EXPERIMENT – 1

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

PART 1: Wireshark

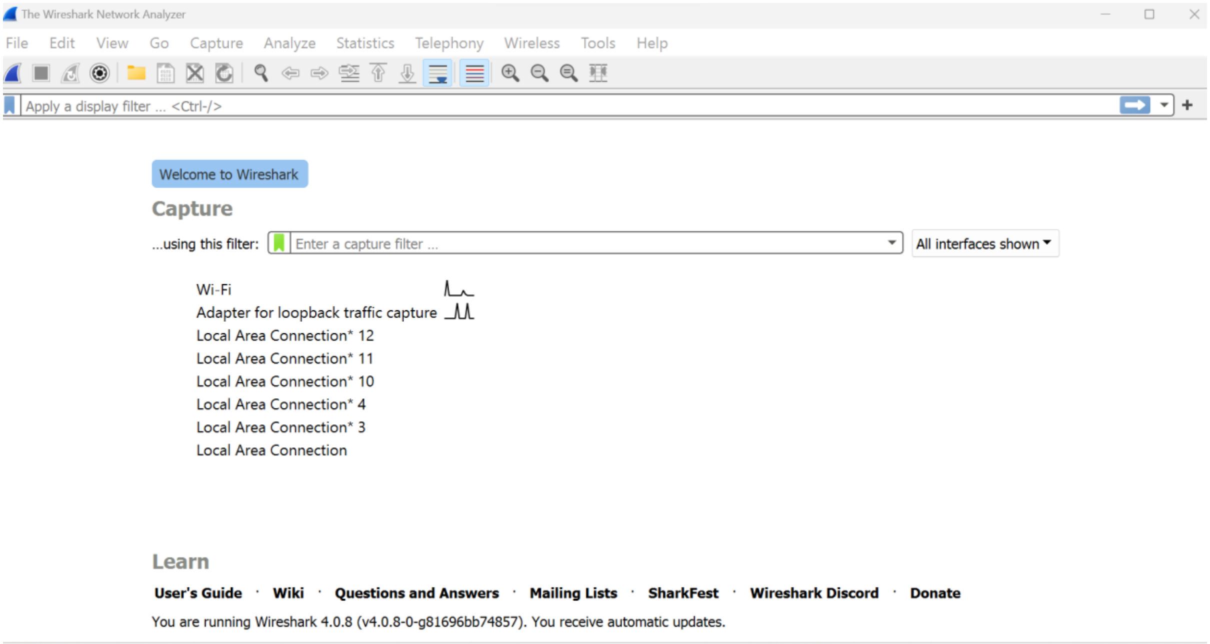
Background

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures (“sniffs”) messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine. A packet sniffer consists of two parts: 1) the packet capture library, which receives a copy of every link-layer frame that is sent from or received by your computer (Note: all messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable), 2) The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must “understand” the structure of all messages exchanged by protocols.

Wireshark is a popular packet sniffer application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, Wireshark "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications. Wireshark is a useful tool for anyone working with networks.

1. **Start Wireshark and begin capturing data.**

- On your PC, click the Windows Start button to see Wireshark listed as one of the programs on the pop-up menu. Double-click Wireshark.
- After Wireshark starts, click the capture interface to be used. Because we are using the WiFi connection on the PC, make sure the WiFi option is on the top of the list.

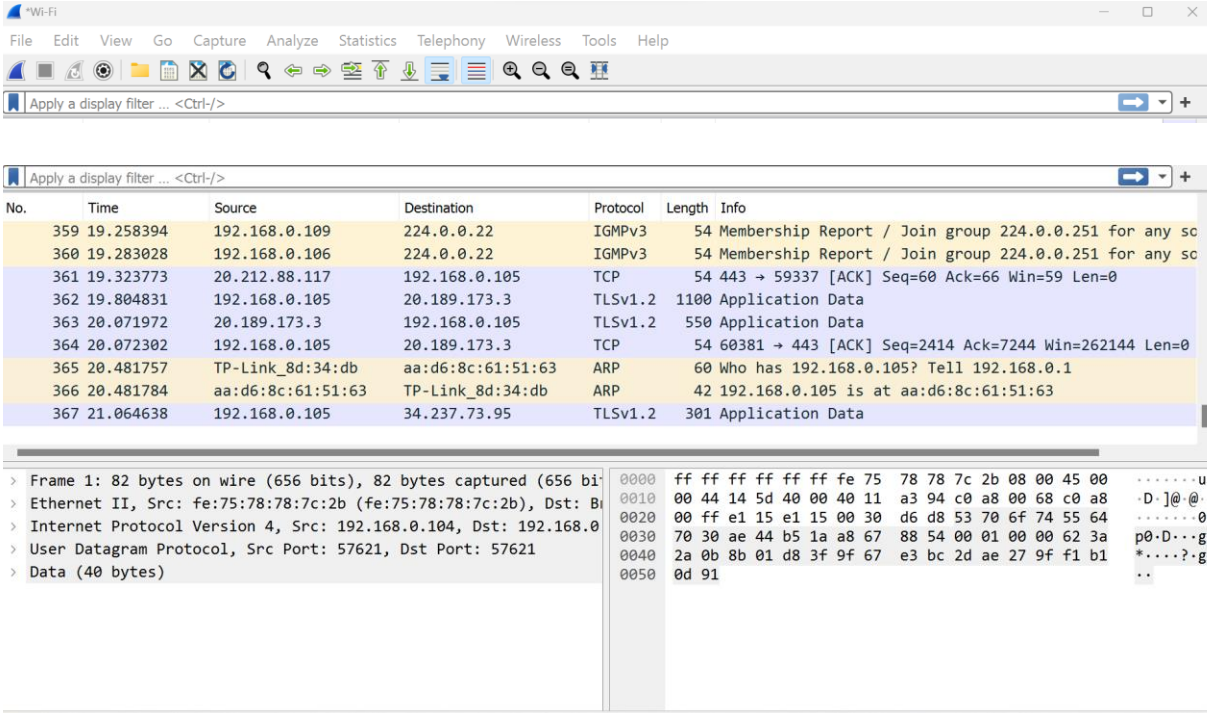

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 12
Local Area Connection* 11
Local Area Connection* 10
Local Area Connection* 4
Local Area Connection* 3
Local Area Connection

You are running Wireshark 4.0.8 (v4.0.8-0-g81696bb74857). You receive automatic updates.

- Manage the capture interface by clicking Capture and Options

- A list of interfaces will display. Make sure the capture interface is checked under Promiscuous.
  Note: We can further manage the interfaces on the PC by clicking Manage Interfaces. Verify that the description matches what you noted in Step 1b. Close the Manage Interfaces window after verifying the correct interface
- After you have checked the correct interface, click Start to start the data capture


*Wi-Fi
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Apply a display filter ... <Ctrl-/>

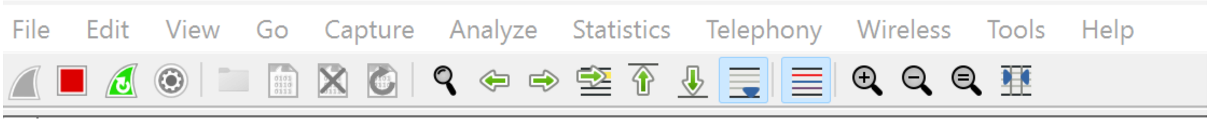
```
No.     Time        Source             Destination        Protocol  Length  Info
    359 19.258394   192.168.0.109      224.0.0.22         IGMPv3      54 Membership Report / Join group 224.0.0.251 for any sc
    360 19.283028   192.168.0.106      224.0.0.22         IGMPv3      54 Membership Report / Join group 224.0.0.251 for any sc
    361 19.323773   20.212.88.117      192.168.0.105      TCP         54 443 → 59337 [ACK] Seq=60 Ack=66 Win=59 Len=0
    362 19.804831   192.168.0.105      20.189.173.3       TLSv1.2   1100 Application Data
    363 20.071972   20.189.173.3       192.168.0.105      TLSv1.2    550 Application Data
    364 20.072302   192.168.0.105      20.189.173.3       TCP         54 60381 → 443 [ACK] Seq=2414 Ack=7244 Win=262144 Len=0
    365 20.481757   TP-Link_8d:34:db   aa:d6:8c:61:51:63  ARP         60 Who has 192.168.0.105? Tell 192.168.0.1
    366 20.481784   aa:d6:8c:61:51:63  TP-Link_8d:34:db   ARP         42 192.168.0.105 is at aa:d6:8c:61:51:63
    367 21.064638   192.168.0.105      34.237.73.95       TLSv1.2    301 Application Data
```

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bi
> Ethernet II, Src: fe:75:78:78:7c:2b (fe:75:78:78:7c:2b), Dst: Bı
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0
> User Datagram Protocol, Src Port: 57621, Dst Port: 57621
> Data (40 bytes)
```

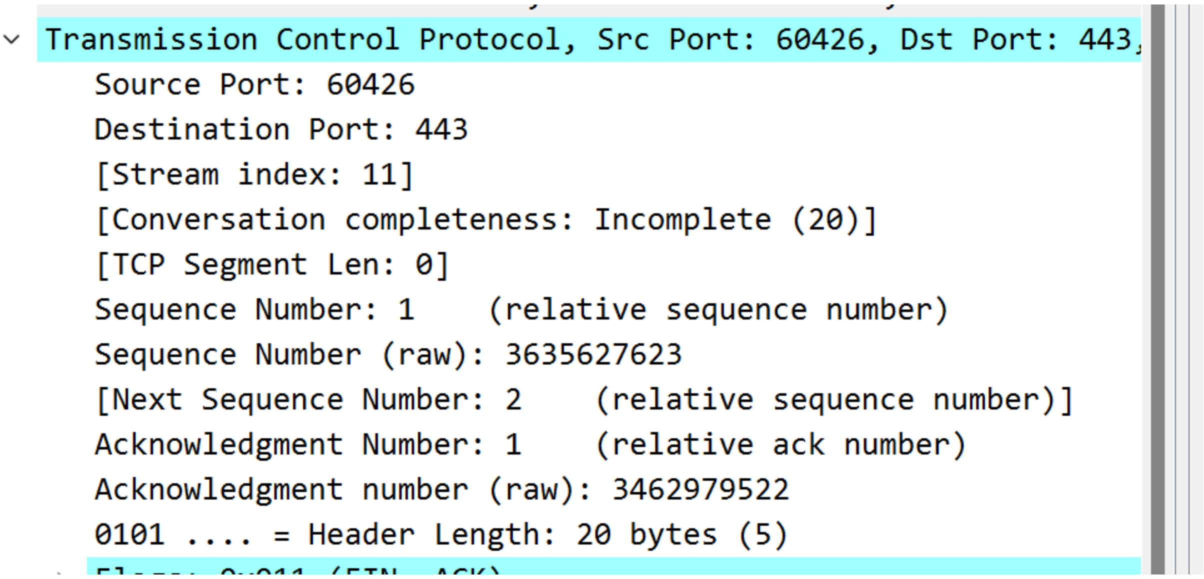
```
0000  ff ff ff ff ff ff fe 75  78 78 7c 2b 08 00 45 00   ·······u
0010  00 44 14 5d 40 00 40 11  a3 94 c0 a8 00 68 c0 a8   ·D·]@·@·
0020  00 ff e1 15 e1 15 00 30  d6 d8 53 70 6f 74 55 64   ·······0
0030  70 30 ae 44 b5 1a a8 67  88 54 00 01 00 00 62 3a   p0·D···g
0040  2a 0b 8b 01 d8 3f 9f 67  e3 bc 2d ae 27 9f f1 b1   *····?·g
0050  0d 91                                              ··
```

Note: You can also start the data capture by clicking the Wireshark icon in the main interface. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

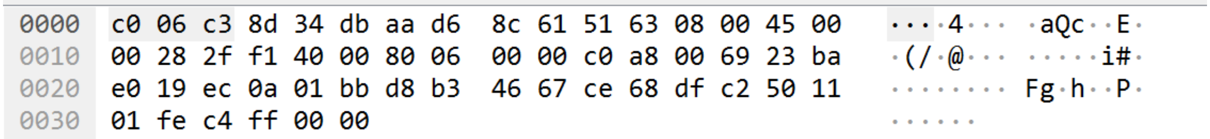
- Stop capturing data by clicking the Stop Capture icon.



2. **Examine the captured data.**
   examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed; 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form



```
Transmission Control Protocol, Src Port: 60426, Dst Port: 443,
    Source Port: 60426
    Destination Port: 443
    [Stream index: 11]
    [Conversation completeness: Incomplete (20)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3635627623
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3462979522
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x011 (FIN, ACK)
```

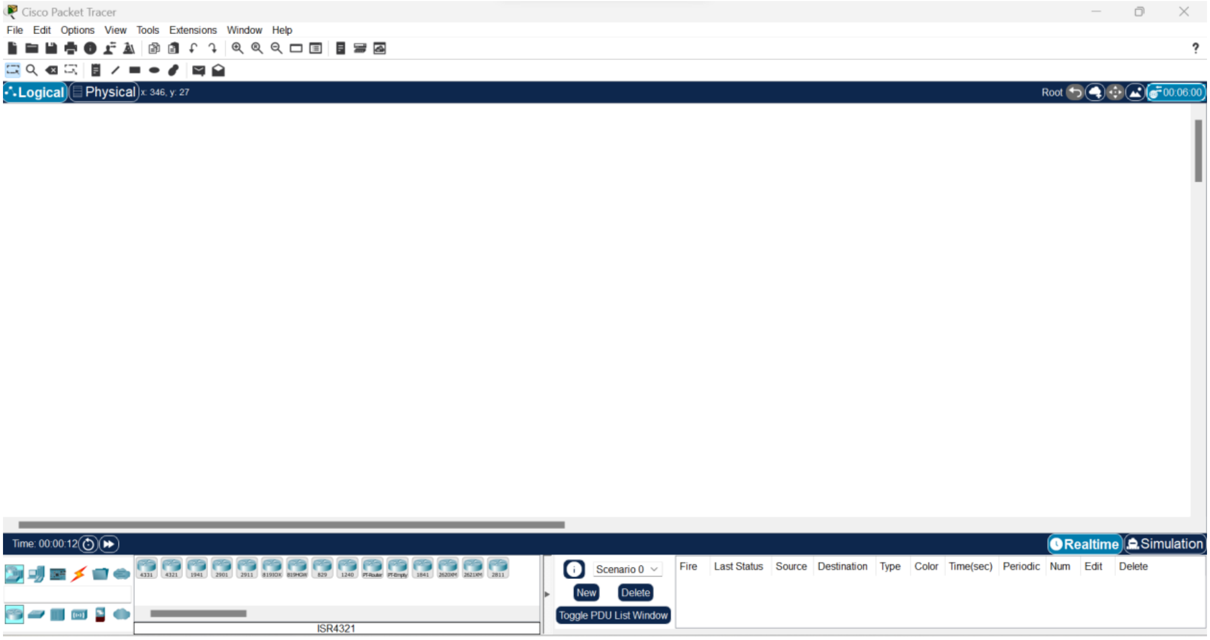


```
0000  c0 06 c3 8d 34 db aa d6  8c 61 51 63 08 00 45 00   ····4···  ·aQc··E·
0010  00 28 2f f1 40 00 80 06  00 00 c0 a8 00 69 23 ba   ·(/·@···  ·····i#·
0020  e0 19 ec 0a 01 bb d8 b3  46 67 ce 68 df c2 50 11   ········  Fg·h··P·
0030  01 fe c4 ff 00 00                                  ······
```

PART 2: Cisco Packet Tracer

Background

Packet Tracer is a protocol simulator developed by Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.



Packet Tracer - Help and Navigation

1. **Access the Packet Tracer Help pages, tutorial videos, and online resources**

i. Access the Packet Tracer Help pages in two ways:

- Click the question mark icon in the top, right-hand corner of the menu toolbar.
- Click the Help menu, and then choose Contents.

ii. Access the Packet Tracer tutorial videos by clicking Help > Tutorials. These videos are a visual demonstration of the information found in the Help pages and various aspects of the

Packet Tracer software program. Before proceeding with this activity, you should gain some familiarity with the Packet Tracer interface and Simulation mode

- View the Interface Overview video in the Getting Started section of Tutorials.
- View the Simulation Environment video in the Realtime and Simulation Modes section of Tutorials.

2. **Toggle between Realtime and Simulation modes**.

i. Find the word Realtime in the bottom right corner of the Packet Tracer interface. In Realtime mode, your network is always running like a real network, whether or not you are working on the network. Your configurations are performed in real time, and the network responds in near real time

ii. Click the tab directly behind the Realtime tab to switch to Simulation mode. In Simulation mode, you can watch your network run at a slower pace, observing the paths that data takes, and inspecting the data packets in detail.

iii. In the Simulation Panel, click Auto Capture / Play. You should now see data packets, represented as envelopes of various colors, traveling between the devices

iv. Click Auto Capture / Play again to pause the simulation.

v. Click Capture / Forward to step through the simulation. Click the button a few more times to see the effect.

vi. In the network topology on the left, click one of the envelopes on an intermediary device and investigate what is inside.

vii. Click the toggle button above Simulation in the bottom right corner to return to Realtime mode.

- Open a new instance of Packet Tracer. Create a new network with at least two LANs connected by a WAN. Connect all the devices. Investigate the original Packet Tracer activity to see what else you might need to do to make your new network functional. Record your thoughts and save your Packet Tracer file. You may want to revisit your network later after you have mastered a few more skills.

EXPERIMENT 2

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

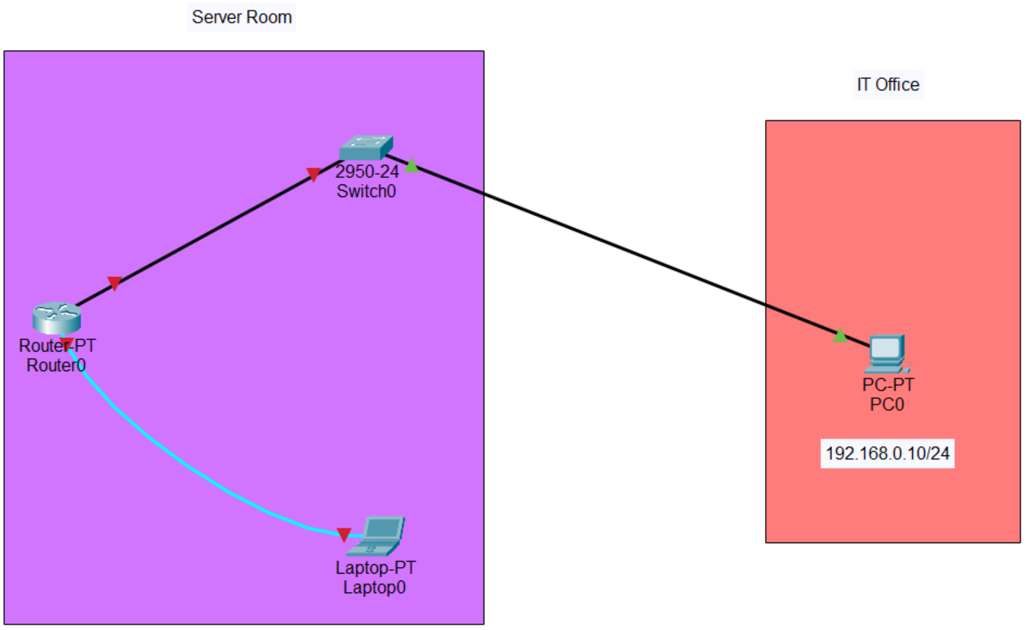
Procedure

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

Theory

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

Network Topology Diagram for TELNET



Input Details for TELNET

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

Router CLI

```
Router#config
Router(config)#line vty 0 4
Router(config-line)#password sai123
Router(config-line)#login local
Router(config-line)#exit
Router(config)#username sai privilege 4 password sai123
Router(config)#exit
```

Output

PINGING FROM PC0 TO SERVER USING TELENET:

```
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time< 1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 192.168.0.1
Trying 192.168.0.1 ...Open
User Access Verification
Username: sai
Password:<type the password---sai123(invisible)>

Router#show ip route(now router can be accessed from pc0)
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o – ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
Router#
```

Result

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

EXPERIMENT 3

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

Background

A subnet, or subnetwork, is a part of a larger network. Subnets are a logical part of an IP network into multiple, smaller network components. The Internet Protocol (IP) is the method for transmitting data from one computer to another over the internet network. Each computer, or host, on the internet, has at least one IP address as a unique identifier.

Steps to Configure and Verify Three Router Connections in Cisco Packet Tracer:

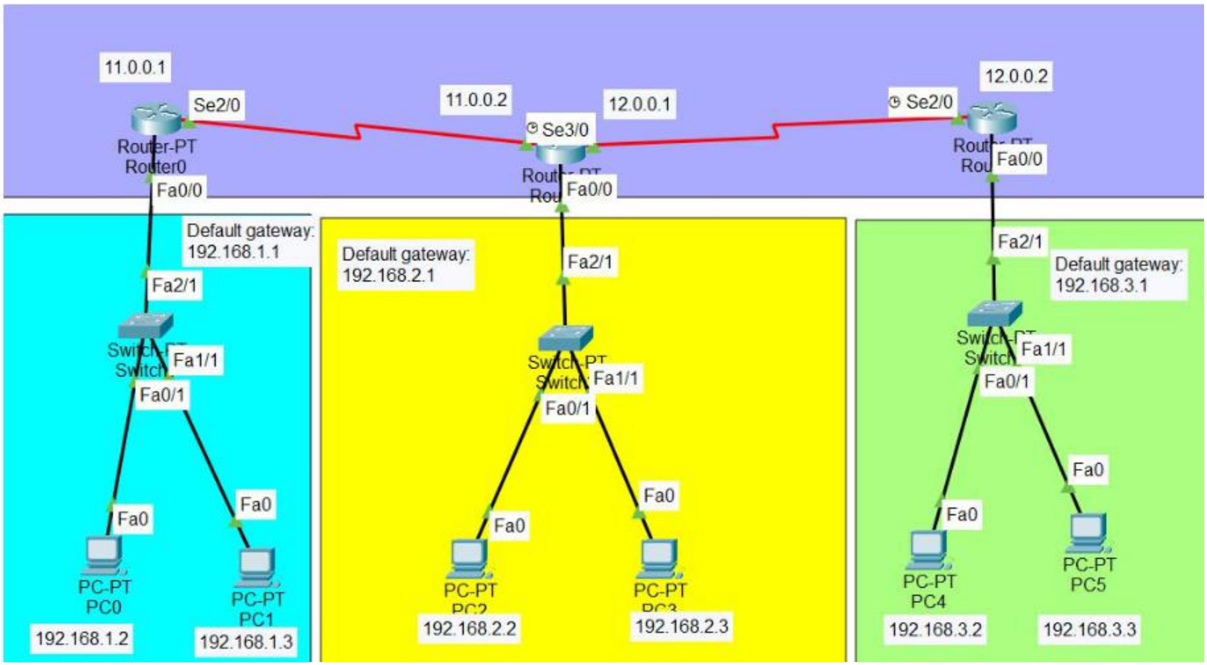
Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

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

IP Addressing Table for PCs

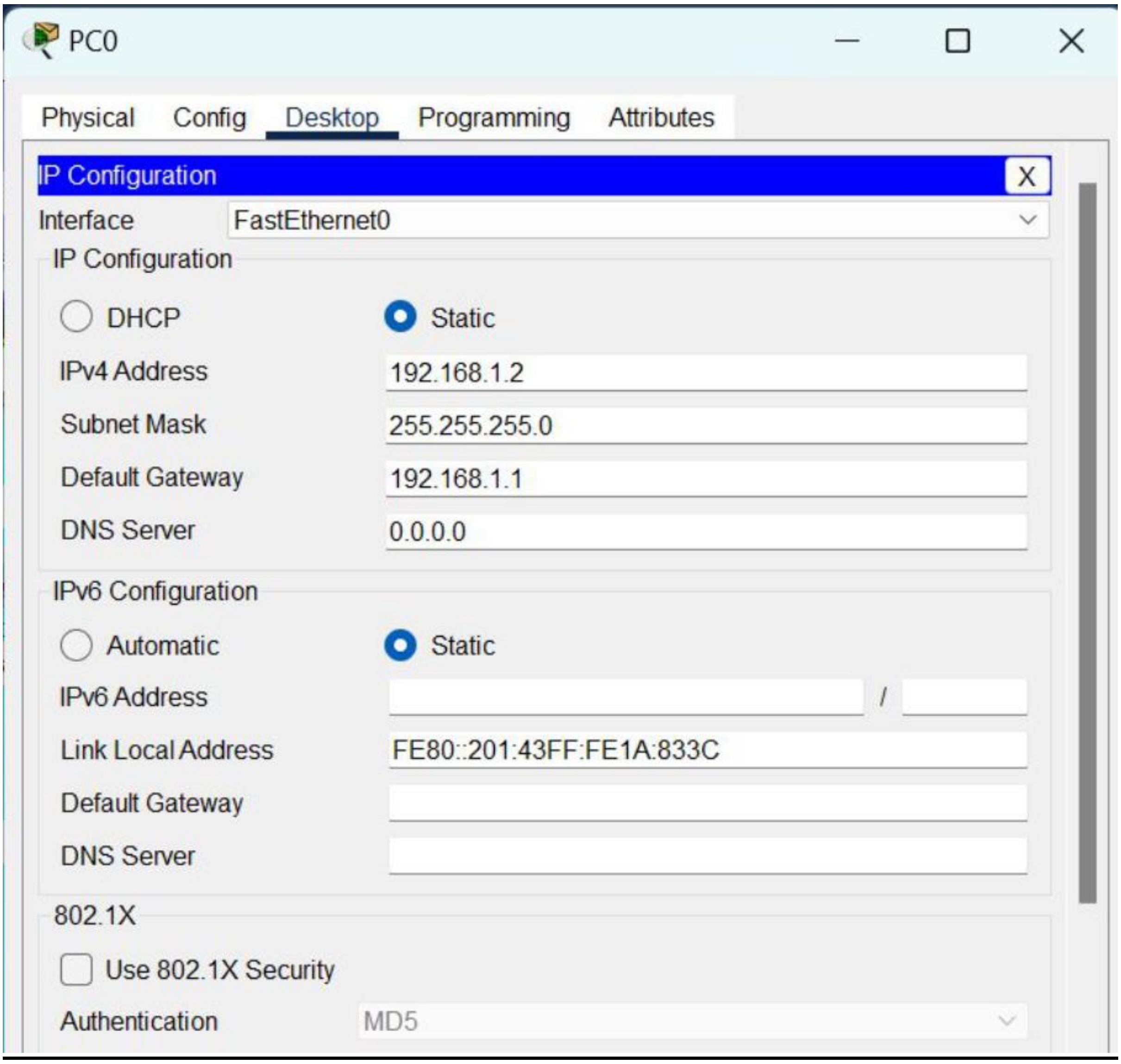
S.NO	Device	IPv4 Address	Subnet Mask	Default-Gateway
1.	pc0	192.168.1.2	255.255.255.0	192.168.1.1
2.	pc1	192.168.1.3	255.255.255.0	192.168.1.1
3.	pc2	192.168.2.2	255.255.255.0	192.168.2.1
4.	pc3	192.168.2.3	255.255.255.0	192.168.2.1
5.	pc4	192.168.3.2	255.255.255.0	192.168.3.1
6.	pc5	192.168.3.3	255.255.255.0	192.168.3.1

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



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.



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:

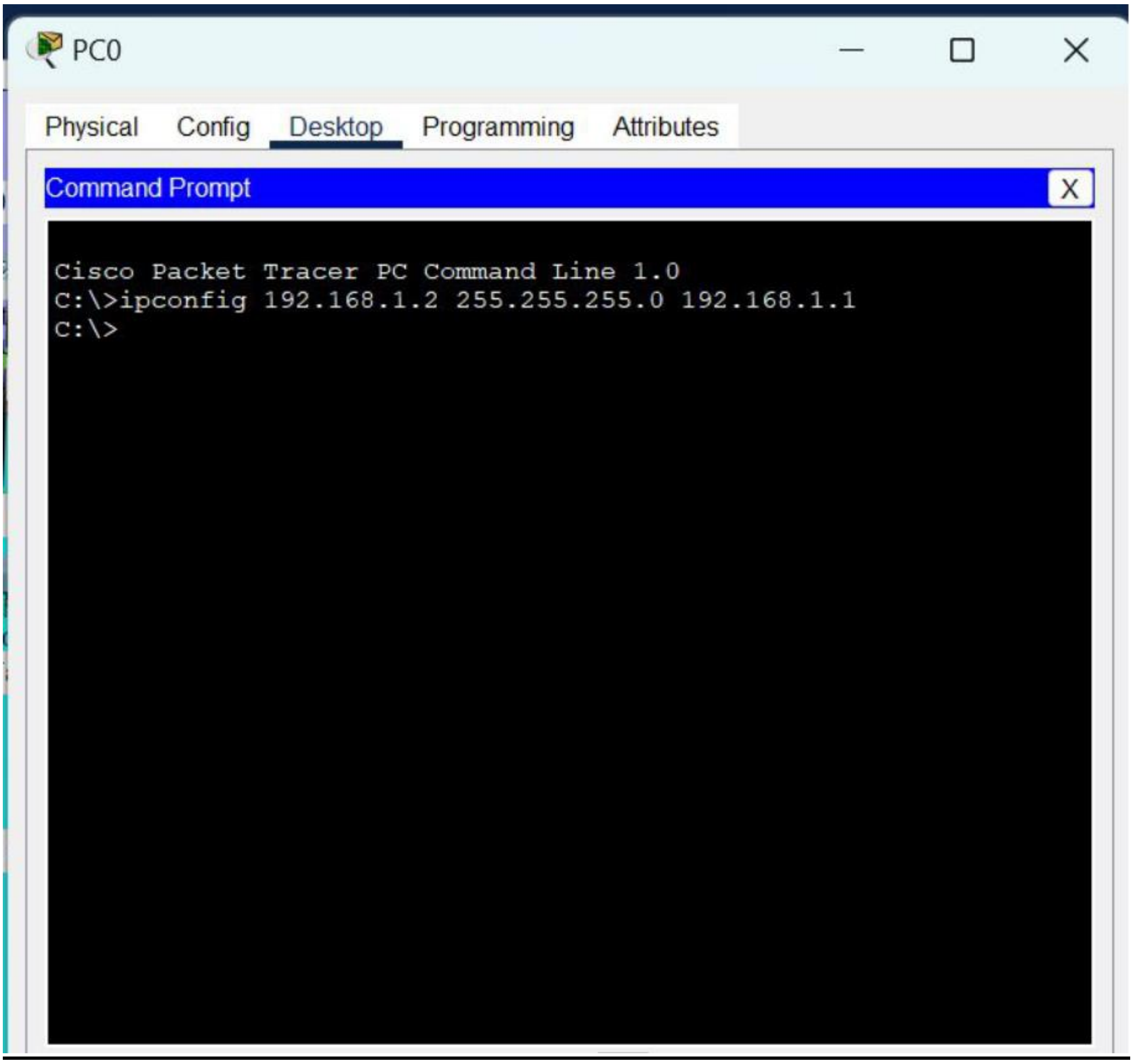
802.1X

□ Use 802.1X Security

Authentication: MD5

Assigning IP address using the ipconfig command.

- Or 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 192.168.1.2 255.255.255.0 192.168.1.1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.1.2 255.255.255.0 192.168.1.1
C:\>
```

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

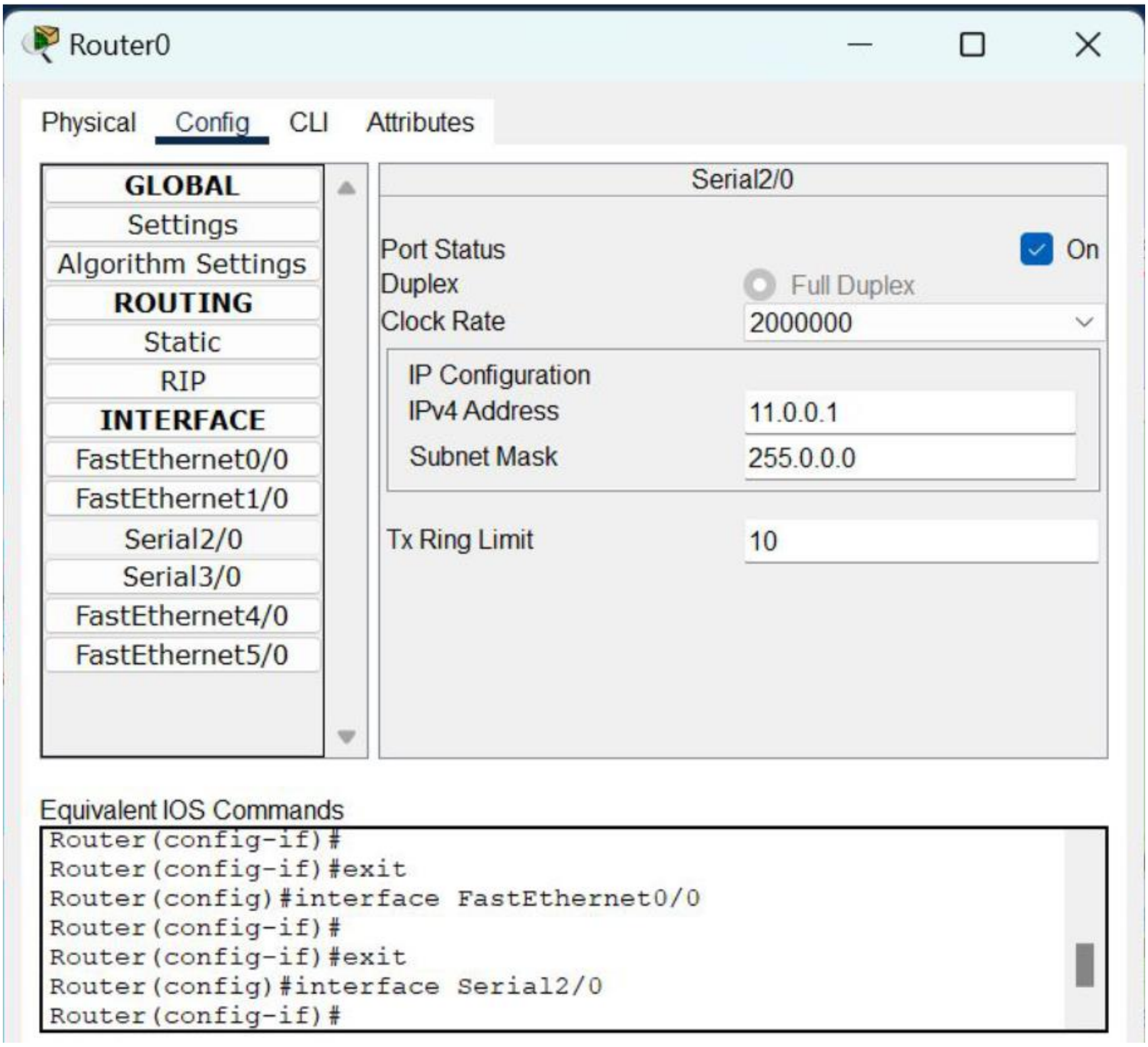
Step 3: Configure router with IP address and subnet mask.

IP Addressing Table Router

S.NO	Device	Interface	IPv4 Address	Subnet mask
1.	router0	FastEthernet0/0	192.168.1.1	255.255.255.0
		Serial2/0	11.0.0.1	255.0.0.0
2.	router1	Serial 2/0	11.0.0.2	255.0.0.0
		Serial 3/0	12.0.0.1	255.0.0.0

S.NO	Device	Interface	IPv4 Address	Subnet mask
3.	router 3	FastEthernet0/0	192.168.3.1	255.255.255.0
		Serial2/0	12.0.0.2	255.0.0.0

- 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.



Serial2/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 11.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
```

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

Step 4: 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 192.168.2.0 255.255.255.0 11.0.0.2
  Router(config)#ip route 11.0.0.0 255.0.0.0 11.0.0.2
  Router(config)#ip route 192.168.3.0 255.255.255.0 11.0.0.2

```
Router(config)#ip route 12.0.0.0 255.0.0.0 11.0.0.2
```

Static Routes for Router1 are given below:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 11.0.0.1
Router(config)#ip route 11.0.0.0 255.0.0.0 11.0.0.1
Router(config)#ip route 192.168.3.0 255.255.255.0 12.0.0.2
Router(config)#ip route 12.0.0.0 255.0.0.0 12.0.0.2
```

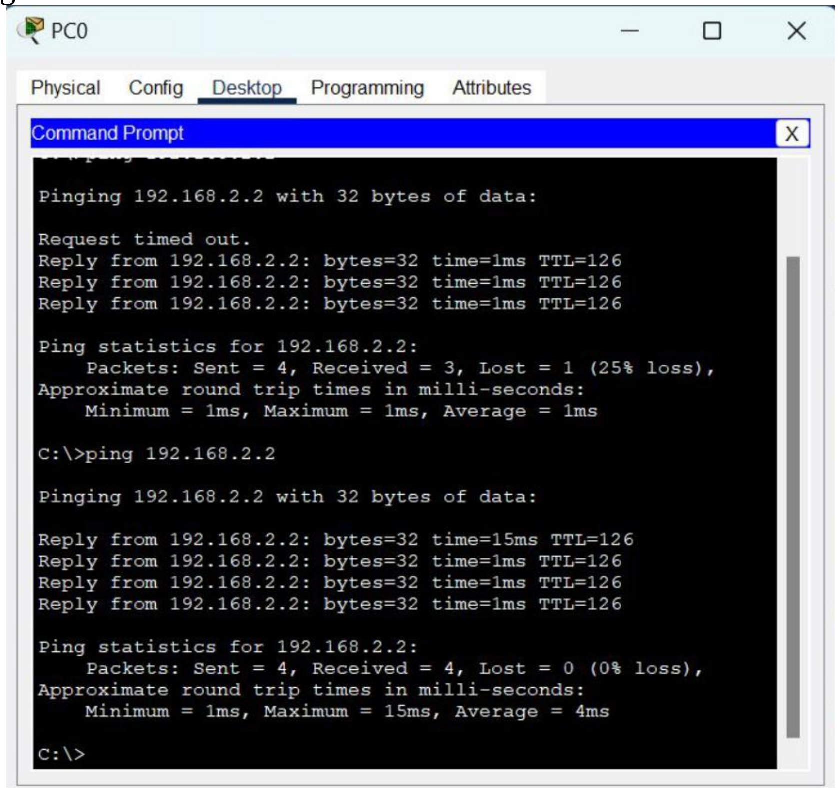
Static Routes for Router2 are given below:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 12.0.0.1
Router(config)#ip route 11.0.0.0 255.0.0.0 12.0.0.1
Router(config)#ip route 12.0.0.0 255.0.0.0 12.0.0.1
Router(config)#ip route 192.168.2.0 255.255.255.0 12.0.0.1
```

Step 5: Verifying the network by pinging the IP address of any PC. We will use the ping command to do so.

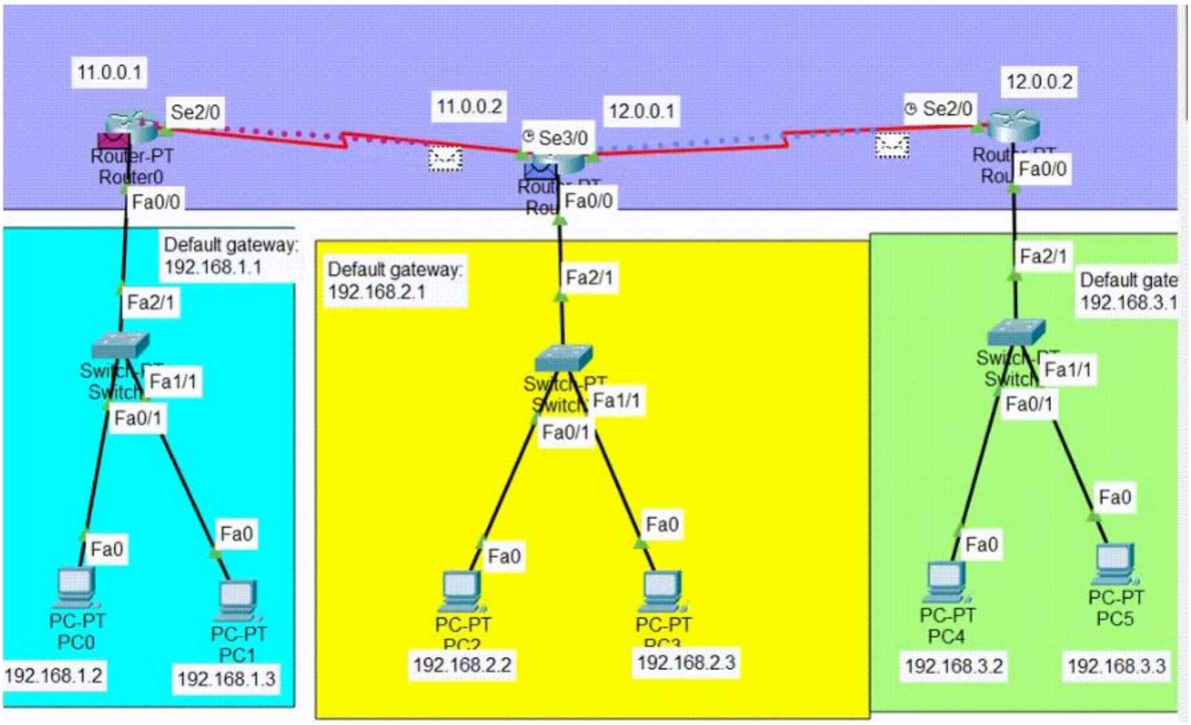
- First, click on PC0 then Go to the command prompt
- Then type ping <IP address of targeted node>
- As we can see in the below image we are getting replies which means the connection is working very fine

Example : ping 192.168.2.2



```
Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms 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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=15ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms 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 = 15ms, Average = 4ms

C:\>
```

- A simulation of the experiment is given below we are sending PDU from PC0 to PC3 and PC2 to PC4:



EXPERIMENT 4

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

Background

Static routing is a routing protocol that helps to keep your network organized and to optimize routing performance. It enables the router to assign a specific path to each network segment and to keep track of network changes. This helps to improve network stability and continuity. This adds security because a single administrator can only authorize routing to particular networks.

Steps to Configure and Verify Two Router Connections in Cisco Packet Tracer :

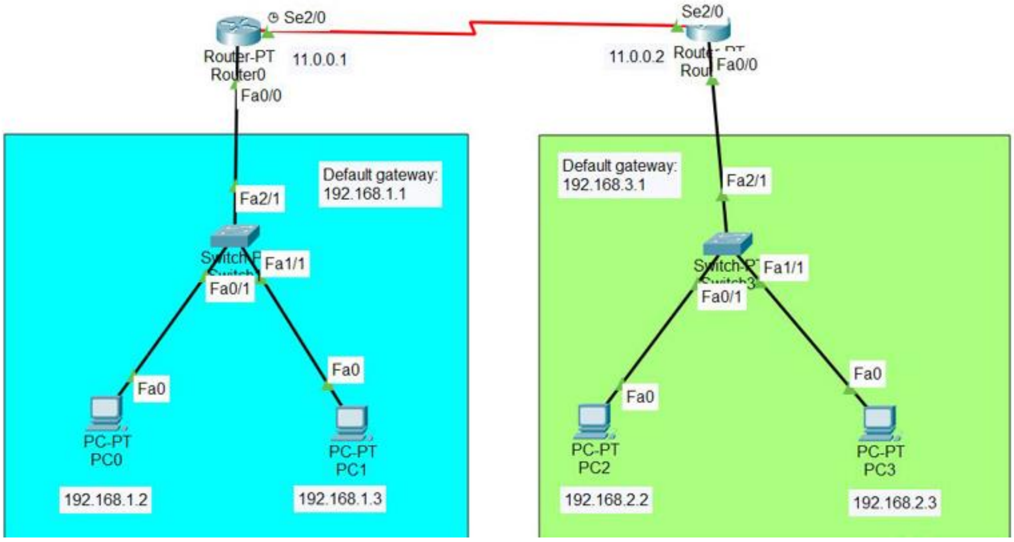
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S.NO	Device	Model Name	Qty.
1.	PC	PC	4
2.	Switch	PT-Switch	2
3.	Router	PT-Router	2

IP Addressing Table For PCs:

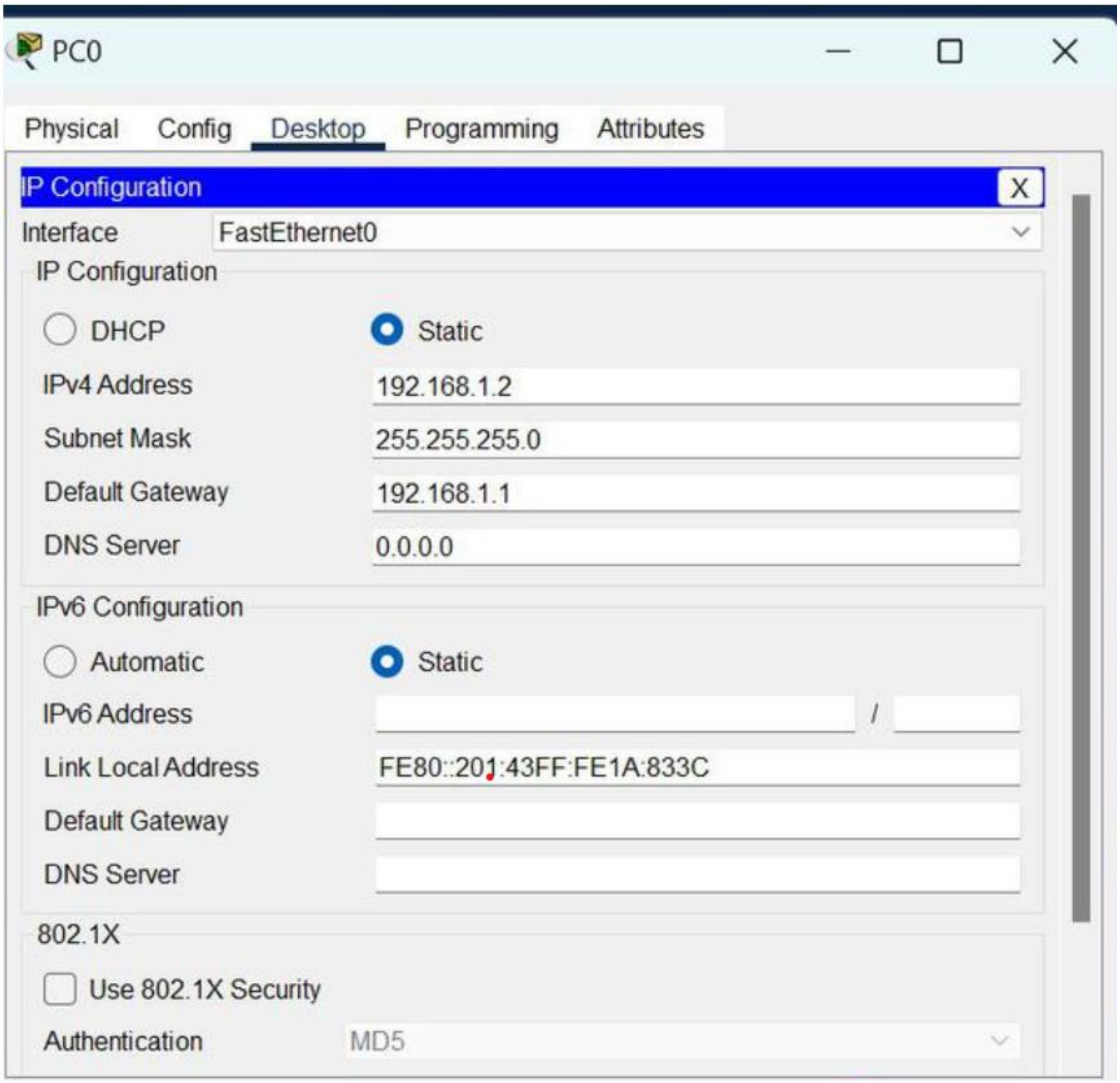
S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway
1.	pc0	192.168.1.2	255.255.255.0	192.168.1.1
2.	pc1	192.168.1.3	255.255.255.0	192.168.1.1
3.	pc2	192.168.2.2	255.255.255.0	192.168.2.1
4.	pc3	192.168.2.3	255.255.255.0	192.168.2.1

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



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.



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

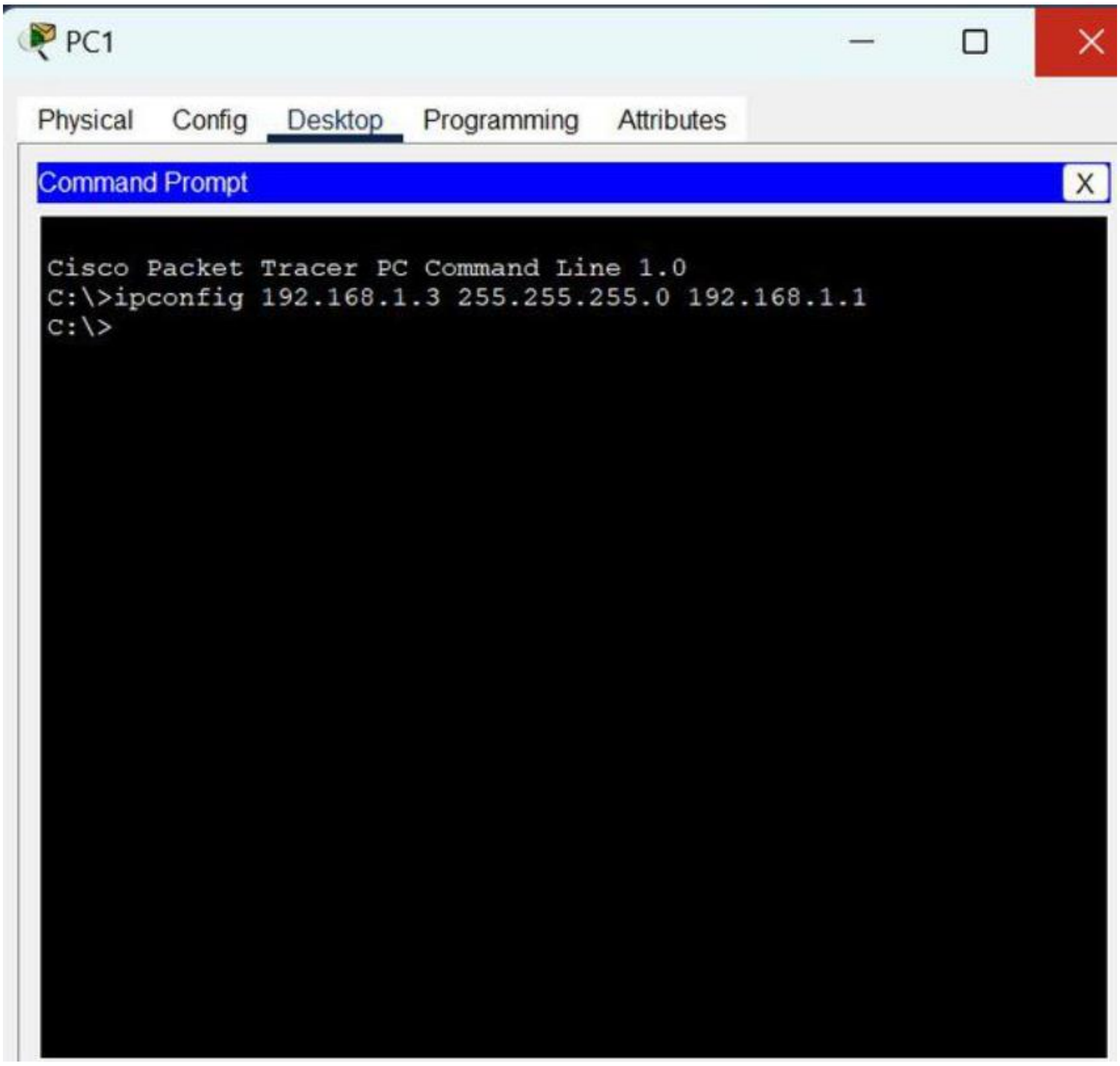
□ Use 802.1X Security

Authentication MD5

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

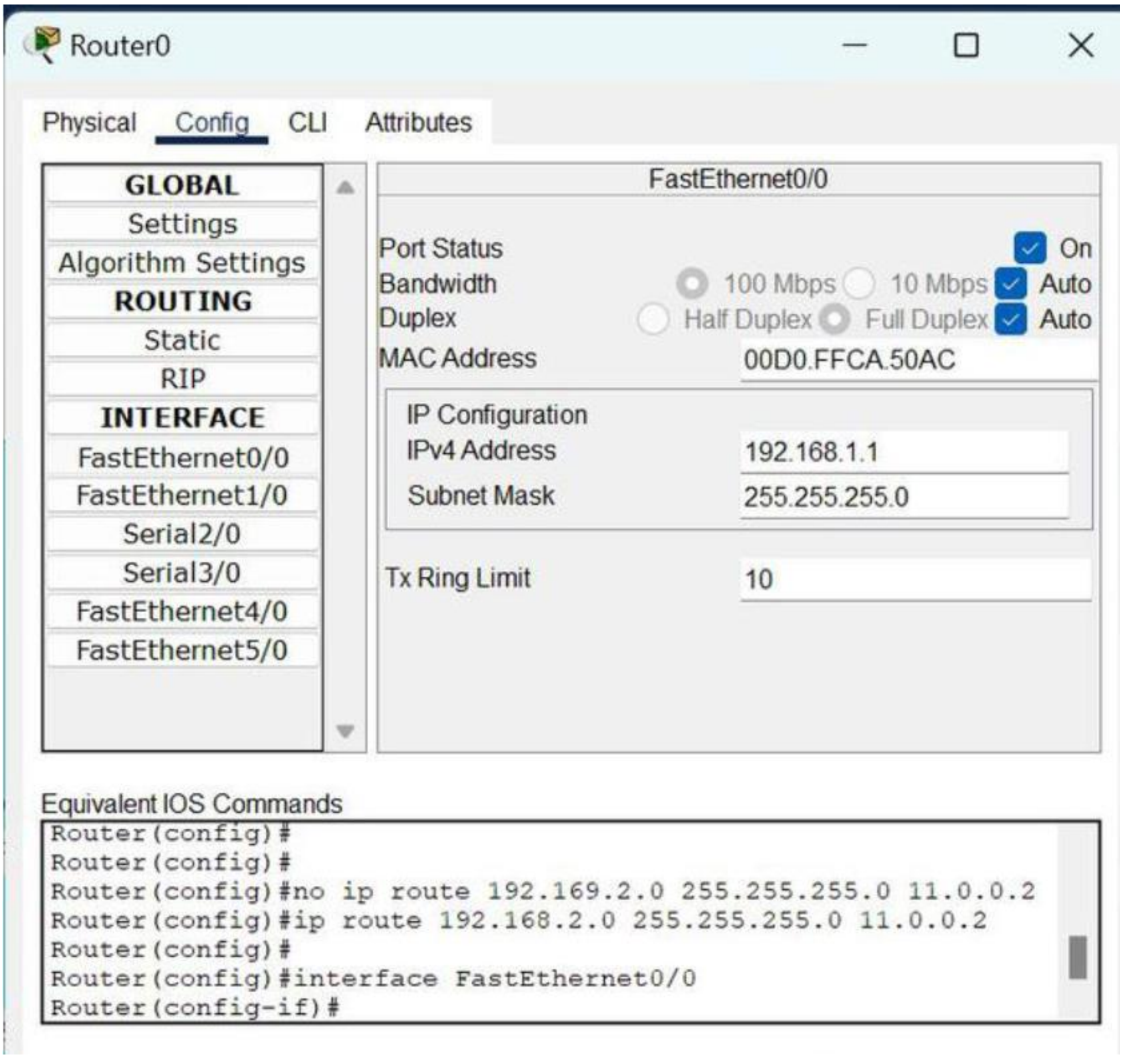


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.1.3 255.255.255.0 192.168.1.1
C:\>
```

- 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
1.	router0	FastEthernet0/0	192.168.1.1	255.255.255.0
		Serial2/0	11.0.0.1	255.255.255.0
2.	router1	FastEthernet0/0	192.168.2.1	255.255.255.0
		Serial2/0	11.0.0.2	255.255.255.0

- 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.



FastEthernet0/0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00D0.FFCA.50AC

IP Configuration

IPv4 Address 192.168.1.1

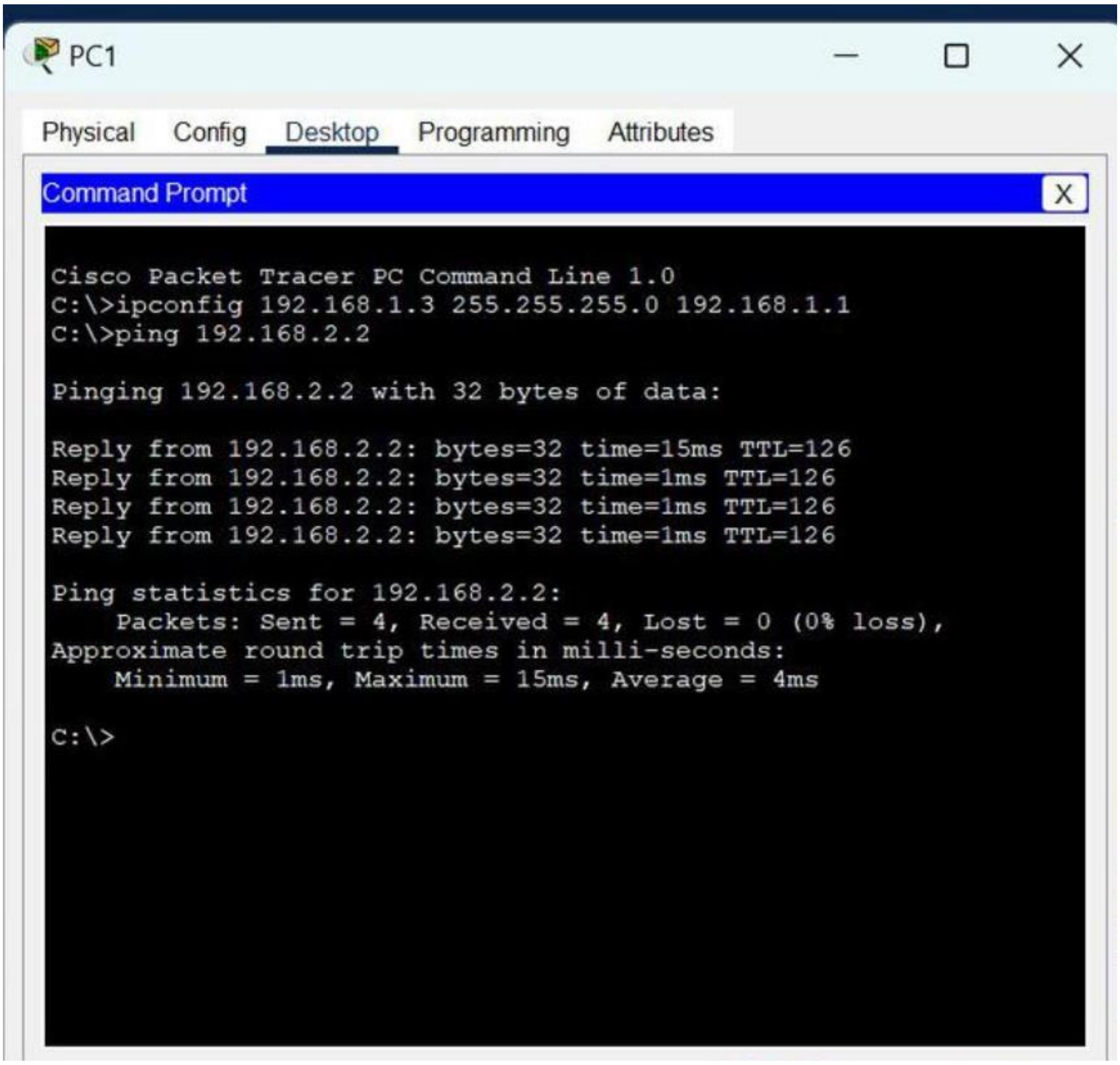
Subnet Mask 255.255.255.0

Tx Ring Limit 10

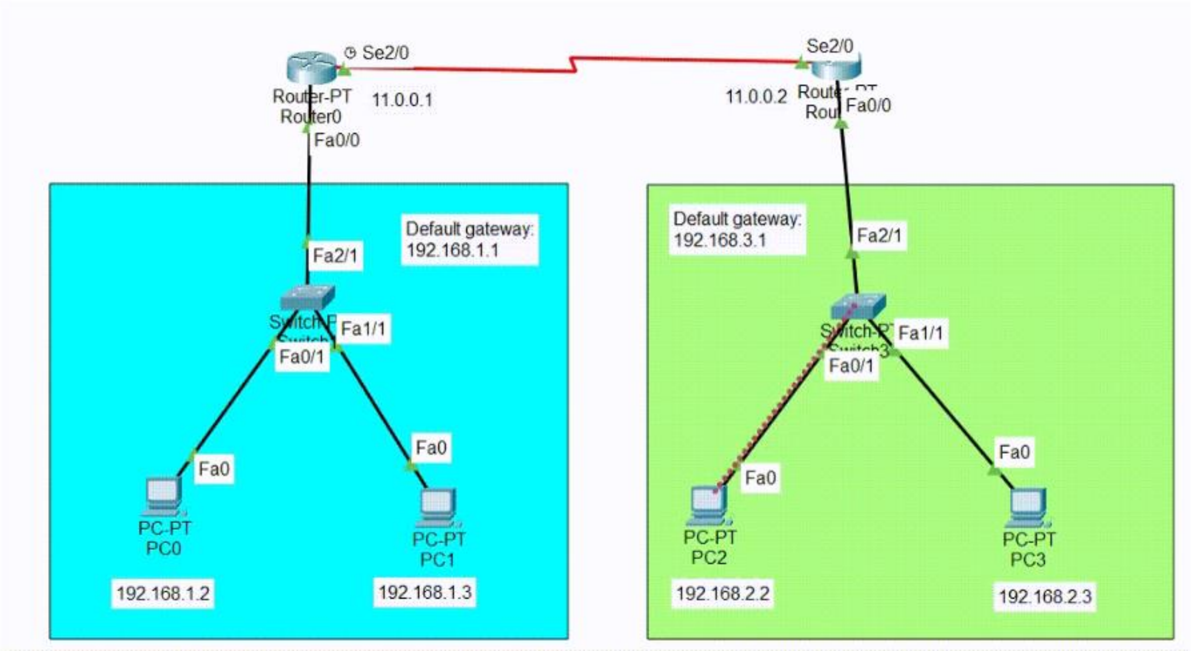
Equivalent IOS Commands

```
Router(config)#
Router(config)#
Router(config)#no ip route 192.169.2.0 255.255.255.0 11.0.0.2
Router(config)#ip route 192.168.2.0 255.255.255.0 11.0.0.2
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

- Repeat the same procedure with other routers to configure them thoroughly.
  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 192.168.2.0 255.255.255.0 11.0.0.2
  Static Routes for Router1 are given below:
  Router(config)#ip route 192.168.1.0 255.255.255.0 11.0.0.1
  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



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.1.3 255.255.255.0 192.168.1.1
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=15ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms 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 = 15ms, Average = 4ms

C:\>
```



EXPERIMENT 5

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

Background

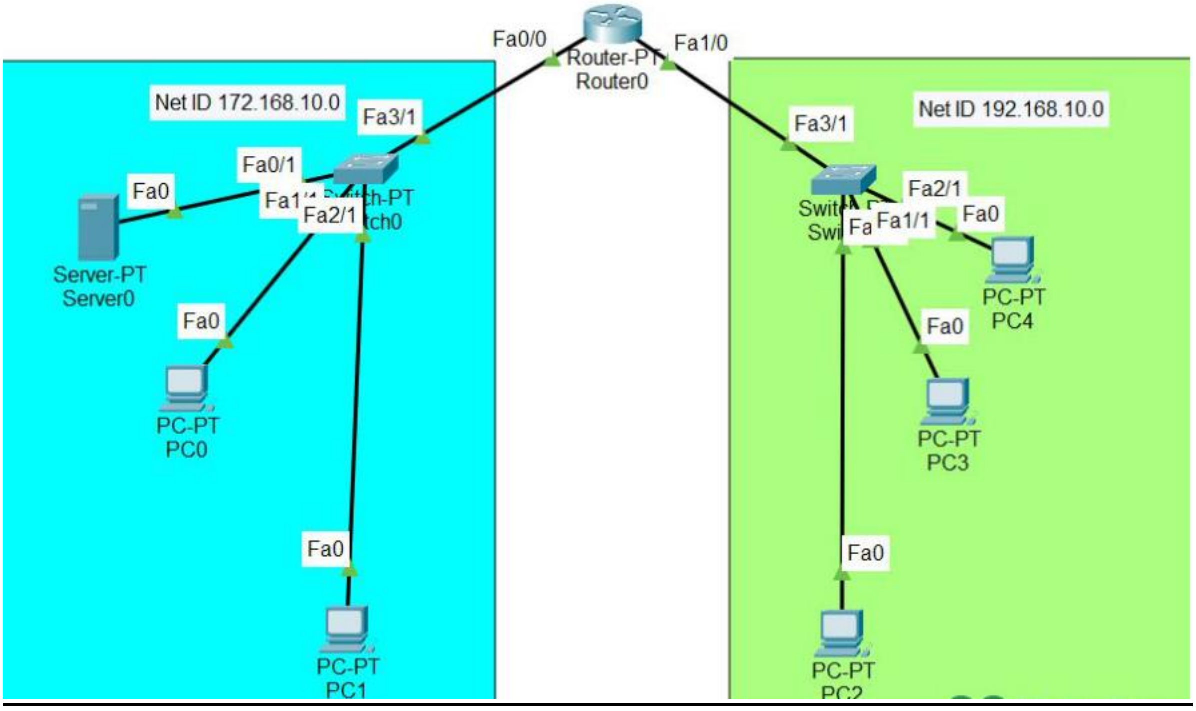
DHCP is a network management protocol used in networks to dynamically assign IP addresses and other network configuration information like default gateway, mask, DNS server address, etc. It is an application layer protocol.

Steps to Configure and Verify DHCP Server in Cisco Packet Tracer:

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

S.NO	Device	Model-Name	Unit
1.	PC	PC	5
2.	Switch	PT-Switch	2
3.	Router	PT-Router	1
4.	Server	Server-PT	1

- Now create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.

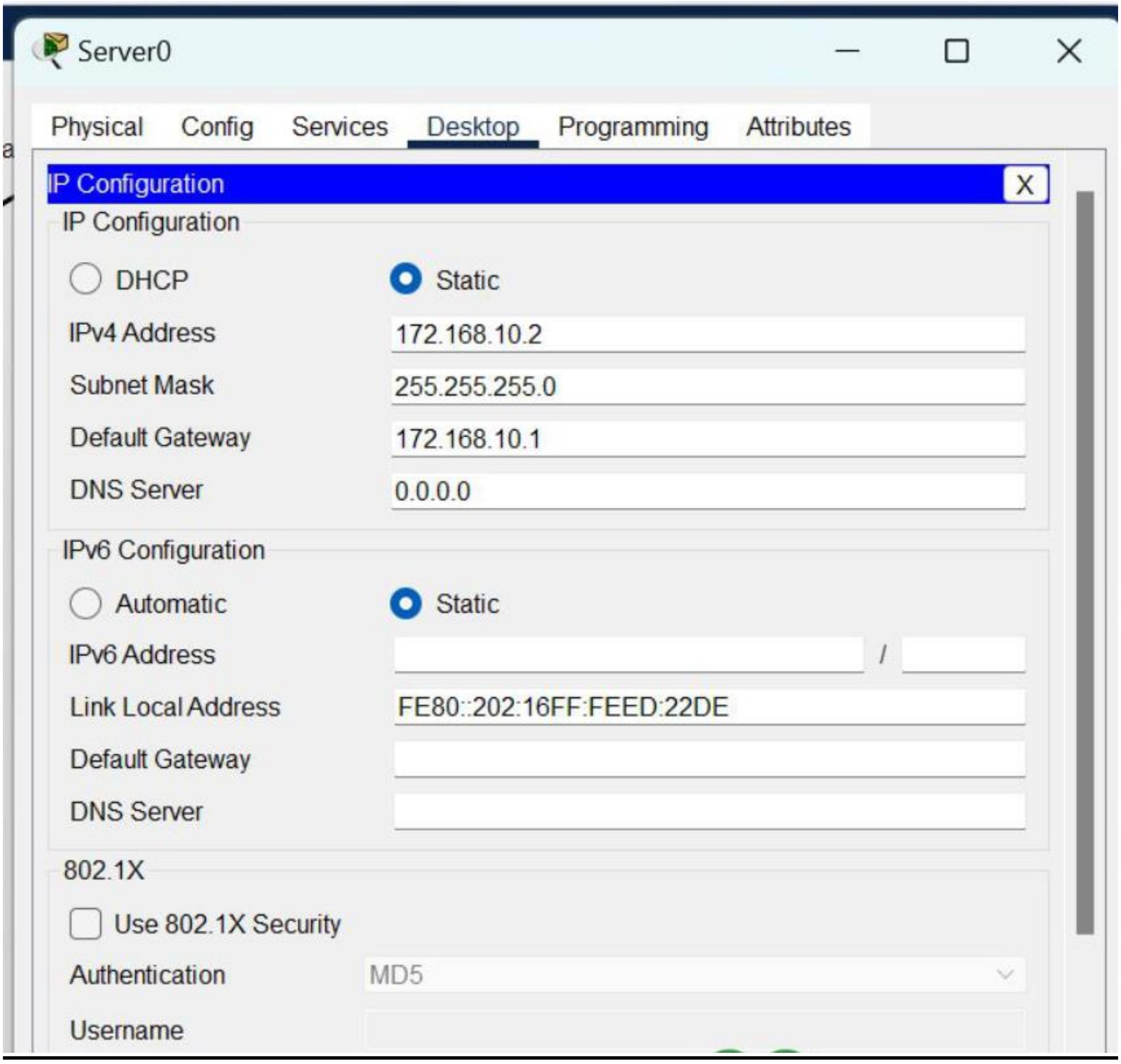


Step 2: Configure the Server with IPv4 address and Subnet Mask according to the Data given above.

- To assign an IP address in Server, click on Server-PT.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Add IPv4 address, subnet mask, and Default Gateway.

Parameters	Address value
IPv4 Address	172.168.10.2

Parameters	Address value
Subnet Mask	255.255.255.0
Default-Gateway	172.168.10.1



IP Configuration

○ DHCP ● Static

IPv4 Address: 172.168.10.2

Subnet Mask: 255.255.255.0

Default Gateway: 172.168.10.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FEED:22DE

Default Gateway:

DNS Server:

802.1X

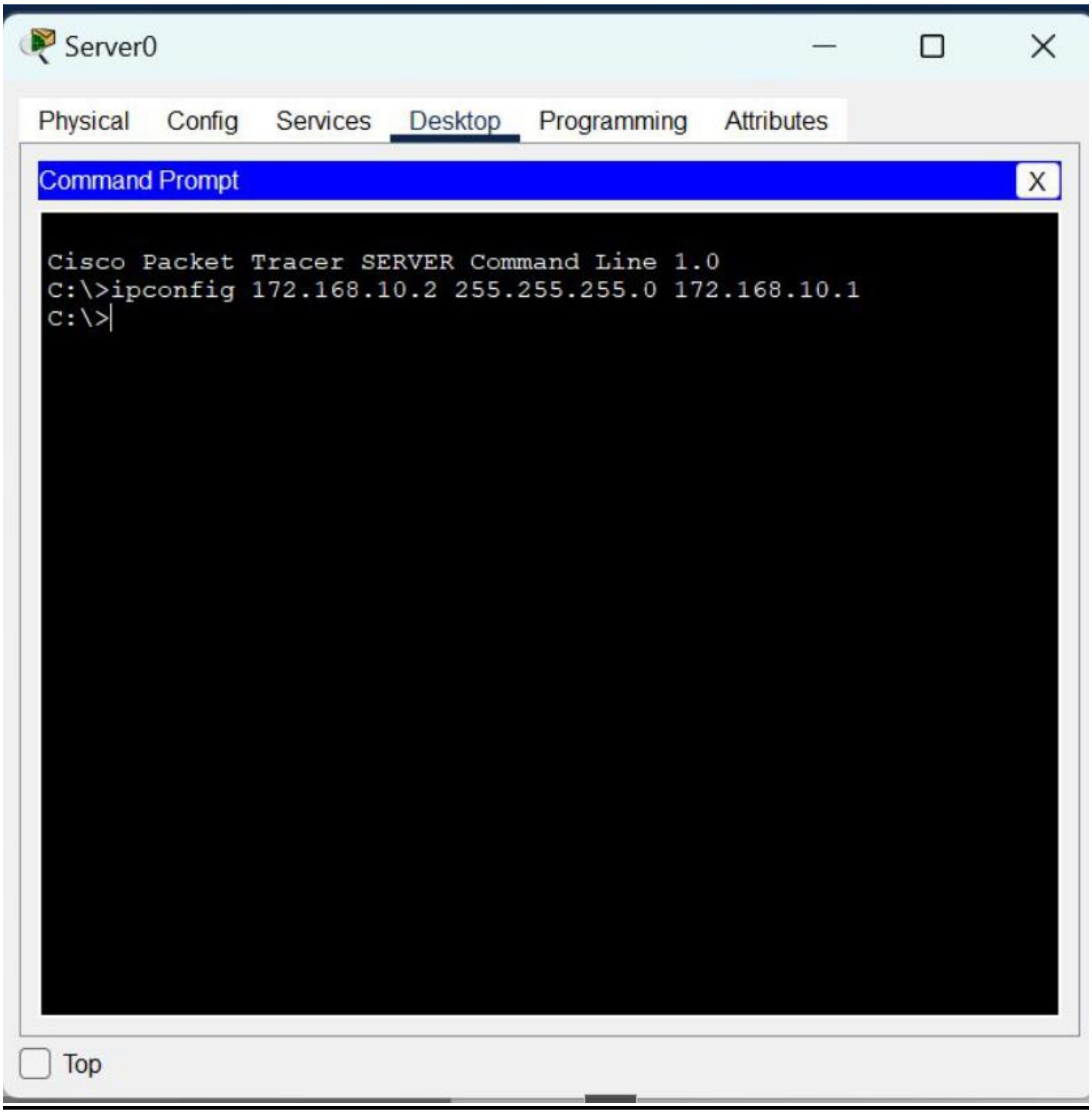
□ Use 802.1X Security

Authentication: MD5

Username:

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 prompt of the server
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed) example: ipconfig 172.168.10.2 255.255.255.0 172.168.10.1



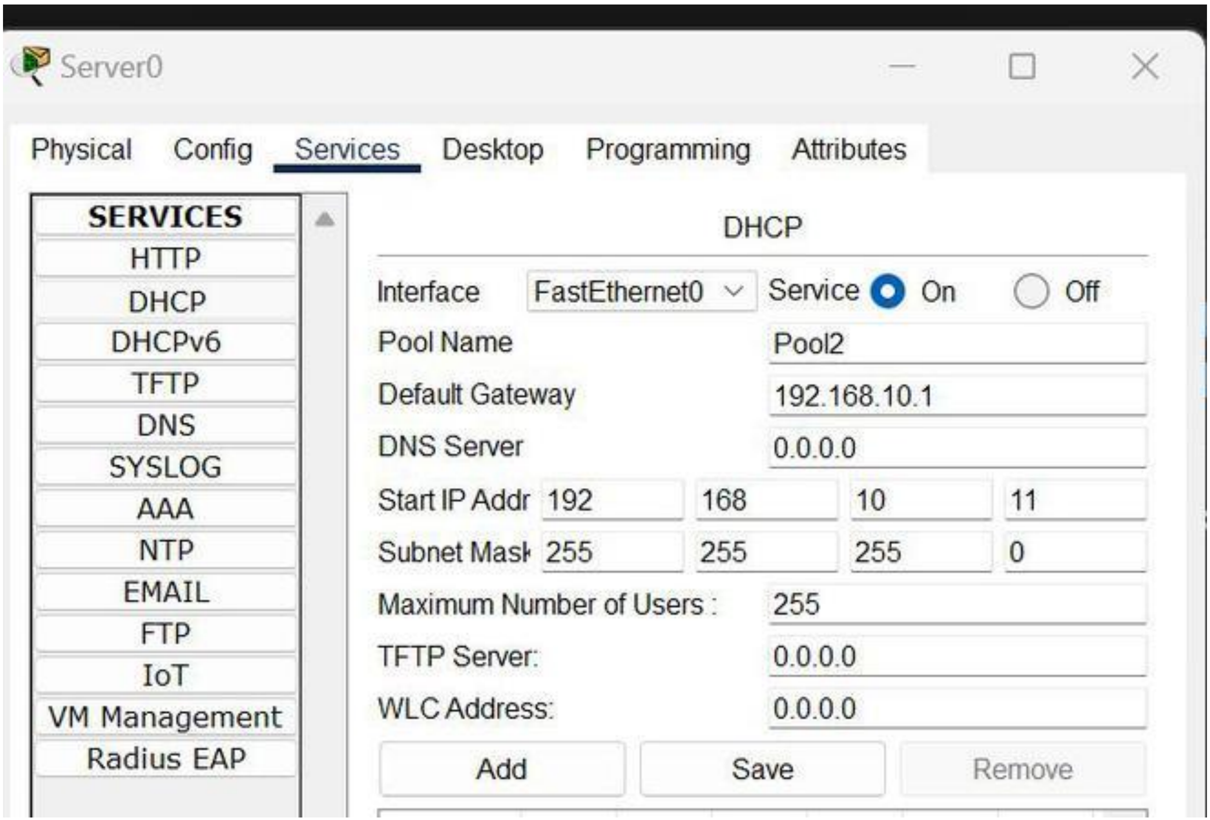
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig 172.168.10.2 255.255.255.0 172.168.10.1
C:\>
```

Step 3: Configuring the DHCP server.

To configure the DHCP server first,

- Click on Server then, Go to services.
- Click on DHCP and turn on the services and, configure the DHCP server with the help of the data given below.
- Delete the default values of Start IP Address and subnet Mask then save the info.
- Create two new pools.

POOL1 and POOL2 and fill the data as shown in the images below.



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: Pool2

Default Gateway: 192.168.10.1

DNS Server: 0.0.0.0

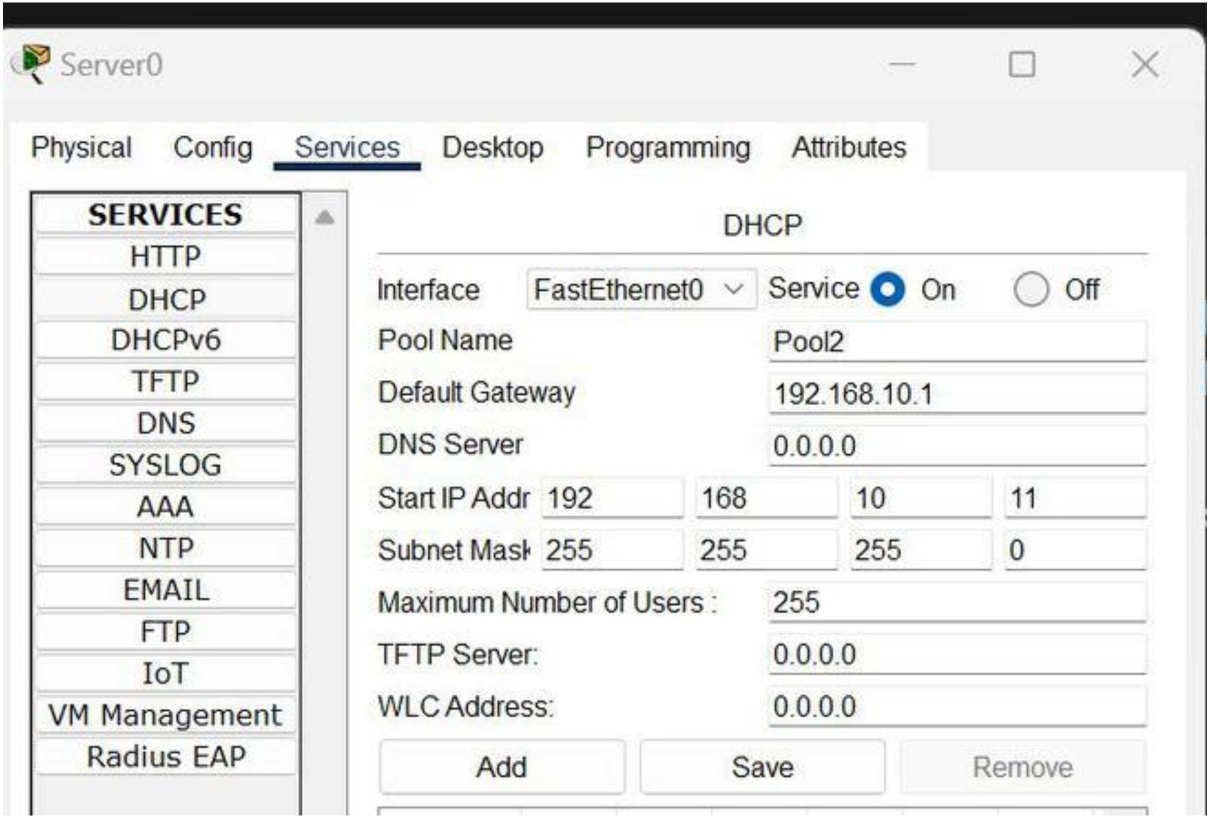
Start IP Addr: 192 168 10 11

Subnet Mask: 255 255 255 0

Maximum Number of Users : 255

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0


DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: Pool2

Default Gateway: 192.168.10.1

DNS Server: 0.0.0.0

Start IP Addr: 192 168 10 11

Subnet Mask: 255 255 255 0

Maximum Number of Users : 255

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Step 4: Configuring Router with IPv4 Address and Subnet Mask.

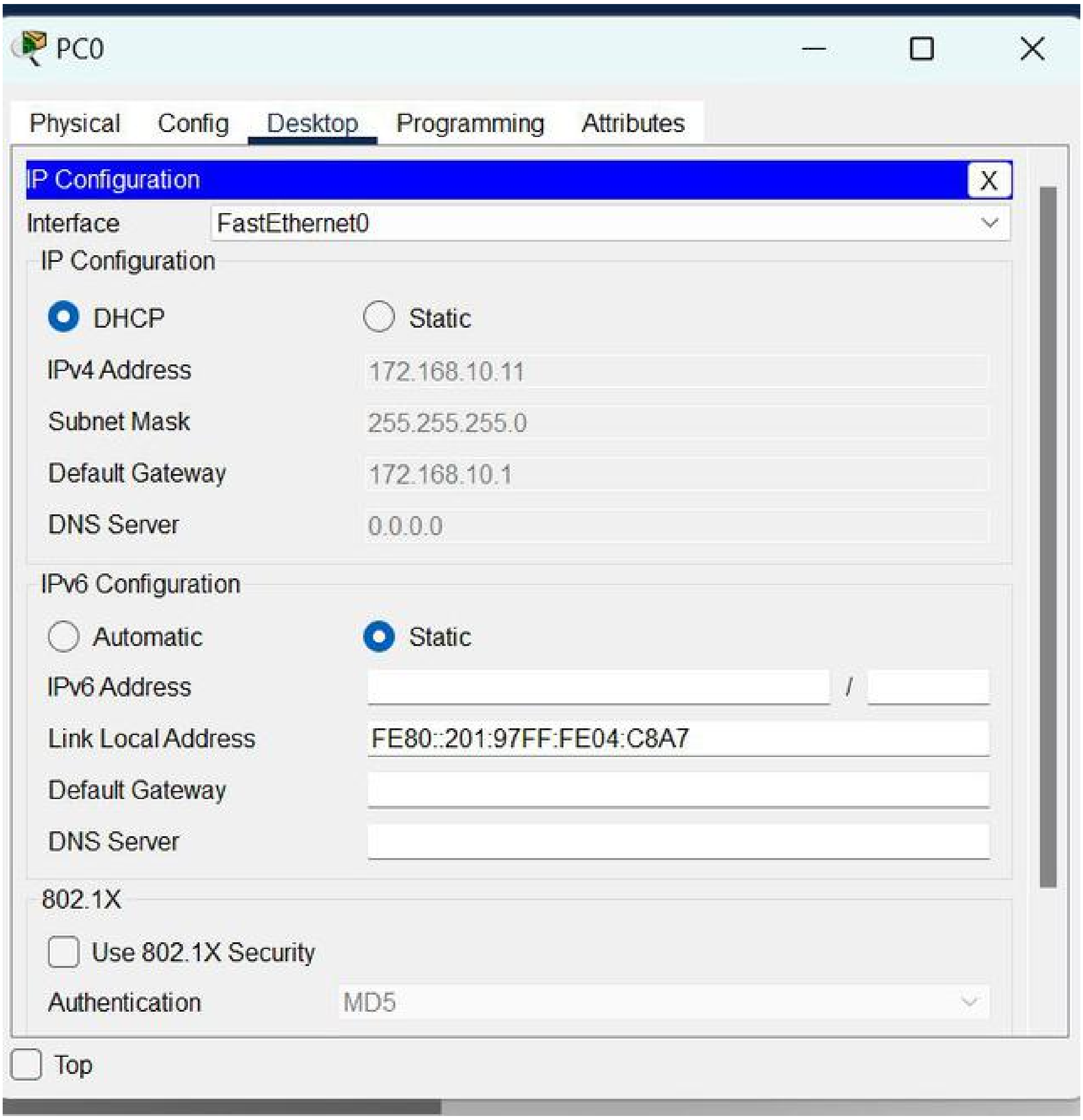
IP Addressing Table for Router:

S.NO	Device	Interface	IPv4 Address	Subnet Mask
1.	router0	FastEthernet0/0	172.168.10.1	255.255.255.0
		FastEthernet0/1	192.168.10.1	255.255.255.0

- To assign an IP address in router0, click on router0.
- Then, go to config and then Interfaces, and make sure to turn on the ports.
- Then, configure the IP address in FastEthernet according to IP addressing Table.
- Fill IPv4 address and subnet mask.

Step 5: Configuring the PCs and changing the IP configuration.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Change its state from static to DHCP.
- It will automatically fetch the data and configure itself



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 172.168.10.11

Subnet Mask: 255.255.255.0

Default Gateway: 172.168.10.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:97FF:FE04:C8A7

Default Gateway:

DNS Server:

802.1X

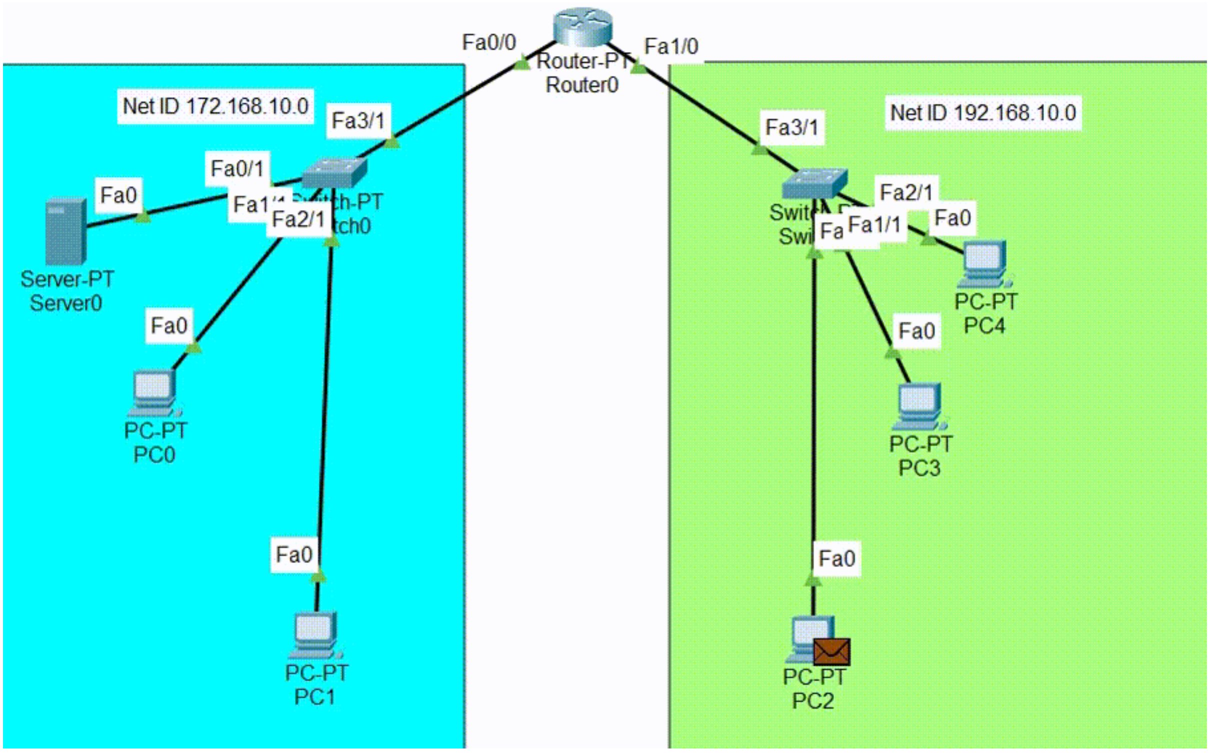
□ Use 802.1X Security

Authentication: MD5

□ Top

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

Output:


Fa0/0
Router-PT
Router0
Fa1/0
Net ID 172.168.10.0
Fa3/1
Fa0/1
Fa0
Fa1/1
Switch-PT
Switch0
Fa2/1
Server-PT
Server0
Fa0
PC-PT
PC0
Fa0
PC-PT
PC1
Fa3/1
Net ID 192.168.10.0
Fa2/1
Swit
Swi
Fa
Fa1/1
Fa0
PC-PT
PC4
Fa0
PC-PT
PC3
Fa0
PC-PT
PC2

EXPERIMENT 6

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

PART 1: Implement DNS Server

Background

DNS means domain name server, and DNS contains a database of domain names and IP mapping. DNS servers are very helpful as we don't have to remember the IP address and we can use the domain name instead. Names are much easier to type and learn so DNS plays an important role in every network.

When we enter google.com in the web browser the DNS server finds out the mapped IP of that domain and the HTTP request is forwarded to that IP address.

Configure DNS on the Cisco router

To configure the Cisco router as DNS, we have to enable the DNS service on the router using the following command.

```
Router(config)#ip dns server
```

Now, we have to map the names with the IP address using the following command.

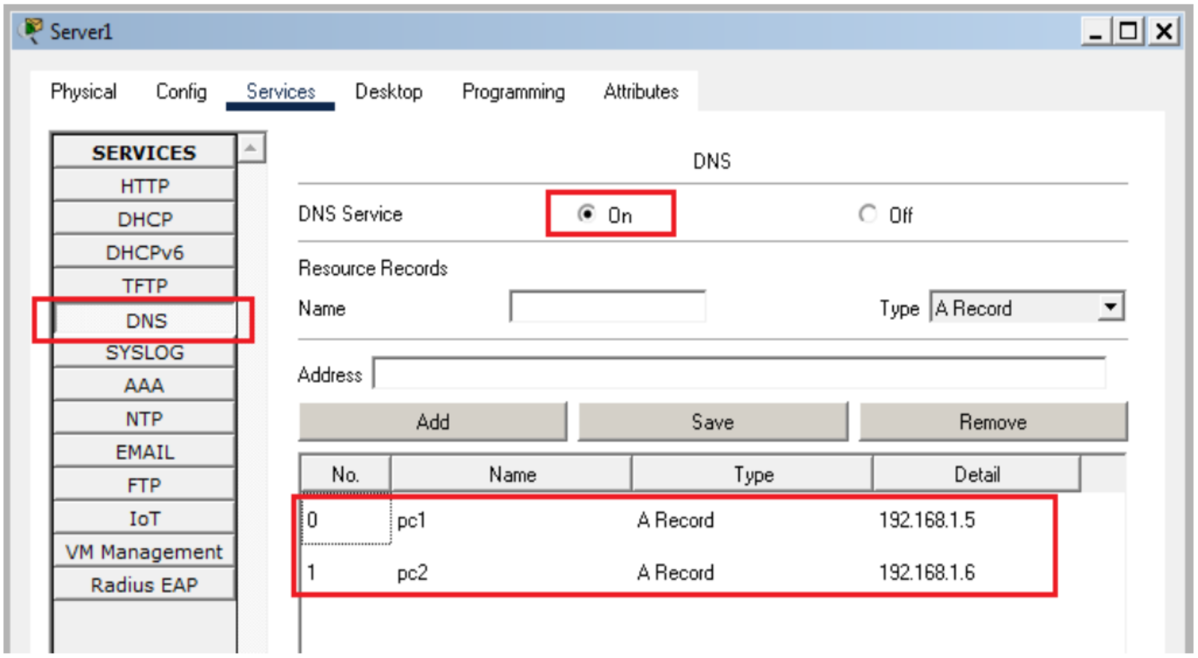
```
Router(config)#ip host PC1 192.168.1.5
Router(config)#ip host PC2 192.168.1.6
```

Finally, we need to configure the DNS server IP in the PC setting. In this case, as the router is configured as a DNS server, we will use the router's IP.

Now, we can ping one PC from another PC with their names.

Please note that Configuring the Cisco router as a DNS server is not possible in packet tracer as it does not provide this functionality

Configuring DNS in Cisco packet tracer with the available server endpoint



DNS

DNS Service ● On ○ Off

Resource Records

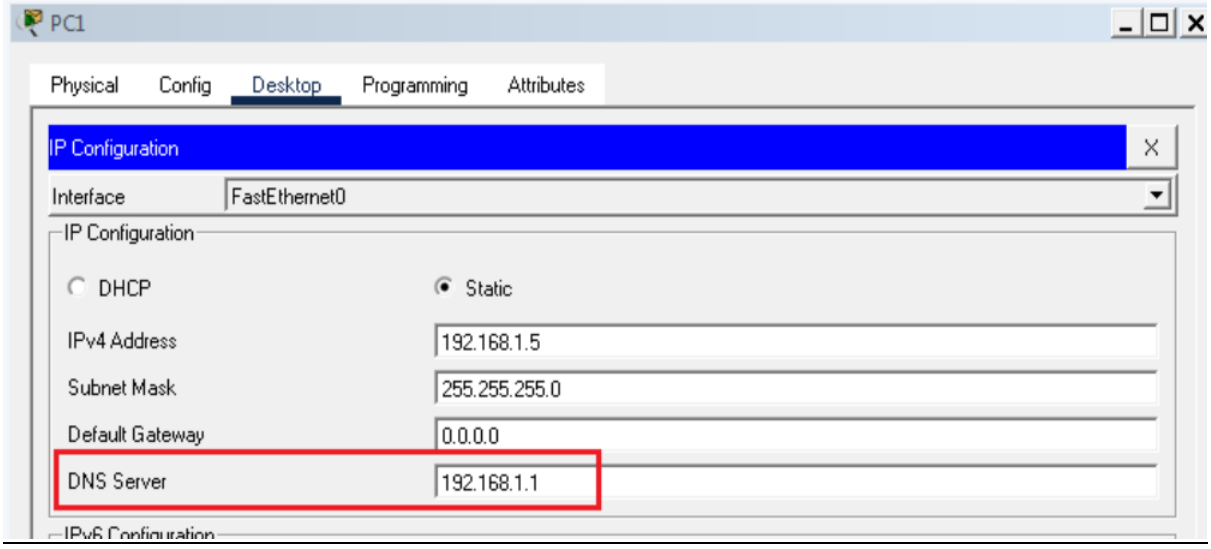
Name: Type: A Record

Address:

No.	Name	Type	Detail
0	pc1	A Record	192.168.1.5
1	pc2	A Record	192.168.1.6

To configure the DNS server, we have to enable the DNS service in the server which is disabled by default.

Now, we have to add an A record or create a name for IP mapping in the server.



PC1

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

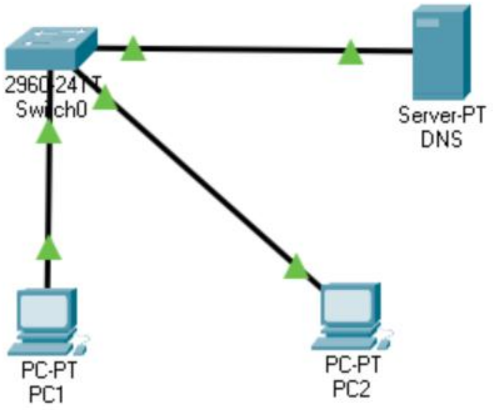
DNS Server: 192.168.1.1

IPv6 Configuration

Finally, PCs should be configured with the IP address of the server in the DNS settings.
That is all required to successfully enable the DNS server in packet tracer.
Now, we should be able to ping the PCs with the names.

```
C:\>ping PC2
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=35ms 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
```

As expected, we can ping one PC from another with the names.



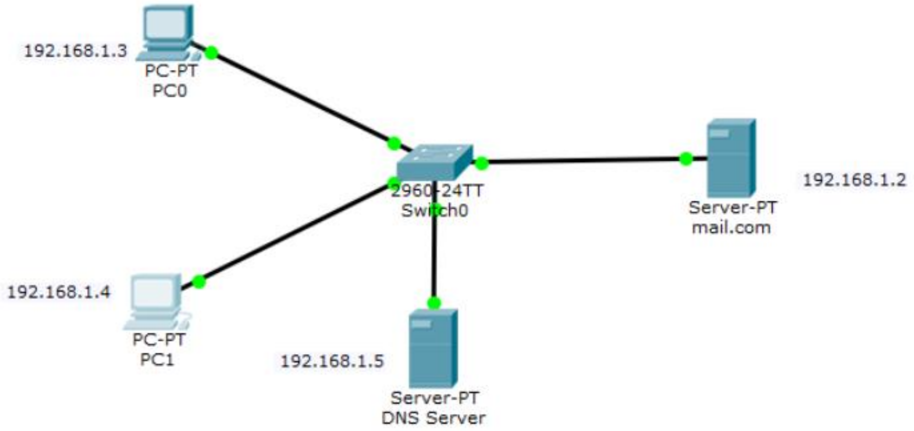
PART 2: Implement Email Services

Background

An email server, such as Gmail stores and sends email messages to email clients on request. We often send and receive emails on our mobile devices or computers. Have you ever imagined how this happens? Well, whenever you compose and send an email to another person, the message you send first goes to a mail server. It’s the mail server which then sends the email when it is requested from the email client(e.g Gmail App) of the recipient’s device.

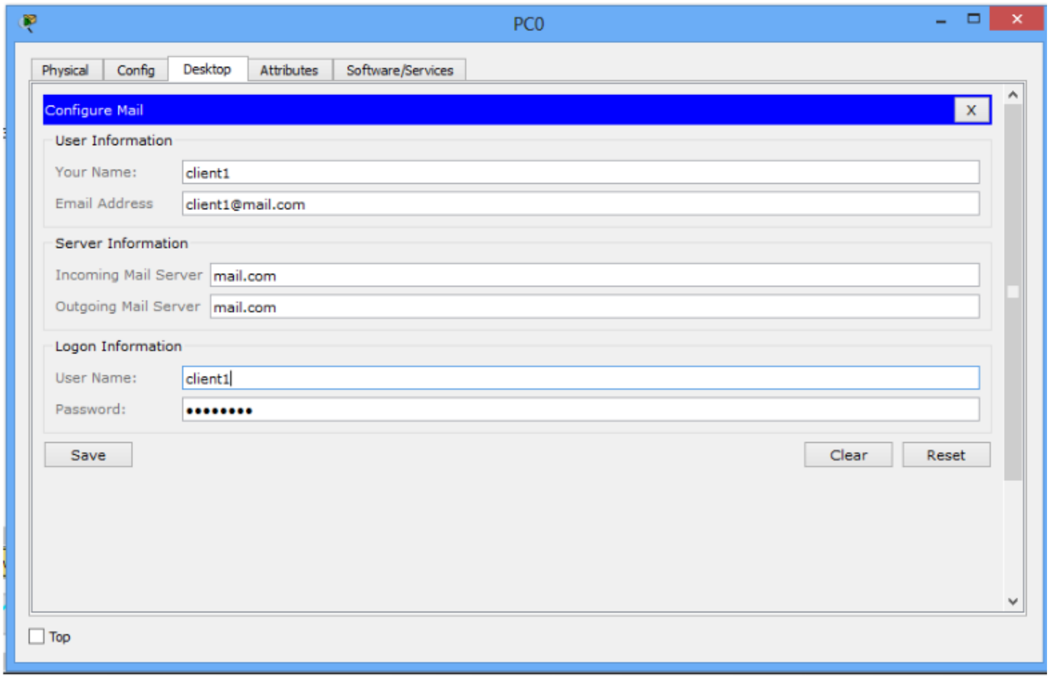
So now, lets configure a mail server in Packet Tracer. And have in mind that although our main focus is configuring an email server, we’ll still need services of a DNS server at one point.

Network Topology



Configure IP addresses on the PCs, DNS Server and the Mail Server.
Mail Server IP address: 192.168.1.2/24
PC0 IP address: 192.168.1.3/24
PC1 IP address: 192.168.1.4/24
DNS server IP address: 192.168.1.5/24
3. Now configure mail clients on the PCs and mail service on the generic server.
Mail Clients:
Click on PC0. Go to its Desktop tab, and click on Email. Configure the email client by filling in the user, server and login information. Be sure to Save.

PC0:

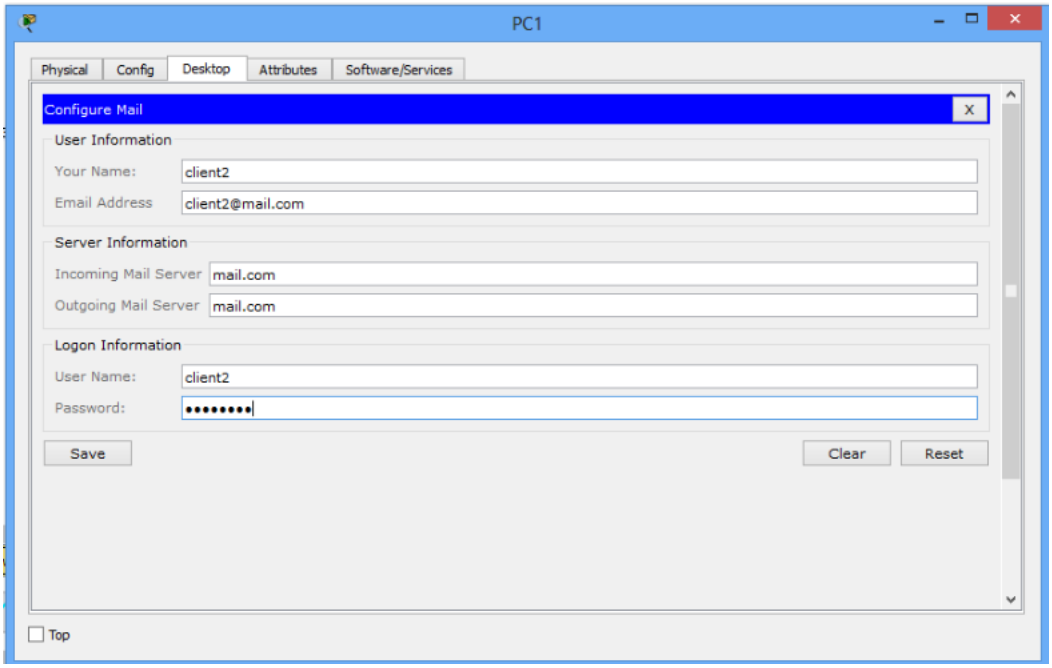


User Information
Your Name: client1
Email Address: client1@mail.com

Server Information
Incoming Mail Server: mail.com
Outgoing Mail Server: mail.com

Logon Information
User Name: client1
Password: ••••••••

Configure mail client on PC1 in a similar way we did for PC1.



User Information

Your Name: client2

Email Address client2@mail.com

Server Information

Incoming Mail Server mail.com

Outgoing Mail Server mail.com

Logon Information

User Name: client2

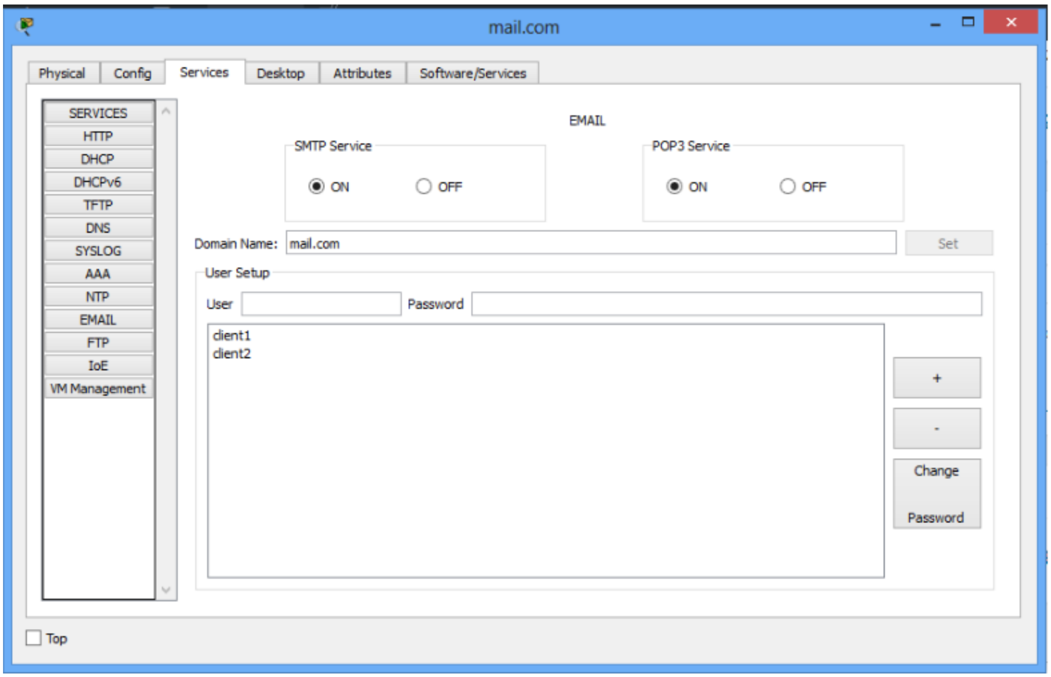
Password: ••••••••

Next, we'll configure the **email server.**

To do this, click on the server, then click **Services** tab, pick **email** server from the menu. Provide the **Domain name** of the server then click on **Set** to set it. In this example I've used the name 'mail.com' .

Proceed and add **users** and provide their **passwords**. I have two email clients(users) with usernames 'client1' and 'client2' with a common password 'adminkim'

After entering a username and password, click on **Add(+)** to add the user to the server. You can optionally remove a user by clicking on **Remove (-).** You can change a user's password by clicking on **change password.**



EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: mail.com

User Setup

User

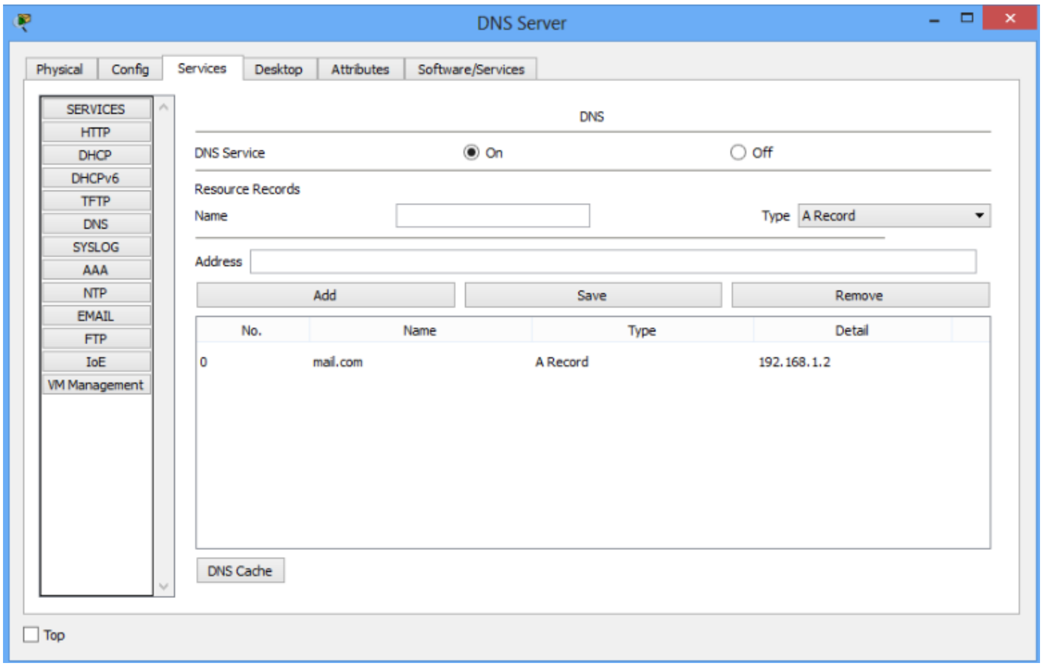
Password

client1
client2

notice that we set a **domain name** for the email server. For that reason, we should have a **DNS server** that will resolve this domain name (plus other domain names if there were) to an IP address.

So let's configure a DNS server.

Click DNS server, click **Services** tab, then pick **DNS**. Turn the service **ON.** Set name-address pairs and add them to the server. You can view the DNS entry below:



DNS

DNS Service ● On ○ Off

Resource Records

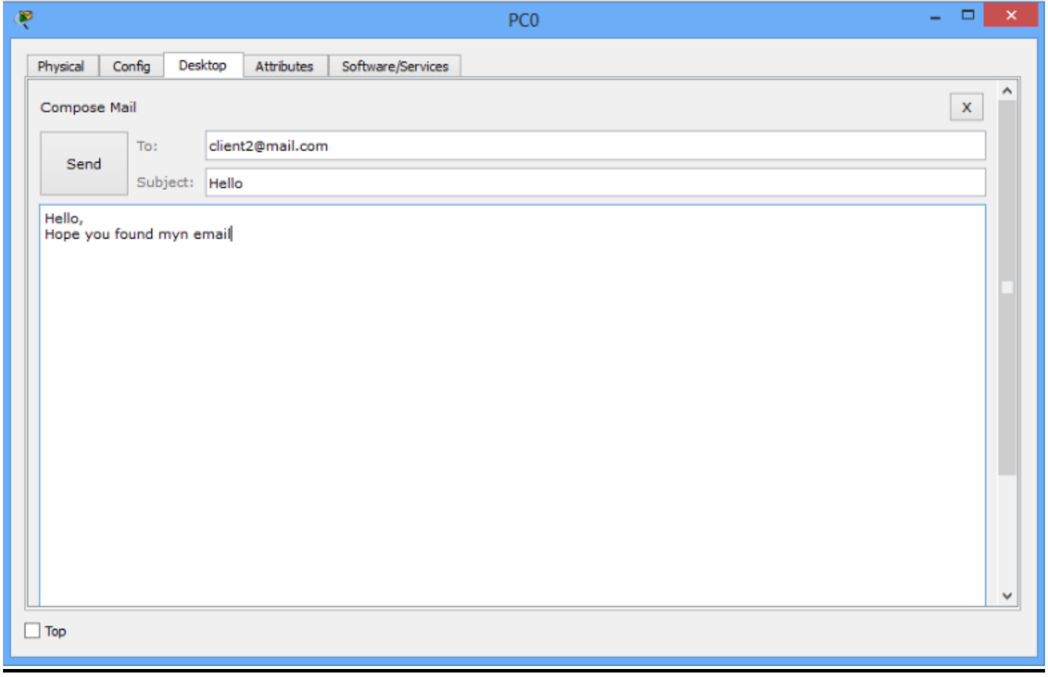
Name

Type A Record

Address

No.	Name	Type	Detail
0	mail.com	A Record	192.168.1.2

Lastly test the email service. Go to **PC0 email** client, **compose** an email and **send** its to **PC1** email address (client2@mail.com).



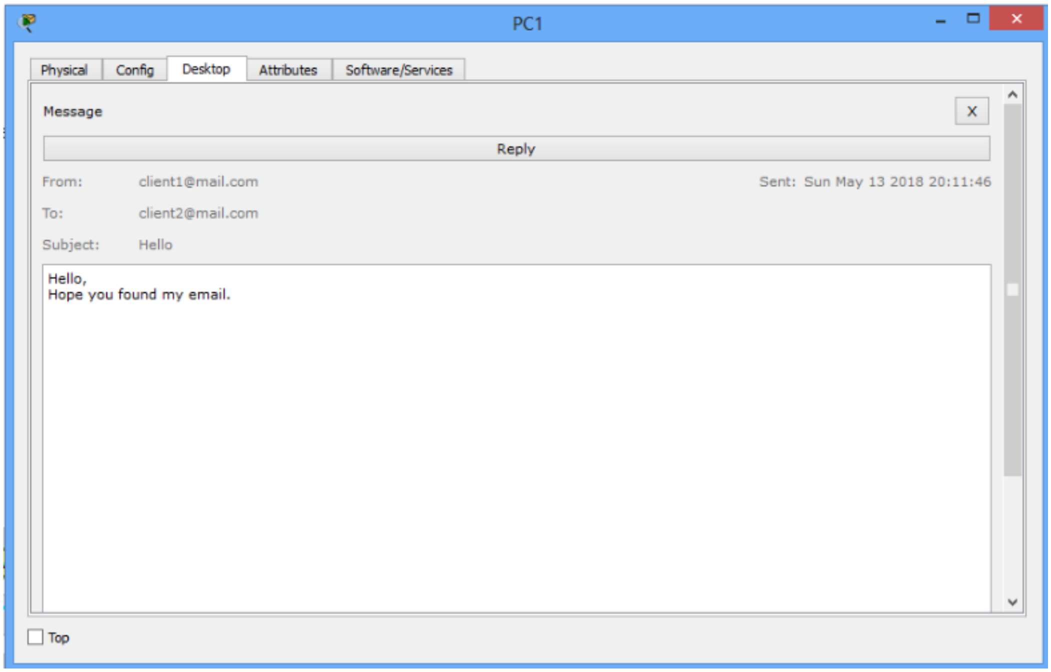
Compose Mail

To: client2@mail.com

Subject: Hello

Hello,
Hope you found myn email

Try to see whether the email from **PC0** is received on **PC1**. On the **email** client of PC1, click on **Receive.**



From: client1@mail.com

Sent: Sun May 13 2018 20:11:46

To: client2@mail.com

Subject: Hello

Hello,
Hope you found my email.

If everything is well set up, the email from **PC0** will be well received on **PC1**.

EXPERIMENT 7

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

PART 1 : RIP Routing protocol

Background

Routing Information Protocol (RIP) is an active routing protocol that operates hop count as a routing metric to find the most suitable route between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model.

Steps to Configure and Verify Three Router Connections in Cisco Packet Tracer using RIP Routing:

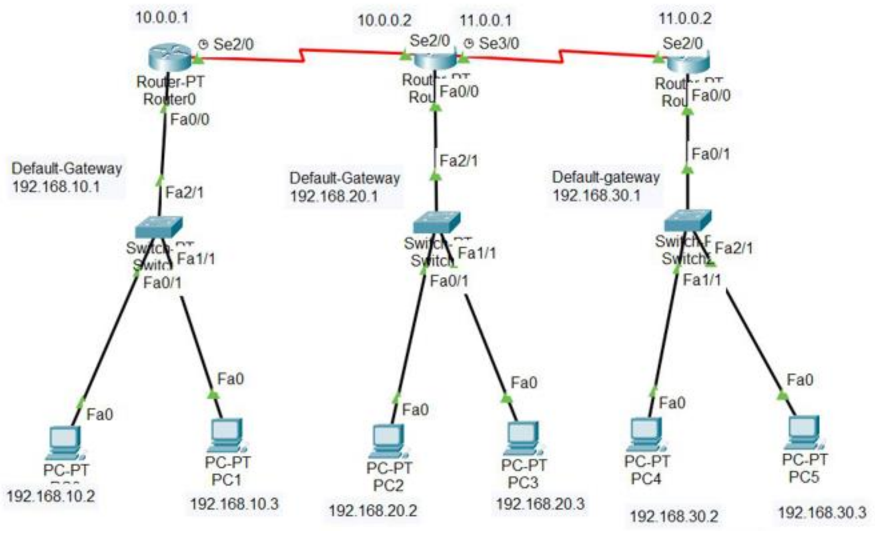
Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

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

IP Addressing Table:

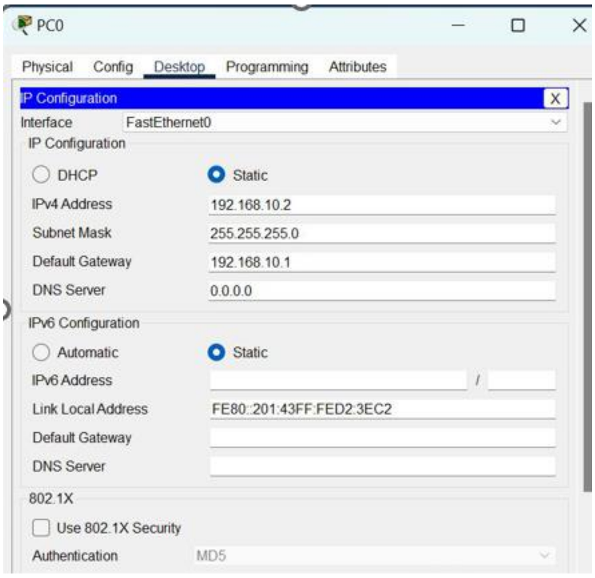
S.NO	Device	IPv4 Address	Subnet mask	Default Gateway
1.	PC0	192.168.10.2	255.255.255.0	192.168.10.1
2.	PC1	192.168.10.3	255.255.255.0	192.168.10.1
3.	PC2	192.168.20.2	255.255.255.0	192.168.20.1
4.	PC3	192.168.20.3	255.255.255.0	192.168.20.1
5.	PC4	192.168.30.2	255.255.255.0	192.168.30.1
6.	PC5	192.168.30.3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

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



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.



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.10.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::201:43FF:FED2:3EC2

Default Gateway

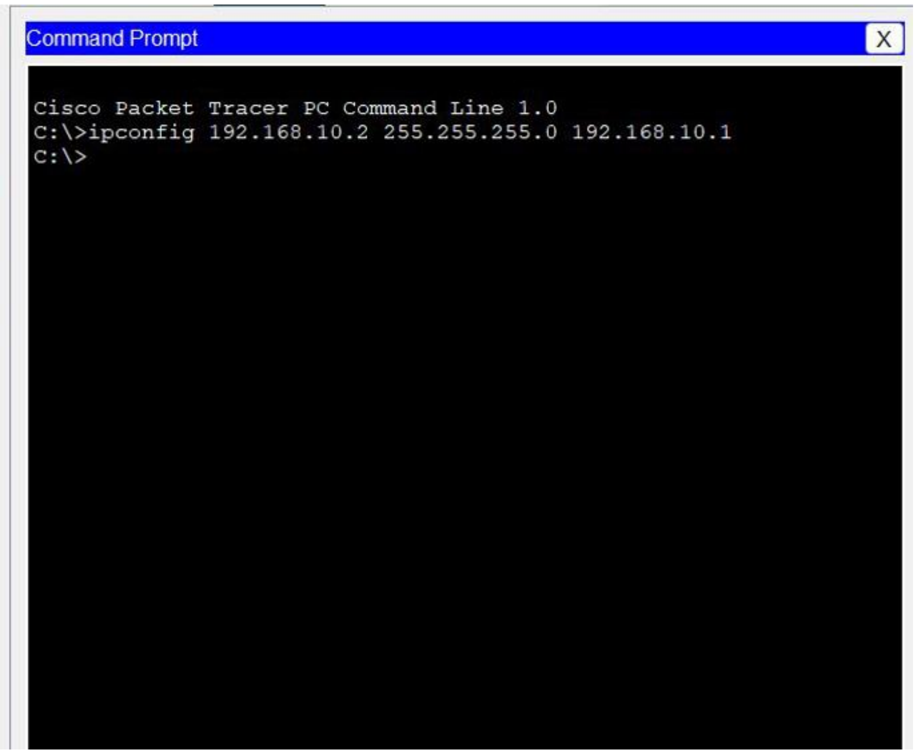
DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

- Assigning an IP address using the ipconfig command, or 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 192.168.10.2 255.255.255.0 192.168.10.1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.10.2 255.255.255.0 192.168.10.1
C:\>
```

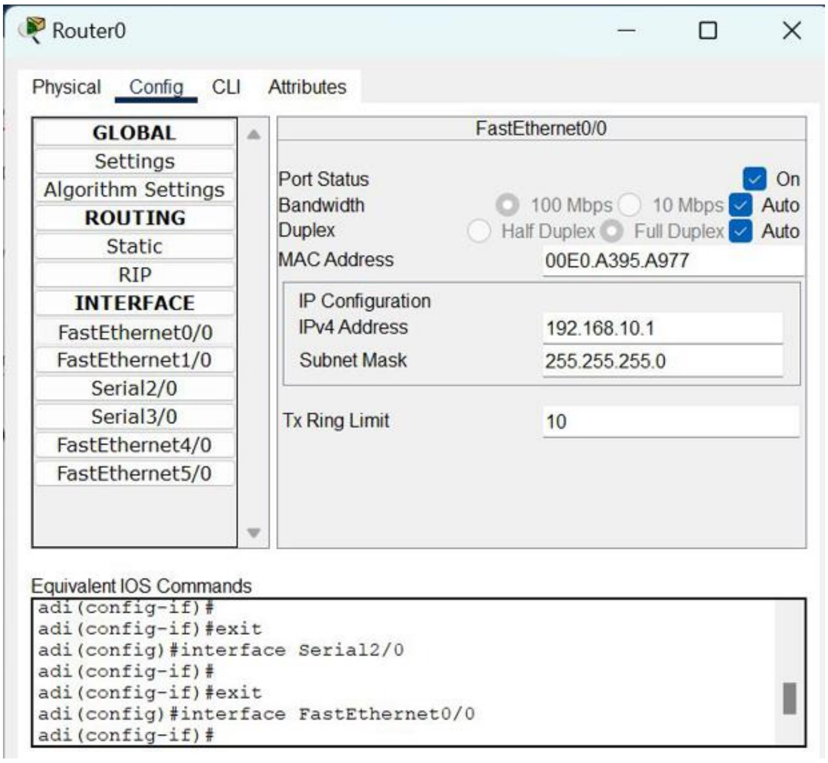
- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: Configure router with IP address and Subnet mask.

IP Addressing Table Router:

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

- To assign an IP address in router0, click on router0.
- Then, go to config and then Interfaces.
- Make sure to turn on the ports.
- Then, configure the IP address in FastEthernet and serial ports according to IP addressing Table.
- Fill IPv4 address and subnet mask.



FastEthernet0/0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.A395.A977

IP Configuration

IPv4 Address 192.168.10.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
adi(config-if)#
adi(config-if)#exit
adi(config)#interface Serial2/0
adi(config-if)#
adi(config-if)#exit
adi(config)#interface FastEthernet0/0
adi(config-if)#
```

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

Step 4: After configuring all of the devices we need to assign the routes to the routers. To assign RIP routes to the particular router:

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

CLI command : router rip
CLI command : network <network id>
RIP Routes for Router0 are given below:

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

RIP Routes for Router1 are given below:

```
Router(config)#router rip
Router(config-router)#network 192.168.20.0
Router(config-router)#network 10.0.0.0
Router(config-router)#network 11.0.0.0
```

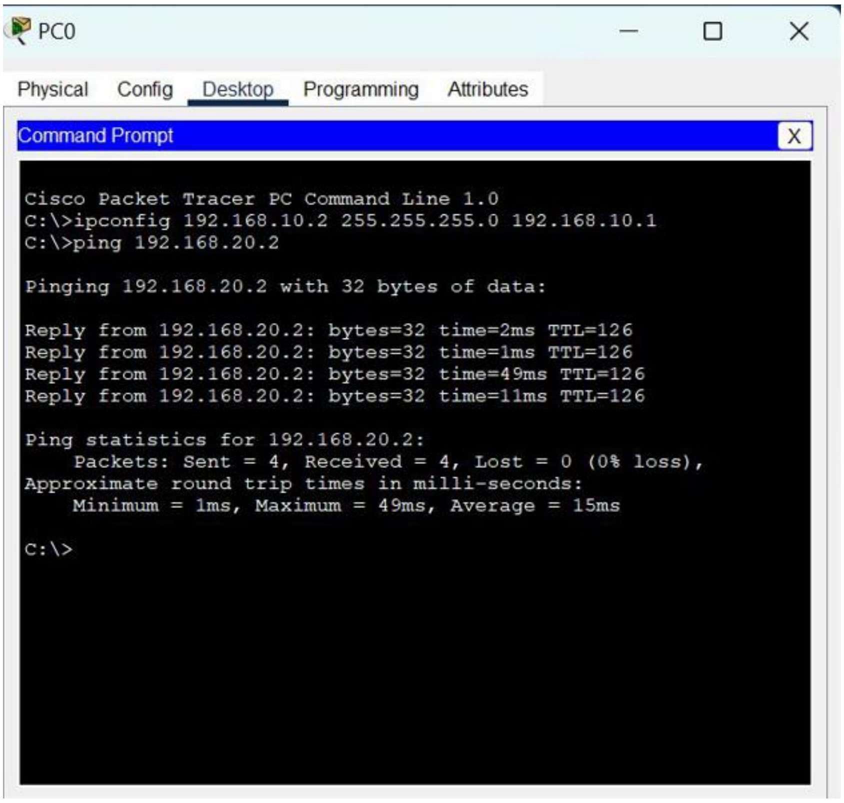
RIP Routes for Router2 are given below:

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

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

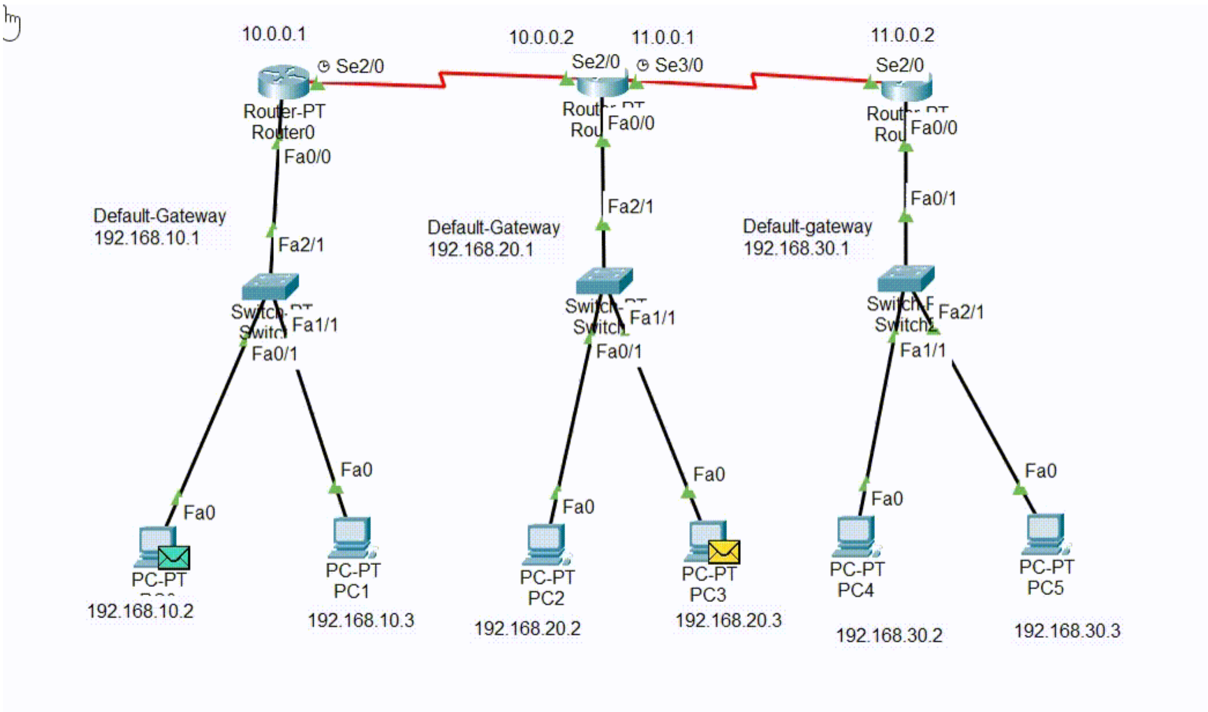
- We will use the ping command to do so.
- First, click on PC0 then Go to the command prompt.
- Then type ping <IP address of targeted node>.
- As we can see in the below image we are getting replies which means the connection is working properly.

Example : ping 192.168.20.2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.10.2 255.255.255.0 192.168.10.1
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=2ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=49ms TTL=126
Reply from 192.168.20.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 49ms, Average = 15ms

C:\>
```

- A simulation of the experiment is given below we are sending PDU from PC0 to PC2 and PC3 to PC5:



PART 2 : IGRP Routing Protocol

Backround

IGRP is a Cisco-proprietary Distance-Vector protocol, designed to be more scalable than RIP, its standardized counterpart. IGRP adheres to the following Distance-Vector characteristics: • IGRP sends out periodic routing updates (every 90 seconds). • IGRP sends out the full routing table every periodic update. • IGRP uses a form of distance as its metric (in this case, a composite of bandwidth and delay). • IGRP uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination. Other characteristics of IGRP include: • IGRP supports only IP routing. • IGRP utilizes IP protocol 9. • IGRP routes have an administrative distance of 100. • IGRP, by default, supports a maximum of 100 hops. This value can be adjusted to a maximum of 255 hops. • IGRP is a classful routing protocol. IGRP uses Bandwidth and Delay of the Line, by default, to calculate its distance metric. Reliability, Load, and MTU are optional attributes that can be used to calculate the distance metric. IGRP requires that you include an Autonomous System (AS) number in its configuration. Only routers in the same Autonomous system will send updates between each other.

Configuring IGRP

Routing protocol configuration occurs in Global Configuration mode. On Router A, to configure IGRP, we would type:

```
 Router(config)# router igrp 10
 Router(config-router)# network 172.16.0.0
 Router(config-router)# network 172.17.0.0
```

The first command, router igrp 10, enables the IGRP process. The “10” indicates the Autonomous System number that we are using. Only other IGRP routers in Autonomous System 10 will share updates with this router. The network statements tell IGRP which networks you wish to advertise to other RIP routers. We simply list the networks that are directly connected to our router. Notice that we specify the networks at their classful boundaries, and we do not specify a subnet mask.
To configure Router B:

```
 Router(config)# router igrp 10
 Router(config-router)# network 172.17.0.0
 Router(config-router)# network 172.18.0.0
```

The routing table on Router A will look like:

```
RouterA# show ip route
Gateway of last resort is not set
C 172.16.0.0 is directly connected, Ethernet0
C 172.17.0.0 is directly connected, Serial0
I 172.18.0.0 [120/1] via 172.17.1.2, 00:00:00, Serial0
```

The routing table on Router B will look like:

```
RouterB# show ip route
Gateway of last resort is not set
C 172.17.0.0 is directly connected, Serial0
C 172.18.0.0 is directly connected, Ethernet0
I 172.16.0.0 [120/1] via 172.17.1.1, 00:00:00, Serial0
```

EXPERIMENT 8

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

Background

The functions of a dynamic routing protocol are the same as a static routing protocol. If the destination is unreachable in from a point of routing then the other path can be created to reach the destination.

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	4
2.	switch	PT-Switch	2
3.	router	PT-Router	2

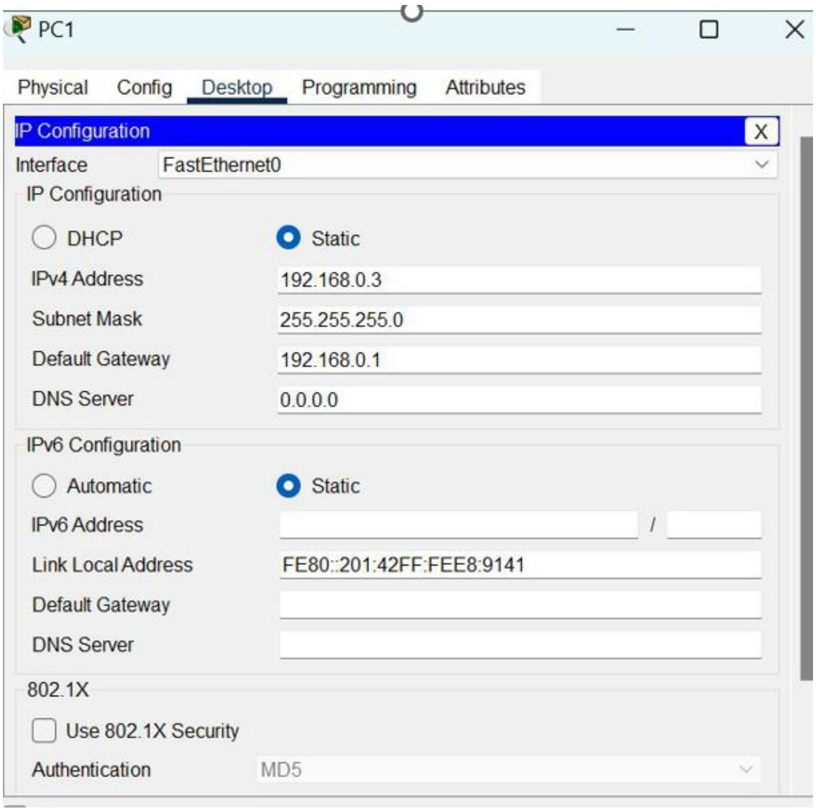
IP Addressing Table:

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

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.
-

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 PC1, click on PC1.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.0.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:42FF:FEE8:9141

Default Gateway:

DNS Server:

802.1X

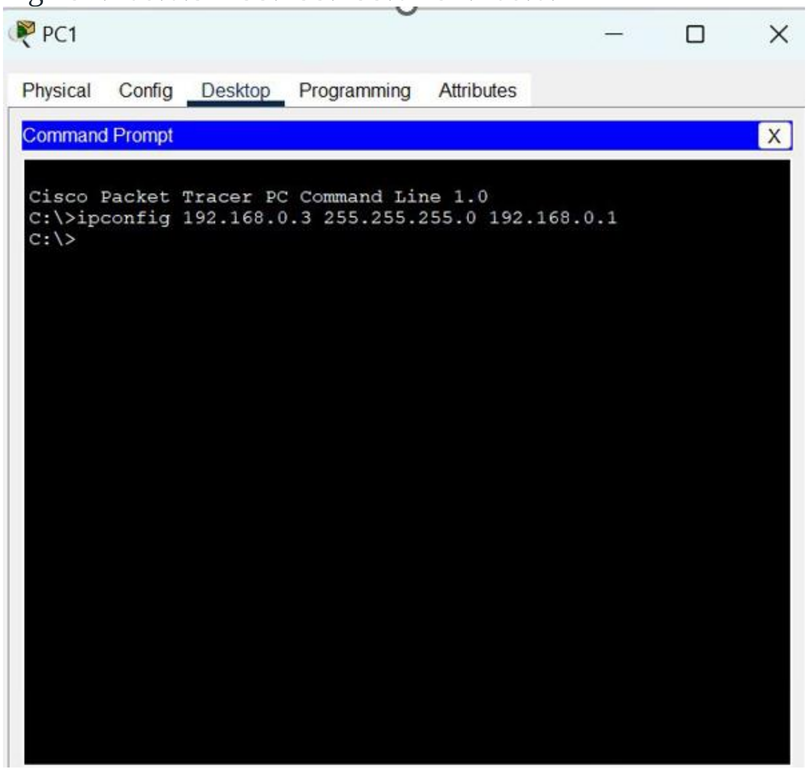
□ Use 802.1X Security

Authentication: MD5

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



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.0.3 255.255.255.0 192.168.0.1
C:\>
```

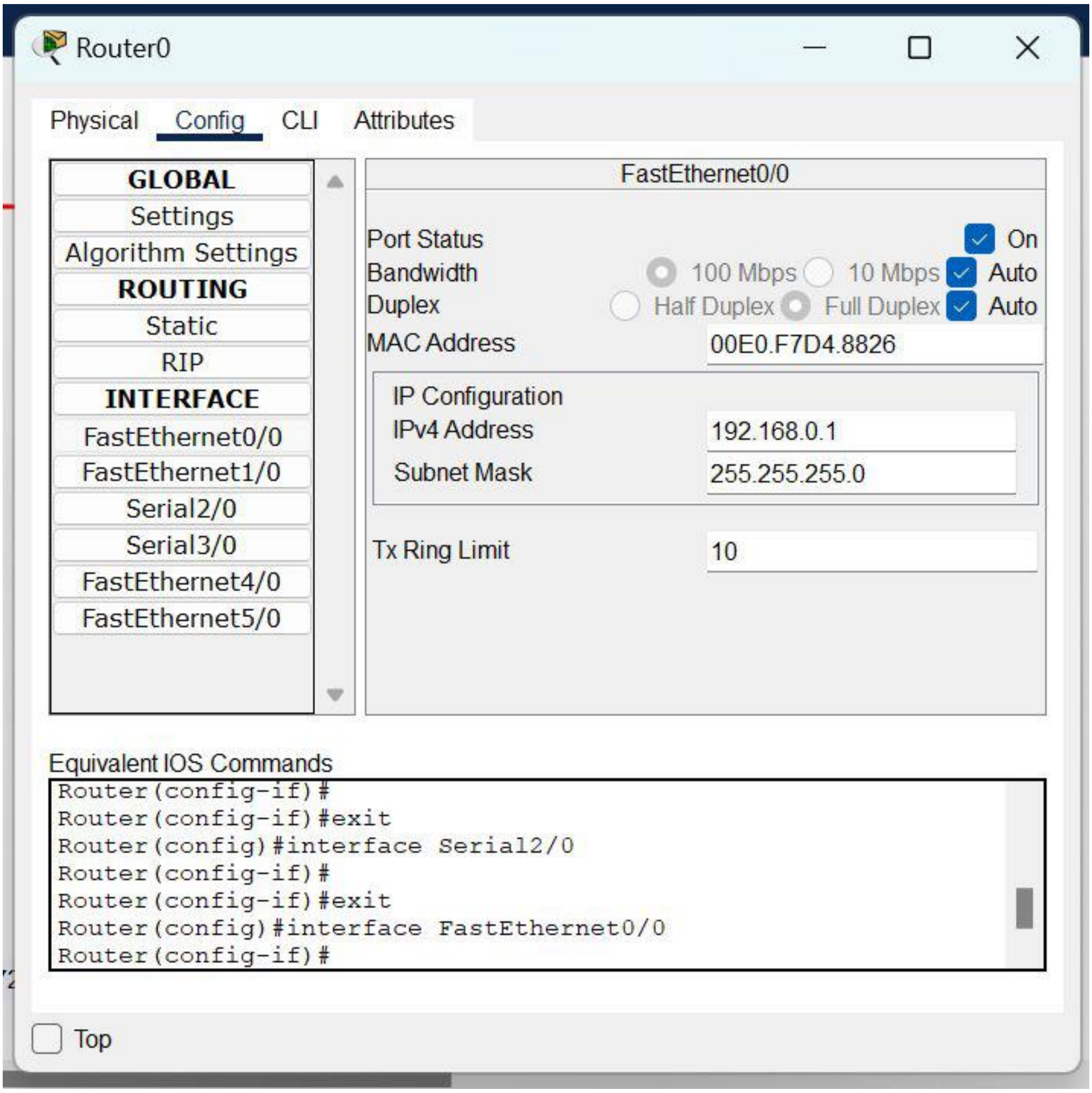
- Repeat the same procedure with other PCs to configure them thoroughly.

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

IP Addressing Table Router:

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

- 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 IP addressing Table.
- Add IPv4 address and subnet mask.



Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.F7D4.8826

IP Configuration

IPv4 Address 192.168.0.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

□ Top

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

  Step 4: After configuring all of 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 : router eigrp 10
  network <network id>
  Protocols for router0

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

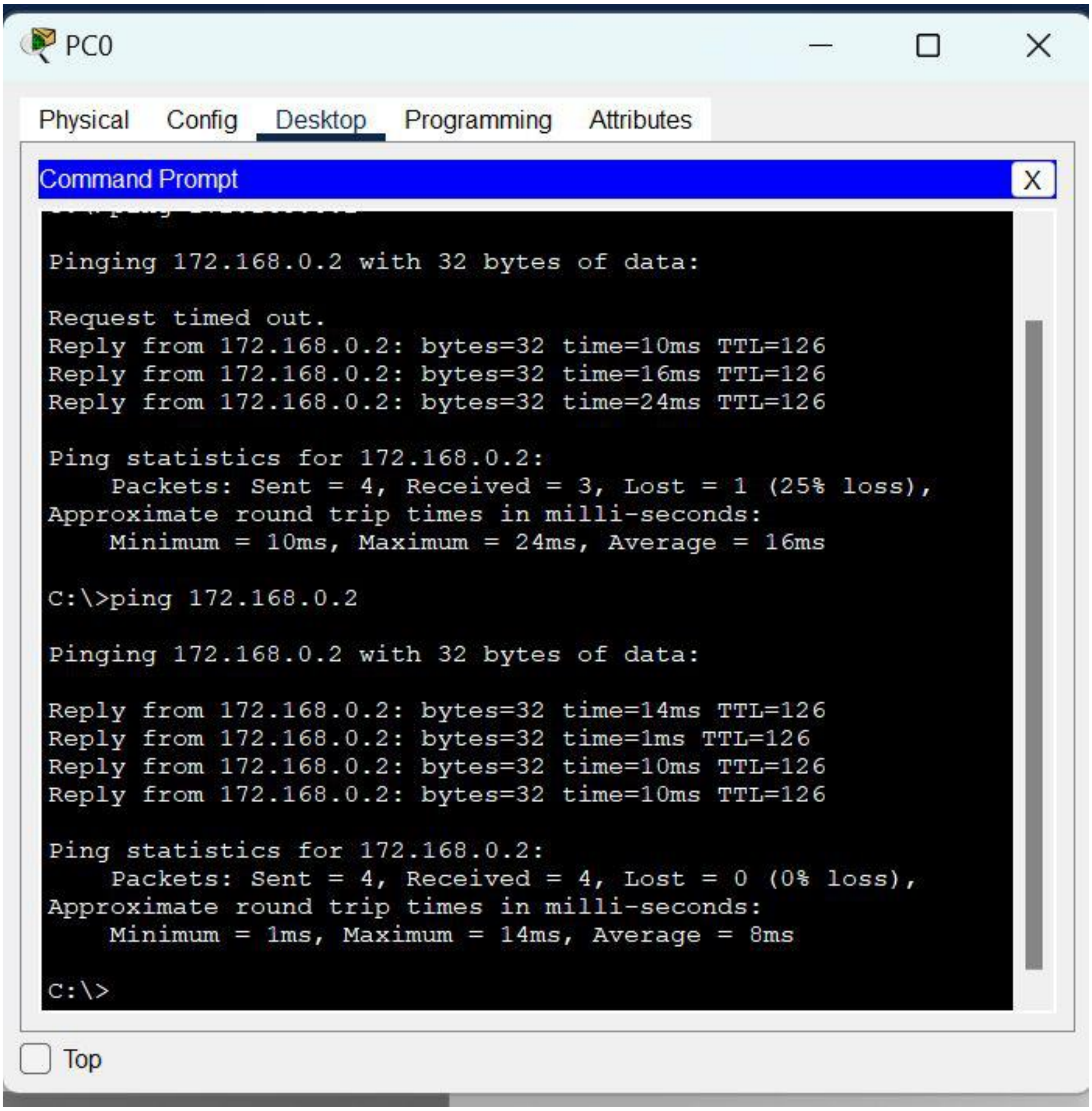
  Protocols for router0

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

  Step 5: Verifying the network by pinging the IP address of any PC. We will use the ping command to do so.

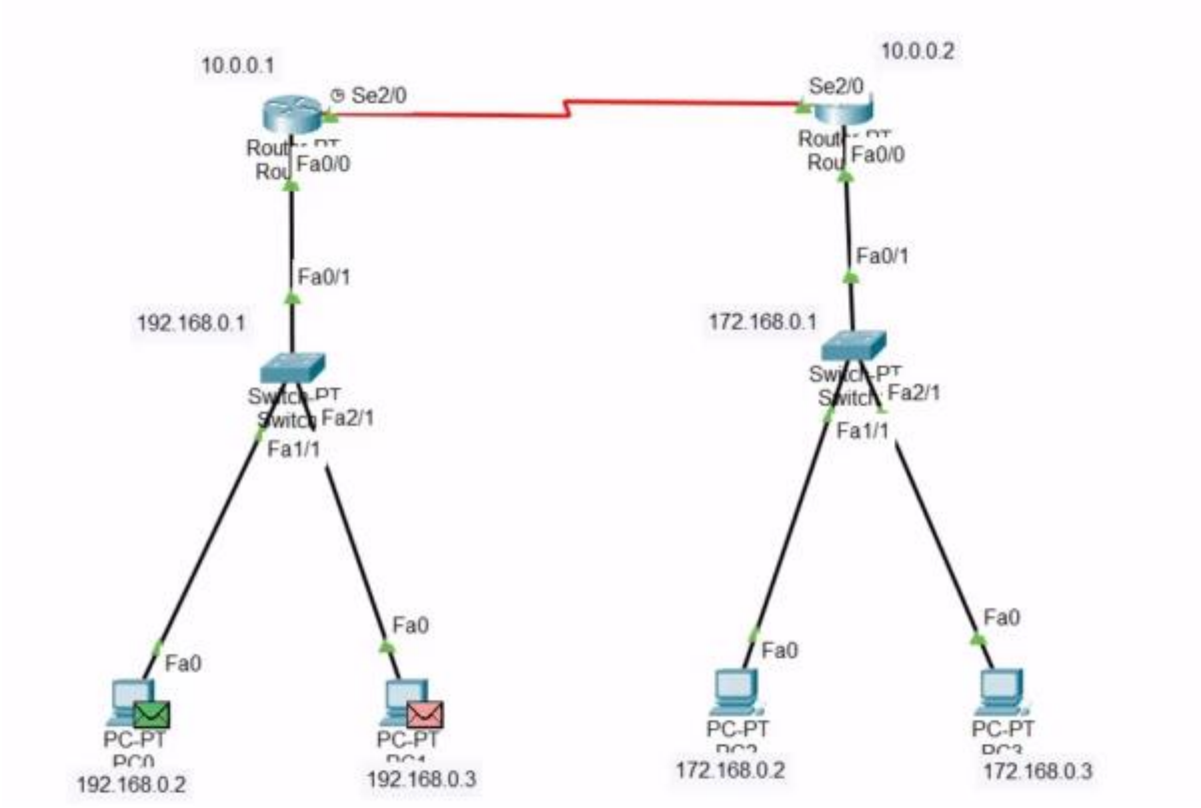
- First, click on PC0 then Go to the command prompt
- Then type ping <IP address of targeted node>
- As we can see in the below image we are getting replies which means the connection is working very fine

  Example: ping 172.168.0.2



```
Pinging 172.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 172.168.0.2: bytes=32 time=10ms TTL=126
Reply from 172.168.0.2: bytes=32 time=16ms TTL=126
Reply from 172.168.0.2: bytes=32 time=24ms TTL=126

Ping statistics for 172.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 24ms, Average = 16ms

C:\>ping 172.168.0.2

Pinging 172.168.0.2 with 32 bytes of data:

Reply from 172.168.0.2: bytes=32 time=14ms TTL=126
Reply from 172.168.0.2: bytes=32 time=1ms TTL=126
Reply from 172.168.0.2: bytes=32 time=10ms TTL=126
Reply from 172.168.0.2: bytes=32 time=10ms TTL=126

Ping statistics for 172.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 8ms

C:\>
```

- A simulation of the experiment is given below we are sending PDU from PC0 to PC2 and PC1 to PC3:


10.0.0.1
Se2/0
Router-PT
Router
Fa0/0
Fa0/1
192.168.0.1
Switch-PT
Switch
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT
PC0
192.168.0.2
PC-PT
PC1
192.168.0.3
10.0.0.2
Se2/0
Router-PT
Router
Fa0/0
Fa0/1
172.168.0.1
Switch-PT
Switch
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT
PC2
172.168.0.2
PC-PT
PC3
172.168.0.3

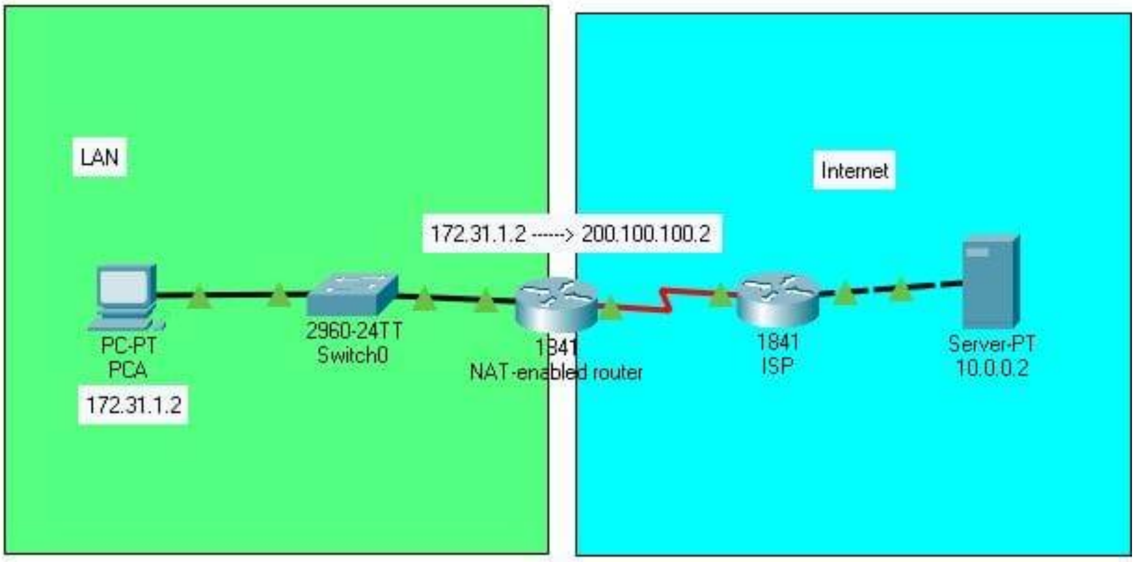
EXPERIMENT 9

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

<u>Background</u>

For a device configured with a private address to access the internet or a remote network, the address must be translated into a public routable address.

This translation takes place on a NAT-enabled router which typically operates on the border of a stub network.



Network Address Translation - Client-Server connection

In the figure above, PCA with an IP address of 172.31.1.2 wants to reach the webserver, but because PCA's address is not routable, it cannot access the webserver directly.

Instead, the NAT-enabled router translates the PC's private address of 172.31.1.2 to a public address of 200.100.100.2, which is routable over the internet.

From the server's perspective, it sees this address as the source address. Suppose the server wants to send data to the PC, it will use the same source address as its destination address.

When the data reaches the NAT-enabled router, the public address is then translated back to its original private address, and the data is forwarded back to the PC.

<u>Types of NAT</u>

Network address translation can be classified into three types.

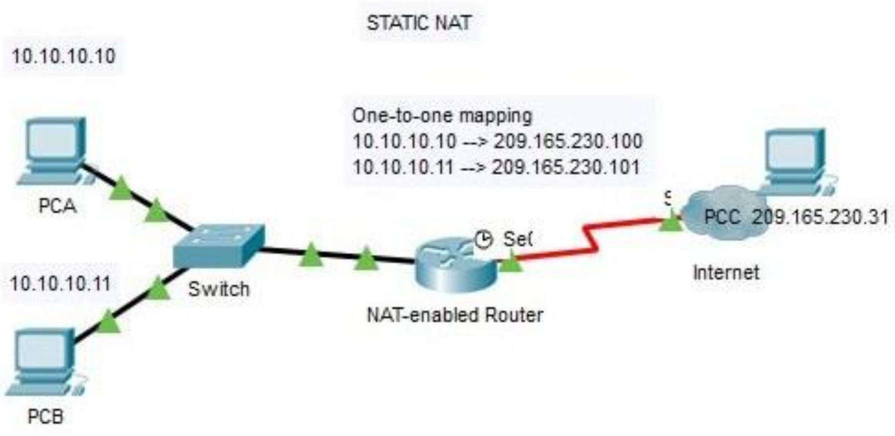
They are:

1. Static Network Translation (Static NAT)
2. Dynamic Network Address Translation (Dynamic NAT)
3. Port Address Translation (PAT)

<u>Static NAT</u>

Static NAT creates a one-to-one mapping between private and public addresses.

Static NAT is usually configured by a network administrator, and this configuration remains constant.



Static Network Address Translation

In the figure above, PCA and PCB wants to reach PCC, which is a remote network.

But because both are configured with private addresses, they can not access PCC directly.

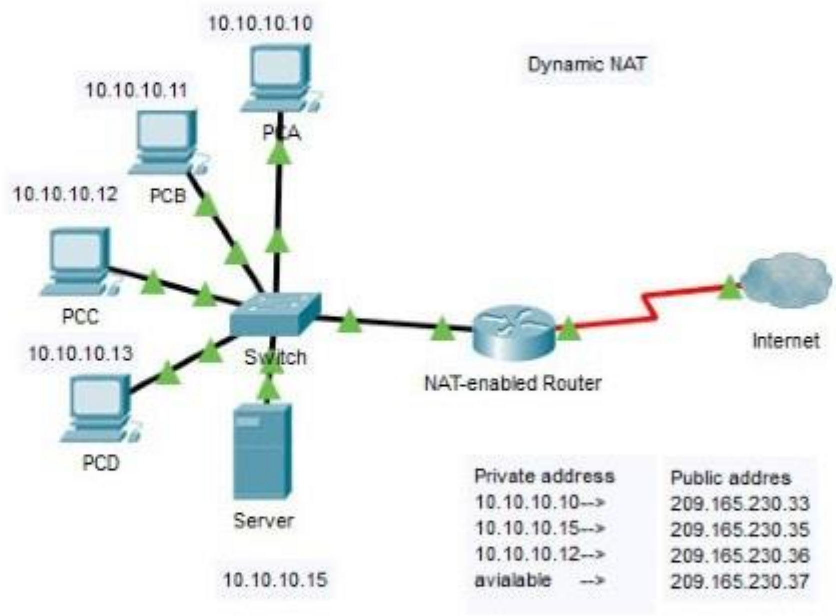
To access PCC, a NAT-enabled router is configured with static NAT, that maps their private addresses to public addresses using one-to-one relationship, thus allowing them to communicate with PCC.

Therefore, static NAT is useful for a device that needs a dedicated address, such as a web server. But, it requires an equal number of public addresses for users using them simulataneously.

Dynamic NAT

Similar to static NAT, the dynamic NAT gives a one-to-one mapping between private and public addresses. But, the mapping is done dynamically.

Dynamic NAT makes a pool of public addresses and assigns them to private addresses on a first-come-first-served (FCFS) basis to determine which private addresses ought to be translated.



Private address	Public addres
10.10.10.10-->	209.165.230.33
10.10.10.15-->	209.165.230.35
10.10.10.12-->	209.165.230.36
avialable -->	209.165.230.37

Dynamic Network Address Translation

In the figure above, an organization is assigned to four different public addresses, but the organization can have more than four internal devices that require access to the internet.

To resolve this problem, the network administrator decides to configure dynamic NAT to allow these devices to access the internet.

If all the internal devices have been assigned to all the available global addresses, then the device requesting for a public address will have to wait until one is made available.

Port Address Translation (PAT)

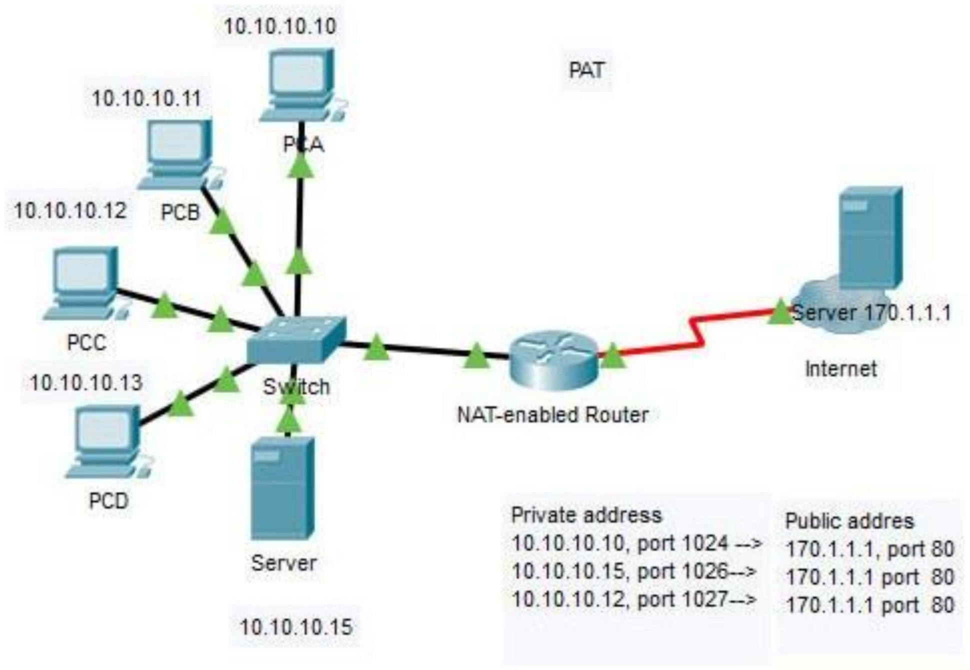
Dynamic NAT is more commonly used by organizations, to connect their devices to the internet. If their network is large, it requires a huge set of registered public addresses. Thus, it completely defeats NAT's goal.

Dynamic NAT reduces this problem to some degree. However, if a large percentage of internal hosts need access to the internet then, we must use Port Address Translation, also called NAT overload.

To understand how PAT works, it is important to recall how the host uses the Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and port numbers to transmit data.

To learn more about TCP and UDP, it is highly recommeded to go over this article before continuing to read.

With these protocols, PAT can map multiple private addresses to one or more public addresses by ensuring that devices use different TCP and UDP port numbers for each session.



Private address	Public addres
10.10.10.10, port 1024 -->	170.1.1.1, port 80
10.10.10.15, port 1026-->	170.1.1.1 port 80
10.10.10.12, port 1027-->	170.1.1.1 port 80

Port Address Translation

NAT configuration

In the first half of this article, we learned briefly about NAT and the different types of NAT. In the second part, we will cover how to implement static NAT, dynamic NAT, and PAT on a Cisco router.

Static NAT

Steps to configure static NAT

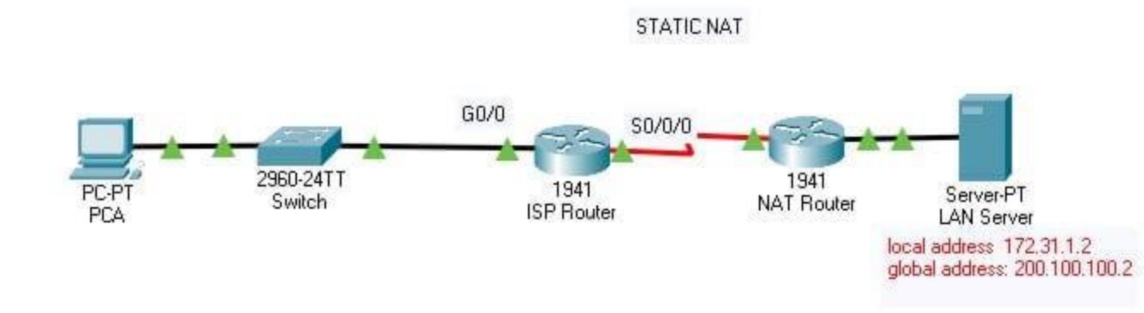
Static NAT can be configured using the following two steps.

They are:

1. Creating a mapping between the private internal address and public global address using the ip nat inside source static [private-address] [public-address] global configuration command.
2. After the mapping is made, the interfaces taking part in the NAT translation are configured as either inside or outside with respect to NAT.

The router interface associated within the LAN is assigned the inside interface using the ip nat inside interface mode command.

Similarly, the router interface associated with the internet is assigned the outside interface using the ip nat inside interface mode command.



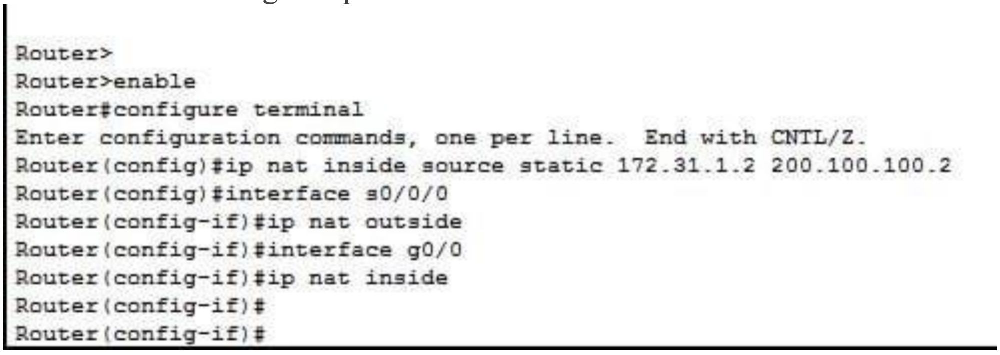
Static NAT topology

In the figure above, the Gigabit 0/0 (g0/0) interface is the inside interface because it is connected to the LAN. In contrast, the S0/0/0 interface is configured as the outside interface because it is connected to the internet.

Configuring static NAT

To configure a static NAT between the private address 172.31.1.2 and public address 200.100.100.2:

- Map the server’s private address 172.31.1.2 to the public routable address 200.100.100.2 using the command ip nat inside source static 172.31.1.2 200.100.100.2.
- Enter the “interface serial s0/0/0/” command and identify the interface as the outside interface using the command ip nat outside.
- Enter the “interface gigabitethernet g0/0” command and identify it as the inside interface relative to NAT using the ip nat inside command.



```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 172.31.1.2 200.100.100.2
Router(config)#interface s0/0/0
Router(config-if)#ip nat outside
Router(config-if)#interface g0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#
```

Static NAT configuration

Dynamic NAT

Steps to configure dynamic NAT

Dynamic NAT still requires that both the inside and the outside interfaces be configured. For allocation, it uses an access control list (ACL) to specify which private addresses are subject to translation and a NAT pool of registered IP addresses.

1. Create an ACL using the access-list 1 permit address wildcard mask command.
2. Create a NAT pool using the ip nat pool [name] [first-address] [last-address] [netmask] [subnet mask] global configuration command.

   This pool will contain the public addresses for the translation. Because, ISP assigns the public addresses contiguous to the organizations.

   The first address is the least in the given address range. And, the last address is the highest address of that range.

   The netmask identifies the network to which of these addresses belong to, using the ip nat inside source list [access-list] [number] pool [name] command to bind the ACL and the NAT Pool created.

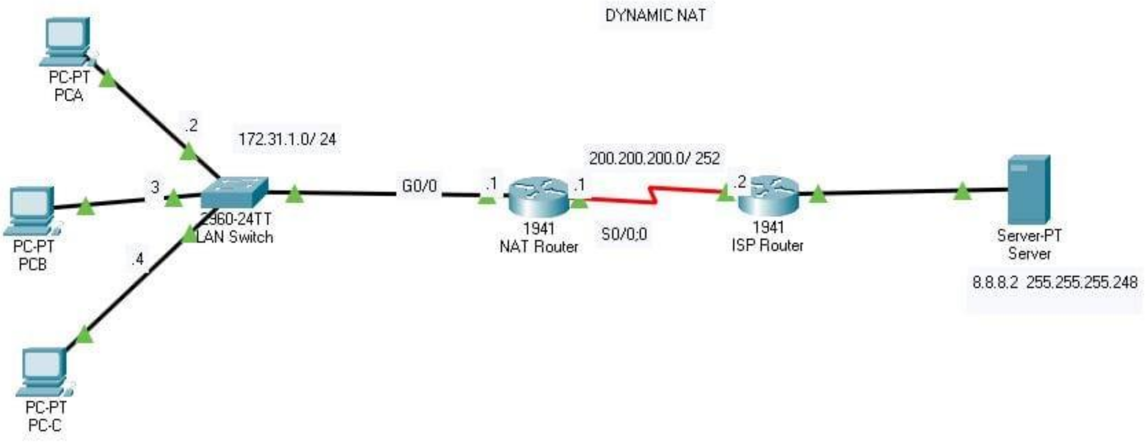
   In this case, the ACL number is 1, and the NAT POOL is LAN.

   NOTE: Different ACL numbers and pool names can be created and used, but ACL 1 and pool name LAN will be used throughout this tutorial for simplicity.

1. Use the ip nat inside interface command to enable the inside interface for NAT translation
2. Use the ip nat outside interface command to enable the outside interface for NAT translation.

Configuring dynamic NAT

An organization is assigned with two public addresses: 200.100.100.1 and 200.100.100.2. It wants to allow its internal hosts, in the private network 172.31.1.0 and 255.255.255.0 to reach the internet using dynamic NAT.

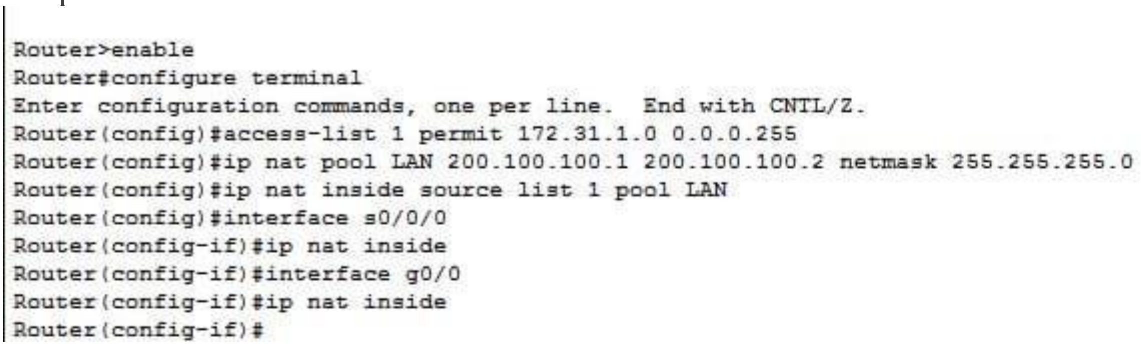


Dynamic NAT topology

To configure the dynamic NAT for the network topology above:

- Create an access list that will specify the private addresses that are allowed to be translated using the access-list 1 permit 172.31.1.0 0.0.0.255.
- Creates a pool that will contain the public addresses to be utilized for translation using the ip nat pool LAN 200.100.100.1 200.100.100.1 netmask 255.255.255.0.

- Bind the access list and the pool together using the ip inside source list 1 pool LAN. This allows for the dynamic translation of the private addresses and the public addresses in a NAT pool named LAN.
- Enter the interface serial 0/0/0/ command and identify it as an outside interface using the ip nat outside command.
- Enter the interface gigabitethernet g0/0 command and identify it as the inside interface using the ip nat inside command.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit 172.31.1.0 0.0.0.255
Router(config)#ip nat pool LAN 200.100.100.1 200.100.100.2 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool LAN
Router(config)#interface s0/0/0
Router(config-if)#ip nat inside
Router(config-if)#interface g0/0
Router(config-if)#ip nat inside
Router(config-if)#
```

PAT with multiple addresses

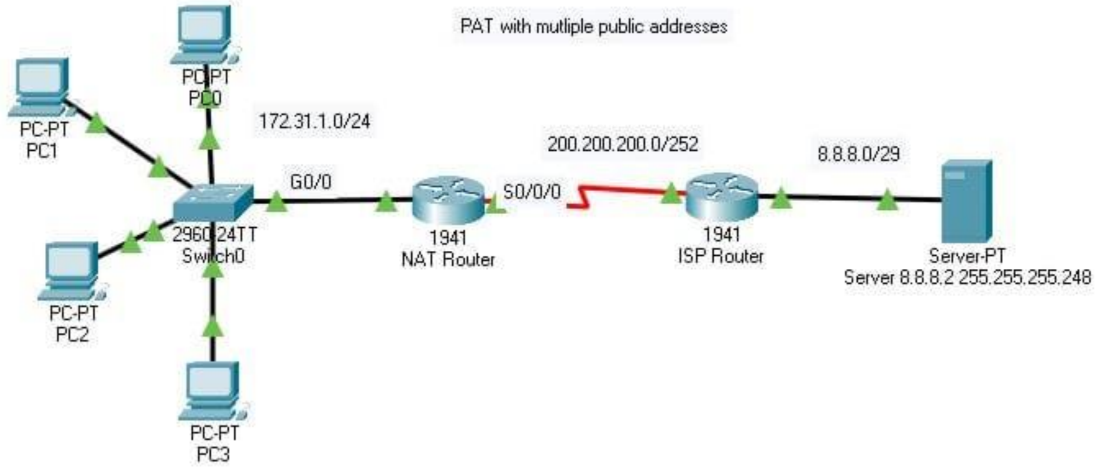
If an organization is to be assigned more than one public address by an Internet Service Provider (ISP), then configuring PAT looks exactly like a dynamic NAT, except that the ip nat inside source list--- pool command in step 3, with an overload keyword added at the end.

Steps to configure PAT with multiple public addresses

1. Create an ACL using the access-list 1 permit [address][wildcard mask].
2. Create a NAT pool using the ip nat pool [name] [first-address] [last-address] [netmask] [subnet mask] global configuration command. This pool will contain the public addresses to be used for the translation.
3. The ip nat inside source list [ACL] [number] pool [name] overload The full command is ip nat inside source list 1 pool LAN overload.
4. Use the ip nat inside interface command to enable the inside interface for NAT translation
5. Use the ip nat outside interface command to enable the outside interface for NAT translation.

Configuring PAT with multiple public addresses

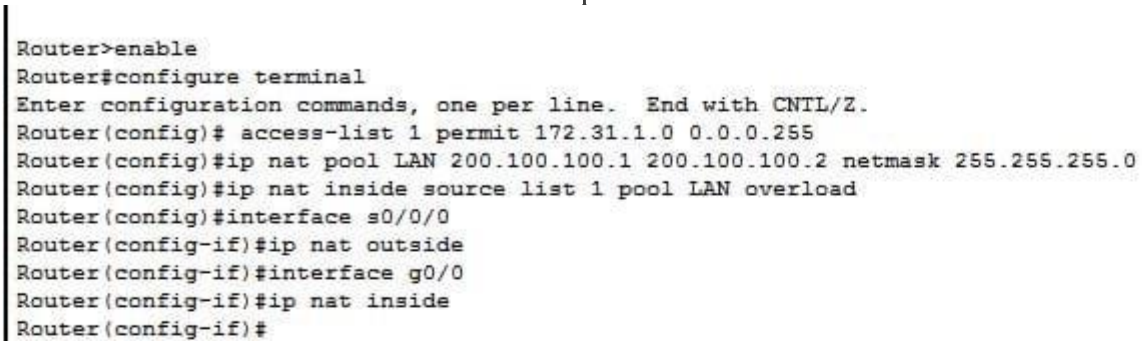
An organization is assigned to two public addressees: 200.100.100.1 and 00.100.100.2, and it wants to allow its internal hosts, in the private network 172.31.1.0 - 255.255.255.0 to reach the internet using PAT.



PAT topology

To configure PAT for the network topology above, the following steps are applied:

1. Create an ace list that will specify which private addresses are allowed to be translated using the access-list 1 permit 172.31.1.0 0.0.0.255
2. ip nat pool LAN 200.100.100.1 200.100.100.1 [netmask] 255.255.255.0 creates a pool that contains the public addresses to be used for translation.
3. Bind the access list and the pool together using the ip inside source list 1 pool LAN overload. This allows for the dynamic mapping of the private addresses and the public address in the NAT pool named LAN. The **overload** keyword used here is the only configuration difference between PAT and dynamic NAT.
4. Enter the interface serial 0/0/0/ to identify the interface as the outside interface using the ip nat outside command.
5. Enter gigabitethernet g0/0 using the interface gigabitethernet g0/0 command and identify it as the inside interface relative to NAT with the ip nat inside command.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-list 1 permit 172.31.1.0 0.0.0.255
Router(config)#ip nat pool LAN 200.100.100.1 200.100.100.2 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool LAN overload
Router(config)#interface s0/0/0
Router(config-if)#ip nat outside
Router(config-if)#interface g0/0
Router(config-if)#ip nat inside
Router(config-if)#
```

PAT with multiple public address configuration

PAT with single public address

Steps to configure PAT with a single address

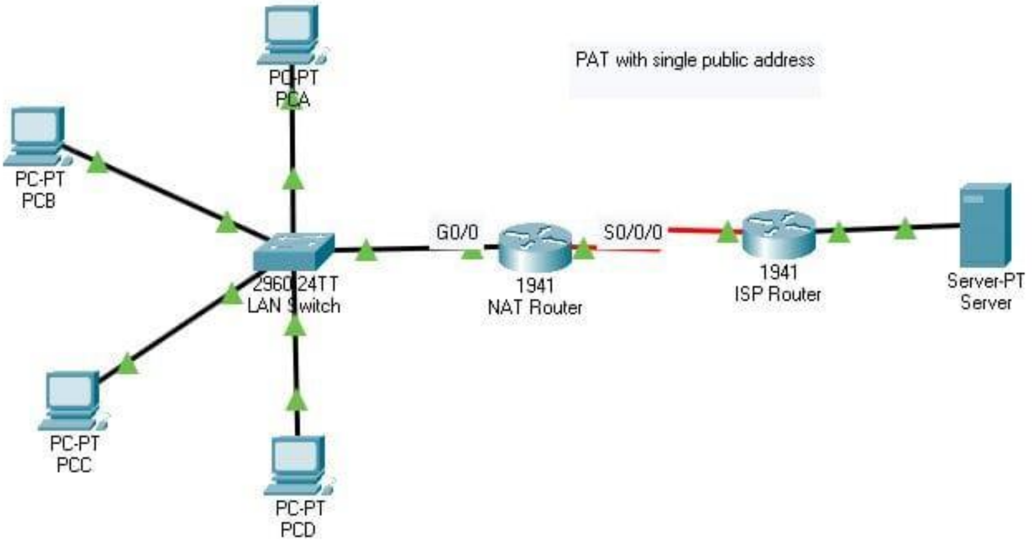
If an organization is assigned a single public address by an ISP. Then, PAT can be configured with a little changes when compared to PAT with multiple addresses.

In this situation, a NAT pool is not created, but an outside interface used for the translation is used in place of the NAT pool as mentioned in step 3 above.

1. Create an ACL using the access-list 1 permit [address] [wildcard mask].
2. PAT is enabled using the ip nat inside source list [ACL] [number] interface [interface-type/number] overload. The interface used for this is an outside interface, and it's configured as the single public address assigned to the organization by an ISP.
3. Use the ip nat inside interface command to enable the inside interface for Nat translation.
4. Use the ip nat outside interface command to enable the outside interface for NAT translation.

Configuring PAT with one public address

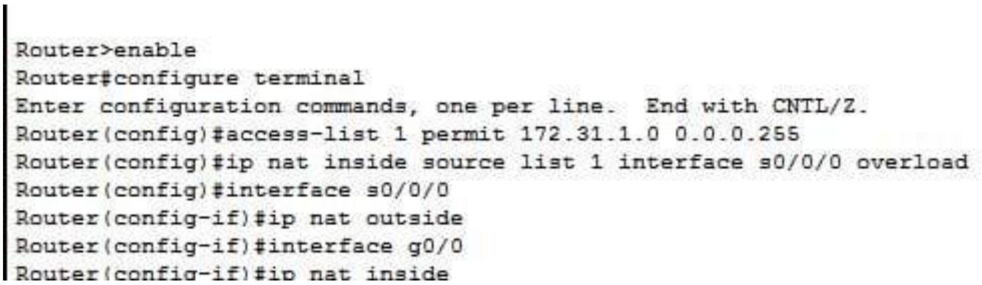
An organization is assigned one public address 200.100.100.1, and it wants to allow its internal hosts in the private network 172.31.1.0 - 255.255.255.0 to reach the internet using PAT.



PAT topology with one public address

To configure PAT for the topology above, the following steps will be applied:

1. Create an ace list that will specify which private addresses are allowed to be translated, using the access-list 1 permit 172.31.1.0 0.0.0.255 command.
2. Bind the access list and the outside interface together using the ip inside source list 1 interface s0/0/0 overload.
3. Enter the interface serial 0/0/0/ command to identify it as an outside interface relative to NAT using the: ip nat outside command.
4. Enter the interface gigabitethernet g0/0 command and identify it as an inside interface relative to NAT using the ip nat inside command.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit 172.31.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface s0/0/0 overload
Router(config)#interface s0/0/0
Router(config-if)#ip nat outside
Router(config-if)#interface g0/0
Router(config-if)#ip nat inside
```

PAT with one public address configuration

The figure above shows the configuration of PAT using one public address on a Cisco router.

EXPERIMENT 10

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

Background

install Wireshark, a well-known network protocol analyzer and monitoring tool. Wireshark captures all packets sent or received by the computer NIC. It can be installed either in the lab or on a PC at home. You will use it to trace and view various types of network protocols and traffic. Wireshark was formerly known as Ethereal.

Wireshark software is freeware and is available from www.wireshark.org. The software installer, wireshark- setup-0.99.5.exe, should be available on the local Networking Academy server.

The following resources are required:

•A Windows XP-based PC with an Ethernet network and at least two hosts

•Wireshark Version 0.99.5 software (or most current version)

•Internet connectivity (optional but desirable)

•Access to the PC command prompt

•Access to PC network TCP/IP configuration

Step 1: Install and launch Wireshark

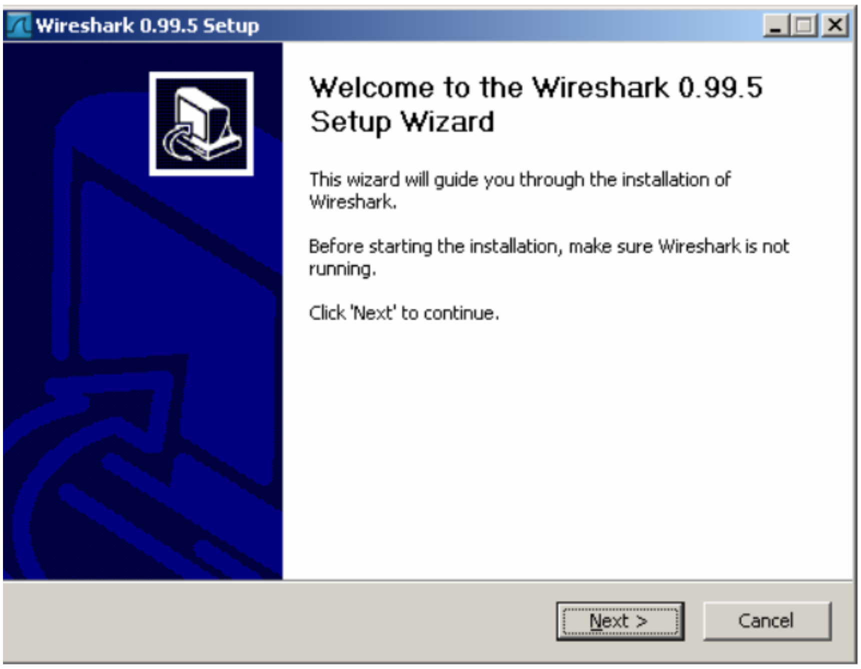
If Wireshark has been loaded on the PC previously, go to the Wireshark program folder Start > All Programs > Wireshark > Wireshark and click the application icon.

If Wireshark has not been installed, follow these steps:

a. Given the local network path to the Wireshark software installer, wireshark-setup-0.99.5.exe,

download the installer to the PC desktop.

b.Double-click the installer and follow the installation prompts, accepting the defaults.



Welcome to the Wireshark 0.99.5 Setup Wizard

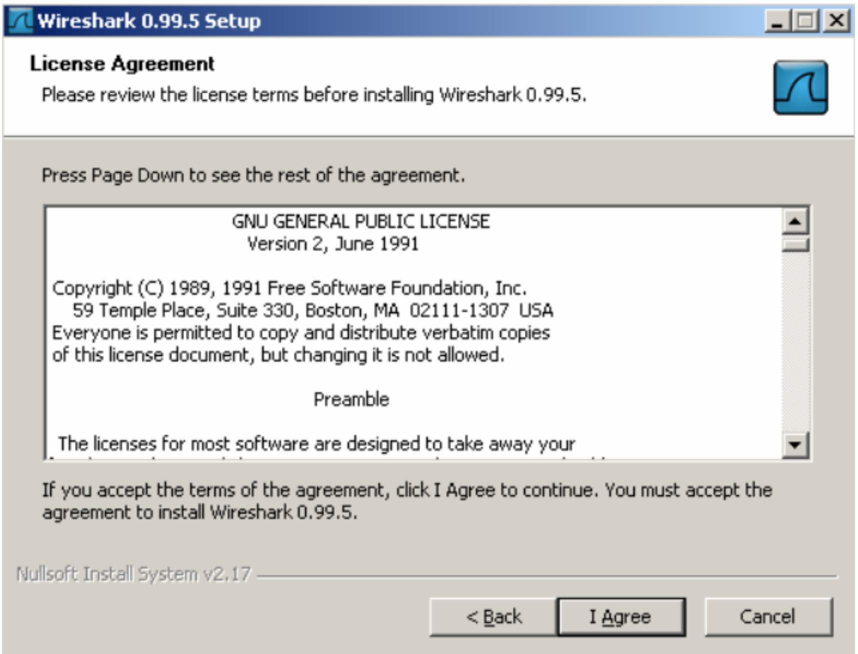
This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

1) Click I Agree

.



Wireshark 0.99.5 Setup

License Agreement

Please review the license terms before installing Wireshark 0.99.5.

Press Page Down to see the rest of the agreement.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

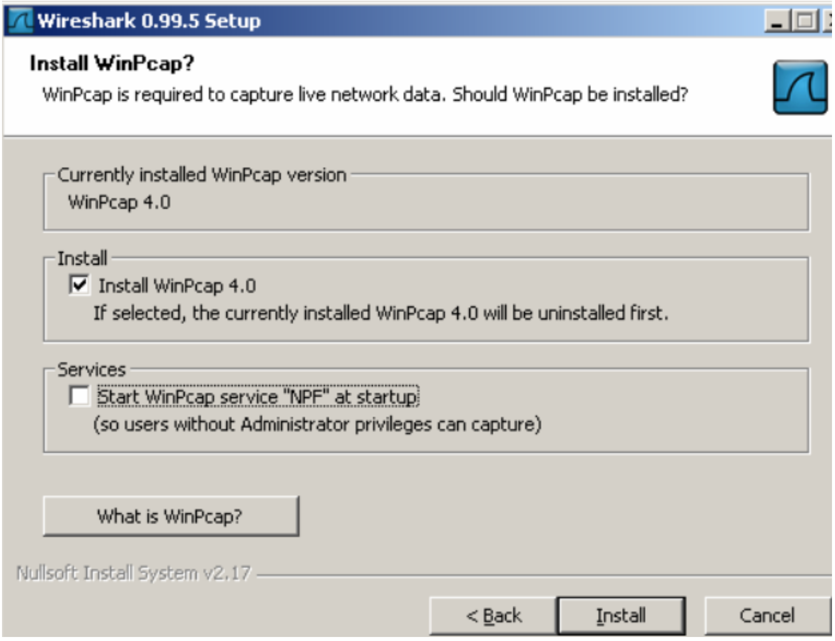
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 0.99.5.

2)Make sure to install WinPcap on the PC. WinPcap includes a driver to support packet capture. Wireshark uses this library to capture live network data with Windows



Wireshark 0.99.5 Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version
WinPcap 4.0

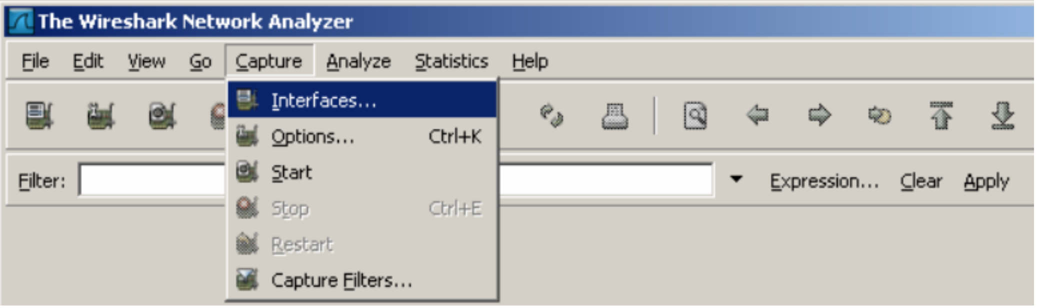
Install
☑ Install WinPcap 4.0
If selected, the currently installed WinPcap 4.0 will be uninstalled first.

Services
□ Start WinPcap service "NPF" at startup
(so users without Administrator privileges can capture)

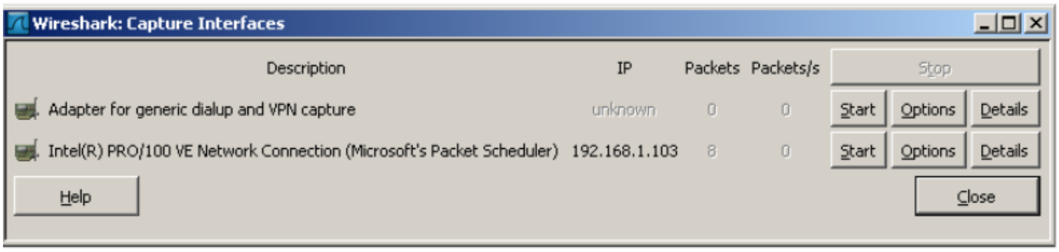
c. Click Install and follow the remaining prompts to the end of the installation process.
d. After the software is installed, click the checkbox to launch Wireshark.

Step 2: Select an interface to use for capturing packets

a. Start the Wireshark application.
b. From the Capture menu, click Interfaces



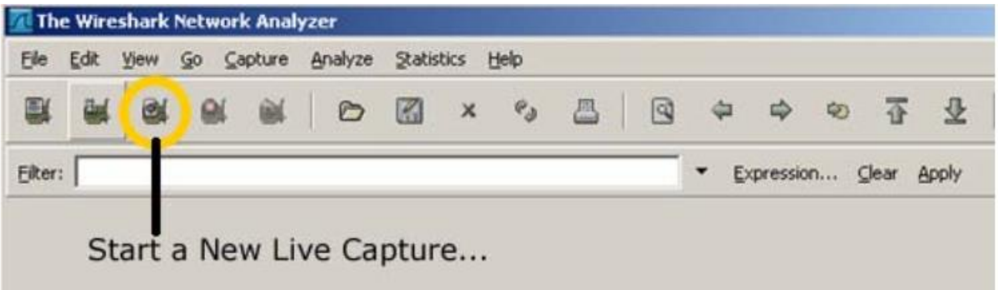
3)Click the Start button for the Ethernet interface (NIC) that you want to use to capture network traffic.



Description	IP	Packets	Packets/s			
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler)	192.168.1.103	8	0	Start	Options	Details

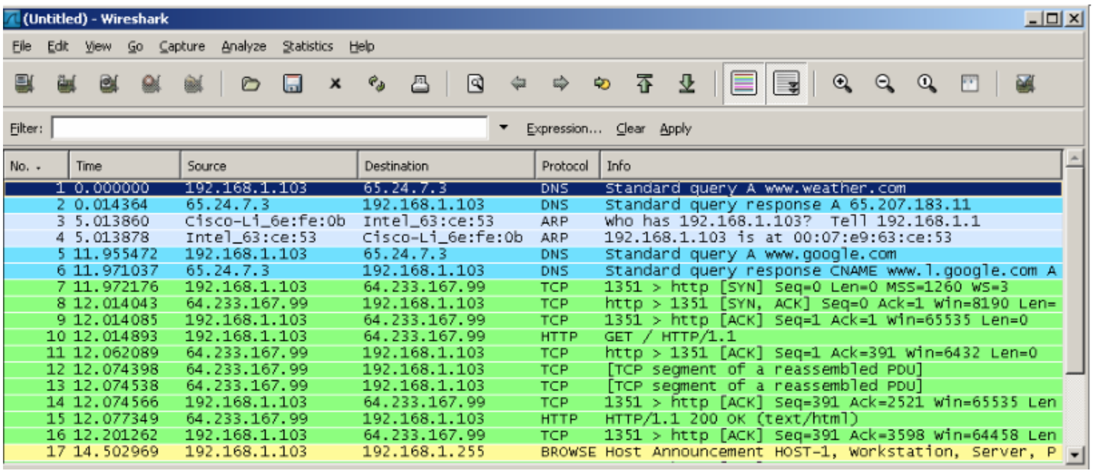
Step 3: Start a network capture

a. Scroll through the menus and view the toolbar on the Wireshark startup Interface.
b. Click the New Live Capture button and observe the information gathered by Wireshark. Allow the capture to continue for a few minutes so that you can observe the different types of traffic on the network.



Step 4: Analyze Web traffic information

a. If Internet connectivity is available, open a browser and go to www.google.com. Minimize the Google window and return to Wireshark. You should see captured traffic similar to that shown below. Locate the Source, Destination, and Protocol columns on the Wireshark display screen.



```
No. -  Time       Source             Destination        Protocol Info
    1 0.000000   192.168.1.103      65.24.7.3          DNS      Standard query A www.weather.com
    2 0.014364   65.24.7.3          192.168.1.103      DNS      Standard query response A 65.207.183.11
    3 5.013860   Cisco-Li_6e:fe:0b  Intel_63:ce:53     ARP      Who has 192.168.1.103?  Tell 192.168.1.1
    4 5.013878   Intel_63:ce:53     Cisco-Li_6e:fe:0b  ARP      192.168.1.103 is at 00:07:e9:63:ce:53
    5 11.955472  192.168.1.103      65.24.7.3          DNS      Standard query A www.google.com
    6 11.971037  65.24.7.3          192.168.1.103      DNS      Standard query response CNAME www.l.google.com A
    7 11.972176  192.168.1.103      64.233.167.99      TCP      1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
    8 12.014043  64.233.167.99      192.168.1.103      TCP      http > 1351 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=
    9 12.014085  192.168.1.103      64.233.167.99      TCP      1351 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
   10 12.014893  192.168.1.103      64.233.167.99      HTTP     GET / HTTP/1.1
   11 12.062089  64.233.167.99      192.168.1.103      TCP      http > 1351 [ACK] Seq=1 Ack=391 Win=6432 Len=0
   12 12.074398  64.233.167.99      192.168.1.103      TCP      [TCP segment of a reassembled PDU]
   13 12.074538  64.233.167.99      192.168.1.103      TCP      [TCP segment of a reassembled PDU]
   14 12.074566  192.168.1.103      64.233.167.99      TCP      1351 > http [ACK] Seq=391 Ack=2521 Win=65535 Len
   15 12.077349  64.233.167.99      192.168.1.103      HTTP     HTTP/1.1 200 OK (text/html)
   16 12.201262  192.168.1.103      64.233.167.99      TCP      1351 > http [ACK] Seq=391 Ack=3598 Win=64458 Len
   17 14.502969  192.168.1.103      192.168.1.255      BROWSE   Host Announcement HOST-1, Workstation, Server, P
```