EXPERIMENT 1

AIM: Introduction to Networking Simulation Tools: Wireshark, Cisco Packet Tracer

THEORY:

Networking Simulation: Exploring and Testing Network Scenarios Virtually

Networking simulation is a technology that allows network professionals, engineers, and students to create, model, and experiment with network environments and scenarios in a virtual or simulated setting. It provides a safe and controlled environment for testing, optimizing, and understanding various aspects of networking, without the need for physical hardware or real-world networks. This approach offers several benefits, including cost-effectiveness, scalability, and a risk-free space for learning and experimentation.

Networking simulation tools play a pivotal role in the field of network engineering and computer science. They provide a platform for designing, analyzing, and experimenting with network configurations and protocols in a controlled, virtual environment. These tools are invaluable for both educational and professional purposes. Two widely used networking simulation tools are Wireshark and Cisco Packet Tracer. In this overview, we'll explore their fundamental features and use cases.

Tools:

1. Wireshark:

Overview:

Wireshark, formerly known as Ethereal, is a popular, open-source network protocol analyzer. It is used for capturing, analyzing, and troubleshooting network traffic. Wireshark is highly versatile and is available for various operating systems, including Windows, macOS, and Linux.

Key Features:

- Packet Capturing: Wireshark allows users to capture network packets from live network interfaces or from pre-recorded packet capture files. This feature is invaluable for monitoring and diagnosing network issues.
- Protocol Analysis: It can dissect and display the details of numerous network protocols, making it a valuable tool for understanding the inner workings of network communication.
- Filtering: Wireshark provides advanced filtering options to focus on specific network traffic, helping users locate and analyze the packets of interest.
- Live Packet Viewing: Real-time analysis of network traffic enables users to observe network behavior as it happens.

Use Cases:

- Network Troubleshooting: Network administrators and engineers use Wireshark to identify and diagnose network issues, such as packet loss, latency, and security breaches.

- Protocol Development: It's a valuable tool for developers working on network protocols to ensure they adhere to specifications and standards.
- Security Analysis: Security professionals can use Wireshark to identify suspicious network traffic patterns and investigate potential security breaches.
- Education: Wireshark is widely used in networking courses and labs to teach students about network protocols and packet analysis.

2. Cisco Packet Tracer:

Overview:

Cisco Packet Tracer is a network simulation tool developed by Cisco Systems. It is primarily designed for learning and practicing networking concepts, particularly those related to Cisco networking equipment. It provides a graphical user interface that simulates the configuration and behavior of network devices.

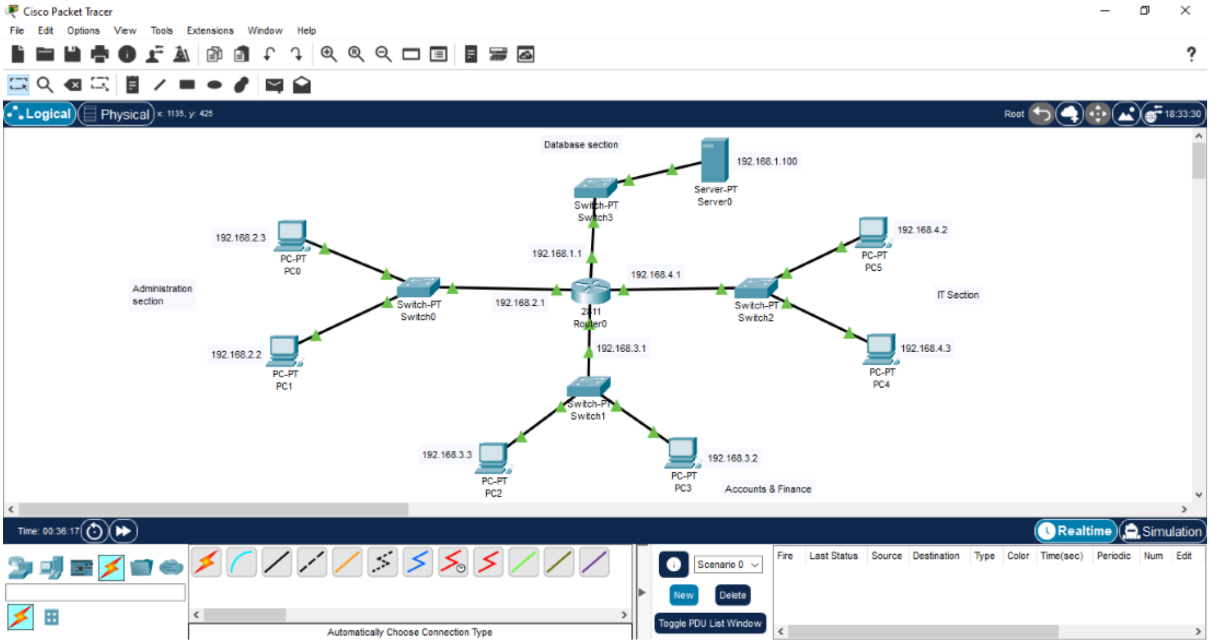
Key Features:

- Device Simulation: Packet Tracer simulates various Cisco networking devices, such as routers, switches, firewalls, and more. Users can create, configure, and interconnect these devices to design complex network topologies.
- Protocols and Services: It supports a wide range of network protocols and services, including routing protocols (e.g., OSPF, EIGRP), security features, and Quality of Service (QoS) settings.
- Real-Time Simulation: Packet Tracer allows users to see real-time network behaviors as they configure and experiment with network devices.
- Networking Labs: Cisco provides a wealth of networking labs and activities that users can complete to gain hands-on experience in a simulated environment.

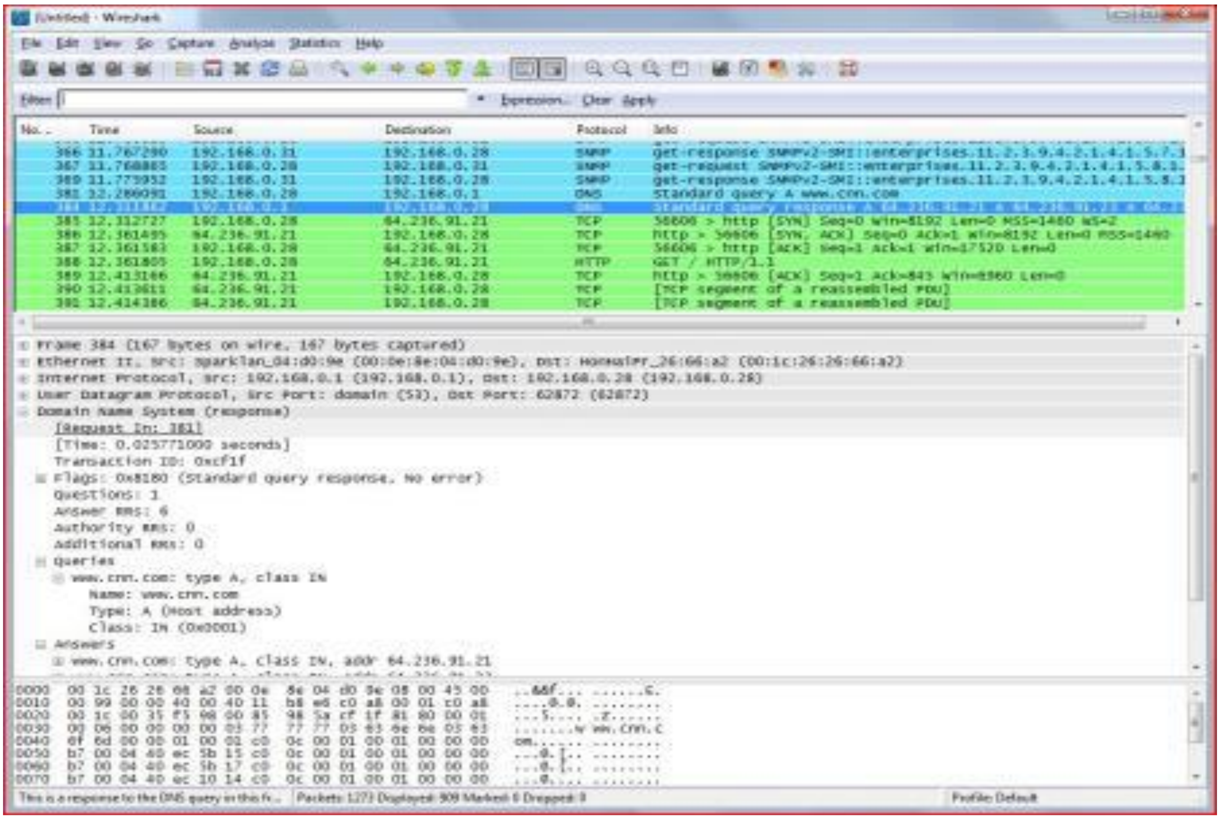
Use Cases:

- Networking Education: Cisco Packet Tracer is a valuable tool in networking courses and certifications like Cisco's CCNA and CCNP. It helps students understand networking concepts practically.
- Network Design and Testing: Network administrators and engineers use Packet Tracer to design, test, and troubleshoot network configurations before implementing them in real environments.
- Cisco Device Familiarization: Packet Tracer is ideal for getting familiar with Cisco networking equipment and software interfaces.
- Prototyping and Experimentation: It's a great platform for experimenting with new network designs or services without the need for physical hardware.

CISCO PACKET TRACER



WIRESHARK



EXPERIMENT 2

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

Theory::

TELNET, short for "TErminaL NETwork," is a widely used network protocol that allows users to establish remote connections to network devices, such as routers, switches, and servers, over a network. It provides a text-based command-line interface for managing and configuring these devices, making it an essential tool for network administrators, engineers, and IT professionals. In this theoretical overview, we'll delve into the operation of TELNET and how it enables remote access to network devices.

The TELNET Protocol:

The TELNET protocol is based on a client-server model, where the client is typically a user's computer, and the server is the network device to which the user wants to connect. TELNET operates over the Transmission Control Protocol (TCP) on port 23, and it relies on a clear text communication model.

Key Components and Concepts:

Client and Server: The client initiates the TELNET session, and the server listens for incoming TELNET connections. In the context of the experiment, the PC in the IT office acts as the client, and the router in the server room serves as the TELNET server.

Port Number: TELNET operates over TCP port 23 by default. This port is used to establish the connection between the client and the server. If a different port is used, it must be explicitly specified.

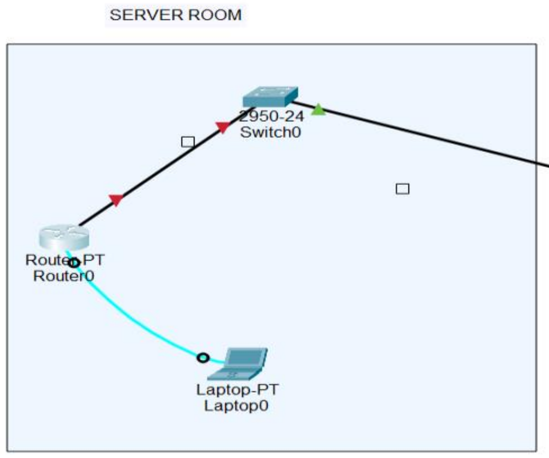
Text-Based Interface: TELNET provides a text-based interface, allowing users to interact with the remote device by sending and receiving text commands. This interface is similar to a command-line interface, which is common in networking devices.

Authentication: To access the remote device, users typically need to provide valid login credentials, such as a username and password. This authentication ensures secure access and prevents unauthorized users from connecting to the device.

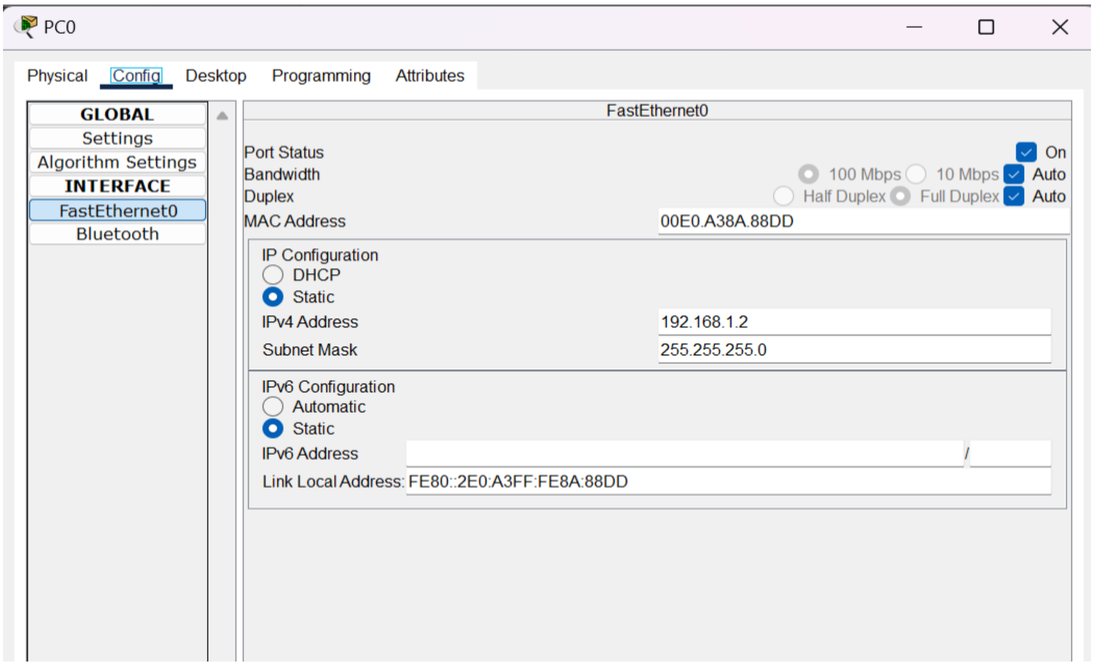
PROCEDURE:

1. Connecting router to end device

NETWORK TOPOLOGY DIAGRAM FOR TELNET



2. Setting the IP and Subnet mask to End Device



3.Setting up the configuration of the Router

```
Enter interface name used to connect to the
management network from the above interface summary: GigabitEthernet0/0/0

Configuring interface GigabitEthernet0/0/0:
  Configure IP on this interface? [yes]:
    IP address for this interface: 192.168.1.1
    Subnet mask for this interface [255.255.255.0] :
```

```
Router>enable
Password:
Password:
Password:
Router#login
Translating "login"...domain server (255.255.255.255)% Bad secrets
```

4. Accessing the router using endpoint

```
PS C:\Users\hp> ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=20ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 20ms, Average = 7ms
```

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Router>enable
Password:
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#exit
R1#exit

[Connection to 192.168.1.1 closed by foreign host]
```

5.The Connection is successfully Established

RESULT:

Thus, verified the operation of TELNET and accessed the router from Pcs

EXPERIMENT 3

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

REQUIREMENTS: Cisco Packet Tracer software , Computer with a minimum of 2GB of RAM and 2GB of free disk space

Theory:

IP Address Basics:

- An IP address is a unique numerical label assigned to each device on a network.
- It is used for identification and communication within a network.
- IP addresses are divided into two main types: IPv4 and IPv6.

IPv4 Addressing:

- IPv4 is the most widely used IP version.
- It uses a 32-bit address represented in four decimal octets (e.g., 192.168.1.1).
- IPv4 addresses are divided into classes (A, B, C, D, E) and further categorized into public and private IP addresses.

IP Addressing Scheme:

Choosing an IP Address Range:

- In our scenario, we select a private IPv4 address range to build our small network: 192.168.0.0/24.
- Private IP address ranges are reserved for internal network use and are not routable on the public internet.

Allocating IP Addresses:

- We allocate specific IP addresses to network devices like routers, switches, and PCs

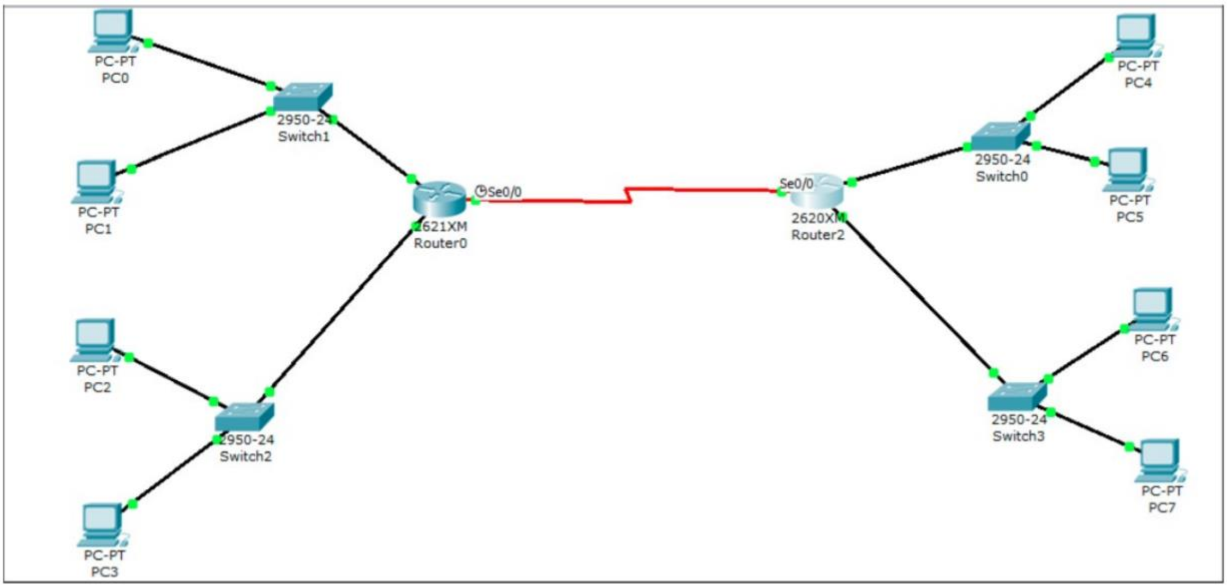
What is Subnetting?

- Subnetting is the process of dividing a larger IP network into smaller, more manageable sub-networks or subnets.
- It helps optimize IP address allocation, enhances network security, and reduces broadcast traffic.

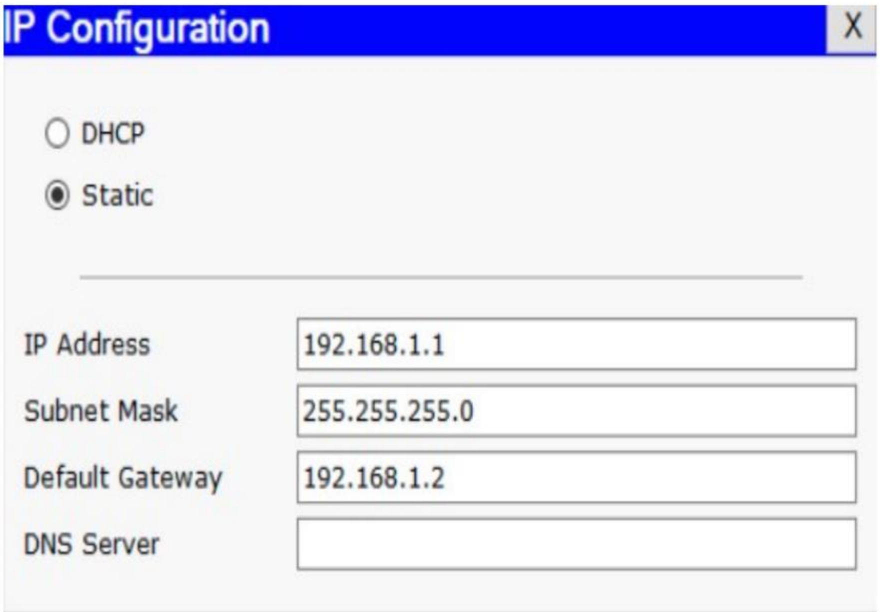
Subnet Examples:Subnet 1 (Marketing): 192.168.0.0/27 , Subnet 2 (Sales): 192.168.0.32/27

PROCEDURE

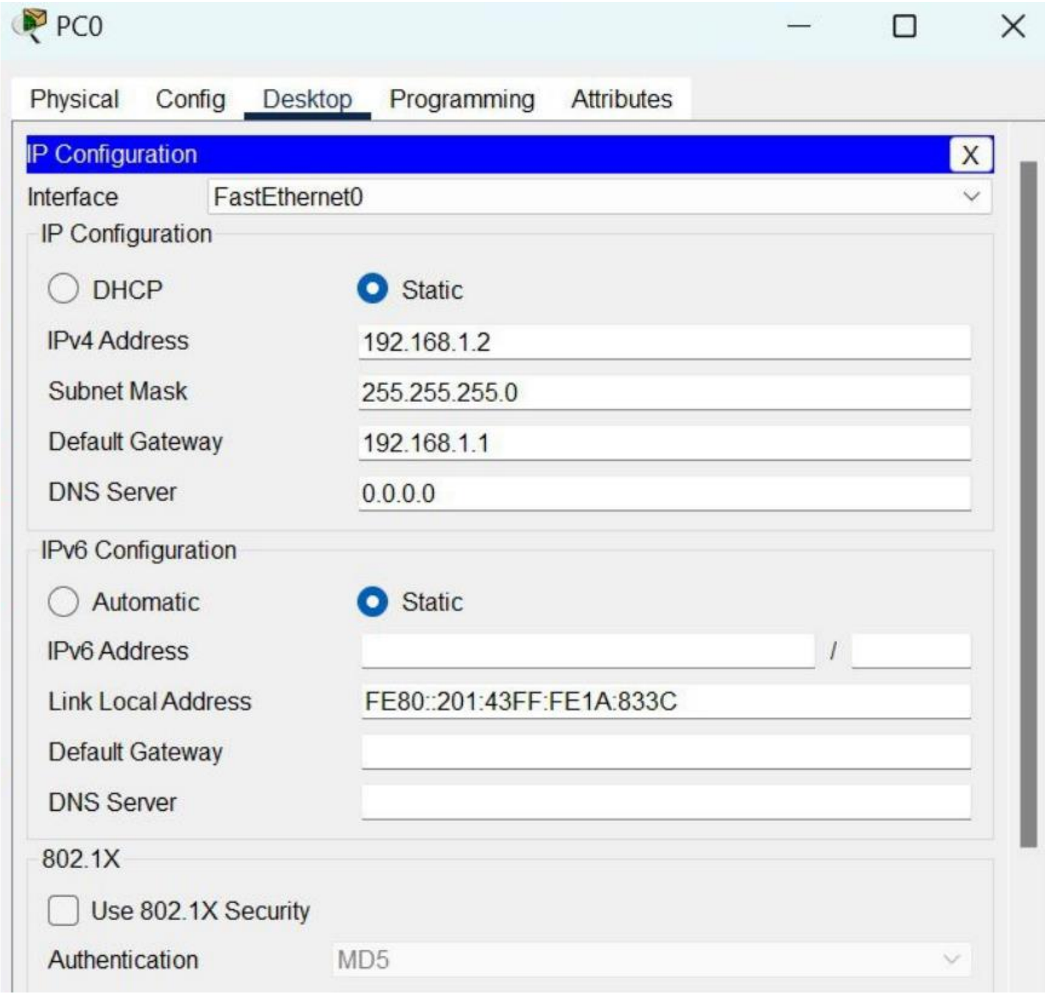
1. **Make the following connection on Cisco Packet Tracer**

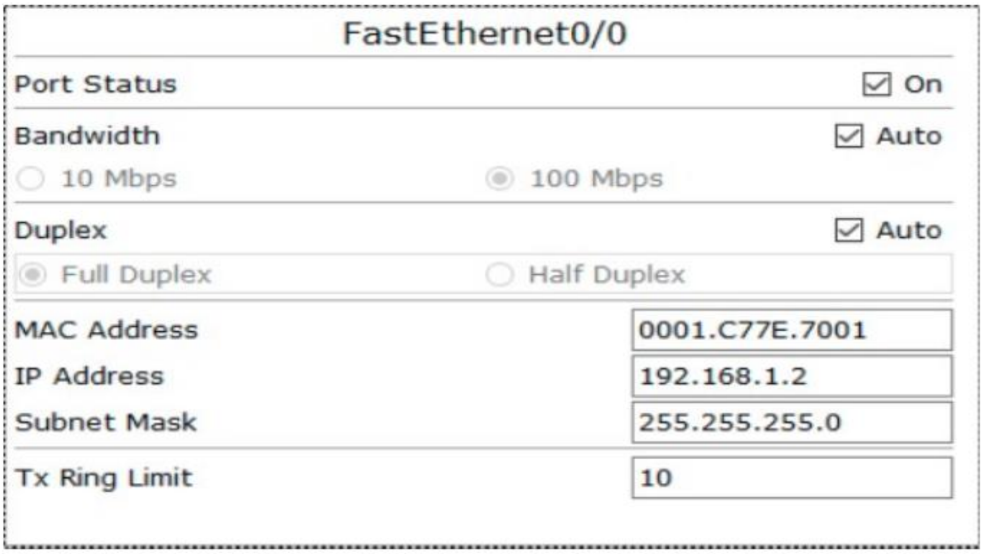


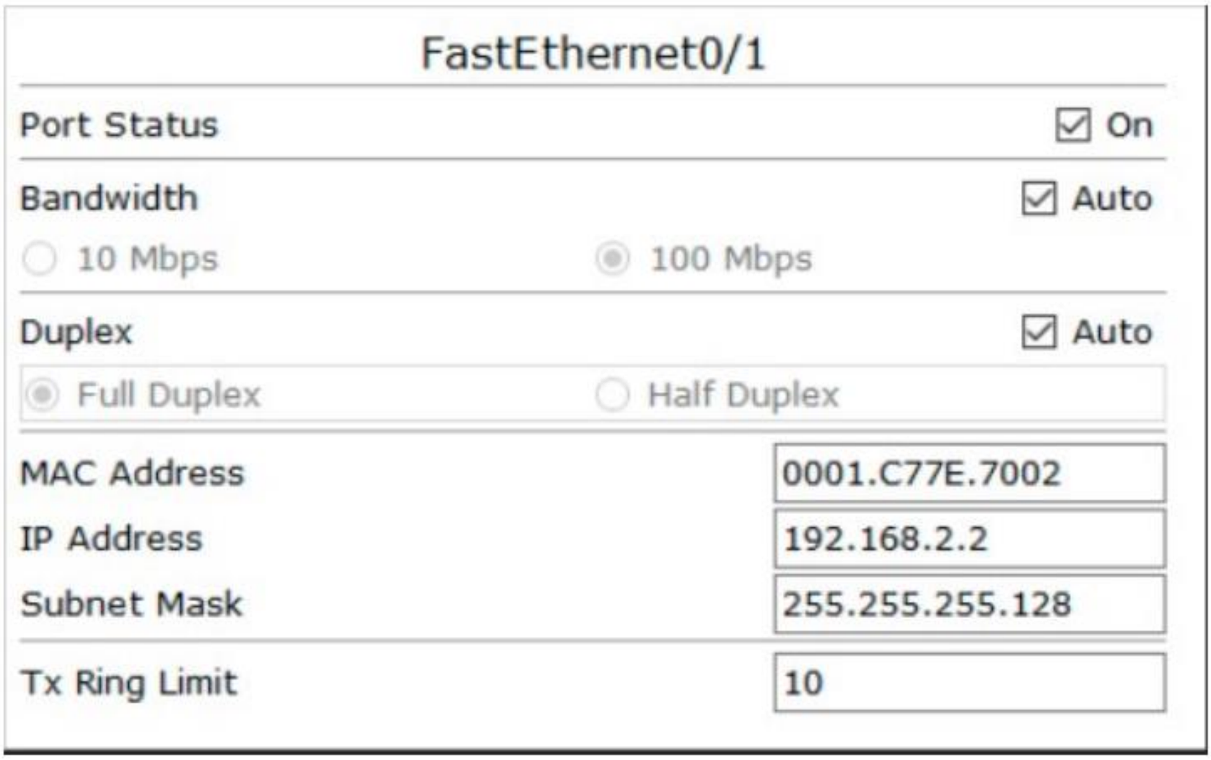
2. **Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shown below)**

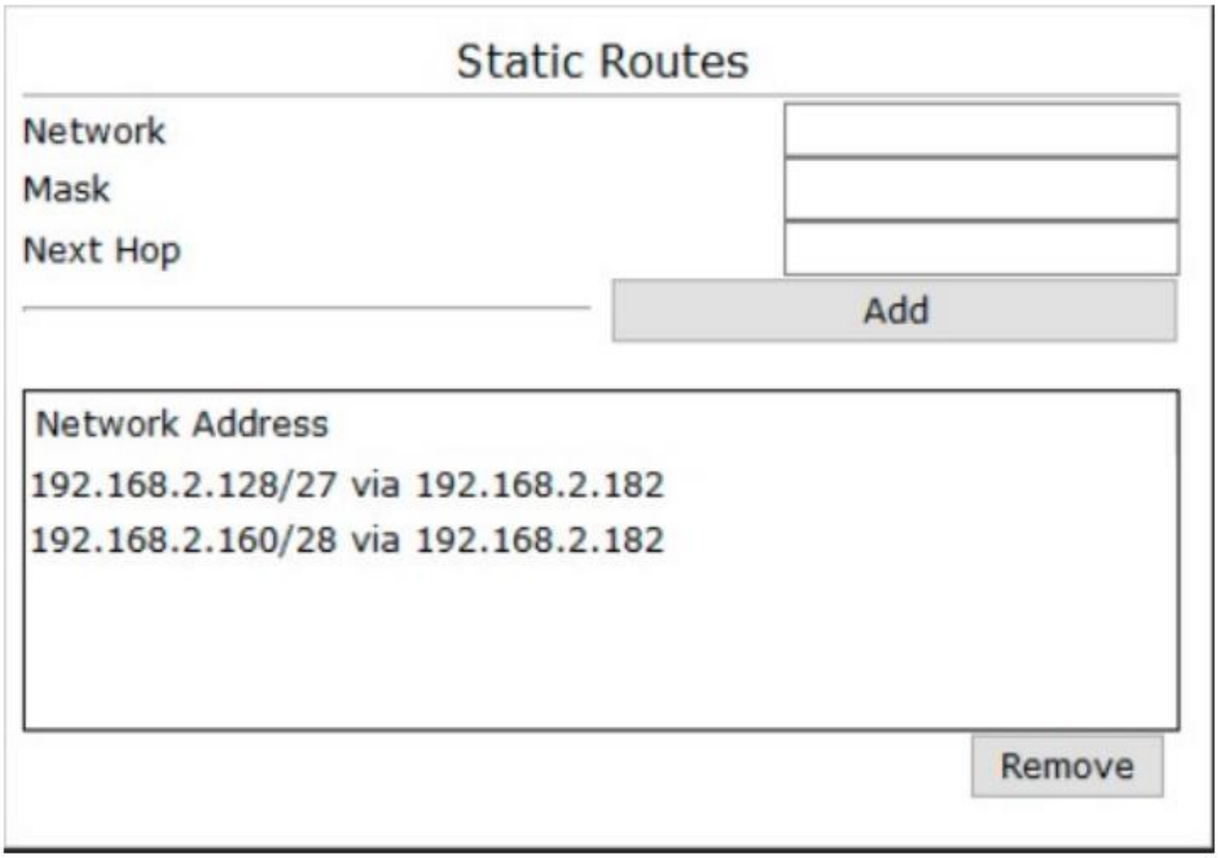


3. **Configure router with IP address and subnet mask.**


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:43FF:FE1A:833C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5


FastEthernet0/0
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0001.C77E.7001
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10





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

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=156ms TTL=126
Reply from 192.168.1.1: bytes=32 time=156ms TTL=126
Reply from 192.168.1.1: bytes=32 time=125ms TTL=126
Reply from 192.168.1.1: bytes=32 time=157ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 125ms, Maximum = 157ms, Average = 148ms
```

RESULT:

In conclusion, mastering IP addressing and subnetting is pivotal for effective network management. Using Cisco Packet Tracer, we've demonstrated the practical implementation of these concepts in a small network environment. This knowledge is essential for network professionals to design and manage networks efficiently and securely.

EXPERIMENT 4

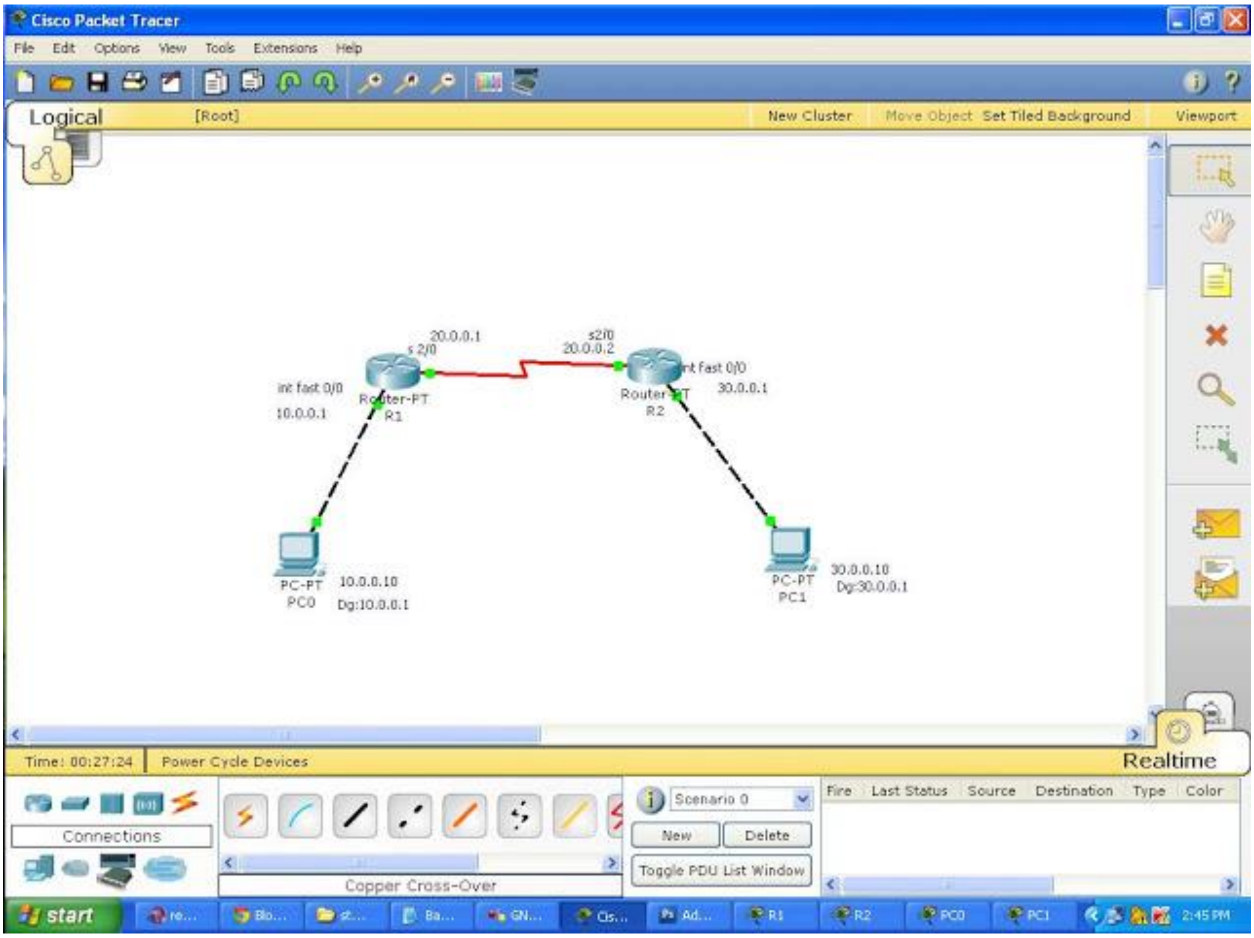
AIM: To implement the static routing using Cisco Packet Tracer.

Theory:

Static routing is a foundational networking concept that involves manually configuring routes on routers to determine the path data packets take in a network. Unlike dynamic routing, static routing doesn't rely on automatic updates but requires administrators to manually define specific routes. In scenarios where network topology is stable and changes infrequently, static routing offers simplicity and predictability. It involves specifying destination networks and their corresponding next-hop addresses. Although less flexible than dynamic alternatives, static routing is efficient for smaller networks and is easier to configure and maintain. Understanding static routing is essential for network administrators seeking control and predictability in their network configurations.

PROCEDURE:

Step 1:First Create a topology like this



you will get a red light first this is configured topology

Step 2: Configure ip address to routers go to global configuration mode in R1 and R2 configure connected interfaces

In Router 1
Interface Fastethernet0/0 in global configuration mode
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit

Interface Serial 2/0

R1(config)#interface serial 2/0

R1(config-if)#ip address 20.0.0.1 255.0.0.0

R1(config-if)#clock rate 64000

R1(config-if)#encapsulation ppp

R1(config-if)#no shutdown

R1(config-if)#exit

In Router 2

Interface Fastethernet 0/0

R2(config)#interface fastethernet 0/0

R2(config-if)#ip address 30.0.0.1 255.0.0.0

R2(config-if)#no shutdown

R2(config-if)#exit

Interface Serial 2/0

R2(config)#interface serial 2/0

R2(config-if)#ip address 20.0.0.2 255.0.0.0

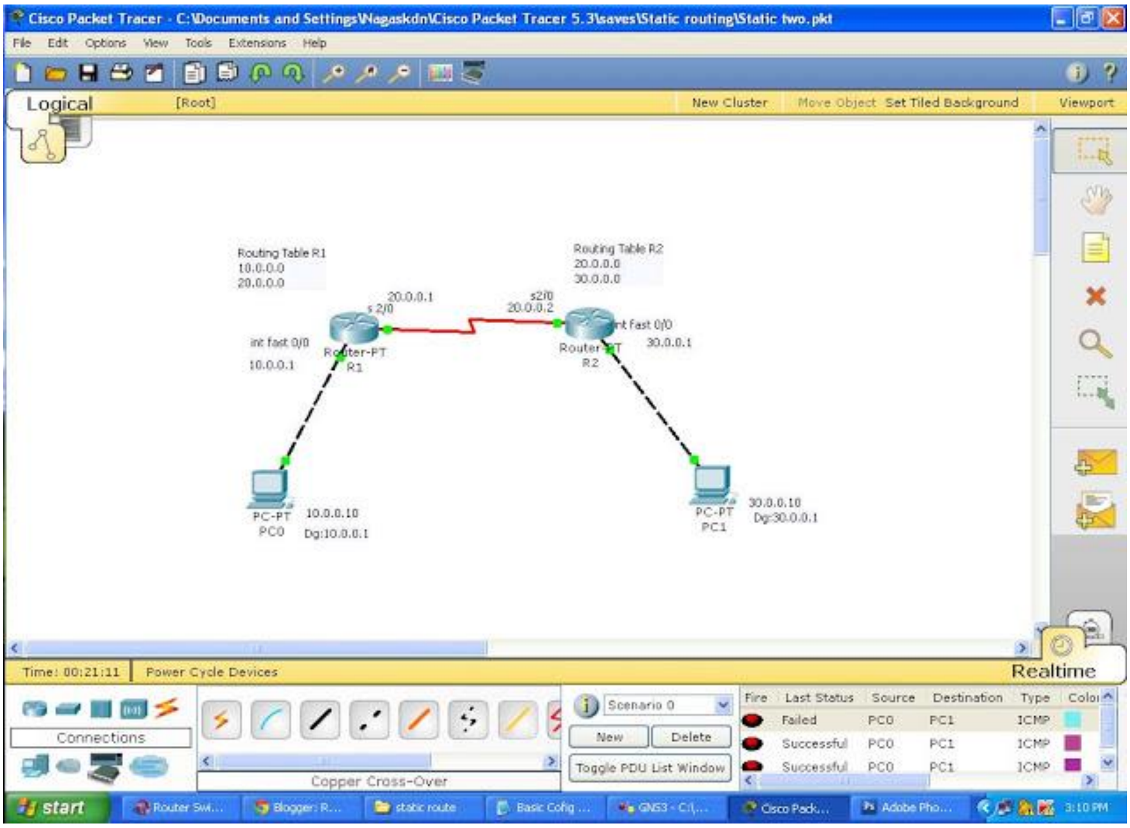
R2(config-if)#encapsulation ppp

R2(config-if)#no shutdown

R2(config-if)#exit

Step 3 : Assign ip address for both Pc's with appropriate ip and subnetmask and default gateway

Step 4: Now configure both router with static route



By default Routers Know only directed connected networks here Router 1 know only 10.0.0.0 and 20.0.0.0 it doesn't know the 30.0.0.0 like this R2 doesn't know about 10.0.0.0.So We are going to add Static route to this both router

R1(config)#ip route Destination Network| Destination N/W Subnet Mask |Next Hop Address

In Router R1,Just give this command, In this case Destination is 30.0.0.0 and its subnet mask is 255.0.0.0 next hop address is 20.0.0.2

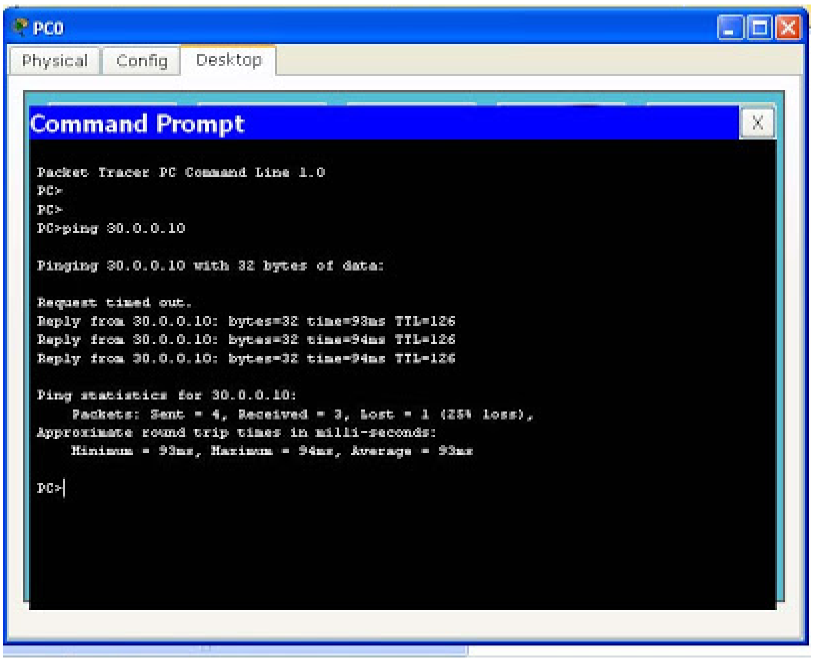
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2

In Router R2

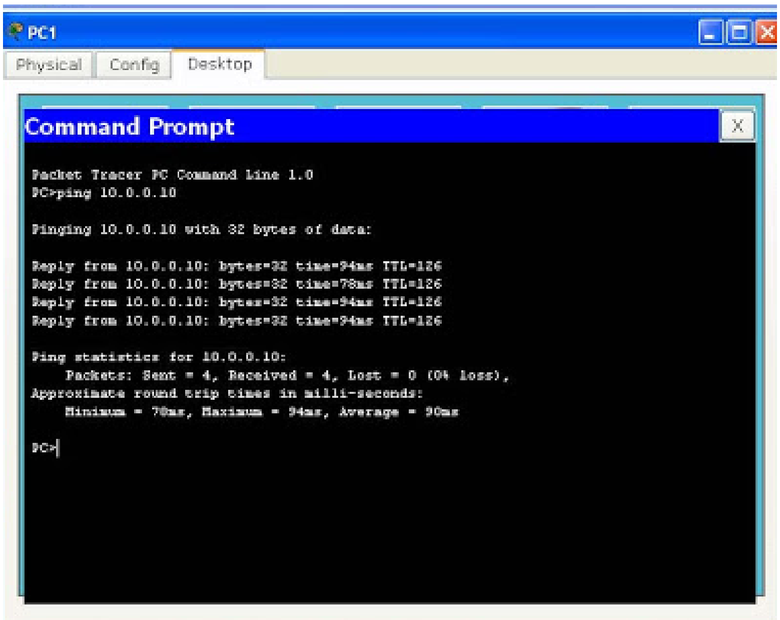
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1

Now both routers know all networks, check by ping ip address of host

Step 5: Double click PC move to desktop then command prompt give the command ping 30.0.0.10 in PC 0 you will get reply from 30.0.0.10 like this



From PC1



RESULT:

The implementation of static routing using Cisco Packet Tracer was successful. Manually configured static routes on the routers effectively directed data packets within the network.

EXPERIMENT 5

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

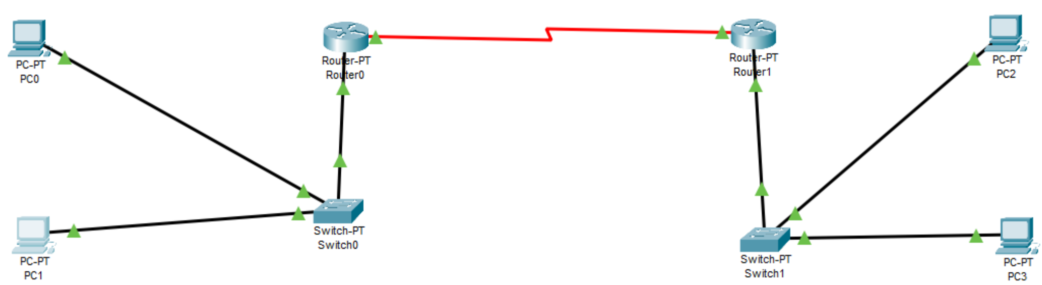
Theory:
DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol used in TCP/IP networks to automatically assign IP addresses and configuration information to devices on a network. DHCP is commonly used in homes and businesses to simplify the process of connecting devices to a network.

DHCP works by:

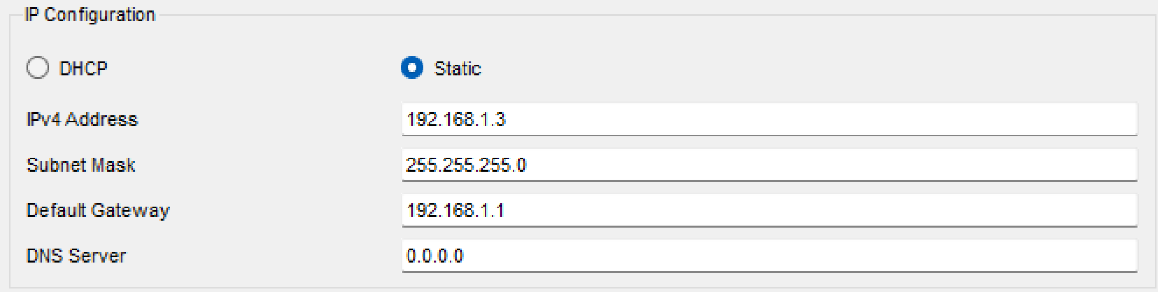
1. Request for IP Address: When a device connects to a network, it sends a DHCP request.
2. DHCP Server: A DHCP server manages a pool of IP addresses and responds to the request.
3. IP Assignment: The server assigns an available IP address to the device, ensuring uniqueness.
4. Configuration Information: DHCP provides additional network settings like subnet mask and DNS addresses.
5. Lease Time: Assignments are temporary; devices renew leases, aiding network management.

PROCEDURE:

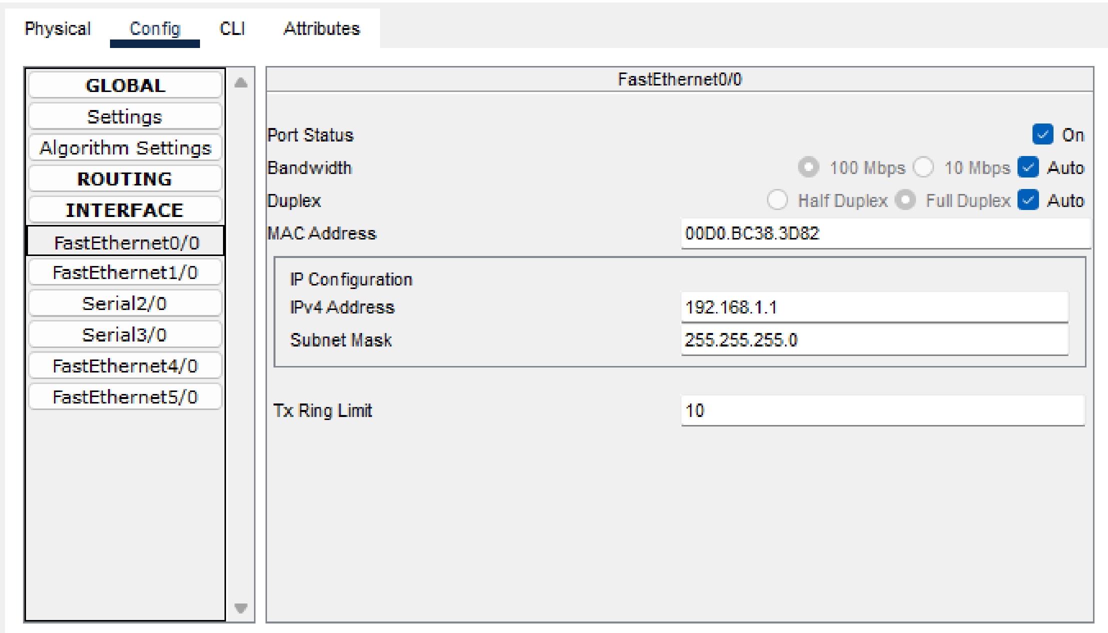
1. Make the following connection on Cisco Packet Tracer

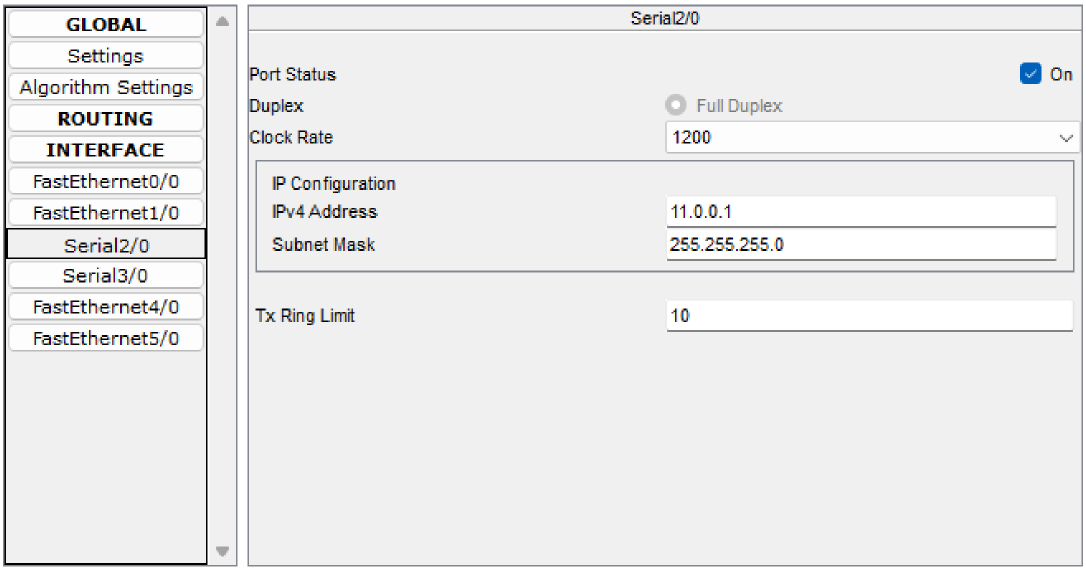


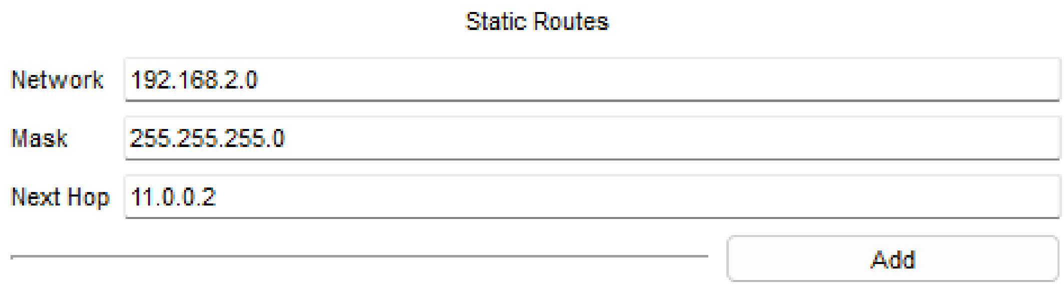
2. Configure the PCs (hosts) with IPv4 address and Subnet Mask (as shown below)



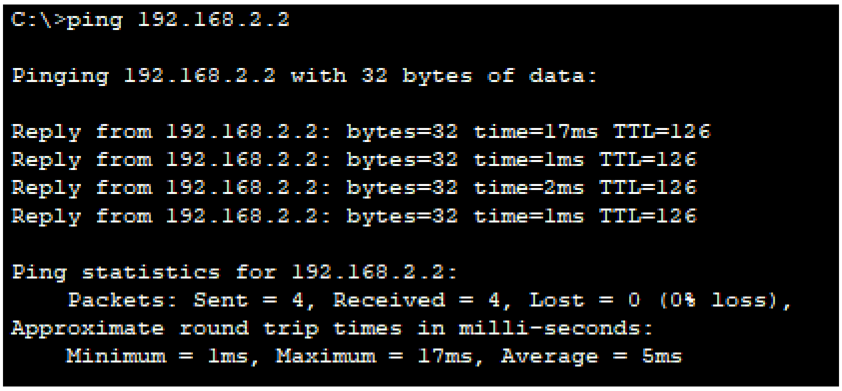
3. Configure router with IP address and subnet mask.







3. Verifying the network by pinging the IP address of any PC.



```
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=17ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms 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 = 1ms, Maximum = 17ms, Average = 5ms
```

RESULT:

The implementation of DHCP onto the network topology using Cisco Packet Tracer was successful.

EXPERIMENT 6

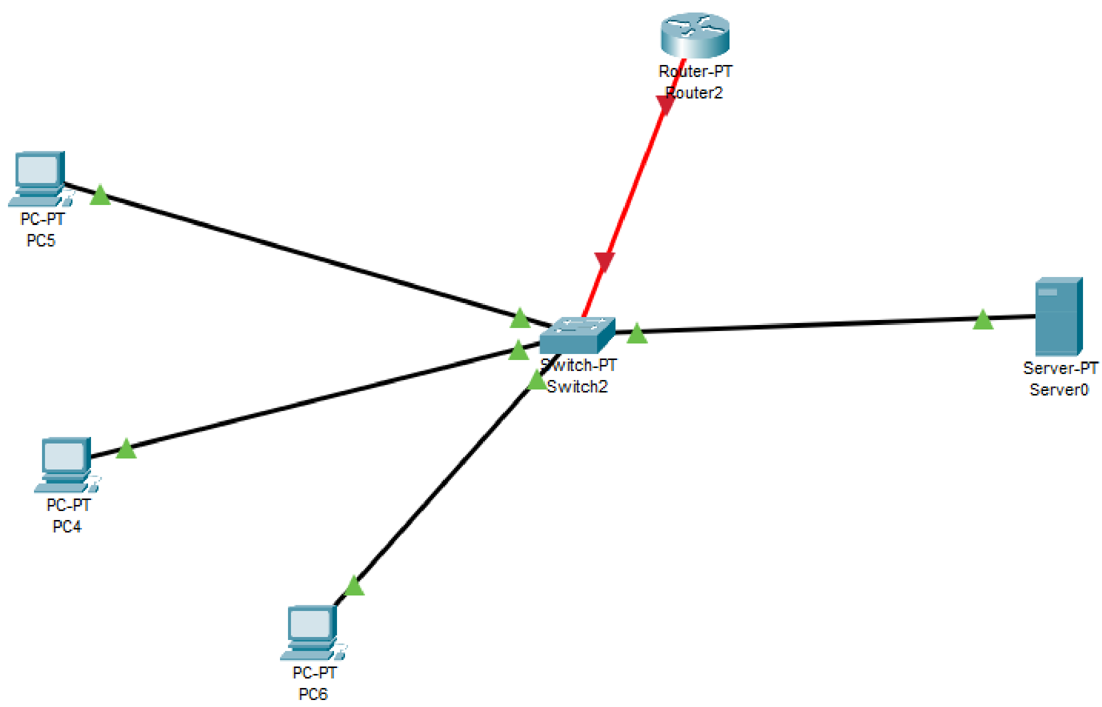
AIM: To implement the DNS, Email Services in the Network using Cisco Packet Tracer.

THEORY:
DNS SERVICE:
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.

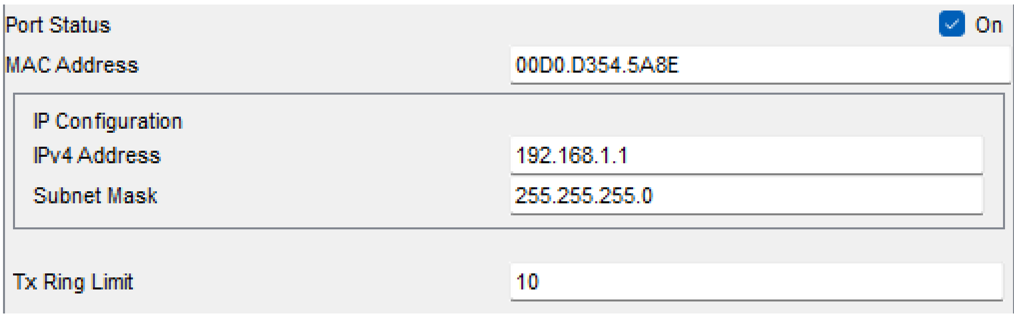
DNS (Domain Name System) is essential as it translates human-readable domain names into numeric IP addresses, making internet navigation user-friendly. Since people find it challenging to remember IP addresses, DNS serves as a mapping system, converting domain names to IP addresses. There are different types of domains, including generic domains like .com, .edu, .mil, .org, and .net; country domains like .in, .us, .uk; and inverse domains, allowing users to find IP addresses for specific domain names. DNS plays a crucial role in simplifying internet access and providing both domain-to-IP and IP-to-domain mappings for efficient online communication.

PROCEDURE:

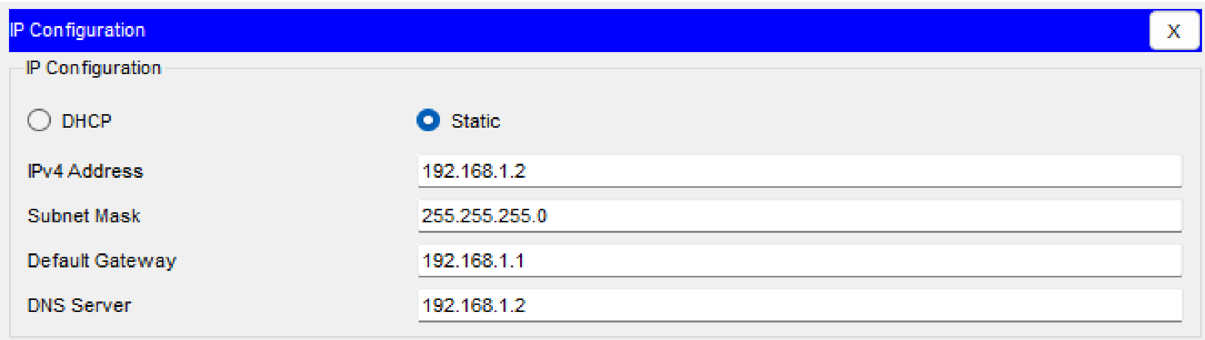
1. Connect server switch and Endpoints

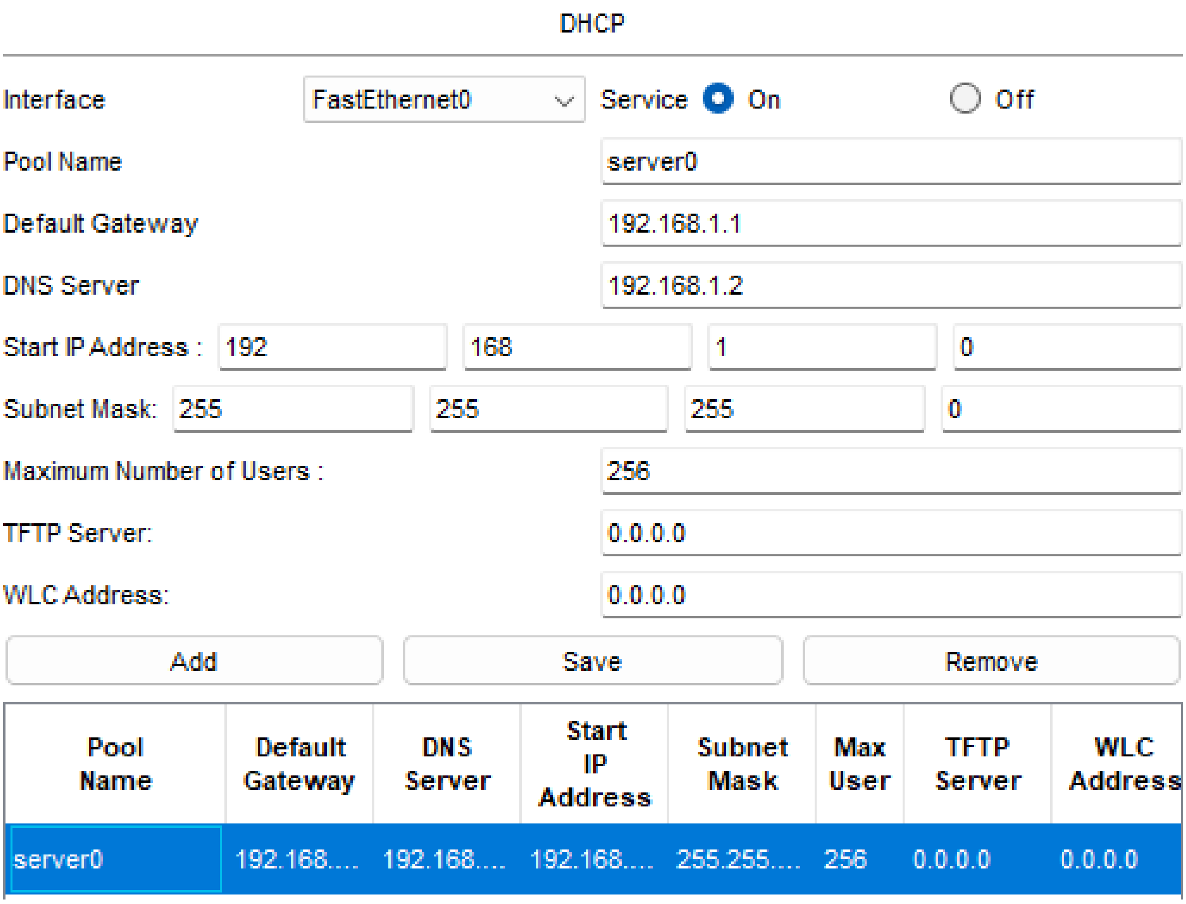


2. Setting the IP and Subnet mask to Router Device

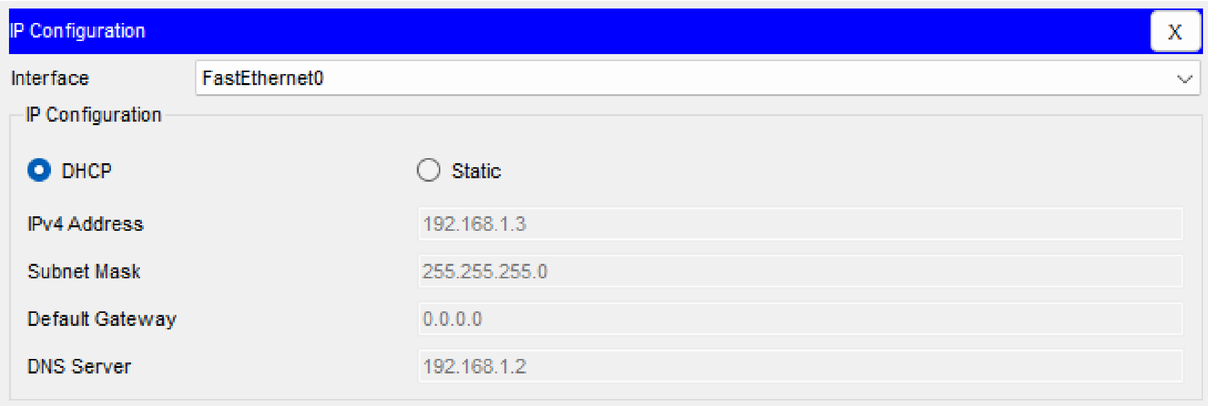


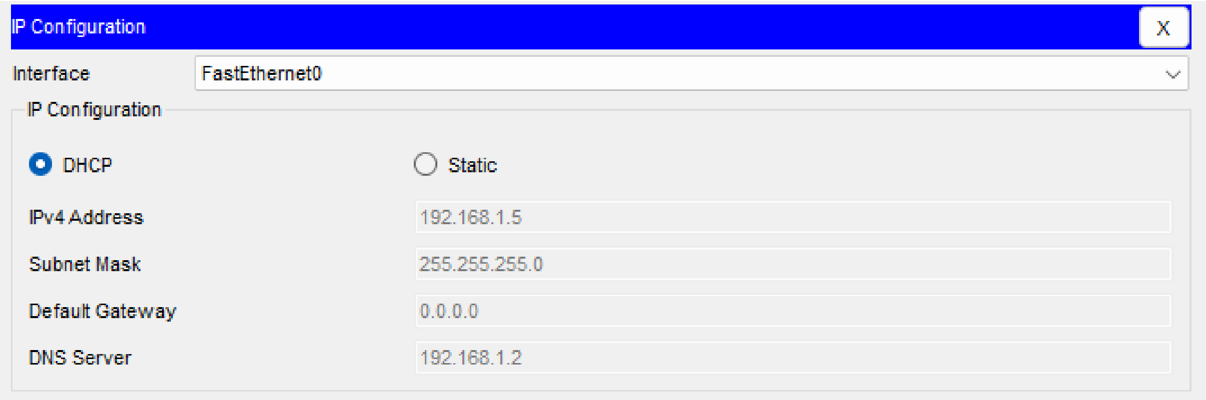
3. Setting up the configuration of server

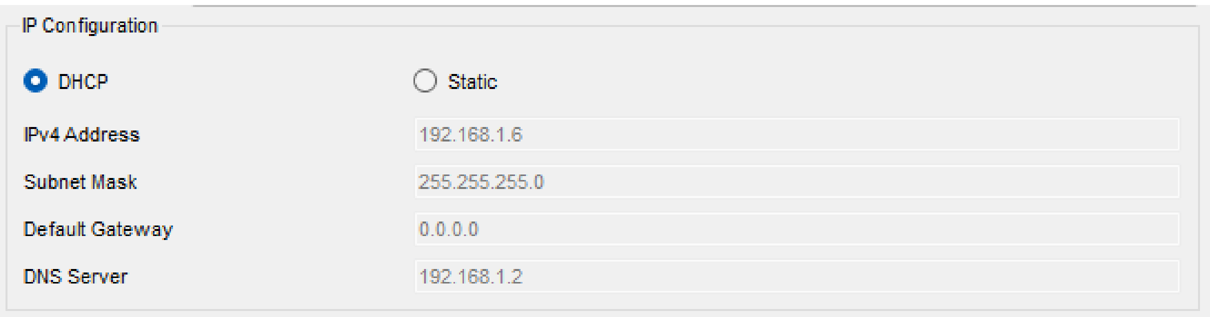




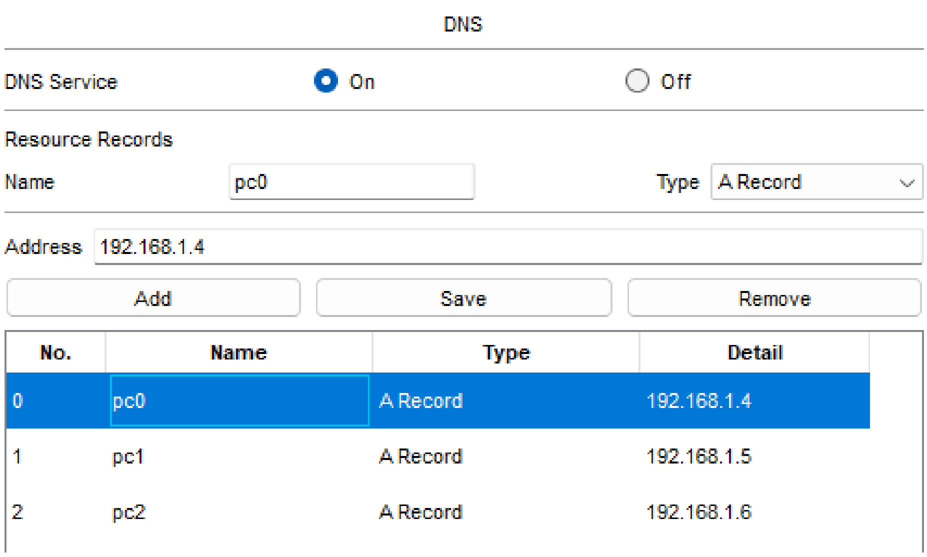
4. Giving IP Address to end devices







5. Adding DNS Service on Server



6. Verifying the connection by two end devices

```
C:\>ping pc2

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

EMAIL SERVICE:

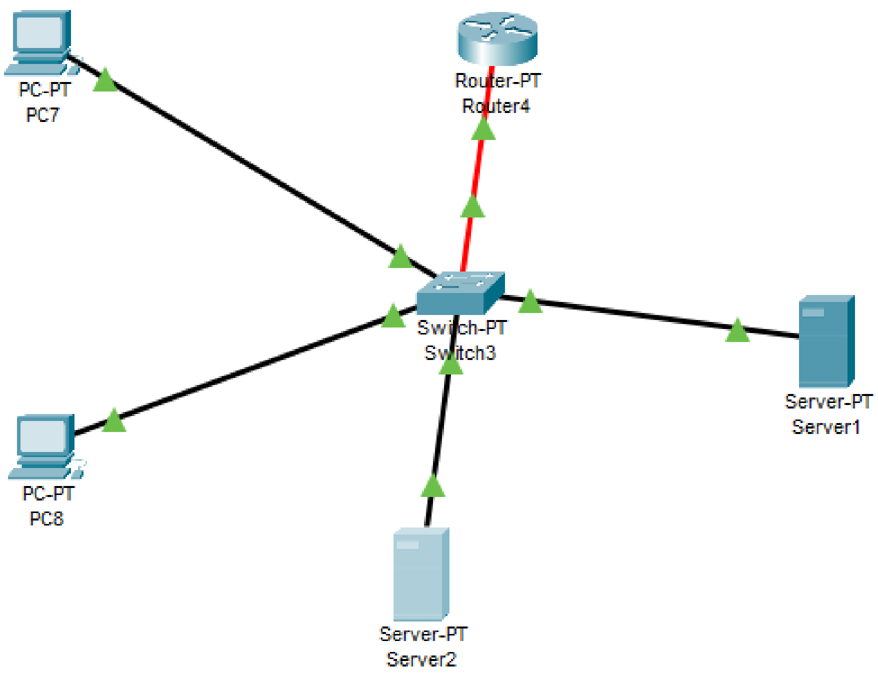
Email protocols are a collection of protocols that are used to send and receive emails properly. The email protocols provide the ability for the client to transmit the mail to or from the intended mail server. Email protocols are a set of commands for sharing mails between two computers. Email protocols 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.

In computer networks, different email services serve distinct purposes:

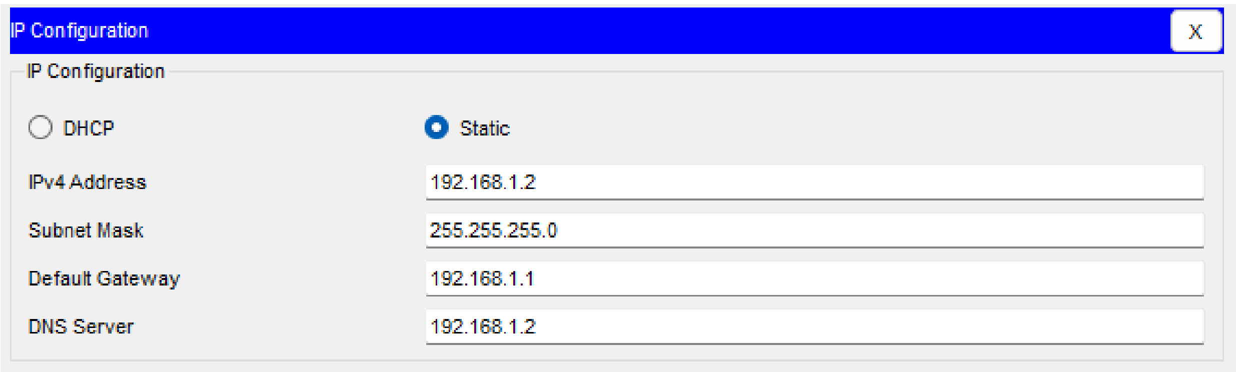
1. SMTP (Simple Mail Transfer Protocol): Sends outgoing emails from a client to a server or between servers.
2. POP (Post Office Protocol): Retrieves emails from a server and downloads them to a client device
3. IMAP (Internet Message Access Protocol): Retrieves emails while allowing users to view and manage them on the server, suitable for multiple devices.
4. Webmail Services: Access emails through a web browser, exemplified by services like Gmail and Outlook.com.
5. Exchange Servers: Comprehensive email solutions, like Microsoft Exchange, with features such as email, contacts, and calendaring, commonly used in business settings.

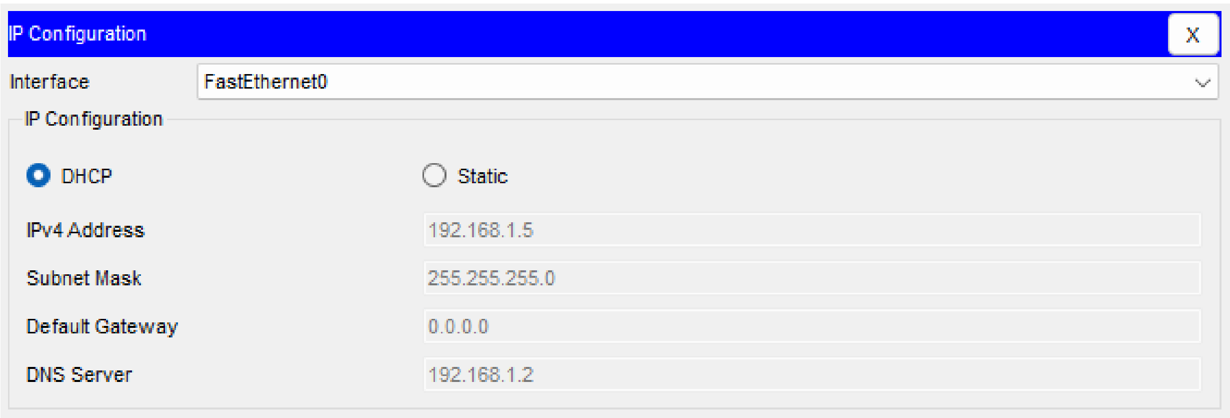
PROCEDURE:

1. Build the network topology

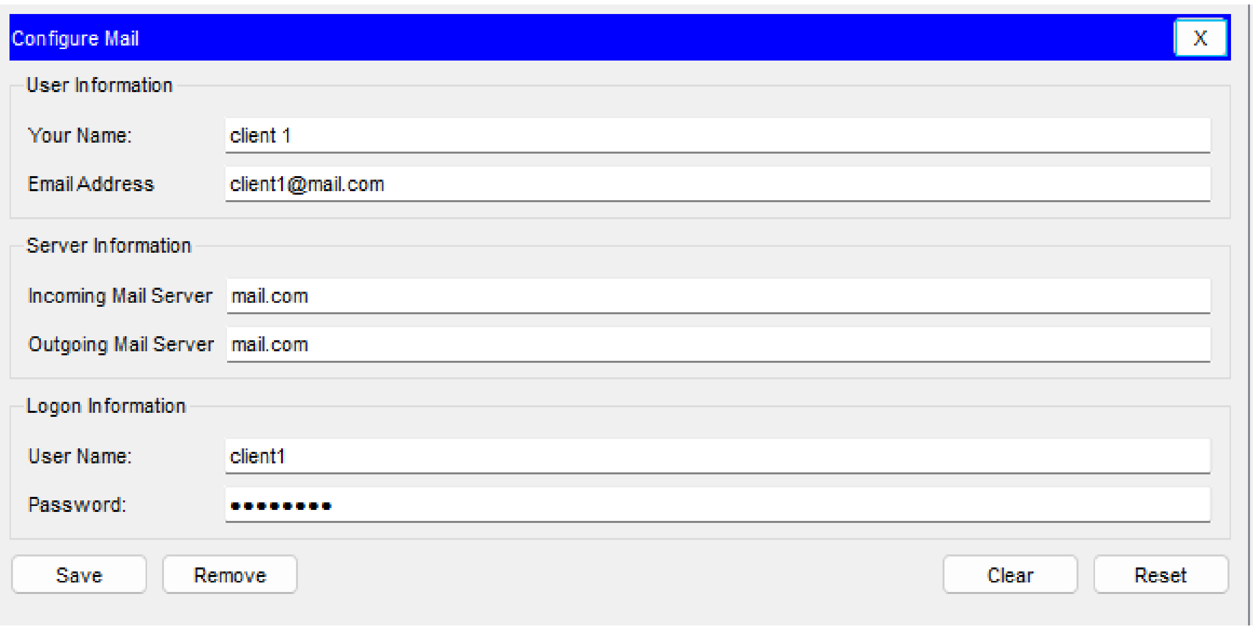


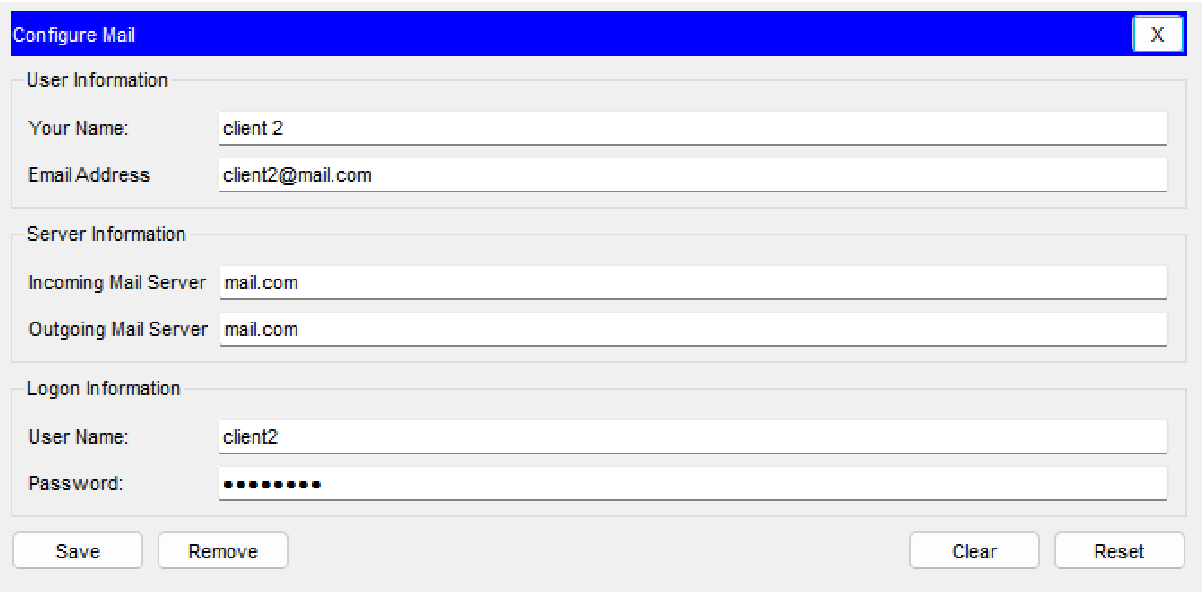
2. Configure IP addresses on the PCs, DNS Server and the Mail Server.



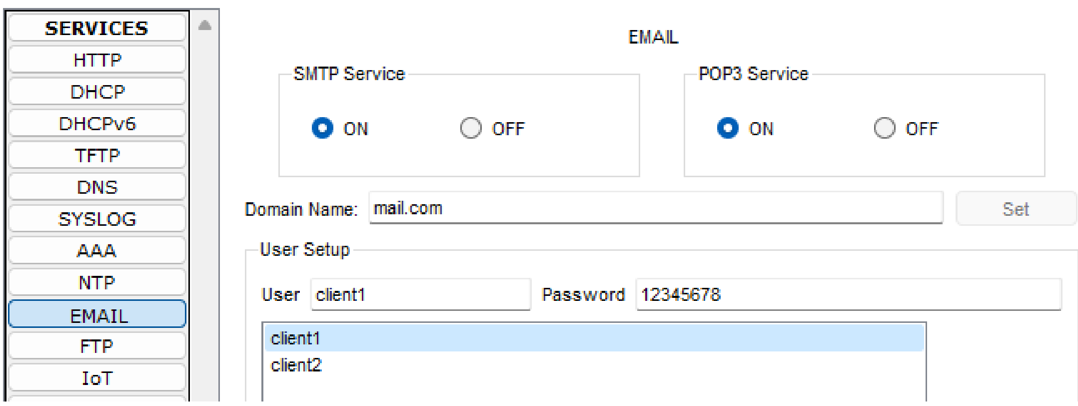


3. Now configure mail clients on the PCs and mail service on the generic server.

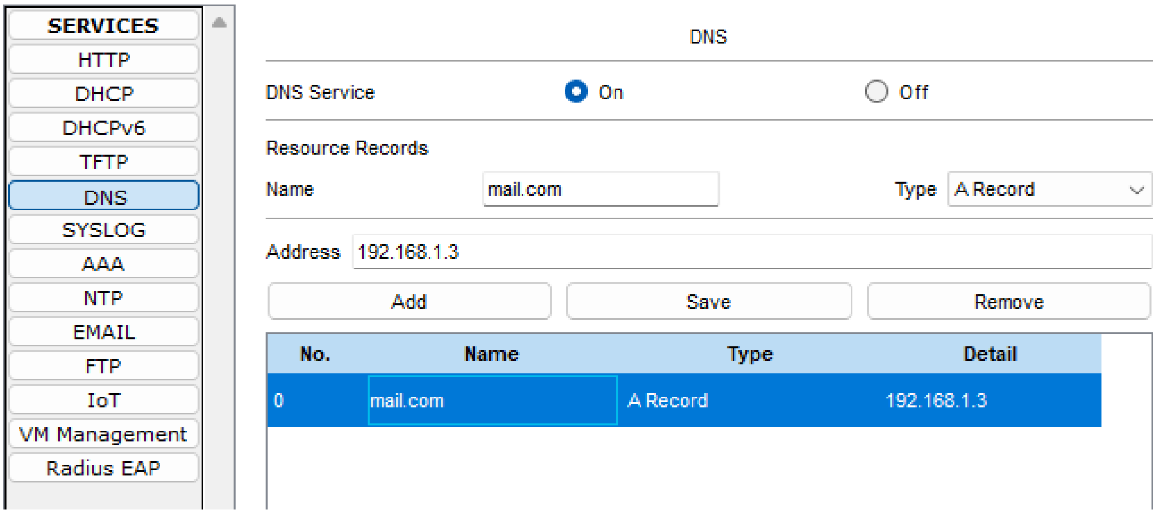




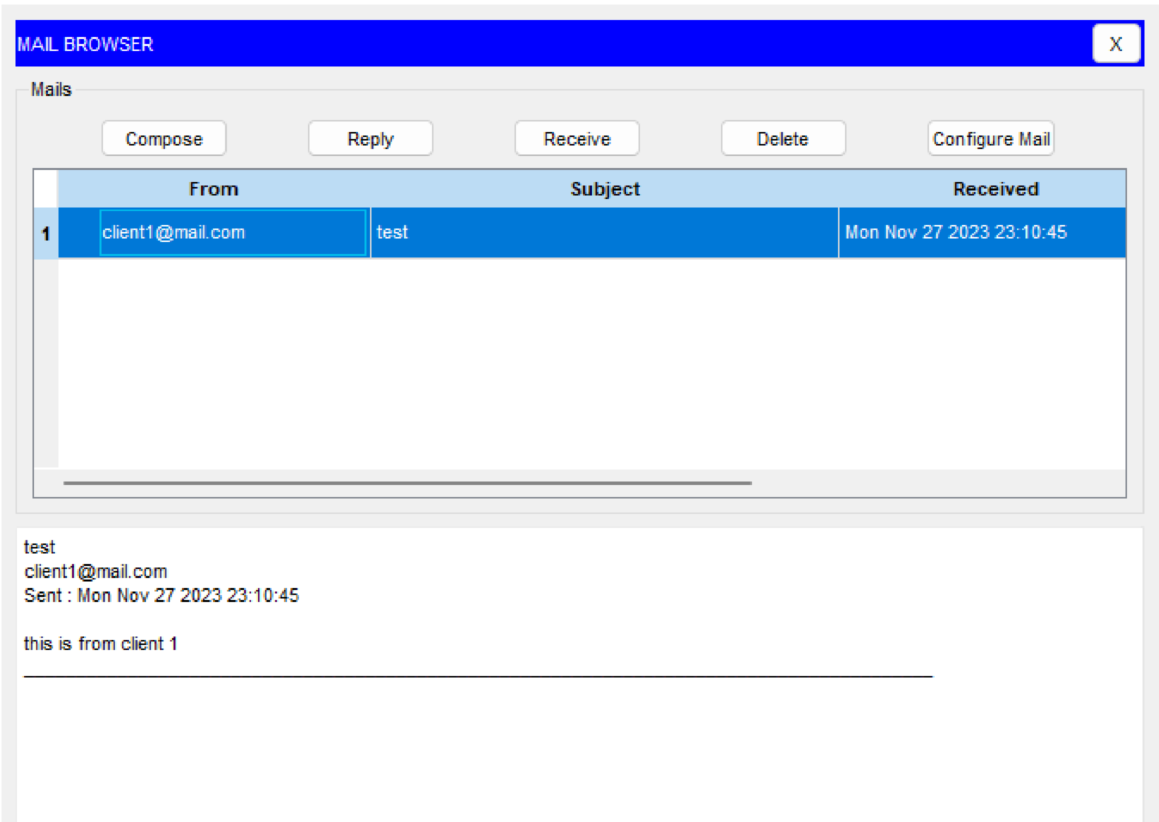
4. Configure the email server



5. Configure DNS server



6. Test the email service



EXPERIMENT 7

AIM: To implement the Dynamic Routing Protocols: RIP, IGRP using Cisco Packet Tracer.

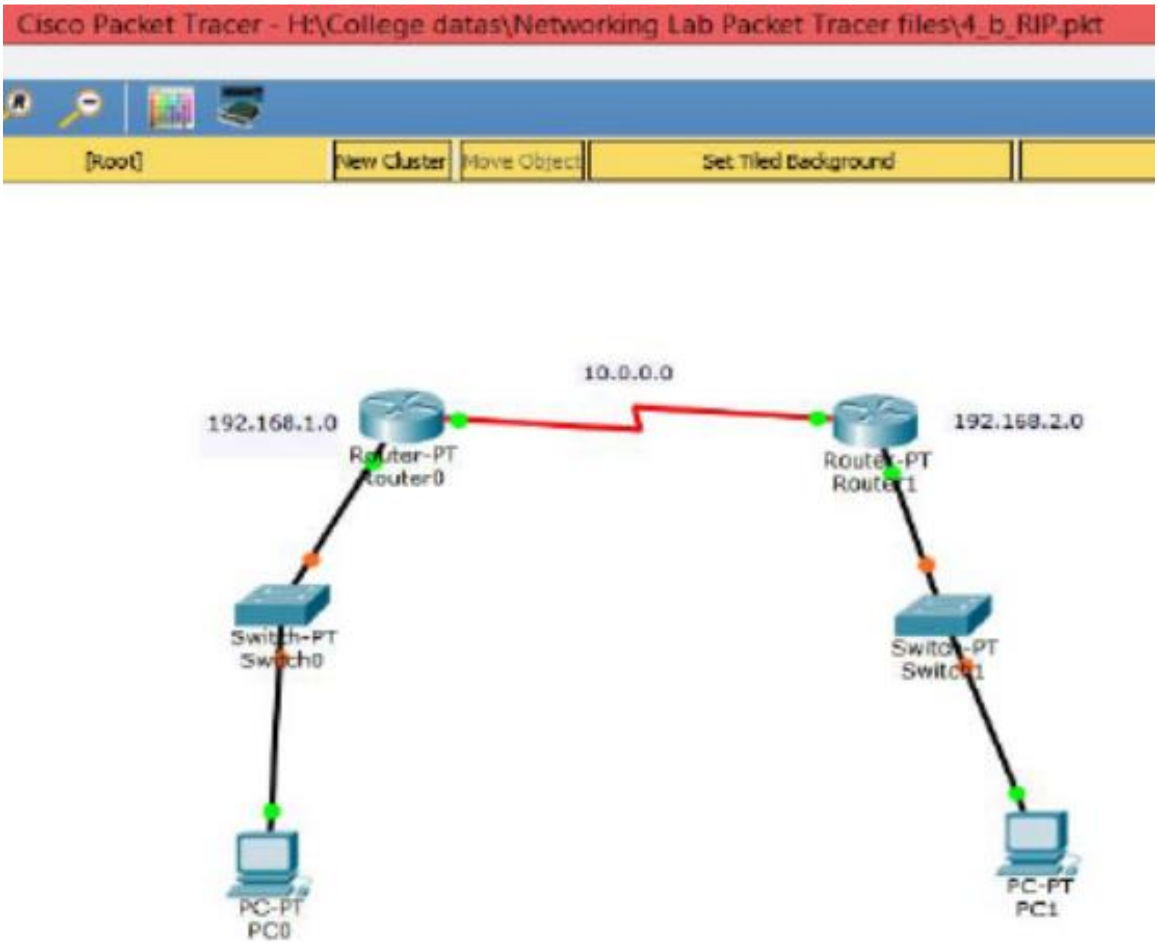
Theory:

RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exist: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn't advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1.

RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth. RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

Procedure

- Open the CISCO Packet tracer software
- Drag and drop 5 pcs 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 and apply clock rate as per the table.
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.



INPUT DETAILS FOR RIP:

PC0 - IP Address : 192.168.1.2 Gate way : 192.168.1.1

PC1- IP Address : 192.168.2.2 Gate way : 192.168.2.1

Router 0- Fast Ethernet 0/0 IP Address: 192.168.1.1

Serial 2/0 : 10.0.0.1

Router 1- Fast Ethernet 0/0 IP Address : 192.168.2.1

Serial 2/0 : 10.0.0.2

OUTPUT:

RIP (PINGING FROM PC0 TO PC1):

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=11ms TTL=126 Reply from

192.168.2.2: bytes=32 time=12ms TTL=126

Reply from 192.168.2.2: bytes=32 time=13ms TTL=126

Reply from 192.168.2.2: bytes=32 time=11ms 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 = 11ms, Maximum = 13ms, Average = 11ms

Result:

Thus, understand the concept and operation of RIP and pinged from PC in are networks to PC to another network.

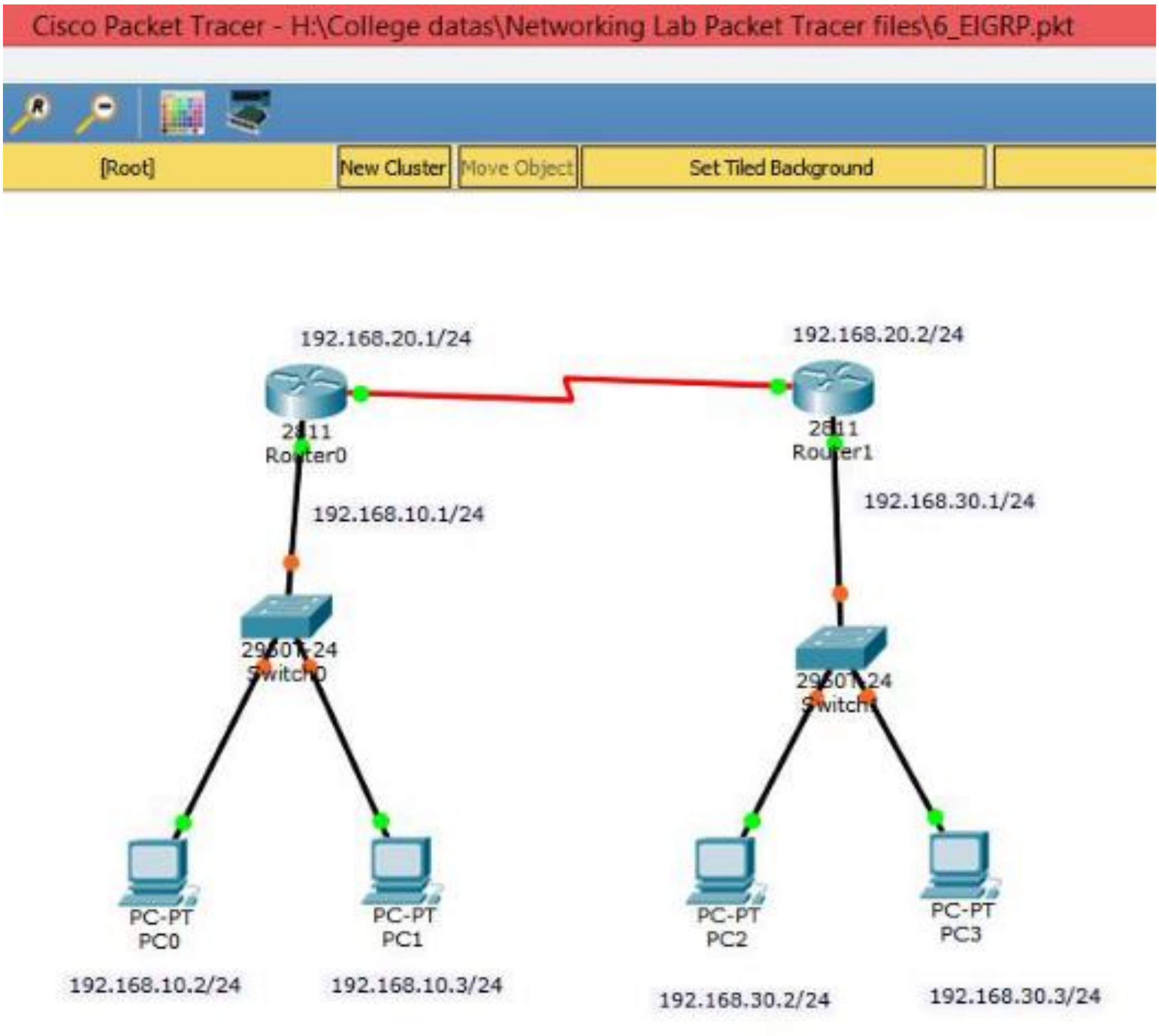
EXPERIMENT 8

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

THEORY:

Enhanced Interior Gateway Routing Protocol (EIGRP Protocol) is an enhanced distance vector routing protocol which Uses Diffused Update Algorithm (DUAL) to calculate the shortest path. It is also considered as a Hybrid Routing Protocol because it has characteristics of both Distance Vector and Link State Routing Protocols. EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balancing and other features.

Network Topology Diagram for EIGRP



INPUT DETAILS FOR EIGRP:

PC0	PC1	PC2	PC3
IP Address: 192.168.10.2 Gate way: 192.168.10.1	IP Address: 192.168.10.3 Gate way: 192.168.10.1	IP Address: 192.168.30.2 Gate way: 192.168.30.1	IP Address: 192.168.30.3 Gate way: 192.168.30.1

Router 0	Router 1
fa 0/0 IP Address: 192.168.10.1 Serial 0/0/0 : 192.168.20.1 @ 6400 clock rate	fa 0/0 IP Address : 192.168.30.1 Serial 0/0/0 : 192.168.20.2

ROUTER0 CLI:

Router(config)#router eigrp 10

Router(config-router)#network 192.168.10.0 255.255.255.0

Router(config-router)#network 192.168.20.0 255.255.255.0

Router(config-router)#exit

ROUTER1 CLI:

Router(config)#router eigrp 10

Router(config-router)#network 192.168.20.0 255.255.255.0

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.20.1 (Serial0/1/0) is up: new adjacency

Router(config-router)#network 192.168.30.0 255.255.255.0

Router(config-router)#exit

OUTPUT:

ROUTER0:

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 192.168.10.0/24 is directly connected, FastEthernet0/0

C 192.168.20.0/24 is directly connected, Serial0/3/0

D 192.168.30.0/24 [90/20514560] via 192.168.20.2, 00:04:51, Serial0/3/0

ROUTER1:

D 192.168.10.0/24 [90/20514560] via 192.168.20.1, 00:05:35, Serial0/1/0

C 192.168.20.0/24 is directly connected, Serial0/1/0

C 192.168.30.0/24 is directly connected, FastEthernet0/0

Result:

Thus, understand the concept and operation of EIGRP and obtained the routing table and observe transfer data packets in real and simulation time.

EXPERIMENT 9

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

THEORY:

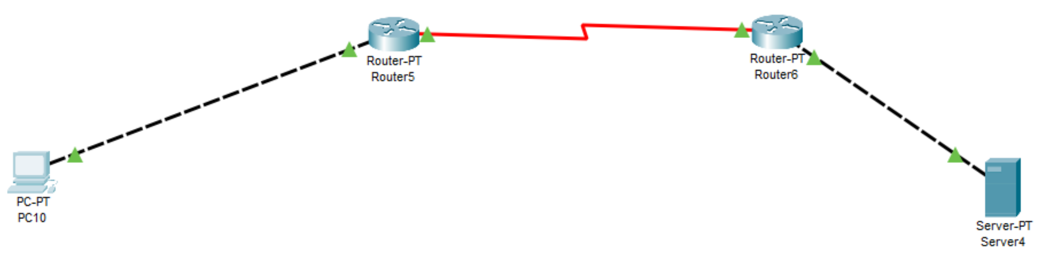
Border routers are typically configured for NAT. H. A router with an interface on the local (internal) network and an interface on the global (external) network. When a packet leaves the local (internal) network, NAT translates its local (private) IP address to a global (public) IP address. Global (public) IP addresses are translated to local (private) IP addresses when packets enter the local network. When NAT runs out of addresses, i. H. 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:

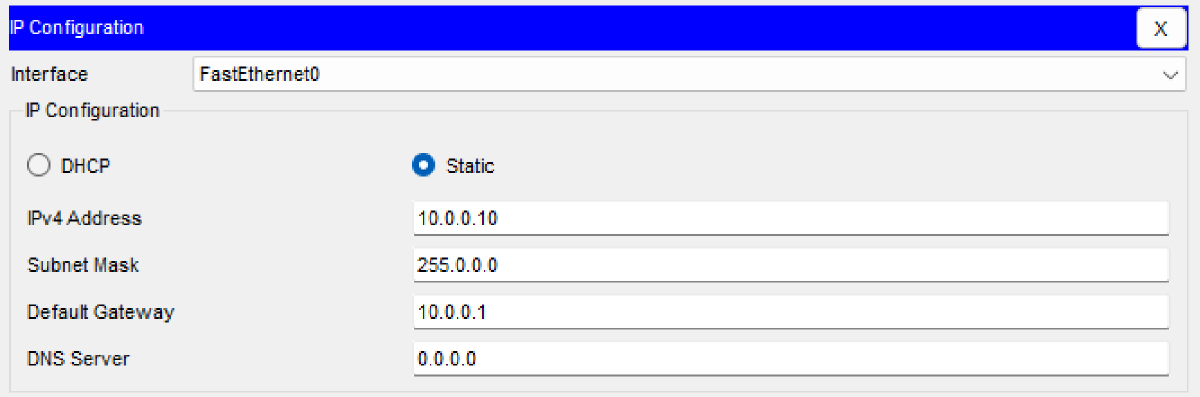
- Inside Local: It is a region inside the Enterprise’s network where the hosts have Private IP addresses.
- Inside Global: It is also a region inside the Enterprise network, but Public IP addresses are used in this region (this region is usually connected to the outside network or Internet).
- Outside 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.
- Outside Global: It is a part of the Enterprise network in a public Internet where Public IP addresses is used.

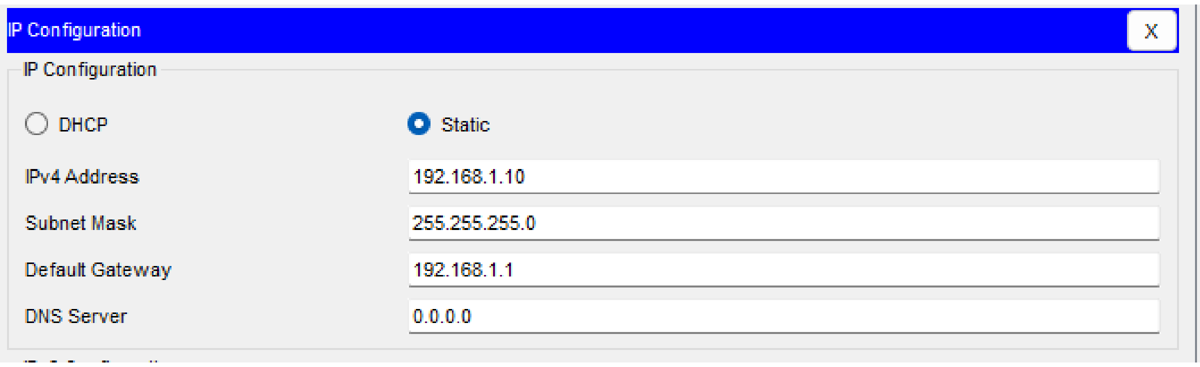
PROCEDURE

1. Create the connections as shown

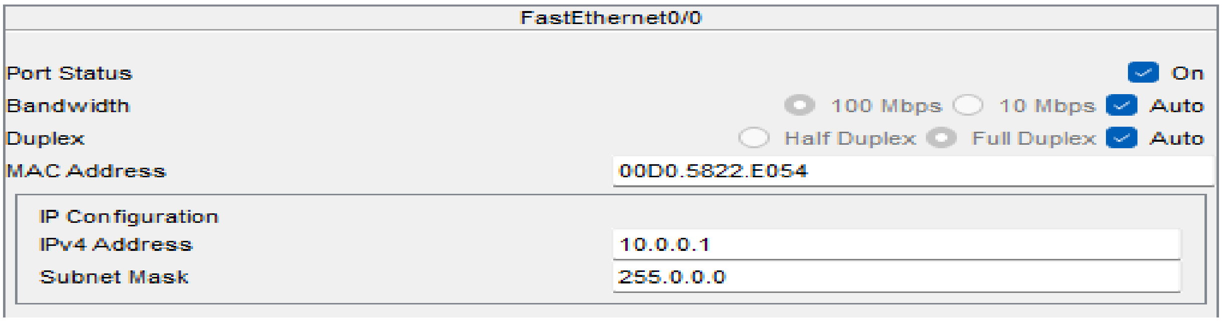


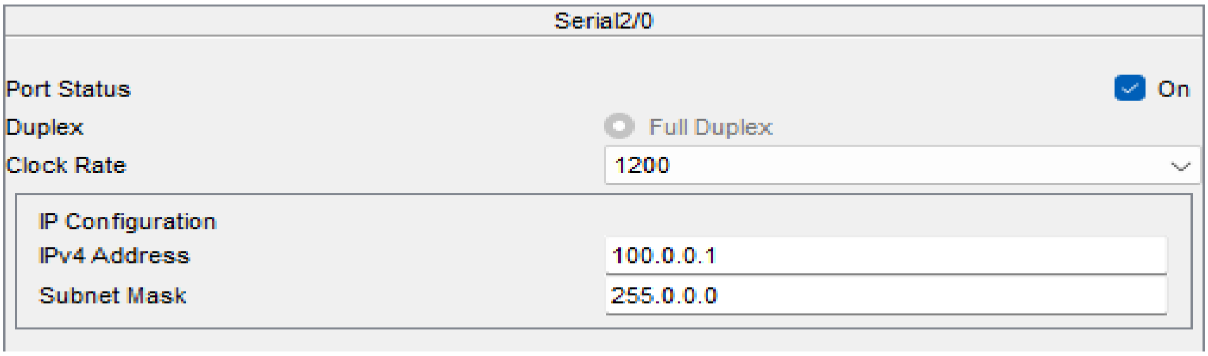
2. Configure IP of client and server endpoints





3. Configure IP in both routers





4. Set the NAT Mapping in both routers

Client router

```
Router(config)#ip nat inside source static 10.0.0.10 50.0.0.10
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Server router

```
Router(config)#ip nat inside source static 192.168.1.10 200.0.0.10
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

5. Test by pinging the outside IP of server from client.

```
C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

EXPERIMENT 10

AIM: Conducting a Network Capture and monitoring with Wireshark Simulation Tool.

Theory:

he screen/interface of the Wireshark is divided into five parts:

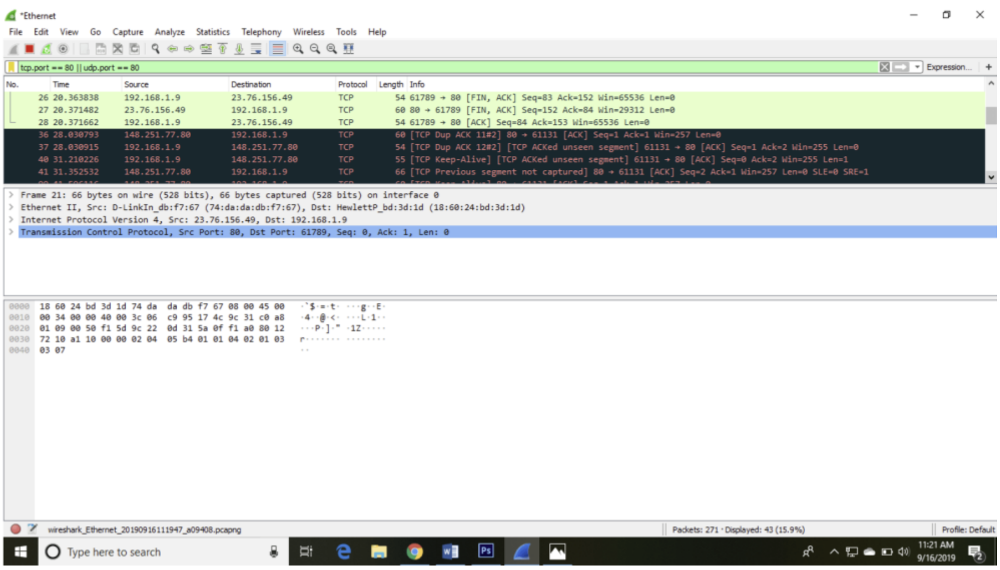
First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.

The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.

Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.

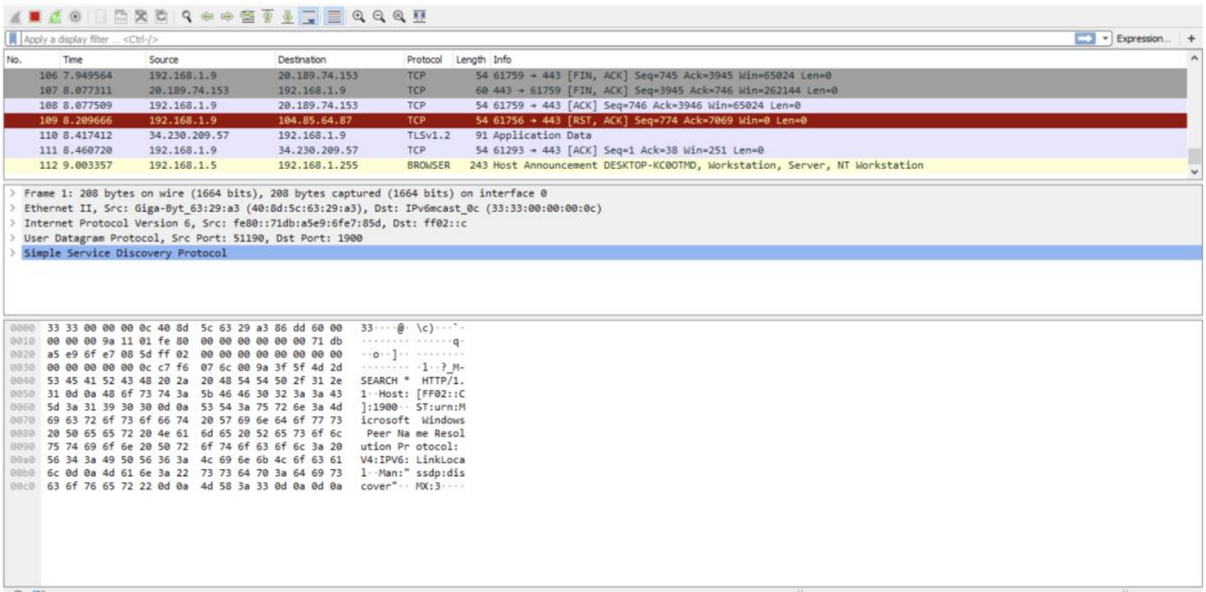
The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.

At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

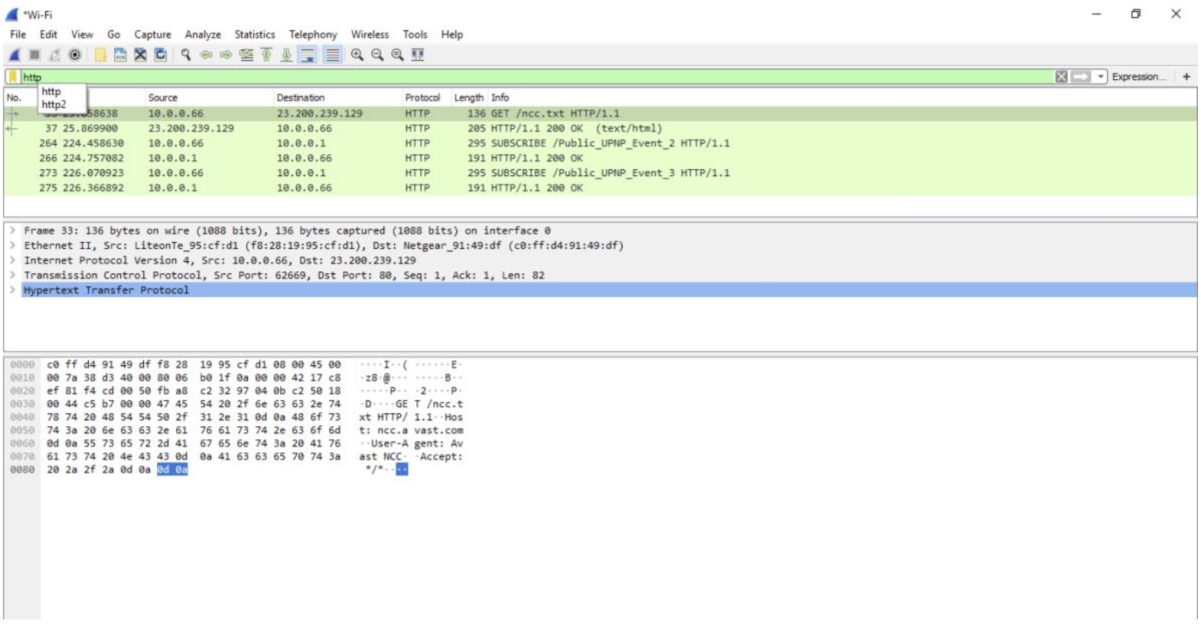


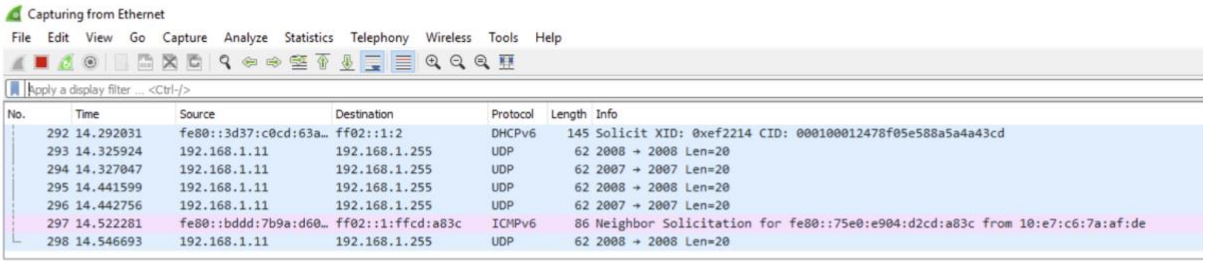
You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

After connecting, you can watch the traffic below:

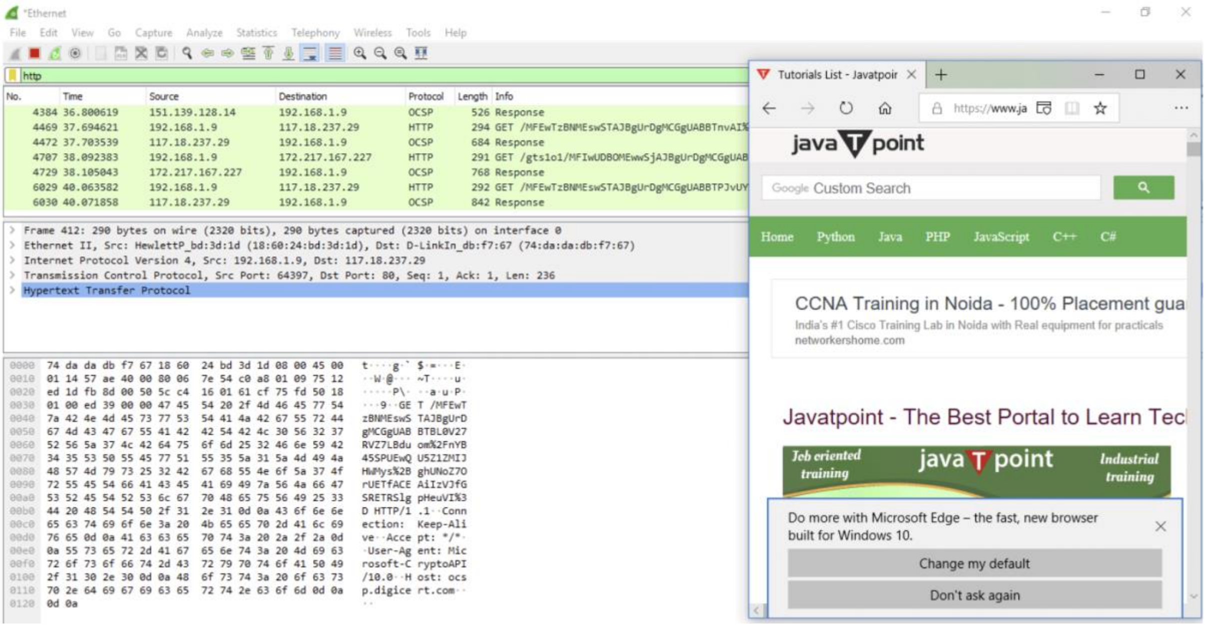


Here is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.





OUTPUT:



CONCLUSION: Network Capturing and monitoring was done successfully using Wireshark Simulation Tool.