Lab Manual for

Computer Networks

Course Name: SE

Semester: I

Second Year

Department of
Artificial Intelligence and Machine Learning

Alard University

Experiment No: 01

Name of Student: _____

Roll Number: _____ **Class:** _____

1. **TITLE:** IP Addressing and Subnetting.

AIM: Case study on IP Addressing and Subnetting

Objective: To study IP addressing and subnetting. It's different Types and classes**.**

Software /Hardware Requirement:

Sr. No	Name of Software and Hardware	Latest Version
1	Windows	10/11

Theory:

Network devices use IP addresses and subnets to identify the source and destination of communications and manage network addresses respectively.

IP addresses contain two parts: a network identifier and a host identifier. The network ID specifies an area of the network where a device resides, much like an area code identifies a section of a telephone network. The host ID labels a specific device in that network section, similar to how a telephone number identifies a specific phone within an area code.

Most business networks still rely on IP version 4 (IPv4) addresses, which offer about 4.3 billion unique variations. Internet identities use most of these, but the newer IP version 6 (IPv6) standard provides more addresses and other benefits.

Computers work with IPv4 addresses as 32-bit binary strings. Humans usually convert binary to a dotted decimal address, which is easier to write and understand. For example, the binary string 11000000.00000000.00000010.00000010 converts to the IP address 192.0.2.2. Its associated subnet mask converts from 11111111.11111111.11111111.11111100 to 255.255.255.252.

Subnet masks clarify which part of the address is the network ID and which is the host ID. Routers, computers and network troubleshooters use IP addresses and subnet masks to manage network traffic, which ensures information sent from one system arrives at its destination.

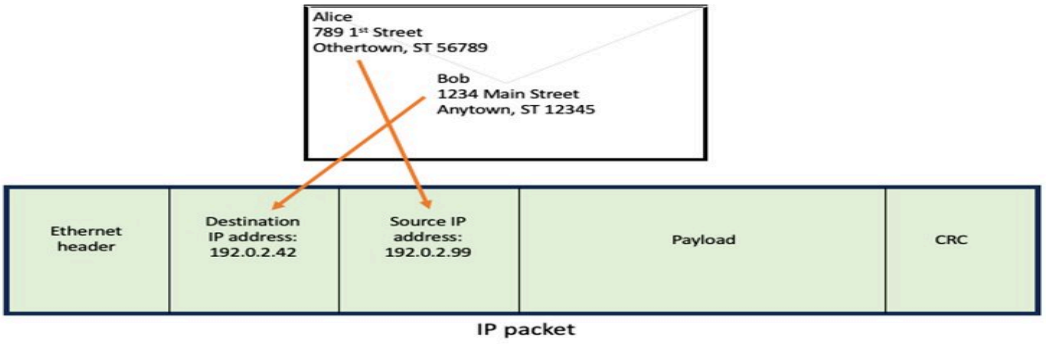
IP address fundamentals:

Network devices typically have the following three identities:

- Physical address. MAC address.
- Logical address. IP address.
- Hostname. Useful for humans to recognize the device.

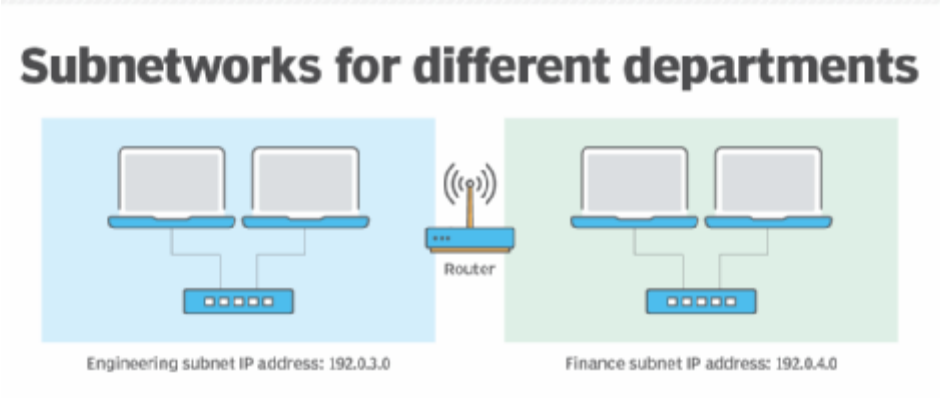
A workstation has three identities: hostname, IP address and MAC address.

In the case of IPv4 addresses, each host has a unique IP address on the network, and nodes rely on it to exchange information. Data breaks down into pieces, known as packets, which then travel across the network. Each packet contains a source and destination IP address, much like postal service mail includes a destination and return address on the envelope.



Administrators can subdivide networks into smaller, more manageable sections. This process lets them control the flow of network traffic, isolate traffic to increase security and limit traffic to certain areas of the network to improve performance.

These network segments are called subnetworks, or subnets. Each subnet has a unique identifier within the larger network ID. When administrators divide a network into parts, such as engineering and finance, the address structure is based on numbers.



Two network segments, each with its own network ID.

Private IP address ranges

Systems and sites on the public internet consume most of the roughly 4.3 billion available IPv4 addresses. However, private networks can reserve some ranges for internal use. Networks in home offices and businesses likely use one of these ranges.

The following table defines private IPv4 address ranges.

Reserved class	Range	Default subnet mask	Description
Class A	10.0.0.0	255.0.0.0	Larger networks with many hosts.
Class B	172.16.0.0	255.255.0.0	Medium networks with a moderate number of hosts.
Class C	192.168.0.0	255.255.255.0	Smaller networks with fewer hosts.

Conclusion: Thus, we studied different types of IP addresses and different classes of IPV4**.**

Experiment No: 02

Name of Student: _____

Roll Number: _____ **Class:** _____

2. TITLE: static routing and default routing.

AIM: Case study on static routing and default routing protocols. Implement it in cisco packet tracer

Objective: To study network simulator. To learn different routing commands and subnetting of given network. Candidate is expected to know the theory involved in the experiment.

Software /Hardware Requirement:

Sr.No	Name of Software and Hardware	Latest Version
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

Static Routing:

Static Routing is also known as **non-adaptive** routing which does not change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and it provides high or more security than dynamic routing.

Default Routing:

It is a type of routing which is useful in those cases when the destination network id is unknown to the router. In such cases, the router will use a default route and will send all the incoming traffic to that route, by default. Generally used on the internet where the destinations are unknown. Default Routing is a method wherein a router is configured to ship all the packets to the equal hop tool, and it would not be counted whether it belongs to a specific community or not. a packet is transmitted to the tool for which it is far configured in default routing.

1. Static Routing:

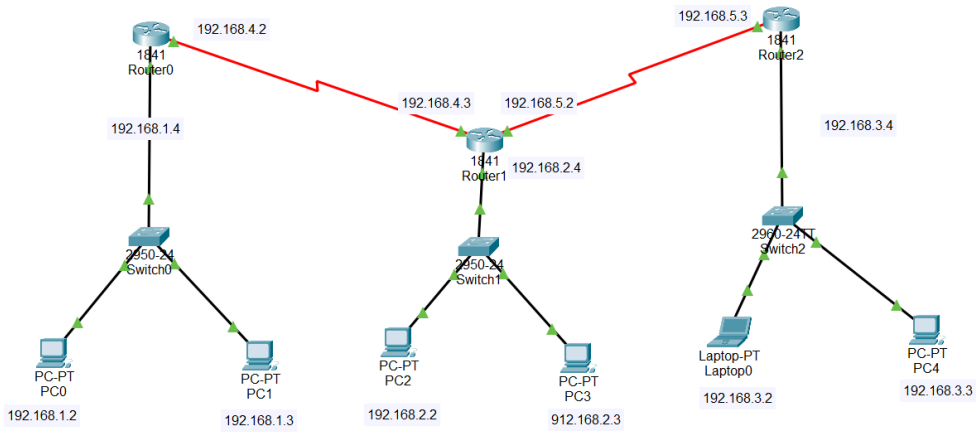
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S.NO	Device	Model Name	Qty.
1.	PC		
2.	Switch		
3.	Router		

IP Addressing Table for PCs:

S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway

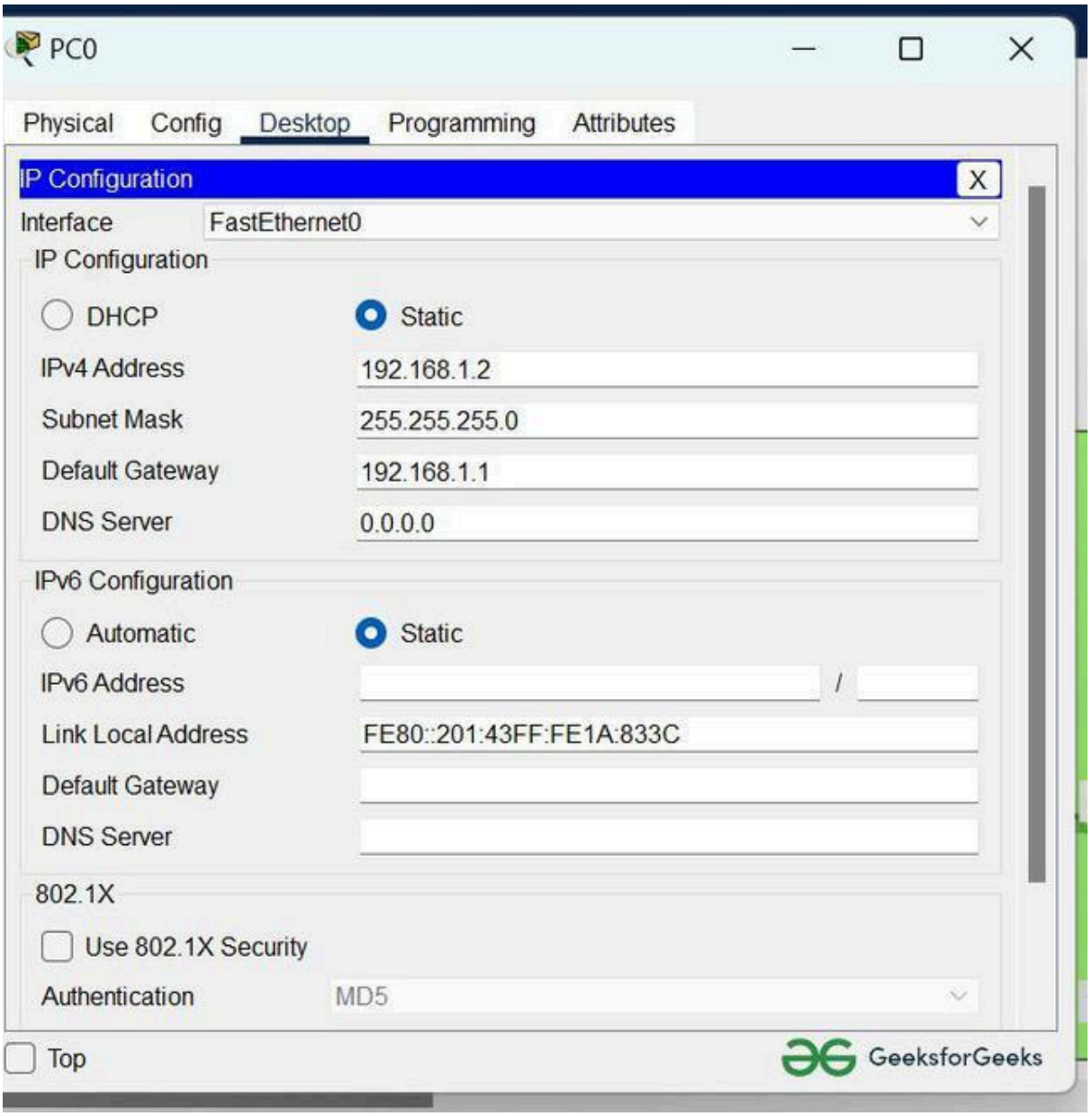
- Then, create a network topology as shown in the image.



- Use an Automatic connecting cable to connect the devices with each other's.

Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

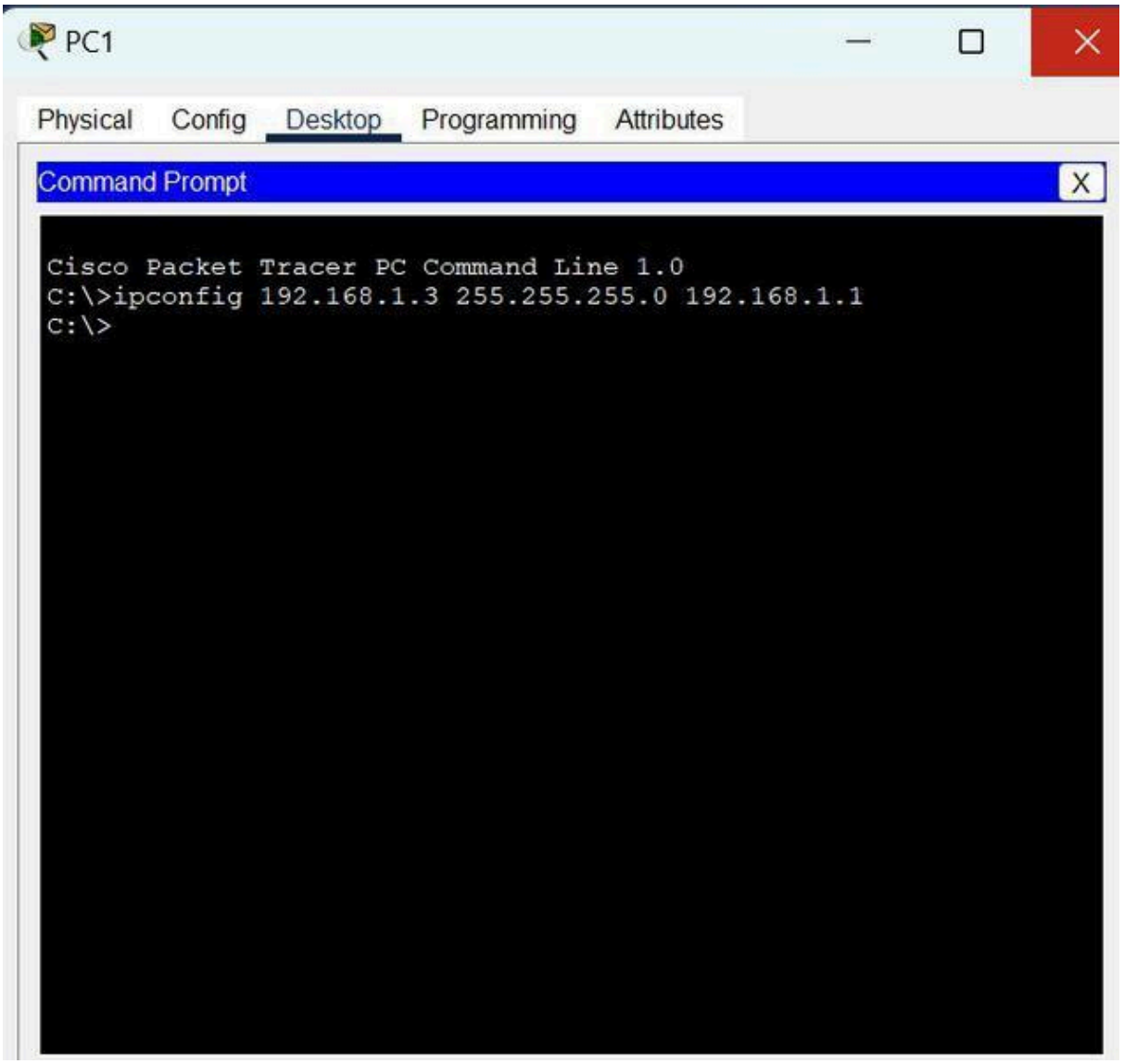
- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask and default gateway.



Step 3: Assigning IP address using the ipconfig command.

- We can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

  Example: ipconfig 192.168.1.3 255.255.255.0 192.168.1.1



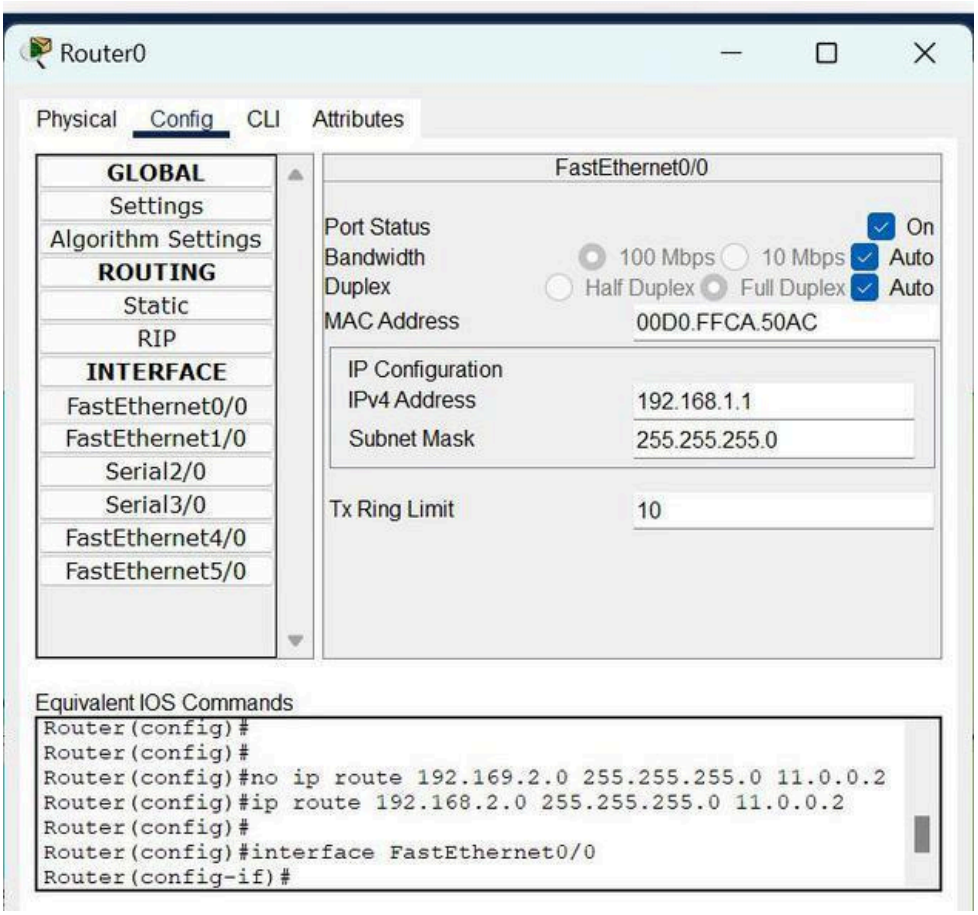
- Repeat the same procedure with other PCs to configure them thoroughly.

Step 4: Configure router with IP address and subnet mask.

S.NO	Device	Interface	IPv4 Addressing	Subnet Mask

- To assign an IP address in router0, click on router0.

- Then, go to config and then Interfaces.
- Then, configure the IP address in FastEthernet and serial ports according to IP addressing Table.
- Fill IPv4 address and subnet mask.



- Repeat the same procedure with other routers to configure them thoroughly.

Step 5: After configuring all of the devices we need to assign the routes to the routers.

To assign static routes to the particular router:

- First, click on router0 then Go to CLI.
- Then type the commands and IP information given below.

CLI command : ip route <network id> <subnet mask><next hop>

Static Routes for Router0 are given below:

Router(config)#ip route

Router(config)#ip route <write your respective nw id's>

Static Routes for Router1 are given below:

Router(config)#ip route

Router(config)#ip route <write your respective nw id's>

Static Routes for Router 2 are given below:

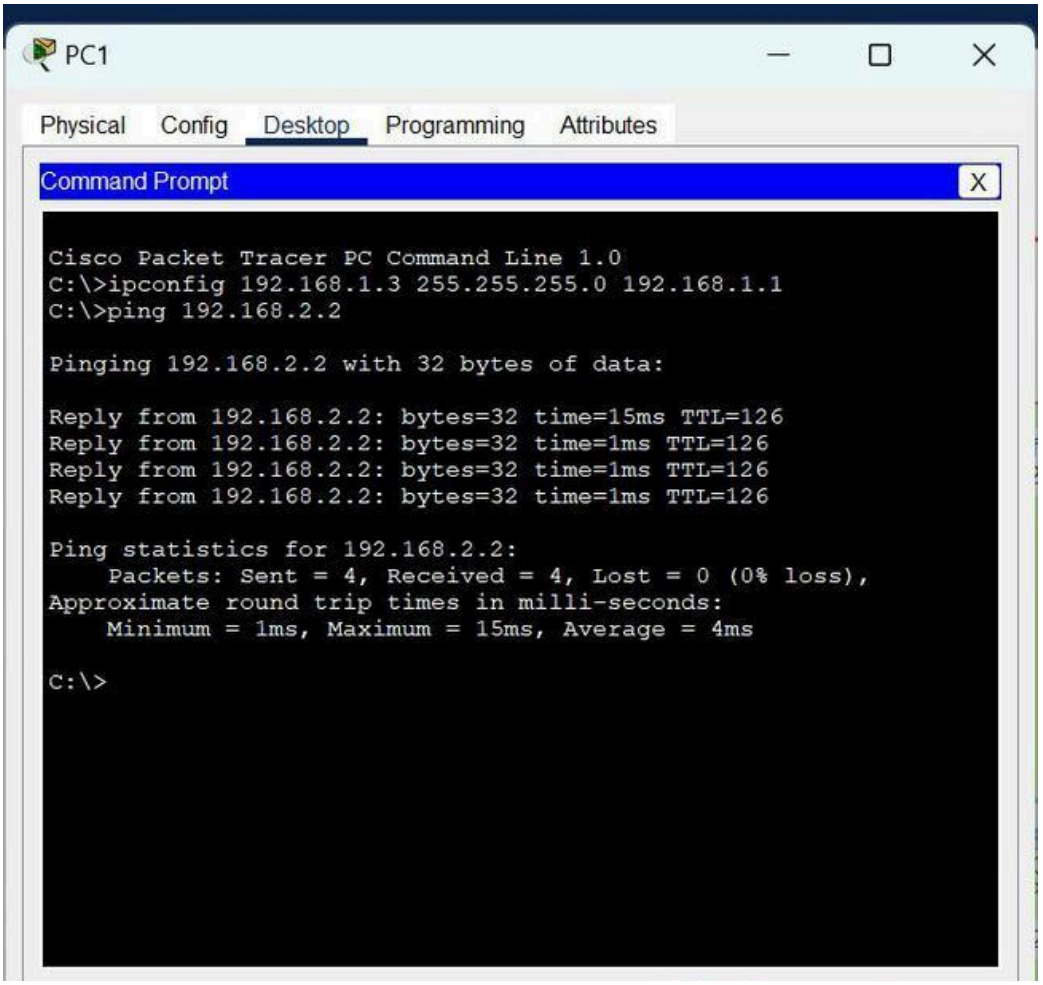
Router(config)#ip route

Router(config)#ip route <write your respective nw id's>

Step 6: Verifying the network by pinging the IP address of any PC. We will use the ping command to do so.

- First, click on PC1 then Go to the command prompt
- Then type ping <IP address of targeted node>
- As we can see in the below image, we are getting replies which means the connection is working very fine

Example : ping 192.168.2.2



Default Routing:

The main concept of configuring default routes is that it has the ability to handle packets transferred to networks not located in the routing table. Default Routes are configured mostly in Stub Network.

Stub Network:

It is a network containing only one exit interface or only one way to reach the destination. When we configure default routes, it requires these packets to another router that has the path to the

destination.

CLI command:

R-1(config)#ip route (any destination) (any subnet mask) (next hop IP address)

R-1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2

Step 1: First, create a network topology of these given devices listed below in the table:

S.NO	Device	Model name	Quantity
1.	PC		
l2.	switch		
3.	router		

Step 2: Configuring Hosts (PCs) with IP addresses and Default Gateway using IP Addressing table given below:

S.NO	Device	IPv4 Address	Subnet mask	Default gateway
1.				
2.				
3.				

Step 3: Configure PCs follow these steps:

1. Click on PC0 then go to desktop.
2. Click on IP configuration.
3. Then on the static route, fill up the IP configuration according to the IP addressing table given above.
4. Repeat the same procedure with other PCs to configure them.

Assigning IP address using the ipconfig command.

1. We can also assign an IP address with the help of a command.
2. Go to the command terminal of the PC.
3. Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

a. *Example: ipconfig 192.168.1.3 255.255.255.0 192.168.1.1*

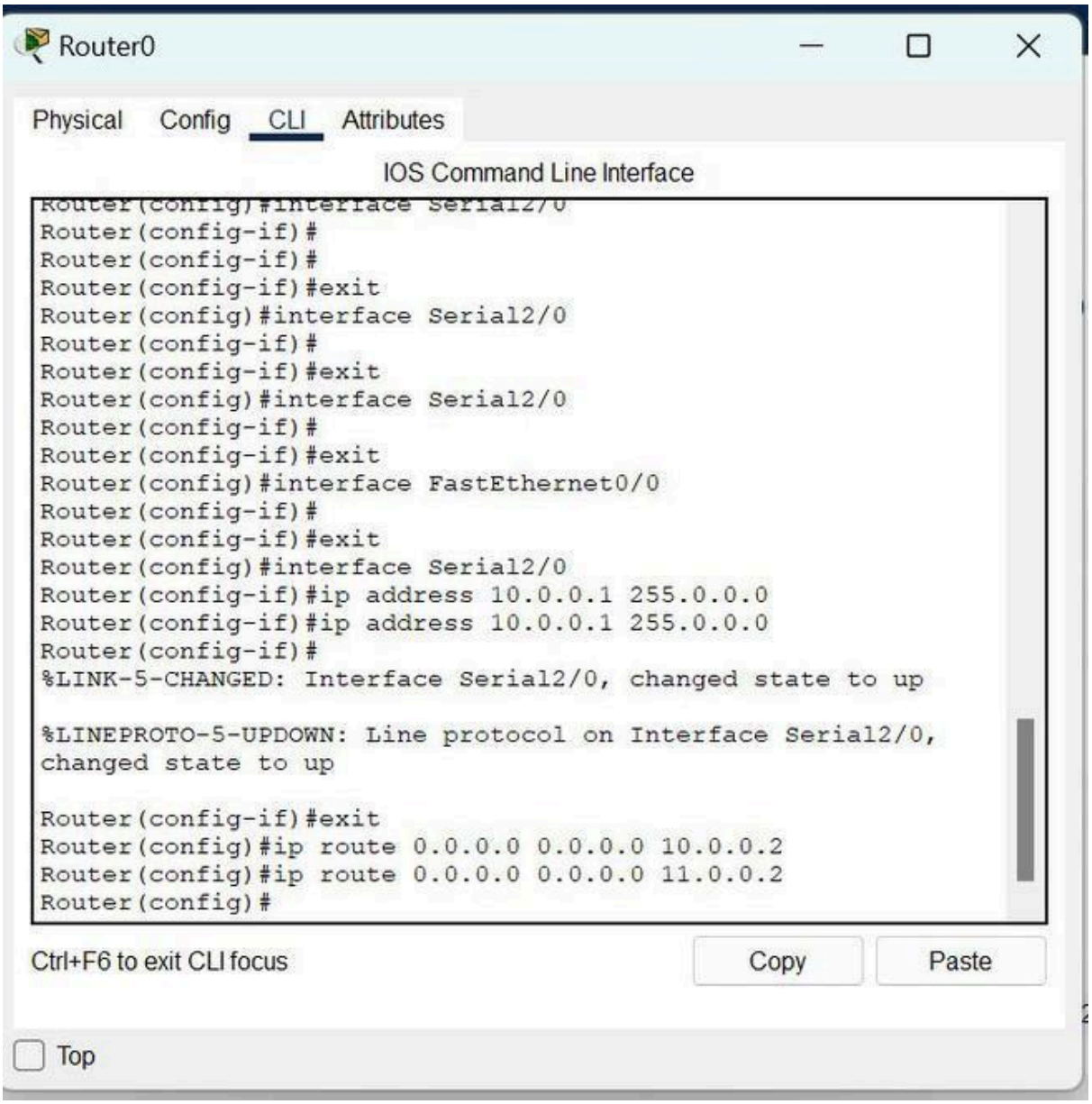
Step 4: Configuring the Interfaces (routers) with IP Addresses and Default gateways and assigning the default routes.

Router0 Configuration:

- Click on router0 then, Go to CLI commands and enter commands to configure them given below.
- Now we will add the IP address of the serial se2/0 and its subnet mask.
- In this step, we will add the IP address of the interface FastEthernet port fa0/0 and its subnet mask.
- Then we need to add Default Routes to configure the router:

R-1(config)#ip route (any destination~reserved) (any subnet mask~reserved) (next hop IP address)

Eg:



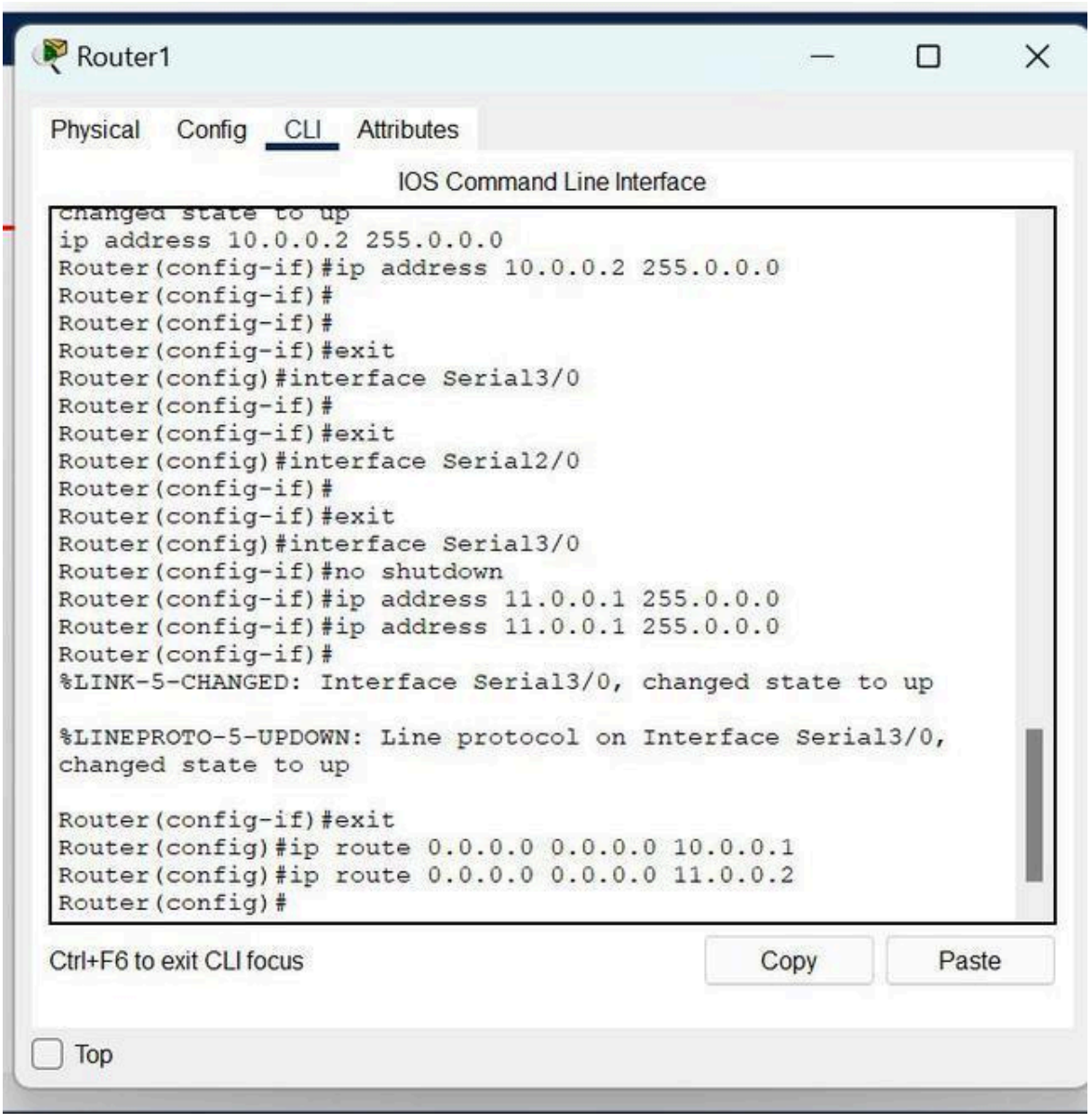
- Add the IP address of the next hope to connect with another LAN.

Router1 Configuration:

- Click on the router1 then, Go to CLI commands, and enter commands to configure them given below.
- Now, we will add the IP address of the serial se2/0 and its subnet mask.
- Second, we will add the IP address of the interface FastEthernet port fa0/0 and its subnet mask.
- Then we need to add Default Routes to configure the router:

R-1(config)#ip route (any destination~reserved)(any subnet mask~reserved) (next-hop IP address)

Eg:



- Add the IP address of the next hop to connect with another LAN.

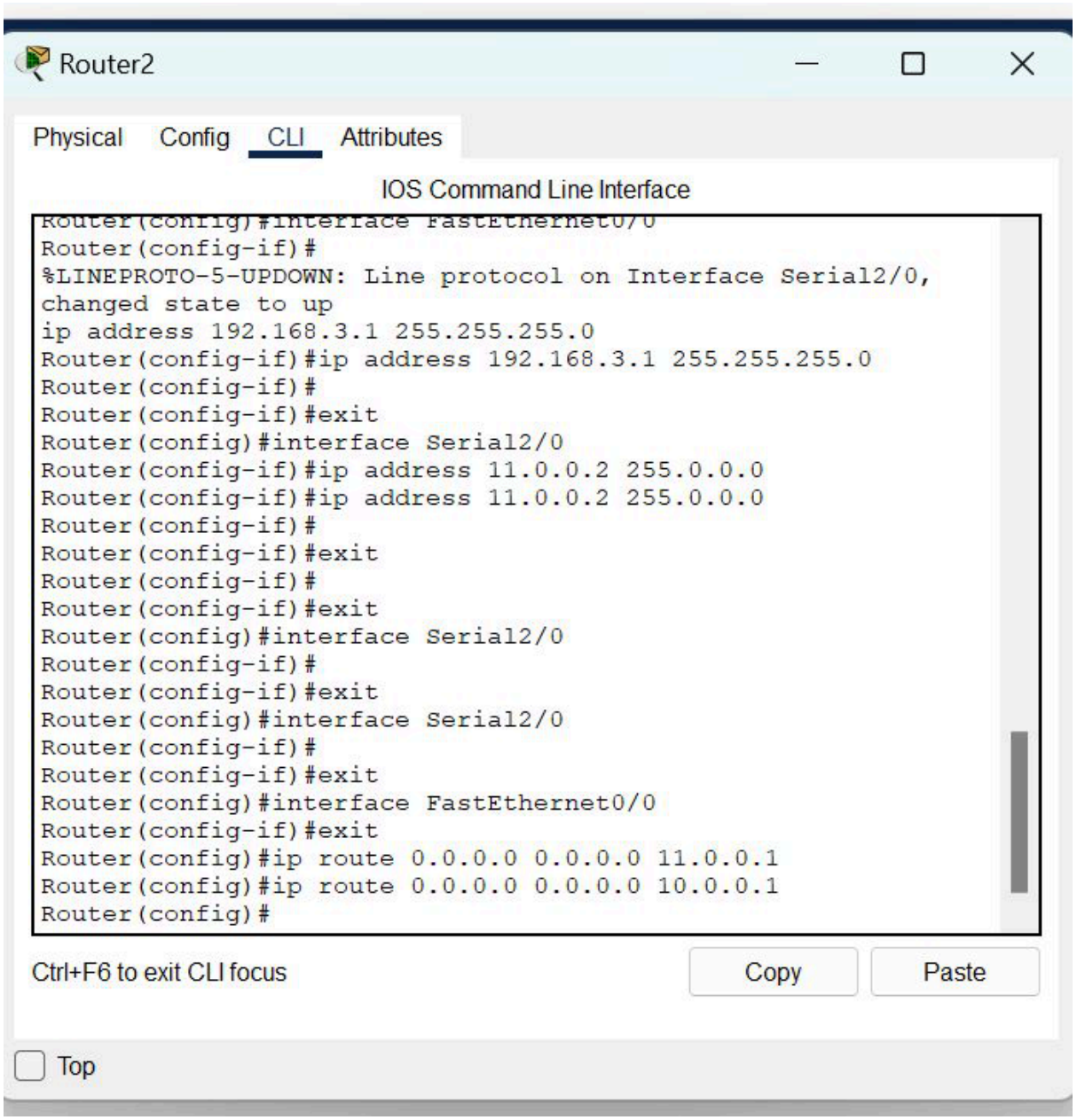
Router 2 Configuration:

- Click on the router2 then, Go to CLI commands, and enter commands to configure them given below.
- Now, we will add the IP address of the serial se2/0 and its subnet mask.

- Second, we will add the IP address of the interface FastEthernet port fa0/0 and its subnet mask.
- Then we need to add Default Routes to configure the router:

R-1(config)#ip route (any destination~reserved)(any subnet mask~reserved) (next-hop IP address)

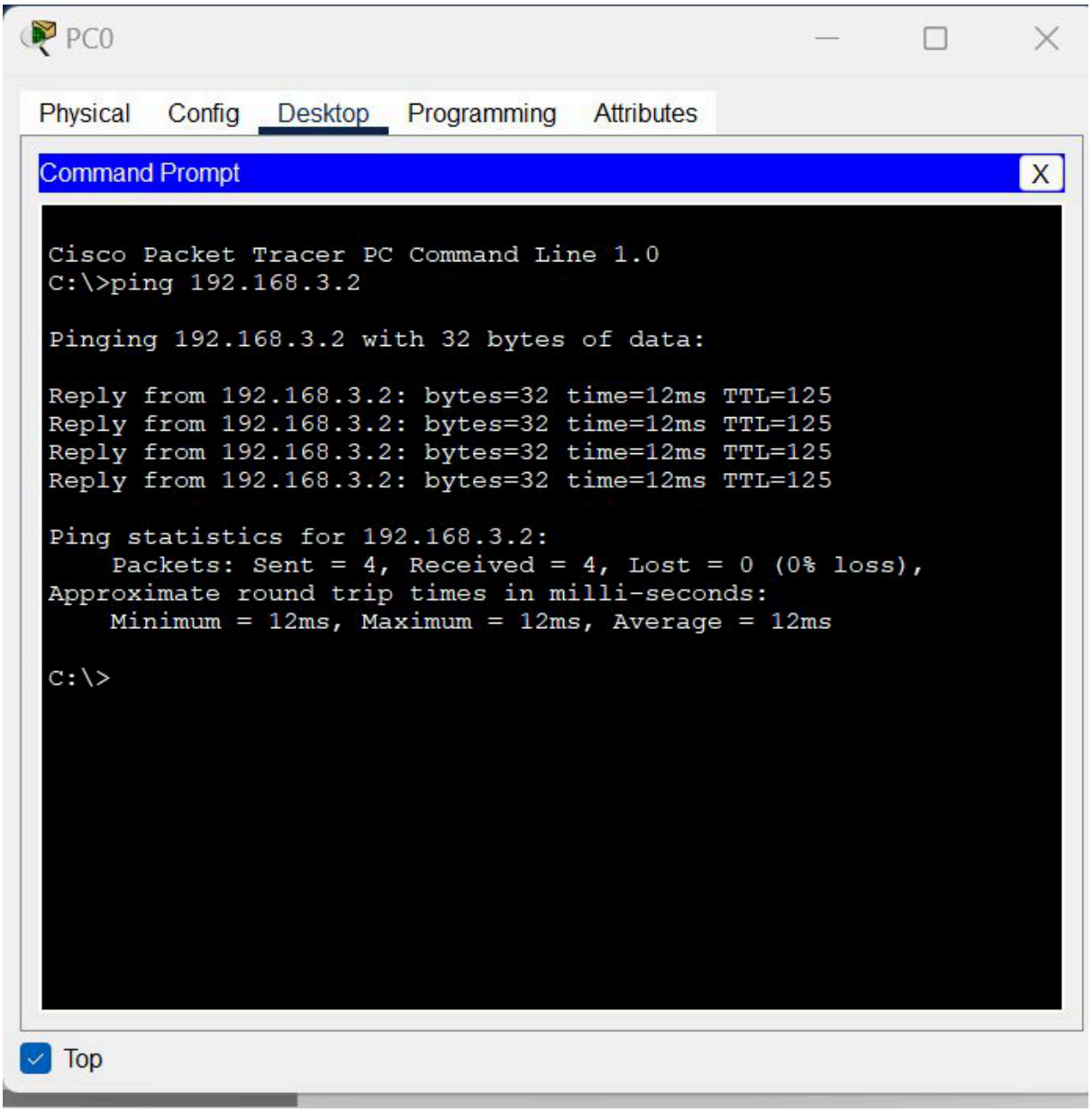
Eg:



Step 5: After configuring all the devices red indicator turns into green and the network is live so we can send and receive packets.

To verify the network, we'll verify the network by pinging the IP address of the target node in any Host.

- Click on PC0 then, Go to the desktop.
- Click on Command Prompt, and type this command "ping 192.168.2.3".
- In the below image we can see that we getting replies from a targeted node which means the connection is established successfully.


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 12ms, Average = 12ms
C:\>
Top

Router1

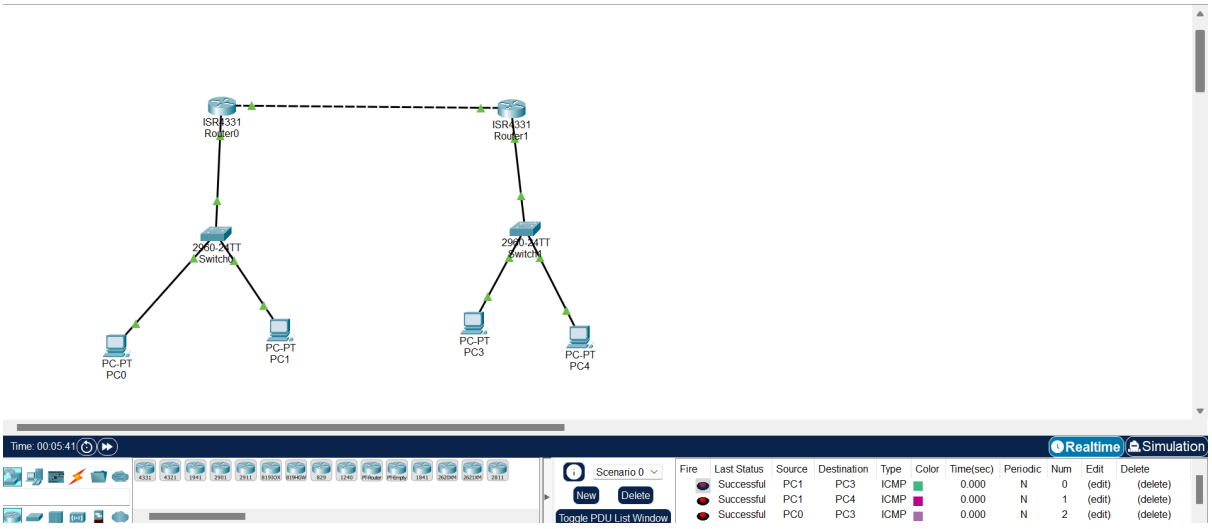
Physical Config CLI Attributes

IOS Command Line Interface

```
If you require further assistance please contact us by sending email to
export@cisco.com.

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet 0/0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router(config-if)#interface GigabitEthernet 0/0/1
Router(config-if)#ip address 11.11.1.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

Copy Paste

Top



Conclusion:

Experiment No: 03

Name of Student: _____

Roll Number: _____ **Class:** _____

3. TITLE: EIGRP Protocol

AIM: To configure EIGRP protocol using network simulator (E.g. Cisco Packet Tracer)

Objective: To study network simulator. To learn different routing commands and configure EIGRP protocol for given network. Candidate is expected to know the theory involved in the experiment.

Software /Hardware Requirement:

Sr. No	Name of Software and Hardware	Latest Version
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

Steps to Configure and Verify EIGRP in Cisco Packet Tracer :
Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

S.NO	Device	Model Name	Qty.
1.	pc	pc	2
2.	switch	PT-Switch	0
3.	router	PT-Router	6

Table 4.2

IP Addressing Table:

S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway
1.	pc0			
2.	pc1			

Table 4.3

- Then, create a network topology as shown.

Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in server0, click on server0.
- Then, go to desktop and then IP configuration, and there you will see IPv4 configuration.
- Fill IPv4 address and subnet mask.

2. Assigning IP address using the ipconfig command.

- We can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

Example: ipconfig 192.168.0.3 255.255.255.0 192.168.0.1

- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: Configure router with IP address and subnet mask.
IP Addressing Table Router:

S.NO	Device	Interface	IPv4 Address	Subnet Mask
1.	router0			
2.	router1			
3.	Router2			

S.NO	Device	Interface	IPv4 Address	Subnet Mask
4	Router3			
5	Router4			
6	Router5			

Table 4.3

Configuring IP through Config:

- To assign an IP address in router0, click on router0.
- Then, go to config and then Interfaces.
- Now, configure the IP address in FastEthernet and serial ports according to the IP addressing Table.
- Add IPv4 address and subnet mask.
- Repeat the same procedure with other routers to configure them thoroughly.

Configuring IP through CLI:

- To configure the IP address and subnet mask of an interface named "FastEthernet0/0", you would enter the following commands:

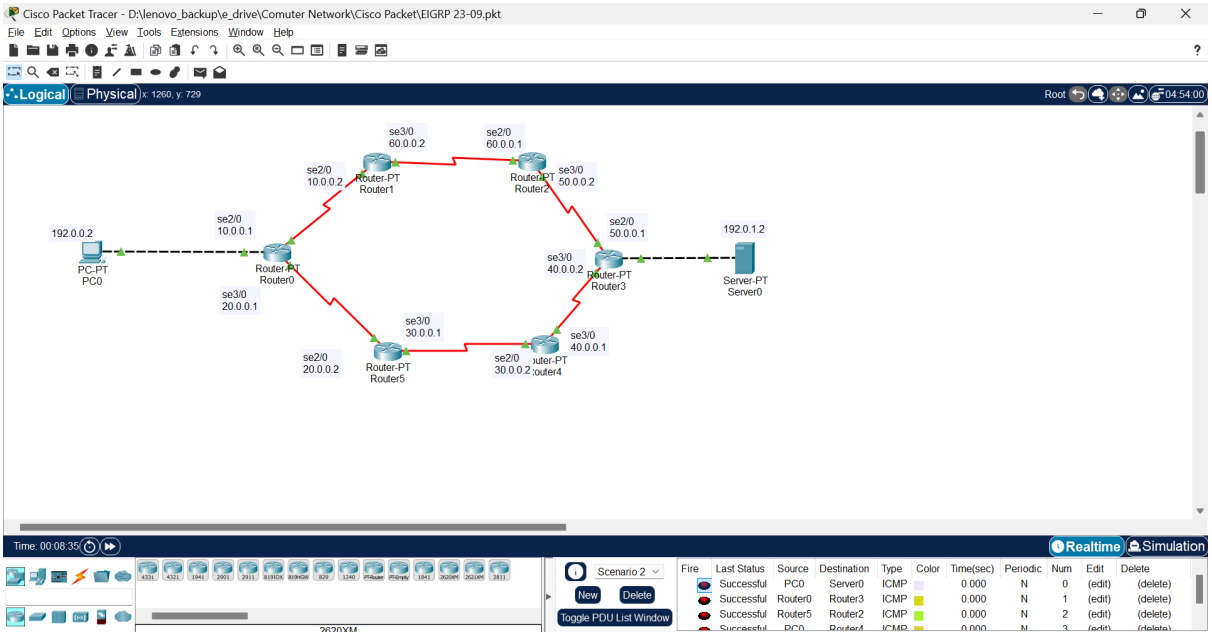
```
Router>enable
Router# configure terminal
Router(config)interface FastEthernet0/0
Router(config-if) ip address 10.0.0.1 255.0.0.0
Router(config-if) no shutdown
```

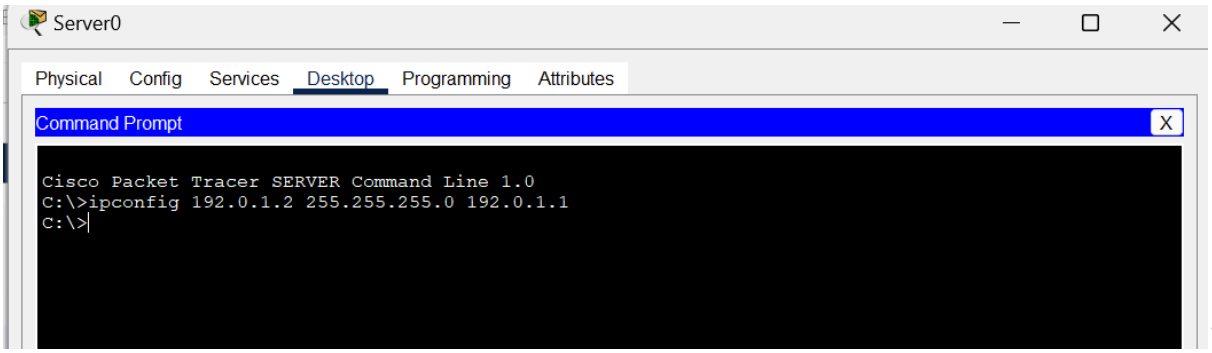
Step 4: After configuring all the devices, we need to configure EIGRP protocols to the routers.

- First, click on router0 then Go to CLI.
- Then type the commands and IP information given below.

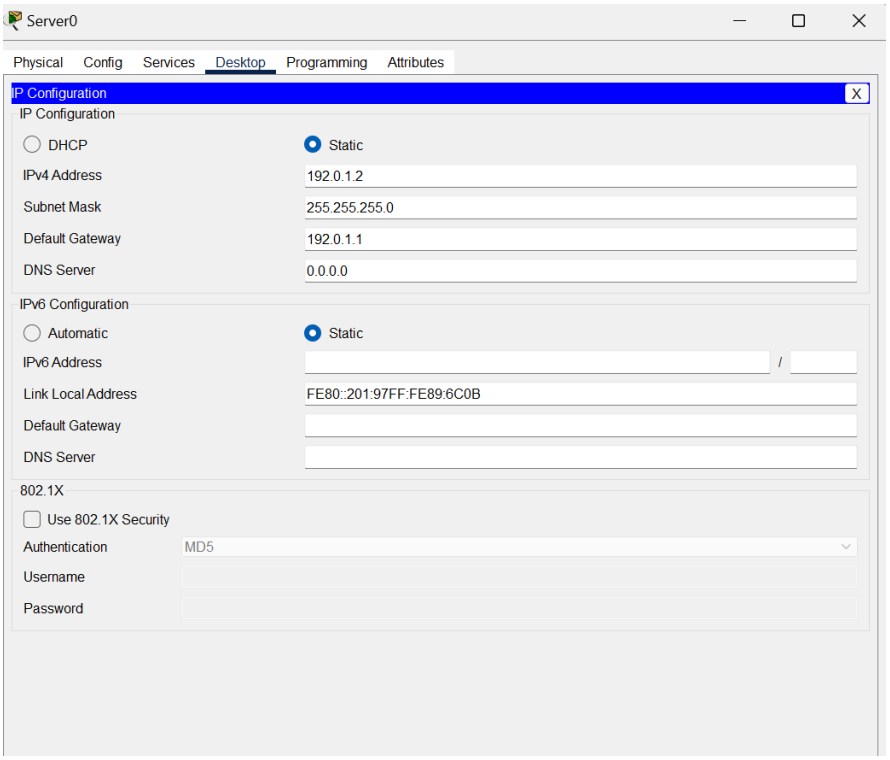
CLI command syntax: Router(config)# router eigrp 1
Router(config)#network <network id>

Topology and PC configuration


Cisco Packet Tracer - D:\lenovo_backup\e_drive\Comuter Network\Cisco Packet\EIGRP 23-09.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
04:54:00
se3/0 60.0.0.2
se2/0 60.0.0.1
se2/0 10.0.0.2
Router-PT Router1
Router-PT Router2
se3/0 50.0.0.2
192.0.0.2
se2/0 10.0.0.1
se2/0 50.0.0.1
192.0.1.2
PC-PT PC0
Router-PT Router0
se3/0 40.0.0.2
Router-PT Router3
Server-PT Server0
se3/0 20.0.0.1
se3/0 30.0.0.1
se3/0 40.0.0.1
se2/0 20.0.0.2
Router-PT Router5
se2/0 30.0.0.2
Time: 00:08:35
Realtime
Simulation
Scenario 2
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Successful PC0 Server0 ICMP 0.000 N 0 (edit) (delete)
Successful Router0 Router3 ICMP 0.000 N 1 (edit) (delete)
Successful Router5 Router2 ICMP 0.000 N 2 (edit) (delete)


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig 192.0.1.2 255.255.255.0 192.0.1.1
C:\>

\


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.0.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.0.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:97FF:FE89:6C0B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password

IP Configuration of Devices:

Pc: 192.0.0.2 255.255.255.0 192.0.0.1
Server:192.0.1.2 255.255.255.0 192.0.0.1

Router 0:

Router>enable
Router# configure terminal
Router(config)interface FastEthernet0/0
Router(config-if) ip address 192.0.0.1 255.0.0.0
Router(config-if) no shutdown

Router(config)interface Serial2/0
Router(config-if) ip address 10.0.0.1 255.0.0.0
Router(config-if) no shutdown

Router(config)interface Serial3/0
Router(config-if) ip address 20.0.0.1 255.0.0.0
Router(config-if) no shutdown

Router 1:

Router(config)interface Serial2/0
Router(config-if) ip address 10.0.0.2 255.0.0.0
Router(config-if) no shutdown

Router(config)interface Serial3/0
Router(config-if) ip address 60.0.0.2 255.0.0.0
Router(config-if) no shutdown

Ruter 2:

Router(config)interface Serial2/0
Router(config-if) ip address 60.0.0.1 255.0.0.0
Router(config-if) no shutdown

Router(config)interface Serial3/0
Router(config-if) ip address 50.0.0.2 255.0.0.0
Router(config-if) no shutdown

Ruter 3:

Router(config)interface Serial2/0
Router(config-if) ip address 50.0.0.1 255.0.0.0
Router(config-if) no shutdown

Router(config)interface Serial3/0

Router(config-if) ip address 40.0.0.2 255.0.0.0

Router(config-if) no shutdown

Ruter 4:

Router(config)interface Serial2/0

Router(config-if) ip address 30.0.0.2 255.0.0.0

Router(config-if) no shutdown

Router(config)interface Serial3/0

Router(config-if) ip address 40.0.0.1 255.0.0.0

Router(config-if) no shutdown

Ruter 5:

Router(config)interface Serial2/0

Router(config-if) ip address 20.0.0.2 255.0.0.0

Router(config-if) no shutdown

Router(config)interface Serial3/0

Router(config-if) ip address 30.0.0.1 255.0.0.0

Router(config-if) no shutdown

EIGRP Configuration with Packet Tracer
Starting with Router 0.

Here our Autonomous system number is 1

Protocols for router0

For router 0 three directly connected networks so we will add all three as below

Router(config)#router eigrp 1

Router(config-router) #network <insert your nw id>

Router(config-router) #network <insert your nw id>

Router(config-router) #network <insert your nw id>

Protocols for router1

For router 1 and router 2 only two directly connected networks are there

Router(config)#router eigrp 1

Router(config-router) #network <insert your nw id>

Router(config-router) #network <insert your nw id>

Protocols for router2

Router(config)#router eigrp 1

Router(config-router)#network <insert your nw id >

Router(config-router)#network <insert your nw id >

Protocols for router3

Router 3 has three directly connected networks so we will add all three networks

Router(config)#router eigrp 1

Router(config-router) #network <insert your nw id >

Router(config-router) #network <insert your nw id >

Router(config-router) #network <insert your nw id >

Protocols for router4

For router 4 and 5 two directly connected networks.

Router(config)#router eigrp 1

Router(config-router) #network <insert your nw id >

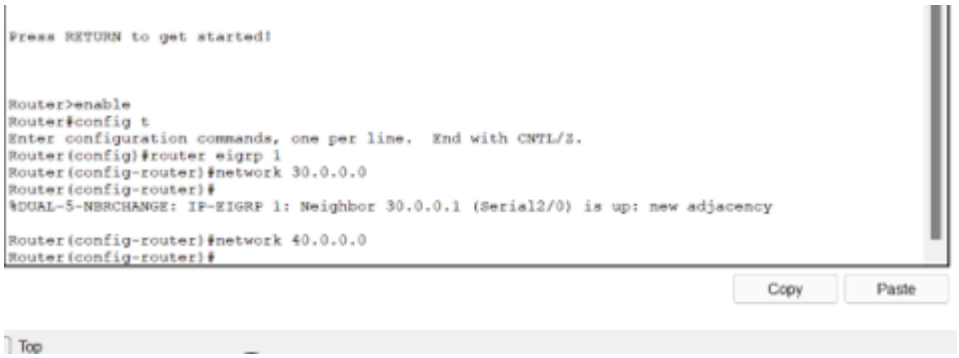
Router(config-router) #network <insert your nw id >

Protocols for router5

Router(config)#router eigrp 1

Router(config-router) #network <insert your nw id >

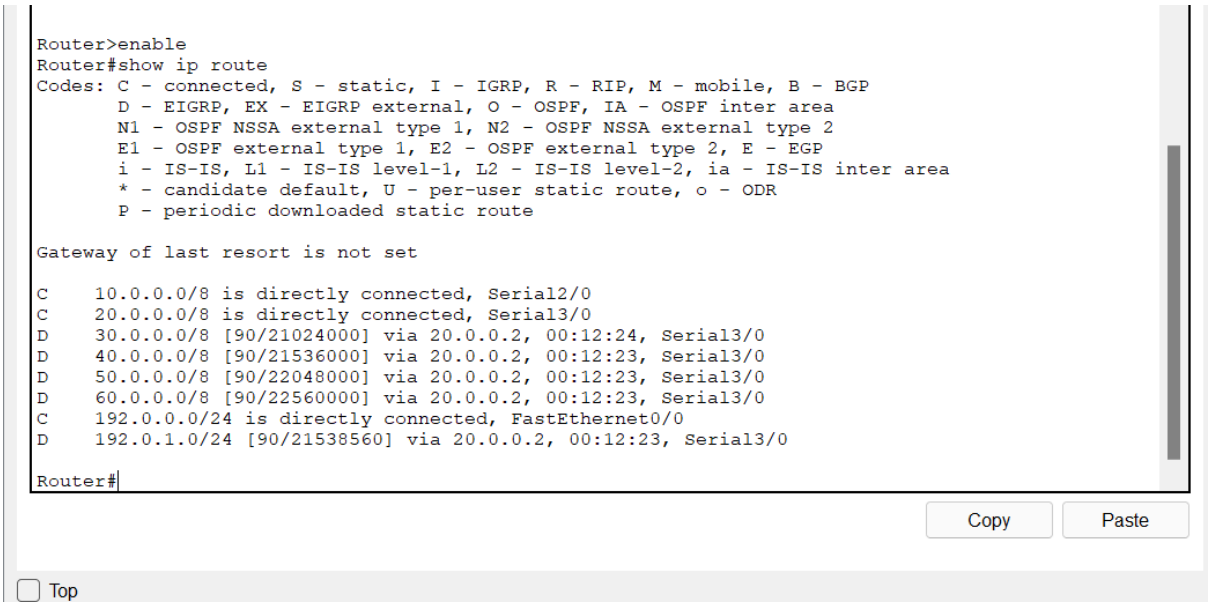
Router(config-router)#network <insert your nw id >



After adding all the neighbors, use following command:

Router#show ip route

This will give all the direct and indirect neighbors of router



EIGRP uses the term **Adjacency** to refer to the neighborship. In the log, it uses the term **New Adjacency** to refer to a new neighborship. The term **New Adjacency** indicates a new neighbor is found and the neighborship with the neighbor has been established.

Verify the network by pinging the IP address of any PC. We will use the ping command to do so.

Example: ping 192.0.0.2

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.0.0.2

Pinging 192.0.0.2 with 32 bytes of data:

Reply from 192.0.0.2: bytes=32 time=19ms TTL=252
Reply from 192.0.0.2: bytes=32 time=51ms TTL=252
Reply from 192.0.0.2: bytes=32 time=52ms TTL=252
Reply from 192.0.0.2: bytes=32 time=40ms TTL=252

Ping statistics for 192.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 52ms, Average = 40ms
```

Experiment No: 04

Name of Student: _____

Roll Number: _____ **Class:** _____

4. TITLE: OSPF and RIP protocol

AIM: To configure OSPF and RIP protocol Using Network Simulator.

Objective: To study network simulator. To learn different routing commands and configure OSPF and RIP protocol for given network. Candidate is expected to know the theory involved in the experiment.

Software /Hardware Requirement:

Sr.No	Name of Software and Hardware	Latest Version
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

Configure OSPF:

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

OSPF Terms

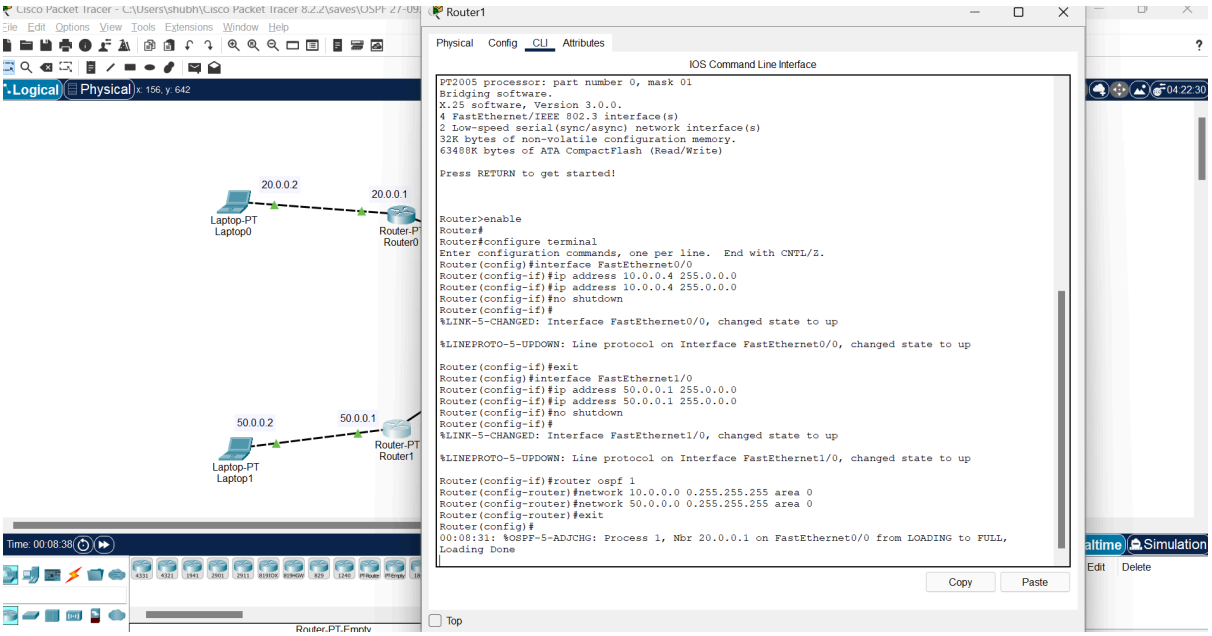
1. **Router Id –** It is the highest active IP address present on the router. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

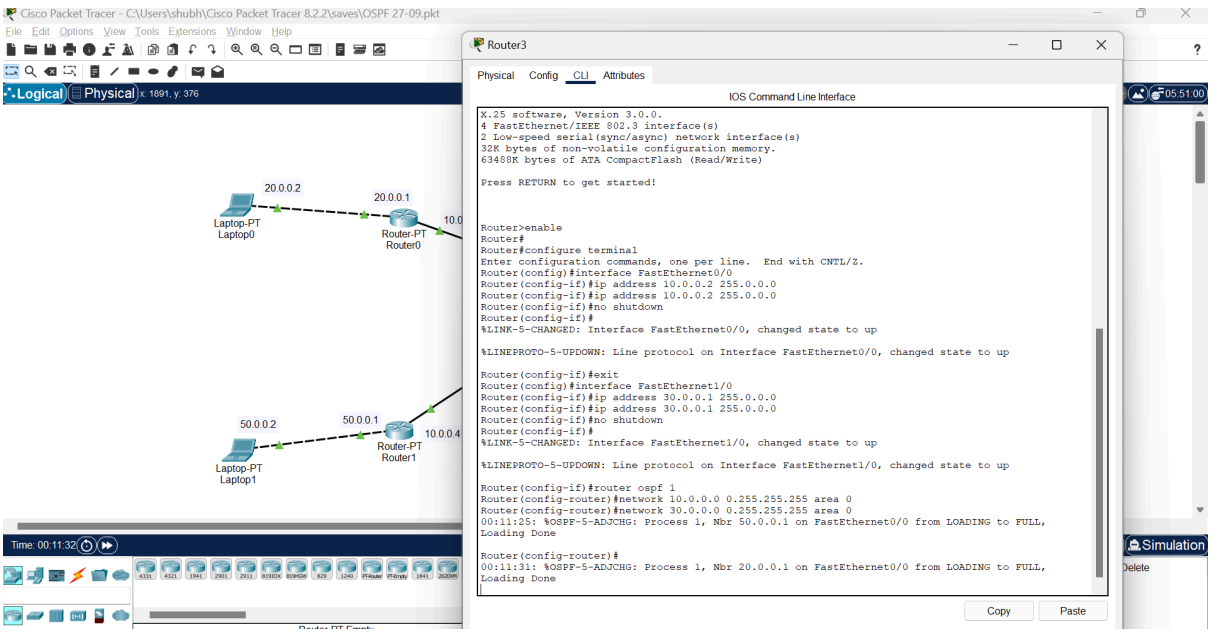
2. **Router priority –** It is an 8-bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

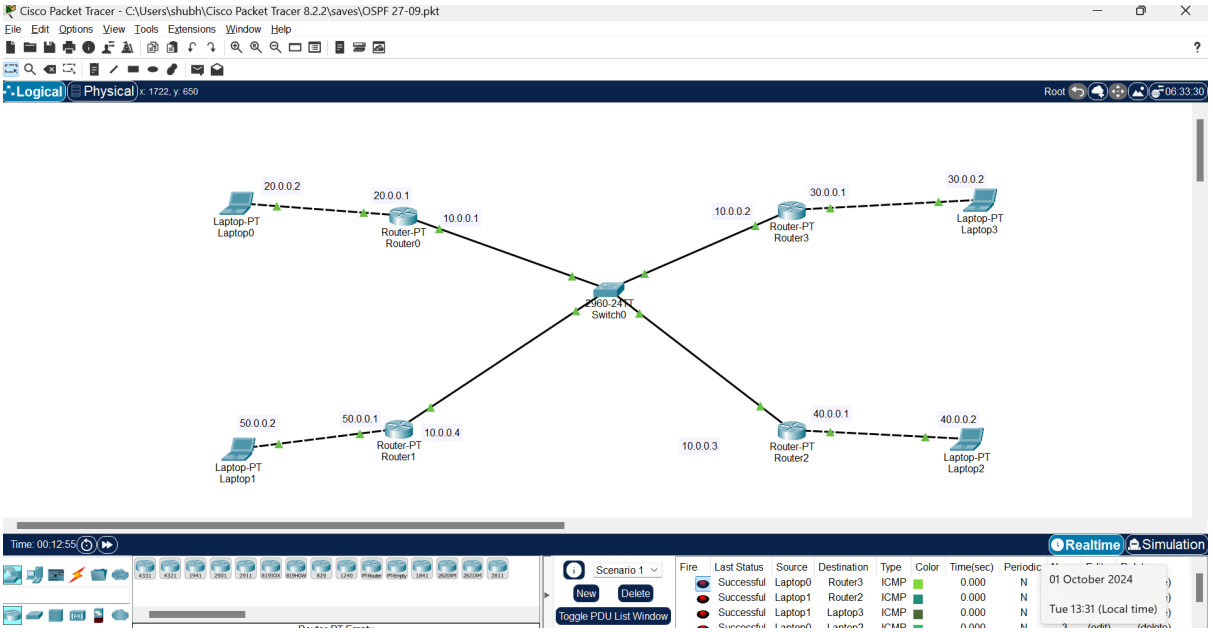
3. **Designated Router (DR) –** It is elected to minimize the number of adjacencies formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers share their DBD. In a broadcast network, the router requests for an update to DR, and DR will respond to that request with an update.

4. **Backup Designated Router (BDR) –** BDR is a backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

5. **DR and BDR election –** DR and BDR election takes place in the broadcast network or multi-access network. Here are the criteria for the election:







Router4

Physical Config CLI Attributes

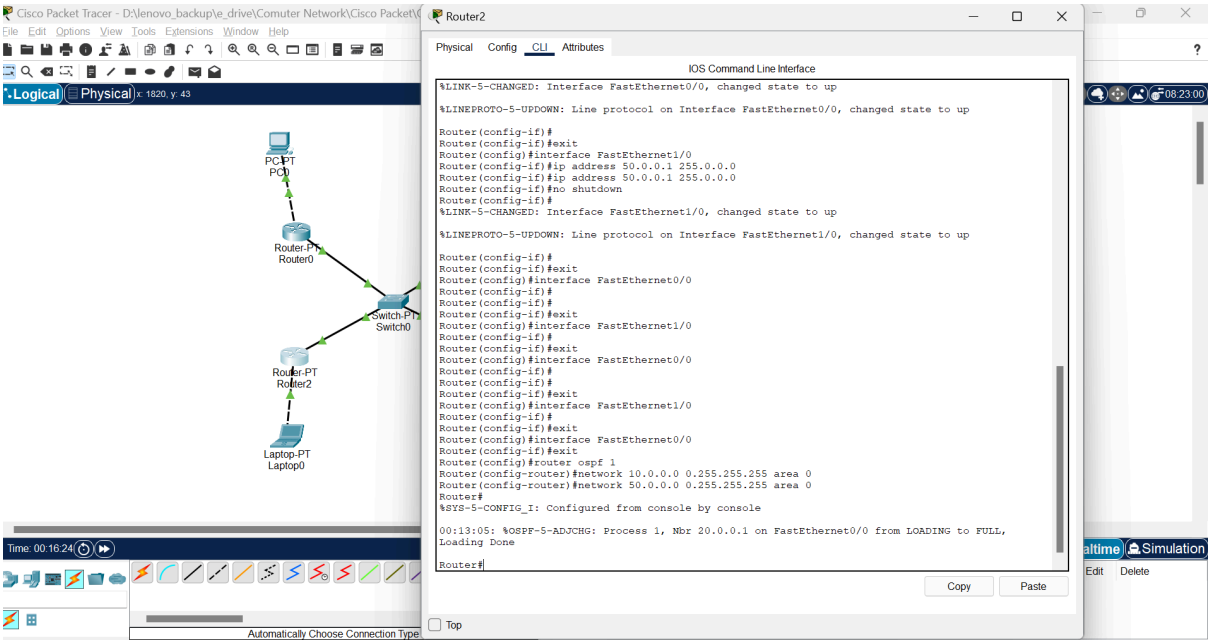
IOS Command Line Interface

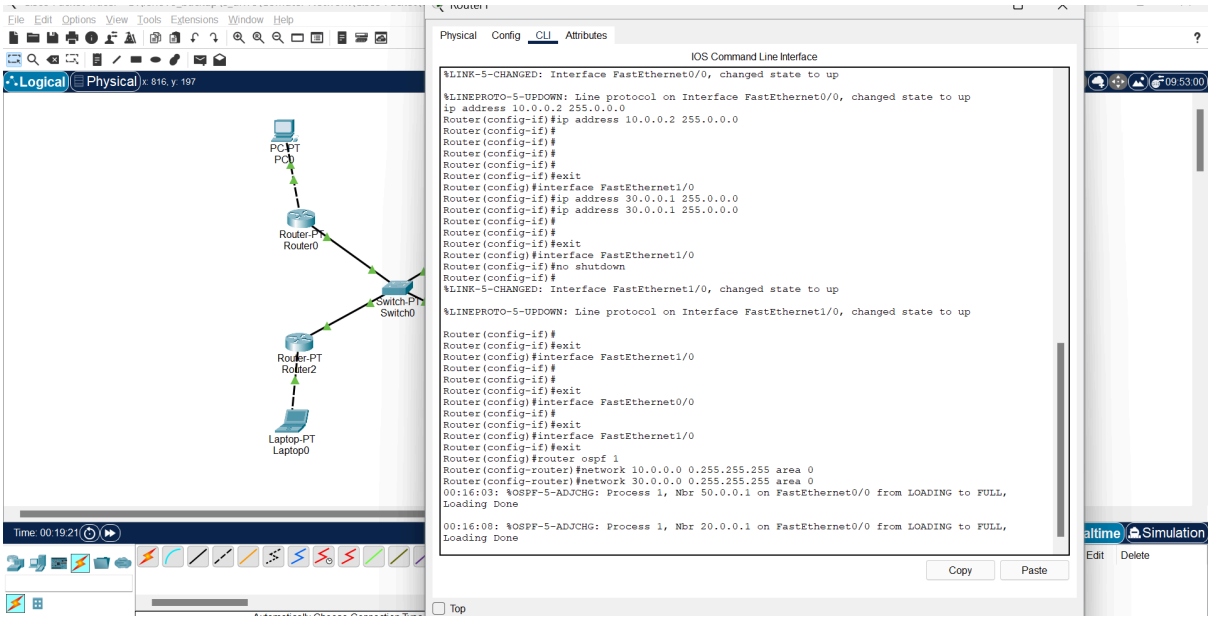
```
Press RETURN to get started!


Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 3
Router(config-router)#network 192.168.3.0 0.255.255.255 area 2
Router(config-router)#network 192.168.5.0 0.255.255.255 area 2
Router(config-router)#
00:34:03: %OSPF-5-ADJCHG: Process 3, Nbr 192.168.5.2 on Serial2/0 from LOADING to FULL, Loading
Done
exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

O    192.168.2.0/24 [110/65] via 192.168.5.2, 00:00:05, Serial2/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
O    192.168.4.0/24 [110/128] via 192.168.5.2, 00:00:05, Serial2/0
C    192.168.5.0/24 is directly connected, Serial2/0

Router#
```

Copy Paste

Top

My Dell





Configuring RIPv2

It supports classless Inter-Domain Routing (CIDR) and has the ability to carry subnet information, its metric is also hopping count, and max hop count 15. It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Advantages of RIP ver2 –

1. It's a standardized protocol.

2. Provides fast convergence.
3. It sends triggered updates when the network changes.
4. Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIP ver2 – There lies some disadvantages as well:

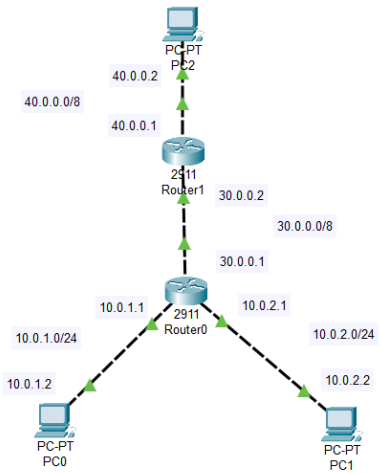
1. Max hop count of 15, due to the 'count-to-infinity' vulnerability.
2. No concept of neighbours.
3. Exchanges entire table with all neighbours every 30 seconds (except in the case of a triggered update).

Steps to configure RIPv2:

Step 1: Select the End Devices category and in the End Devices sub-category, select and drag 3 PCs as shown in the illustration below in the workspace.

Step 2: Select the Network Devices category and drag 2 2911 routes from the Router sub-category into the workspace.

Step 3: Connect all devices using crossover with the cables as shown below.



Step 4: Assign IPs to PCs using the same method as described in the previous section.

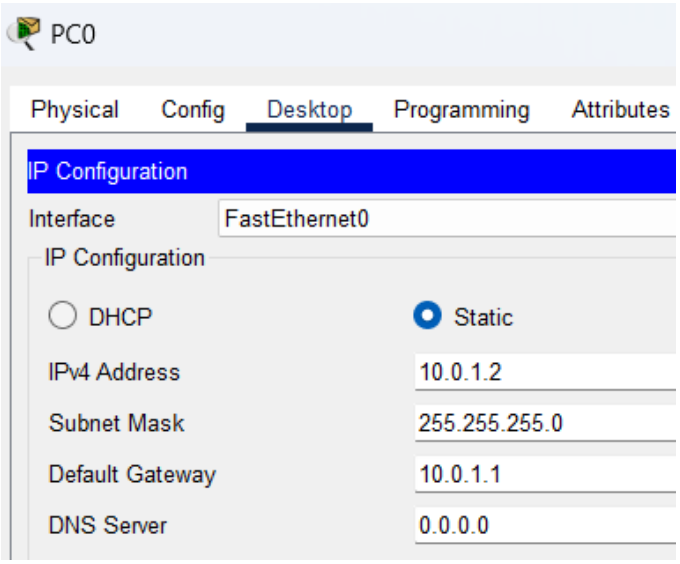


Fig4.13

Step 5: Configure Router interface IPs according to the above topology diagram using the same commands described in the previous section.

Step 6: Now for Routing using RIP v2, open the CLI in routers and enter the following commands, for Router 0

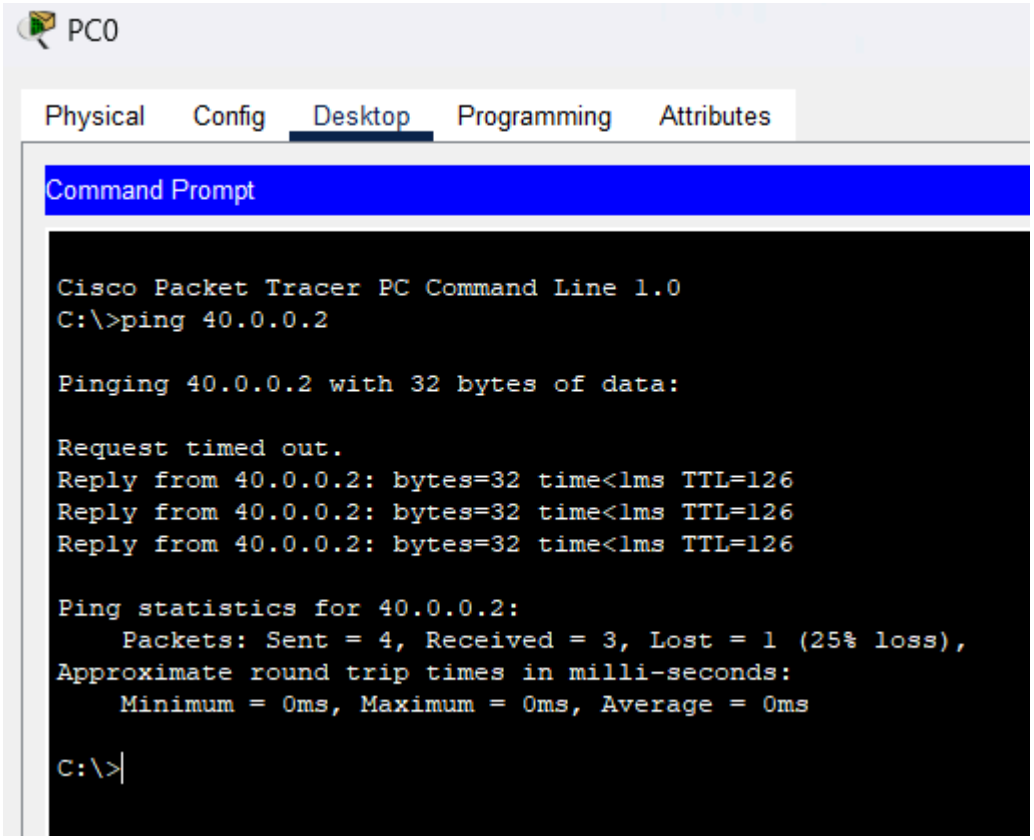
```
Router>enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 10.0.1.0
Router(config-router)#network 10.0.2.0
Router(config-router)#network 30.0.0.0
Router(config-router)#version 2
```

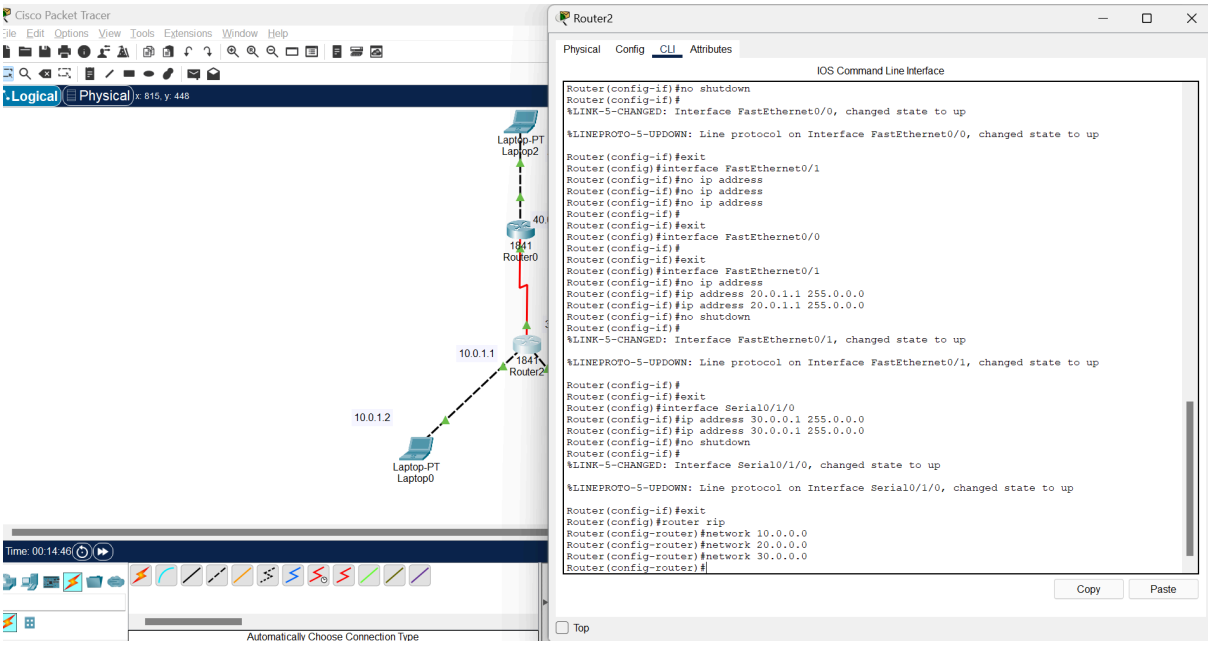
and similarly, configure RIPv2 on other routers using the same syntax with their directly connected networks.

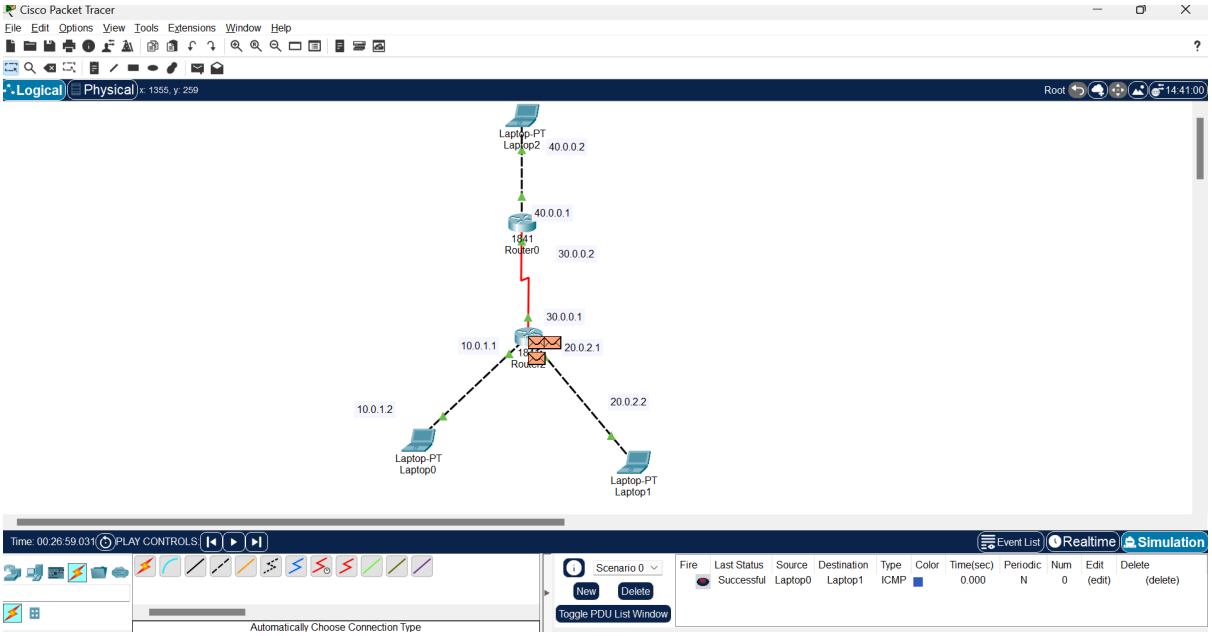
Step 7: Connectivity can be confirmed by ping utility, below is an example where we ping PC2 using PC0.

RIP Configuration through Packet Tracer:

Router:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 40.0.0.2
Pinging 40.0.0.2 with 32 bytes of data:
Request timed out.
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126
Ping statistics for 40.0.0.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>


Cisco Packet Tracer
Logical
Physical
Laptop-PT
Laptop2
1841
Router0
10.0.1.1
1841
Router2
10.0.1.2
Laptop-PT
Laptop0
Time: 00:14:46
Automatically Choose Connection Type
Router2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no ip address
Router(config-if)#no ip address
Router(config-if)#no ip address
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no ip address
Router(config-if)#ip address 20.0.1.1 255.0.0.0
Router(config-if)#ip address 20.0.1.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#
Copy
Paste
Top



Experiment No: 05

Name of Student: _____

Roll Number: _____ **Class:** _____

5. **TITLE:** Static, Dynamic NAT and Virtual LAN

AIM: Case study on Network Address Translation. Configure

A. Static, Dynamic NAT
B. Virtual LAN.

Objective: To study network simulator. To learn different routing commands and configure Static NAT ,Dynamic NAT and VLAN for given network. Candidate is expected to know the theory involved in the experiment.

Software /Hardware Requirement:

Sr.No	Name of Software and Hardware	Latest Version
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

Network Address Translation (NAT)

Network Address Translation (NAT) allows private IP addresses to be translated into public IP addresses when communicating with external networks.

The three types of NAT are:

1. Static NAT: Maps a single internal IP address to a single public IP address.
2. Dynamic NAT: Maps a group of internal IP addresses to a pool of public addresses.
3. PAT (Port Address Translation): Multiple internal IP addresses share a single public IP address using different port numbers.

Access Control Lists (ACLs)

Access Control Lists (ACLs) are used in networking to permit or deny traffic based on criteria such as IP addresses, protocols, or ports.

1. Standard ACLs: Filter traffic based only on the source IP address.
2. Extended ACLs: Provide more granular control by filtering traffic based on source and destination IP addresses, protocols, and port numbers.

VLANs (Virtual Local Area Networks)

VLANs (Virtual Local Area Networks): Used to segment network traffic, providing security and efficient use of network resources.

DTP (Dynamic Trunking Protocol): Negotiates trunking between switches dynamically, allowing VLAN information to be shared.

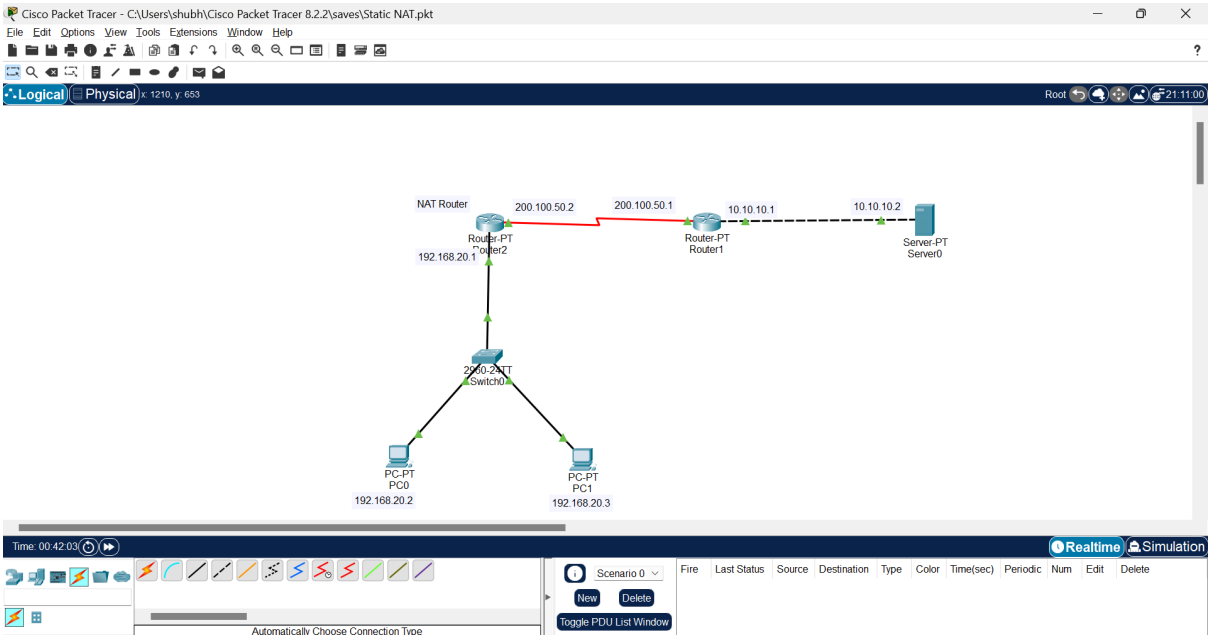
STP (Spanning Tree Protocol): Ensures a loop-free network topology by blocking redundant paths and providing backup links.

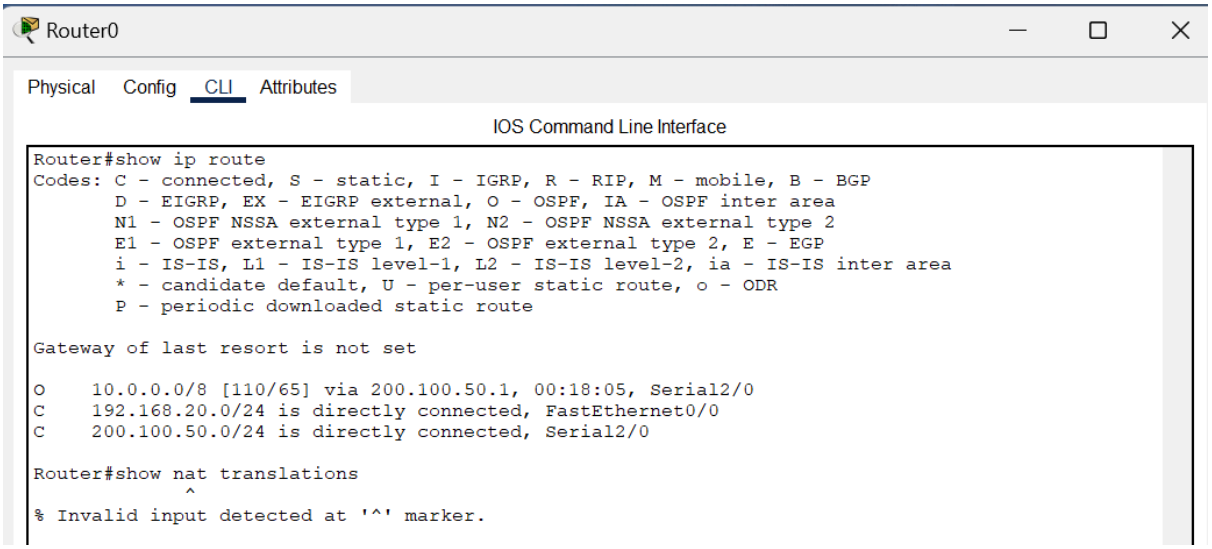
Static NAT

Step1: Make topology as shown below.

Step 2: configure Pc's and Routers with IP's Shown.

Step 3: Configure router with OSPF protocol to establish connectivity





Step 4: Configure router ports as inside and outside

- Configure the interface in the outside local as:
    - ip nat outside
- Configure the interface in the inside local as:
    - ip nat inside

step 5: Lastly, enable Static Nat by using the command:

Router(config)#ip nat inside source
static <inside-local-ip> <inside-global-ip>
R1(config)#int GigabitEthernet0/1
R1(config-if)#ip nat outside
R1(config-if)#exit

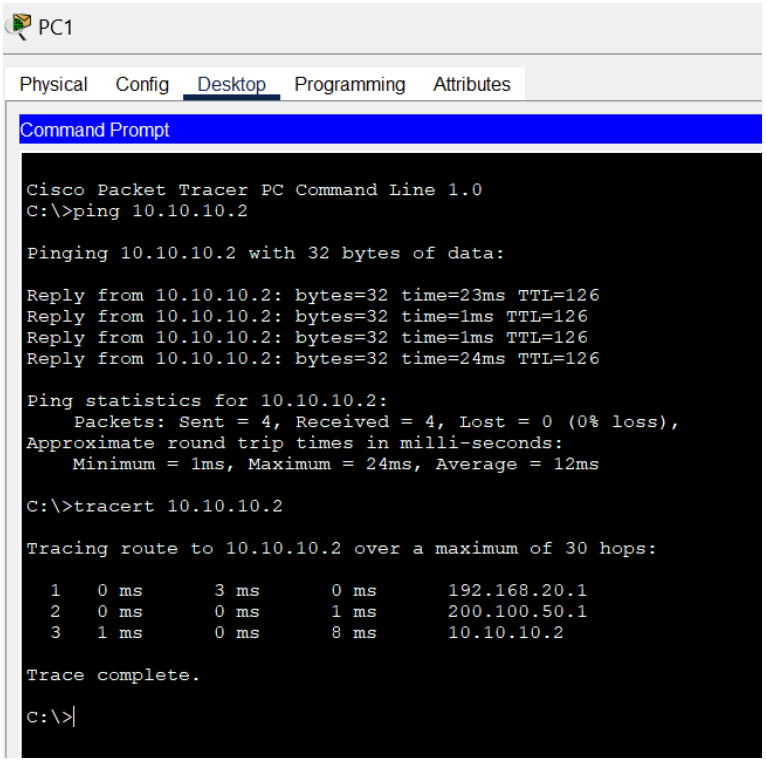
R1(config)#int GigabitEthernet0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#ip nat intside source static 192.168.20.10 200.100.50.1

Step 6: to Verify NAT use command as:

Router#Show ip nat translations

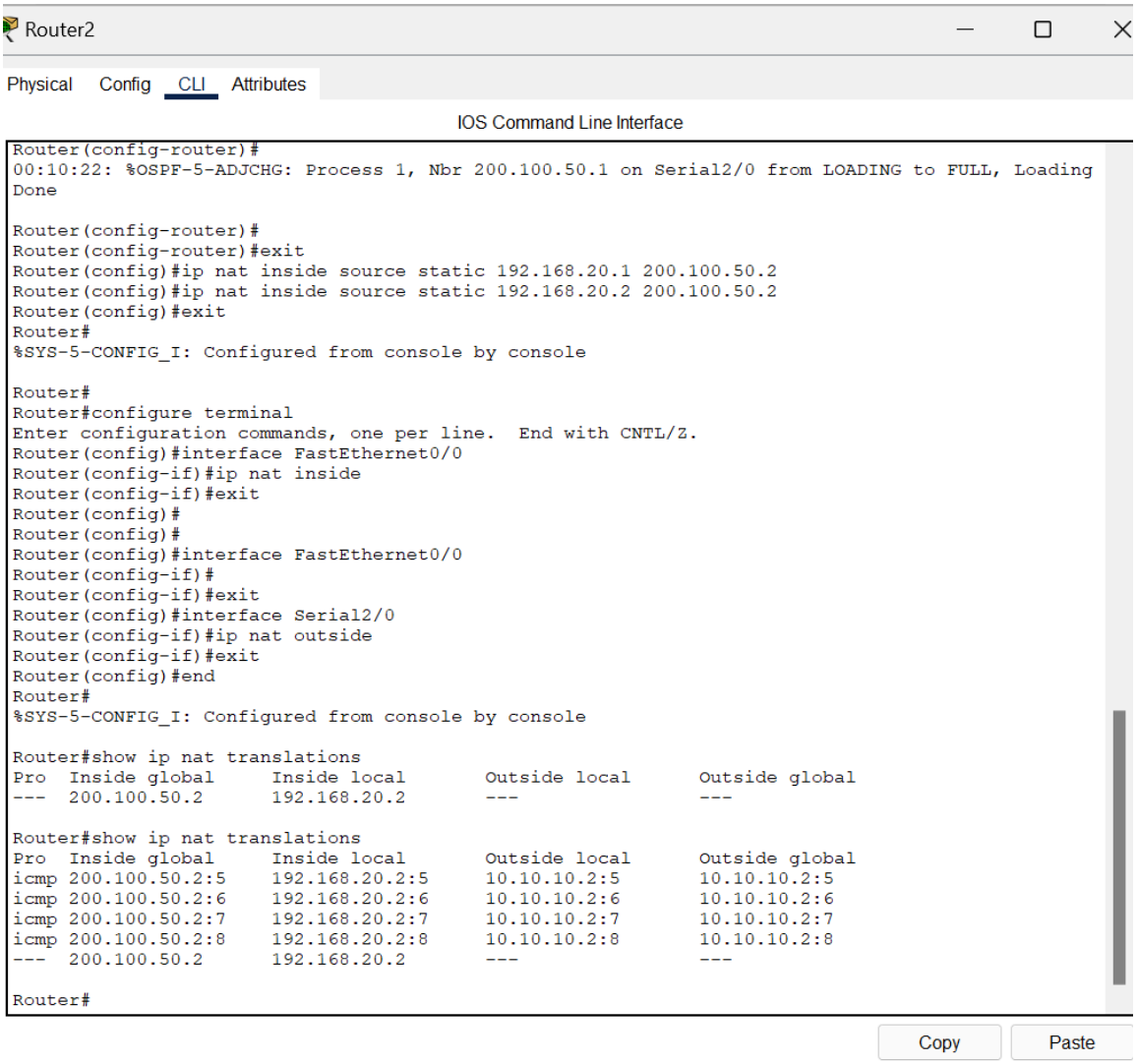
Initially without any data transmission it will not show any Translations.

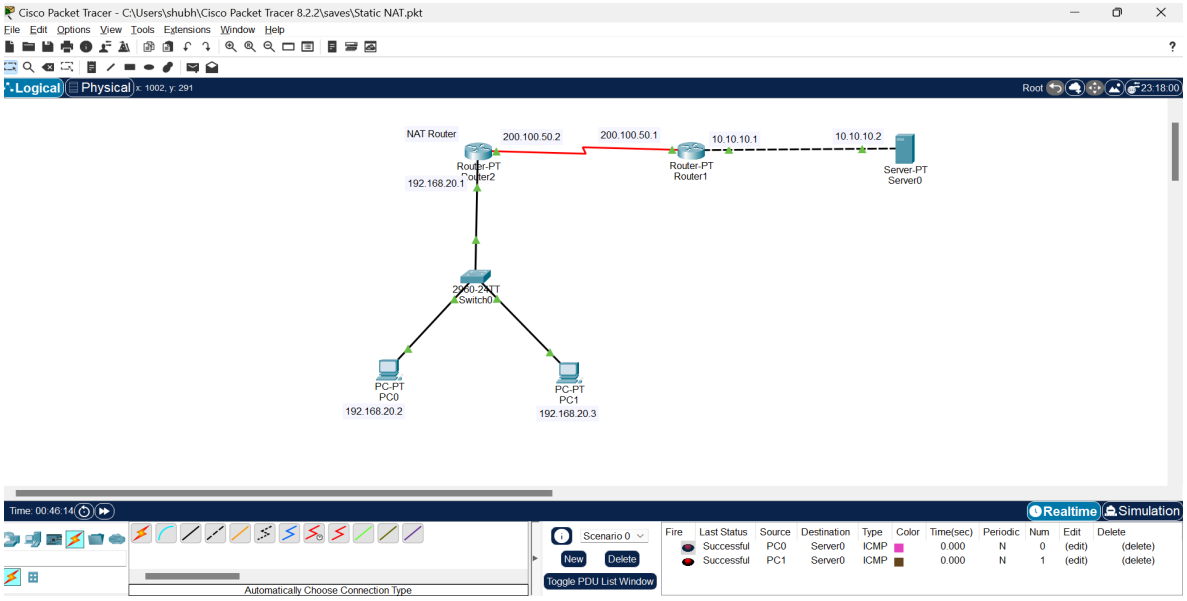
Step 7: use ping 10.10.10.20 on command prompt of PC 0.



Step 8: Then again use command on CLI as:

Router#Show IP nat translations





Dynamic NAT

Configuration for Dynamic NAT is same as static Nat till step 4.

Step 5: Create an access list to permit a certain network of IP addresses

Router(config)#access-list <acl-number> permit <source-ip-network><wildcard-mask>

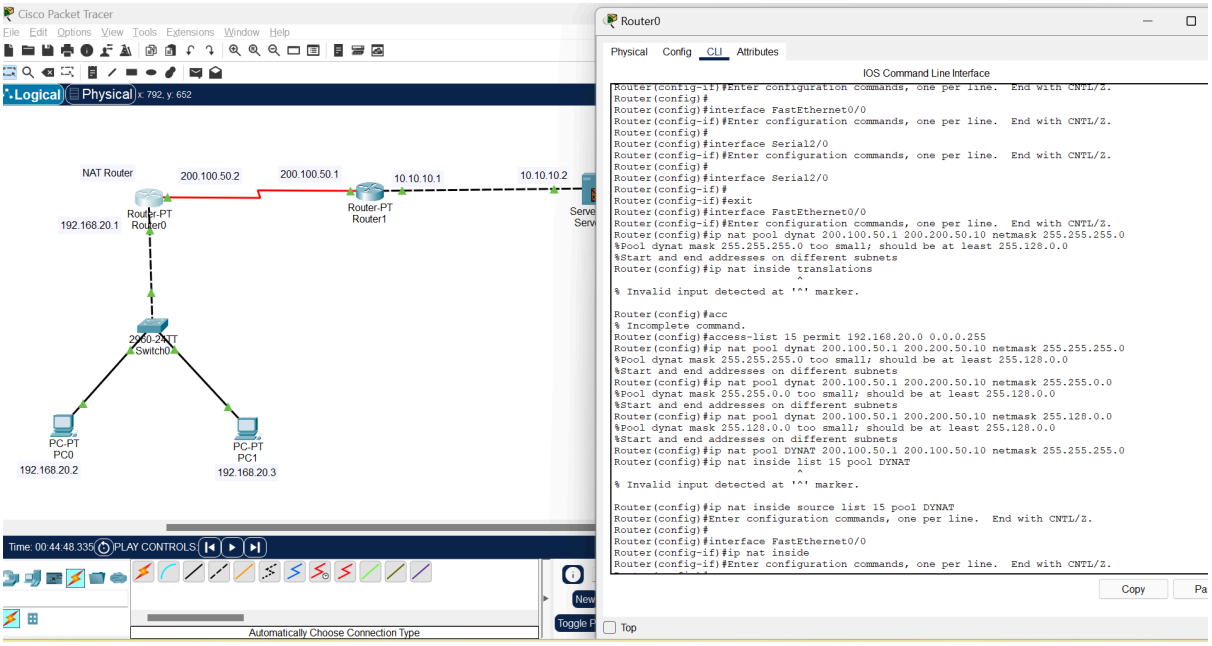
Step 6: Create a pool of Global IP addresses

Router(config)#ip nat pool <pool-name><starting-IP> <ending-IP> prefix-length <prefix-length>

Step 7: Lastly, enable Dynamic NAT by using the command:

Router(config)#ip nat inside source list <acl-number> pool <pool-name>

```
Router(config)# access-list 15 permit 192.168.20.0 0.0.0.255
Router(config)#ip nat pool dynat 200.100.50.1 200.100.50.10 netmask 255.255.255.0
Router(config)#ip nat inside source list 15 pool dynat
```

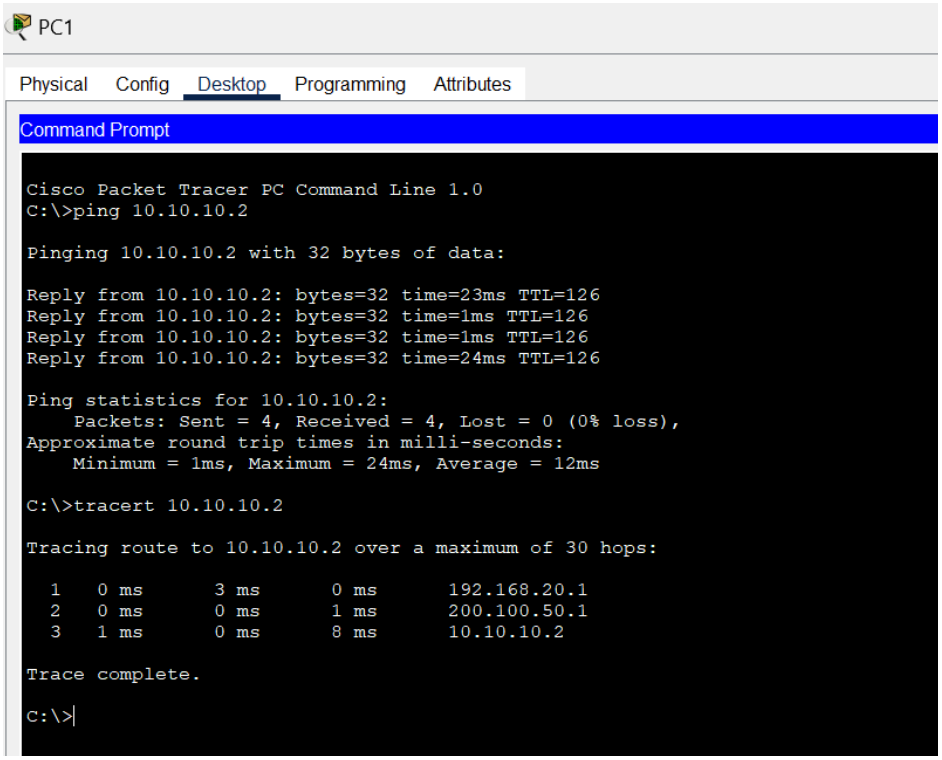


Step 8: To Verify Dynamic NAT use command as:

Show ip nat translations

Initially without any data transmission it will not show any Translations.

Step 7: use ping 10.10.10.20 on command prompt of PC 0.



Step 8: Use following command to check Dynamic Nat configuration. It will show following output

Router#ip Nat translations

```
Router#show ip nat translations
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.3:10   192.168.20.2:10    10.10.10.2:10      10.10.10.2:10
icmp 200.100.50.3:11   192.168.20.2:11    10.10.10.2:11      10.10.10.2:11
icmp 200.100.50.3:8    192.168.20.2:8     10.10.10.2:8       10.10.10.2:8
icmp 200.100.50.3:9    192.168.20.2:9     10.10.10.2:9       10.10.10.2:9

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.3:10   192.168.20.2:10    10.10.10.2:10      10.10.10.2:10
icmp 200.100.50.3:11   192.168.20.2:11    10.10.10.2:11      10.10.10.2:11
icmp 200.100.50.3:12   192.168.20.2:12    10.10.10.2:12      10.10.10.2:12
icmp 200.100.50.3:13   192.168.20.2:13    10.10.10.2:13      10.10.10.2:13
icmp 200.100.50.3:14   192.168.20.2:14    10.10.10.2:14      10.10.10.2:14
icmp 200.100.50.3:15   192.168.20.2:15    10.10.10.2:15      10.10.10.2:15
icmp 200.100.50.3:8    192.168.20.2:8     10.10.10.2:8       10.10.10.2:8
icmp 200.100.50.3:9    192.168.20.2:9     10.10.10.2:9       10.10.10.2:9

Router#
```

Router0

Physical Config CLI Attributes

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

O    10.0.0.0/8 [110/65] via 200.100.50.1, 00:18:05, Serial2/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
C    200.100.50.0/24 is directly connected, Serial2/0

Router#show nat translations
             ^
% Invalid input detected at '^' marker.

Router#show dynat translations
             ^
% Invalid input detected at '^' marker.

Router#show ip nat translations
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.3:10   192.168.20.2:10    10.10.10.2:10      10.10.10.2:10
icmp 200.100.50.3:11   192.168.20.2:11    10.10.10.2:11      10.10.10.2:11
icmp 200.100.50.3:8    192.168.20.2:8     10.10.10.2:8       10.10.10.2:8
icmp 200.100.50.3:9    192.168.20.2:9     10.10.10.2:9       10.10.10.2:9

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.3:10   192.168.20.2:10    10.10.10.2:10      10.10.10.2:10
icmp 200.100.50.3:11   192.168.20.2:11    10.10.10.2:11      10.10.10.2:11
icmp 200.100.50.3:12   192.168.20.2:12    10.10.10.2:12      10.10.10.2:12
icmp 200.100.50.3:13   192.168.20.2:13    10.10.10.2:13      10.10.10.2:13
icmp 200.100.50.3:14   192.168.20.2:14    10.10.10.2:14      10.10.10.2:14
icmp 200.100.50.3:15   192.168.20.2:15    10.10.10.2:15      10.10.10.2:15
icmp 200.100.50.3:8    192.168.20.2:8     10.10.10.2:8       10.10.10.2:8
icmp 200.100.50.3:9    192.168.20.2:9     10.10.10.2:9       10.10.10.2:9

Router#
```

Experiment No: 06

Name of Student: _____

Roll Number: _____ **Class:** _____

TITLE: Socket programming

AIM: To Implement Socket programming using C/C++/Java:

i. TCP Client, TCP Server
ii. UDP Client, UDP Server

Objective: To study network simulator. To implement communication between Client Serve. Candidate is expected to know the theory involved in the experiment.

Software /Hardware Requirement:

Sr.No	Name of Software and Hardware	Latest Version
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

What is TCP/IP?

TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocols that define

the standards for transmitting data over computer networks, including the internet. The TCP/IP protocol is the foundation of the internet and enables devices to communicate with each other using a common language.

What is UDP?

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections over the network. The UDP enables process-to-process communication.

Socket Programming Overview

Sockets provide a way for programs to communicate with each other over a network. They are an abstraction over the network protocols (TCP/UDP) that allows for data exchange between devices over a network.

• TCP (Transmission Control Protocol):

TCP provides reliable, ordered, and error-checked delivery of a stream of data between applications. It's connection-oriented, meaning it establishes a connection between a client and server before data transfer.

• UDP (User Datagram Protocol):

UDP is a simpler, connectionless protocol. It provides a means to send datagrams without the overhead of establishing a connection, making it faster but less reliable than TCP.

TCP Client/Server Concept:

• The TCP Server listens for incoming client requests on a specific port. Once a connection is established, data can be exchanged between the server and multiple clients using separate threads or processes.

• The TCP Client connects to the server using the server's IP address and port number, initiating the communication.

UDP Client/Server Concept:

• The UDP Server listens for incoming datagrams from clients. It doesn't require a connection to be established and waits to receive data from clients.

• The UDP Client sends datagrams to the server, which processes and optionally replies to the client.

Program:(to Print with o/p)

Implement a TCP Client and TCP Server.

1.Client.java

```
import java.io.*;
import java.net.*;
class Client
{
public static void main(String args[]) throws Exception
{
 String line, newLine;
 try
 {
DataInputStream in=new DataInputStream(System.in);
Socket cs=new Socket("LocalHost", 6789);
System.out.println("Client Started...");
DataInputStream inp=new DataInputStream (cs.getInputStream());
DataOutputStream out=new DataOutputStream(cs.getOutputStream());
while(true) {
newLine = in.readLine();
if (newLine.equals("q")) {
out.writeBytes("Client is down..." +"\n");
return;
```

```
} else {
out.writeBytes(newLine + "\n");
}
line = inp.readLine();
System.out.println("Received from server. "+line);
}
}
catch(Exception e)
{
}
}
}
```

2.server.java

```
import java.io.*;
import java.net.*;
class server
{
public static void main(String args[]) throws Exception {
try
{
String line, newLine;
ServerSocket ss=new ServerSocket(6789);
while(true)
{
Socket s=ss.accept();
System.out.println("Server Started...");
DataInputStream inp=new DataInputStream(s.getInputStream());
DataOutputStream out = new DataOutputStream(s.getOutputStream());
DataInputStream in=new DataInputStream(System.in);
while(true) {
System.out.println("Press 'q' if you want to exit server"); line =
inp.readLine();
System.out.println("Received from client: " + line);
newLine = in.readLine();
if (newLine.equals("q")) {
```

```
out.writeBytes("Server is down..." +'\n');
return;
} else {
out.writeBytes(newLine + '\n');
}
}
}
}
catch(Exception e) {
}
}
}
```

Implement a UDP Client and UDP Server.

1.UDPClient.java

```
import java.io.*;
import java.net.*;
class UDPClient {
public static void main(String args[]) throws Exception {
DatagramSocket clientSocket = new DatagramSocket();
byte[] sendData = new byte[1024];
byte[] receiveData = new byte[1024];
BufferedReader inFromUser = new BufferedReader(new
InputStreamReader(System.in));
InetAddress IPAddress = InetAddress.getByName("localhost");
String sentence = inFromUser.readLine();
sendData = sentence.getBytes();
DatagramPacket sendPacket = new DatagramPacket(sendData,
sendData.length, IPAddress, 8080);
clientSocket.send(sendPacket);
DatagramPacket receivePacket = new DatagramPacket(receiveData,
receiveData.length);
clientSocket.receive(receivePacket);
String modifiedSentence = new String(receivePacket.getData());
System.out.println("FROM SERVER: " + modifiedSentence);
clientSocket.close();
```

```
}
}
```

2.UDPServer.java

```
import java.io.*;
import java.net.*;
class UDPServer {
 public static void main(String args[]) throws Exception {
 DatagramSocket serverSocket = new DatagramSocket(8080);
 byte[] receiveData = new byte[1024];
 byte[] sendData = new byte[1024];
 while (true) {
 DatagramPacket receivePacket = new DatagramPacket(receiveData,
receiveData.length);
 serverSocket.receive(receivePacket);
 String sentence = new String(receivePacket.getData()).trim();
 System.out.println("RECEIVED: " + sentence);
 InetAddress IPAddress = receivePacket.getAddress();
 int port = receivePacket.getPort();
 String capitalizedSentence = sentence.toUpperCase();
 sendData = capitalizedSentence.getBytes();
 DatagramPacket sendPacket = new DatagramPacket(sendData,
sendData.length, IPAddress, port);
 serverSocket.send(sendPacket);
 }
 }
}
```

Experiment No: 07

Name of Student: _____

Roll Number: _____ **Class:** _____

6. **TITLE:** Introduction to server administration

2. **AIM:** Introduction to server administration (server administration commands and their applications) and configuration of any three of below Server: (Study/Demonstration Only) FTP, Web Server, DHCP, Telnet, Mail, DNS

Objective: To study administration techniques for different servers. To understand different protocols and their working Candidate should be able to tell different administrative commands and their applications.

Software /Hardware Requirement:

Sr.No	**Name of Software and Hardware**	**Latest Version**
1	Windows	10/11
2	Packet Tracer	8.2

Theory:

What is FTP?

File Transfer Protocol, or FTP, is a protocol used for transferring files from one computer to

another - typically from your computer to a web server. FTP is the preferred method of exchanging files because it's faster than other protocols like HTTP or POP. If you need to exchange large files, you should consider FTP.

FTP data is sent and received through computer port 21 and under the TCP protocol. The transfer is asynchronous, meaning not at the same time, and therefore faster than other protocols.

Objectives of FTP were:

1. to promote sharing of files (computer programs and/or data),
2. to encourage indirect or implicit (via programs) use of remote computers,
3. to shield a user from variations in file storage systems among hosts, and to transfer data reliably and efficiently. The USER-PI is responsible for establishing the connection with the FTP server, sending FTP commands, receiving responses from the SERVER-PI and controlling the USER-DTP if needed.

What is web Server?

Web server is a program which processes the network requests of the users and serves them with files that create web pages. This exchange takes place using Hypertext Transfer Protocol (HTTP).Web servers are computers used to store HTTP files which makes a website and when a client requests a certain website, it delivers the requested website to the client.

For example, you want to open Facebook on your laptop and enter the URL in the search bar of google. Now, the laptop will send an HTTP request to view the Facebook webpage to another computer known as the webserver. This computer (webserver) contains all the files (usually in HTTP format) which make up the website like text, images, gif files, etc. After processing the request, the webserver will send the requested website-related files to your computer and then you can reach the website.

What is DHCP ?

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to assign IP addresses and provide configuration information to devices such as servers, desktops, or mobile devices, so they can communicate on a network using the Internet Protocol (IP). ISC DHCP is a collection of software that implements all aspects of the DHCP (Dynamic Host Configuration Protocol) suite. It includes:

- A DHCP server, which receives clients' requests and replies to them.
- A DHCP client, which can be bundled with the operating system of a client computer or other IP capable device and which sends configuration requests to the server. Most devices and operating systems already have DHCP clients included.
- A DHCP relay agent, which passes DHCP requests from one LAN to another so that there need not be a DHCP server on every LAN.

The DHCP server, client and relay agent are provided both as reference implementations of the protocol and as working, fully-featured sample implementations. Both the client and the server provide functionality that, while not strictly required by the protocol, is very useful in practice. The DHCP server also makes allowances for non-compliant clients that need to be supported. The ISC DHCP server will answer requests from any client that complies with the protocol standards, and the ISC DHCP client can interact with any server that complies with those standards. The components of ISC DHCP need not all be used together. That is, after all, the purpose behind the published standards. The latest ISC DHCP software includes cryptographic software.

TENET:

TELNET stands for Teletype Network. It is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet. The local computer uses a telnet client program and the remote computers use a telnet server program. In this article, we will discuss every point about TELNET.

TELNET is a type of protocol that enables one computer to connect to the local computer. It is used as a standard **TCP/IP protocol** for virtual terminal service which is provided by **ISO**. The computer which starts the connection is known as the **local computer**. The computer which is being connected to i.e. which accepts the connection known as the **remote computer**. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle.

MAIL

Mail Server, similar to the post office, is a computer system program responsible for receiving, routing, delivering e-mail. It is also known as MTA (Mail Transfer Agent) and store incoming mail for distribution to users and deliver e-mail to client computers.

Example: Yahoo!, Gmail incoming mail server, Gmail outgoing mail server, etc.

DNS:

Domain Name System (DNS) Zones is any distinct, connecting segment of domain name space in Domain Name System (DNS) for which administrative responsibility has been delegated to single administrative space which allows for more smooth control of DNS components. Namespace of web is organized into hierarchical layout of subdomains below DNS root domain. Individual domains of this tree may function as delegation points for administrative authority and management.

Conclusion: Server administration is an important part of managing and maintaining a server.

Server administers a variety of tools and technique to manage their servers including server administration command, configuration, and monitoring. Thus we learnt about DHCP, Telnet, DNS etc.