter 1

5. *Verifying the network by pinging the IP address of any PC.*

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.168.0.2

Pinging 172.168.0.2 with 32 bytes of data:

Reply from 172.168.0.2: bytes=32 time=1ms TTL=126
Reply from 172.168.0.2: bytes=32 time=18ms TTL=126
Reply from 172.168.0.2: bytes=32 time=1ms TTL=126
Reply from 172.168.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

C:\>ping 172.168.0.3

Pinging 172.168.0.3 with 32 bytes of data:

Reply from 172.168.0.3: bytes=32 time=20ms TTL=126
Reply from 172.168.0.3: bytes=32 time=42ms TTL=126
Reply from 172.168.0.3: bytes=32 time=10ms TTL=126
Reply from 172.168.0.3: bytes=32 time=10ms TTL=126

Ping statistics for 172.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 42ms, Average = 20ms
```

EXPERIMENT – 9

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

THEORY:

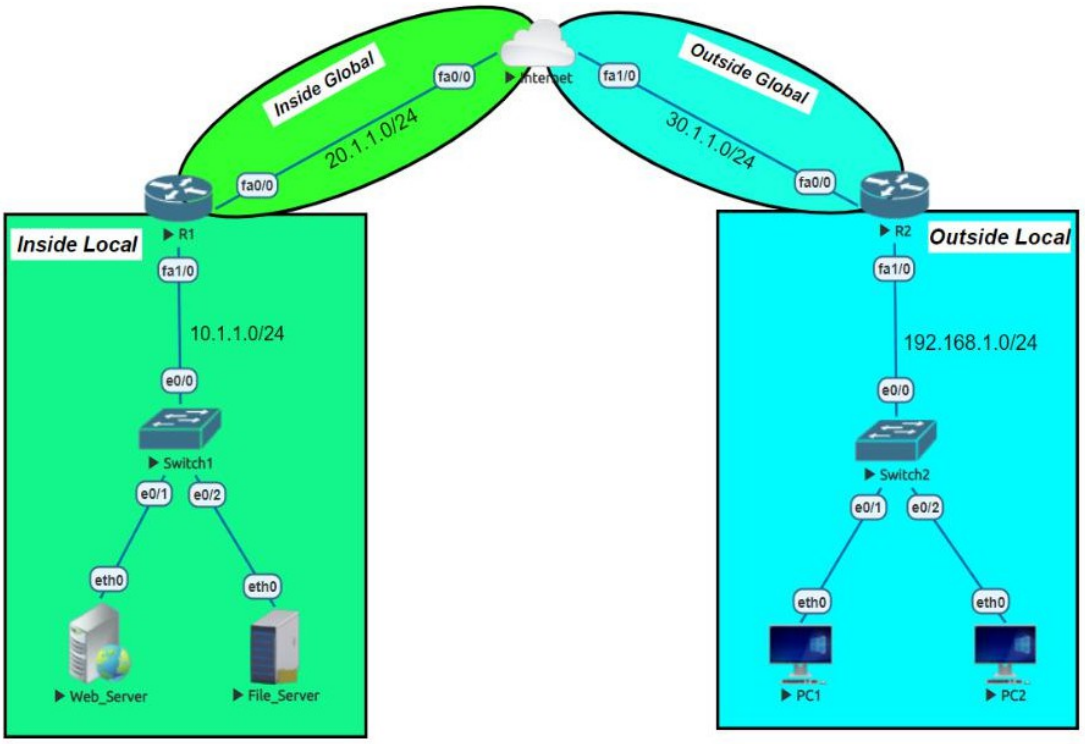
Border routers are typically configured for NAT. A router with an interface on the local (internal) network and an interface on the global (external) network. When a packet leaves the local (internal) network, NAT translates its local (private) IP address to a global (public) IP address. Global (public) IP addresses are translated to local (private) IP addresses when packets enter the local network. When NAT runs out of addresses, i.e. if there are no more addresses in the configured pool, the packet is dropped and an Internet Control Message Protocol (ICMP) host unreachable packet is sent to the destination.

Terminology of NAT:

1. **Inside Local:** It is a region inside the Enterprise's network where the hosts have Private IP addresses.
2. **Inside Global:** It is also a region inside the Enterprise network, but Public IP addresses are used in this region (this region is usually connected to the outside network or Internet).
3. **Outside Local:** It is a region that is generally part of the Enterprise network but in a public Internet (or outside the Enterprise Network). The hosts of the Outside Local region have private IP addresses.
4. **Outside Global**: It is a part of the Enterprise network in a public Internet where Public IP addresses is used.

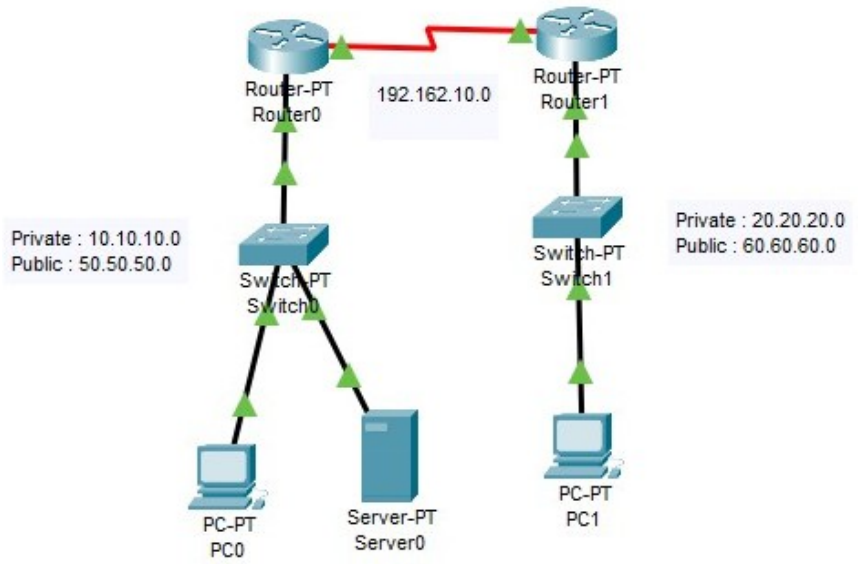
Range of Private IP addresses	Class of IP addresses	No. of Networks
10.0.0.0 to 10.255.255.255	A	1
172.16.0.0 to 172.31.255.255	B	16
192.168.0.0 to 192.168.255.255	C	256

These Private IP addresses cannot be advertised on the Internet using any routing protocol.

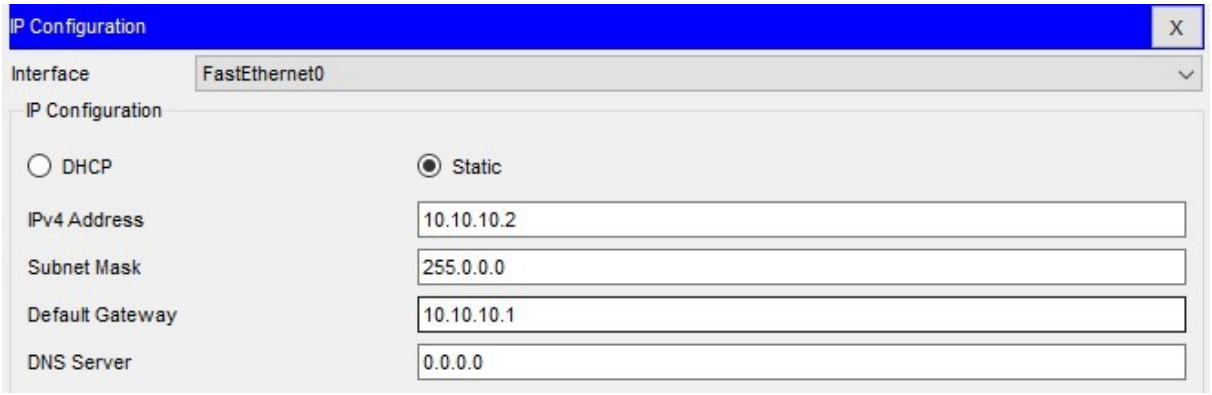


PROCEDURE :

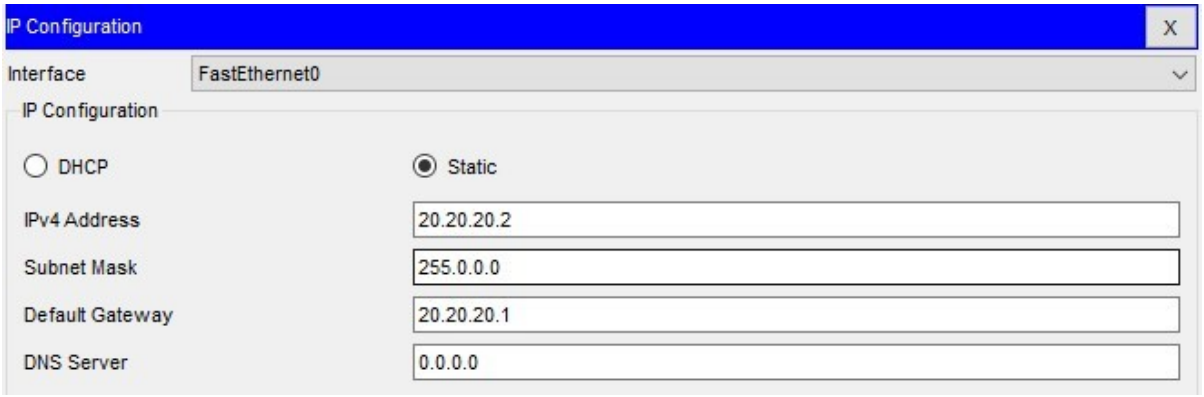
1. **Make the following connection on Cisco Packet Tracer**

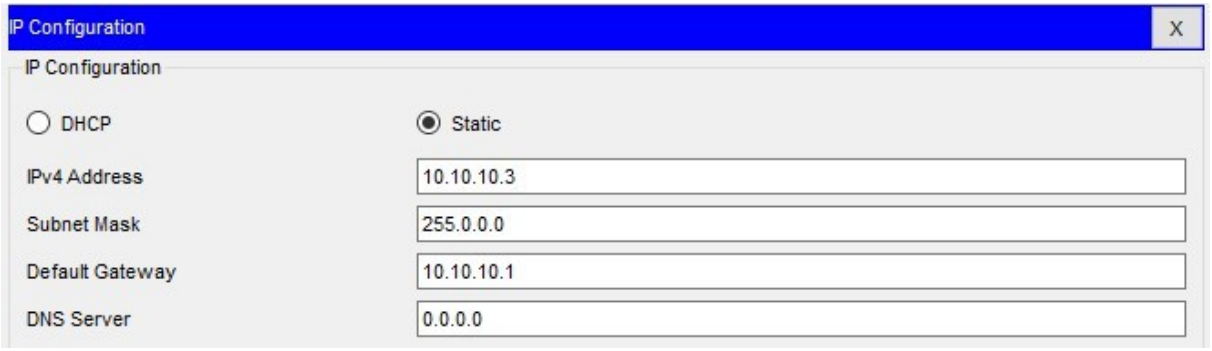


2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shown below)**



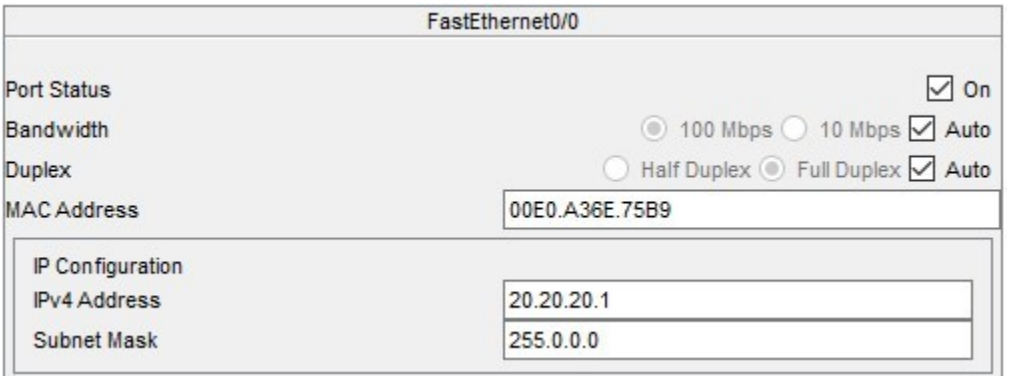
PC0

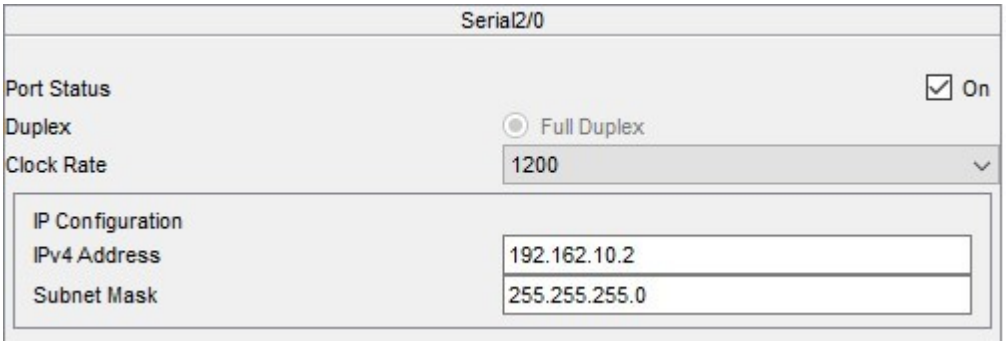




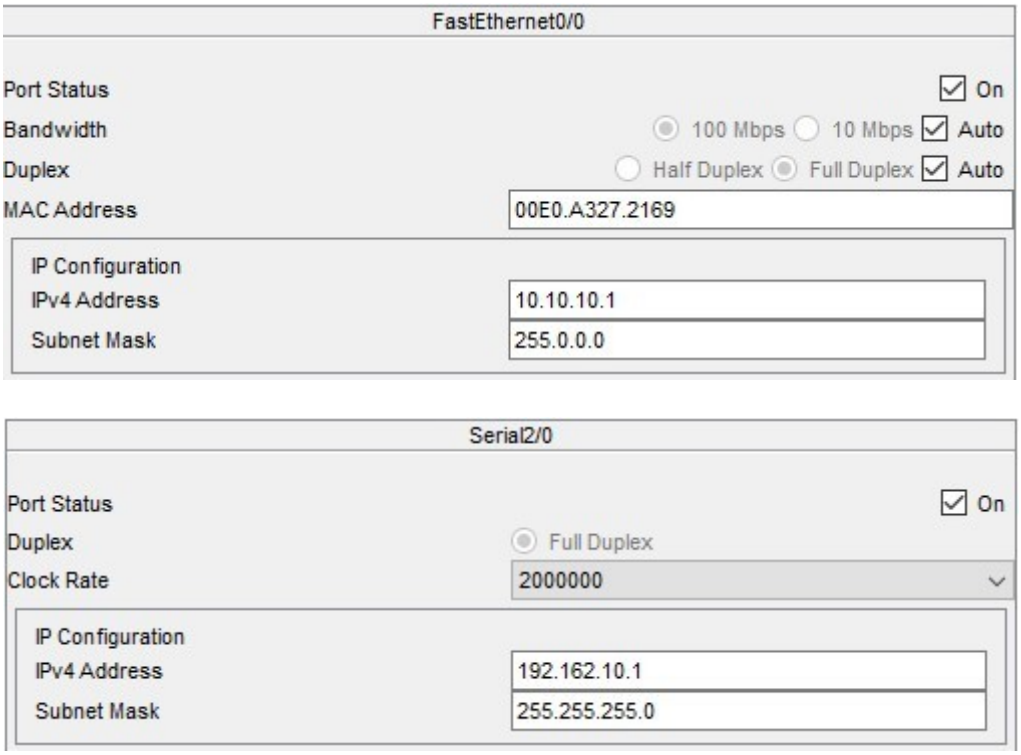
Server0

3. Configure routers with IP address and subnet mask.





Router1



Router0

4. **After configuring all of the devices we need to assign the NAT and routes to the routers.**

IOS Command Line Interface

```
Router(config)#ip nat inside source static 10.10.10.2 50.50.50.2
Router(config)#ip nat inside source static 10.10.10.3 50.50.50.3
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 60.0.0.0 255.0.0.0 192.162.10.2
Router(config)#exit
```

Router 0

IOS Command Line Interface

```
Router(config)#ip nat inside source static 20.20.20.2 60.60.60.2
Router(config)#
Router(config)#
Router(config)#interface Serial2/0
Router(config-if)#ip nat outside
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#ip route 50.0.0.0 255.0.0.0 192.162.10.1
Router(config)#
```

Rotuter 1

5. Verifying the routes and Translations.

IOS Command Line Interface

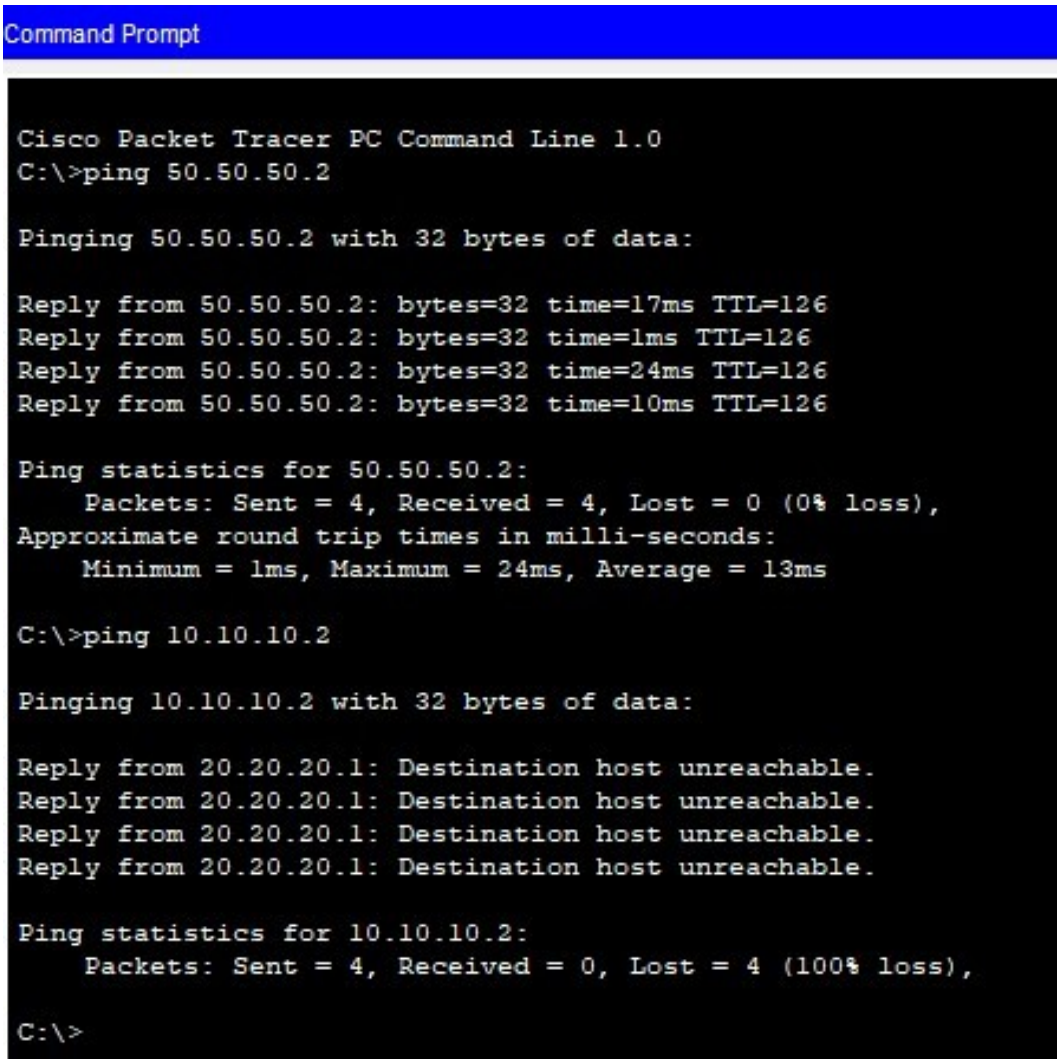
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

C    20.0.0.0/8 is directly connected, FastEthernet0/0
S    50.0.0.0/8 [1/0] via 192.162.10.1
C    192.162.10.0/24 is directly connected, Serial2/0

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  60.60.60.2        20.20.20.2         ---                ---
```

6. **Verifying the network by pinging the IP address of any PC.**



EXPERIMENT – 10

AIM: Conducting a Network Capture and Monitoring with WiresharkSimulation Tool.

THEORY:

What is Wireshark?

Wireshark is an open-source network protocol analysis software program, widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods.

- Wireshark is the world's foremost network protocol analyzer. It lets you seewhat's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.
- Wireshark is cross-platform, using the Qt widget toolkit in current releases toimplement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unixlike operating systems, and Microsoft Windows.

Light Blue: Light blue packets typically represent DNS (Domain Name System)traffic. DNS packets are used to resolve domain names to IP addresses.

Red: Red packets indicate potential issues or errors in the network traffic. These can include TCP retransmissions, checksum errors, or other anomalies.

Yellow: Yellow packets often represent ICMP (Internet Control Message Protocol) traffic. ICMP is used for network diagnostics, error reporting, andother control functions.

Black: Black packets represent TCP resets, which are used to abruptlyterminate a TCP connection.

Gray: Gray packets are packets that do not fit into any of the predefined color categories. They can include various types of network traffic that don't fall intothe common protocol categories.

Additional Wireshark Features

Beyond the capture and filtering, several other features in Wireshark can make yourjob easier.

Wireshark Colorization Options

You can configure Wireshark to color your packets in the Packet List according to thedisplay filter, which allows you to emphasize the packets you want to highlight.

Wireshark Promiscuous Mode

By default, Wireshark only captures packets going to and from the computer where itruns. By checking the box to run Wireshark in promiscuous mode in the capture settings, you can capture most of the traffic on the LAN.

Wireshark Command Line

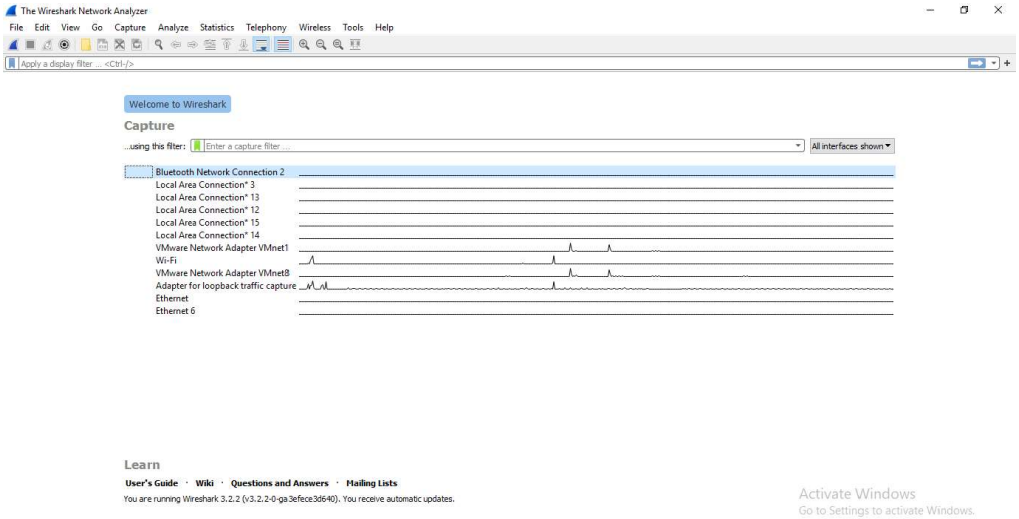
Wireshark does provide a command line interface (CLI) if you operate a system without a graphical user interface (GUI). The best practice would be to use the CLI tocapture and save a log so you can review the log with the GUI.

Wireshark Command Line

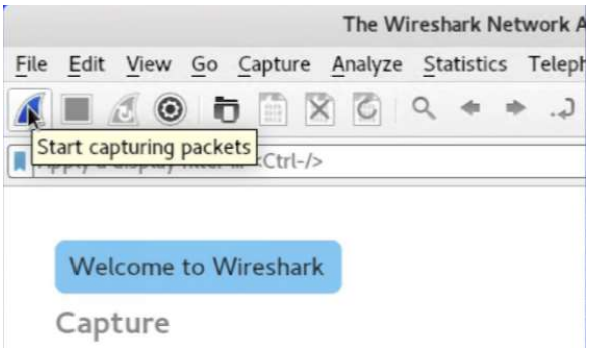
- wireshark : run Wireshark in GUI mode
- wireshark –h : show available command line parameters for Wireshark
- wireshark –a duration:300 –i eth1 –w wireshark. : capture traffic on the ethernet interface one for five minutes. –a means automatically stop thecapture, -i specifies which interface to capture

Wireshark Command Line

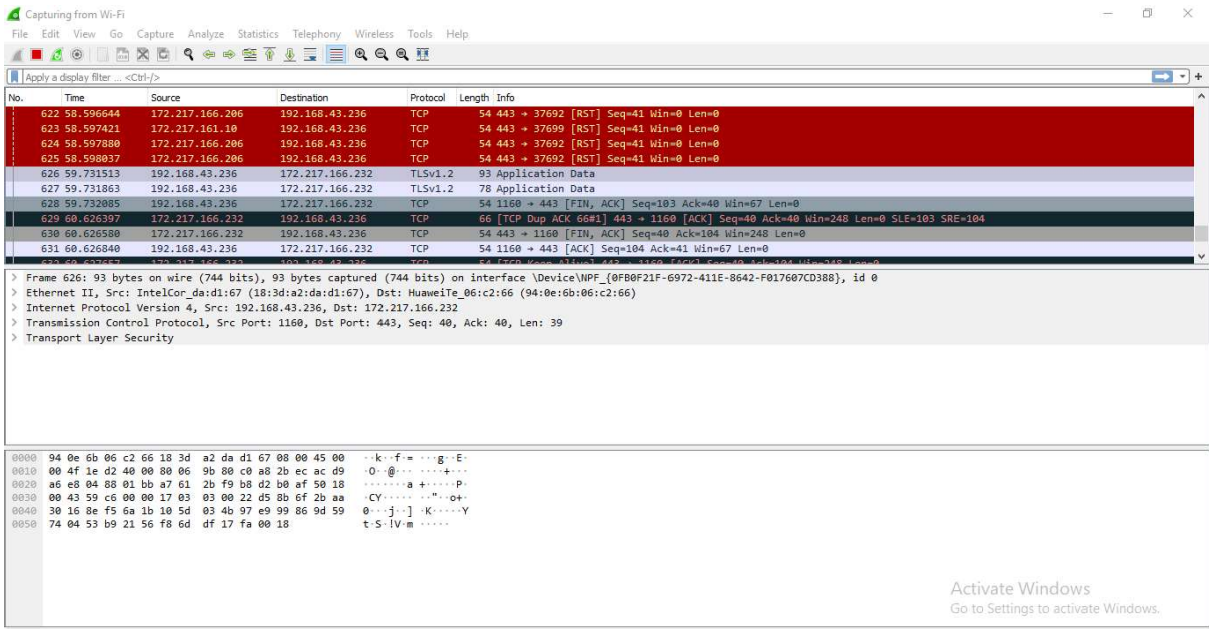
1. **Getting Up and Running:** After installation launch Wireshark, approve the administrator or superuser privileges and you will be presented with a windowthat looks like this:



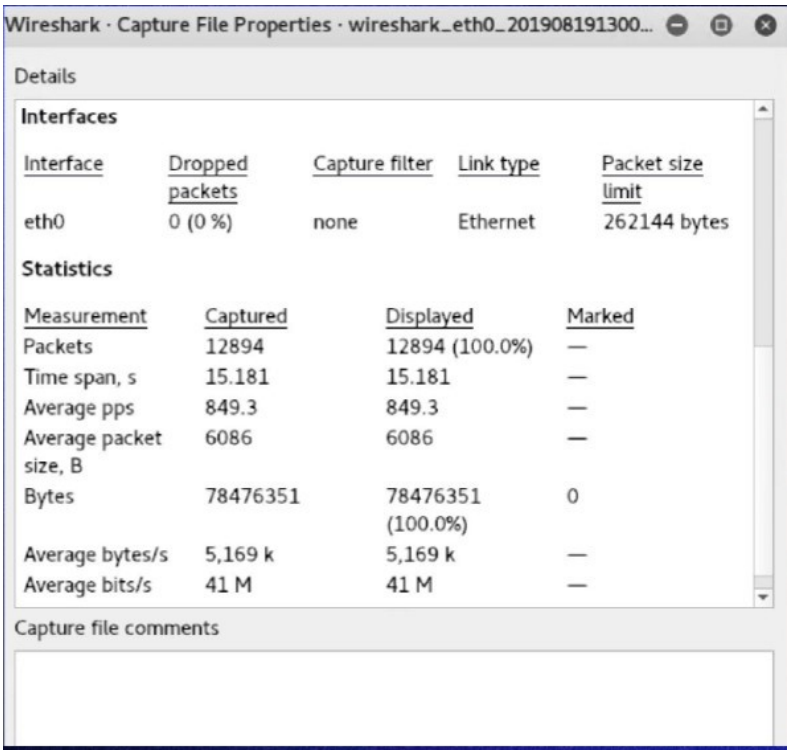
2. **Click the first button on the tool bar, titled "Start Capturing packets"**



3. **During the capture, Wireshark will show you the packets captured inreal-time.**



Capture File Properties



Wireshark I/O Graph: