Name: Priyush B. Khobragade

PRN: 211112018

Batch: 03

EXPERMINT: 07

●Aim: -RIP protocol graphical simulation using packet trace.

●Theory:

Routing Information Protocol (RIP):

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

Hop Count

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

Features of RIP:

- Updates of the network are exchanged periodically.
- Updates (routing information) are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.

RIP versions:

There are three versions of routing information protocol – RIP Version1, RIP Version2, and RIPng.

Steps Implementing RIP Protocol 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

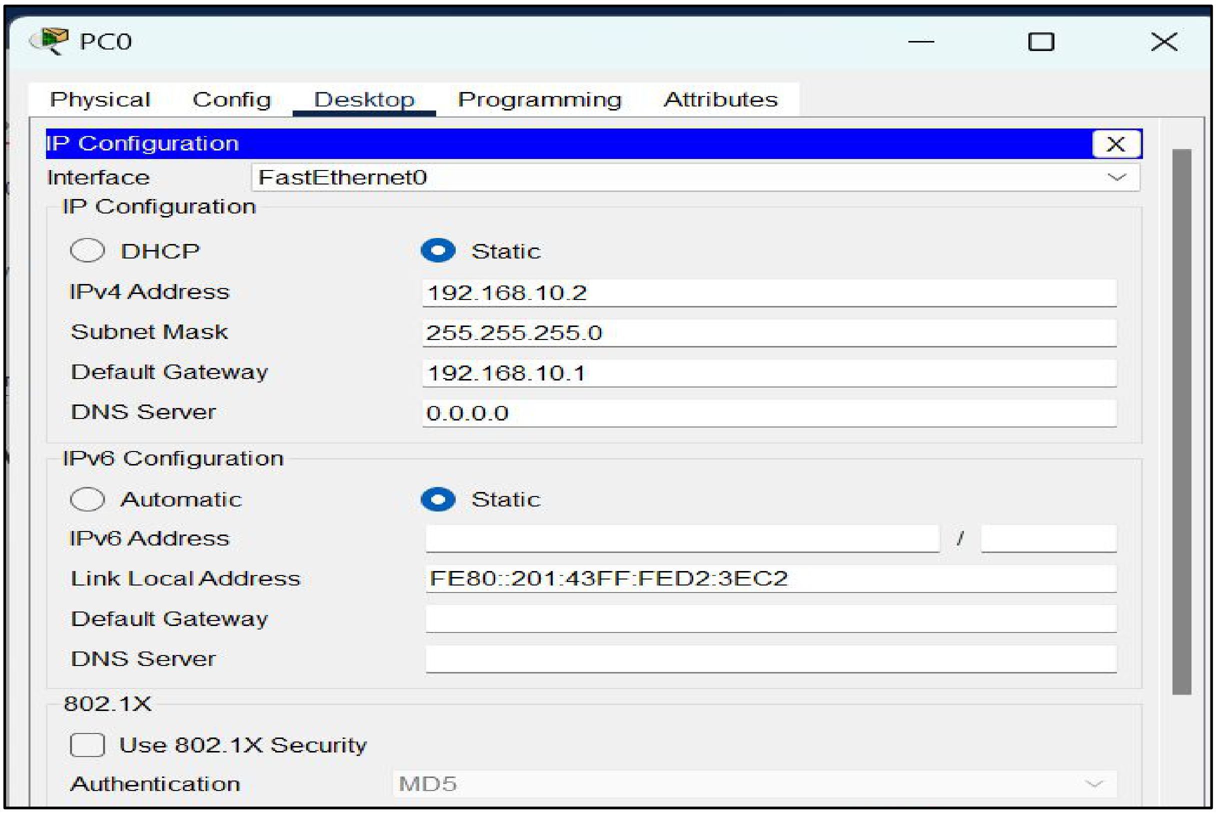
IP Addressing Table:

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

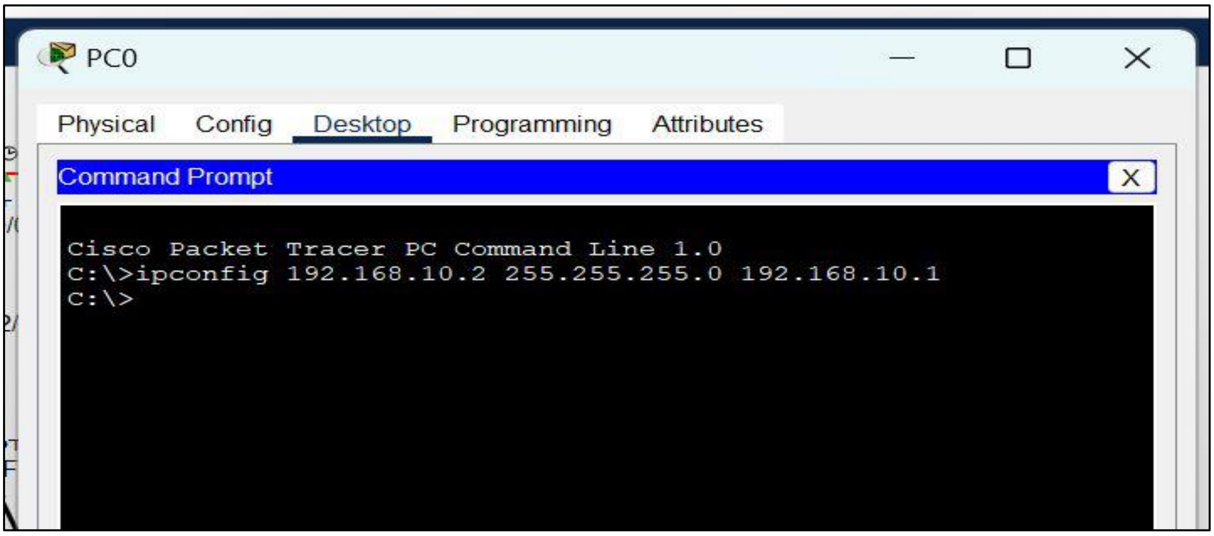
□ Use 802.1X Security

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

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



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

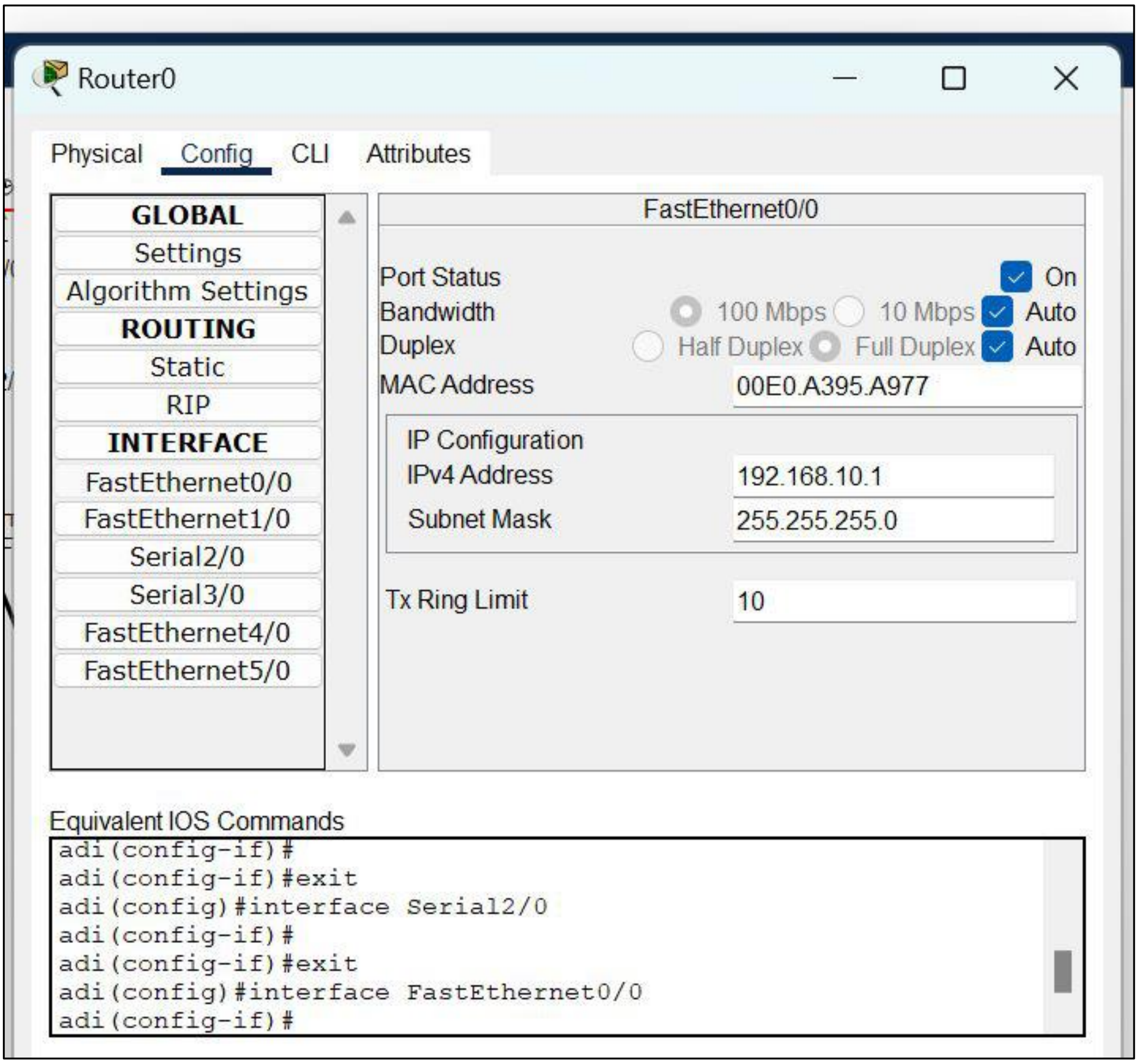
Step 3: Configure router with IP address and Subnet mask.

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 : network <network id>

RIP Routes for Router0 are given below:

Router(config)#network 192.168.10.0

Router(config)#network 10.0.0.0

RIP Routes for Router1 are given below:

Router(config)#network 192.168.20.0

Router(config)#network 10.0.0.0

Router(config)#network 11.0.0.0

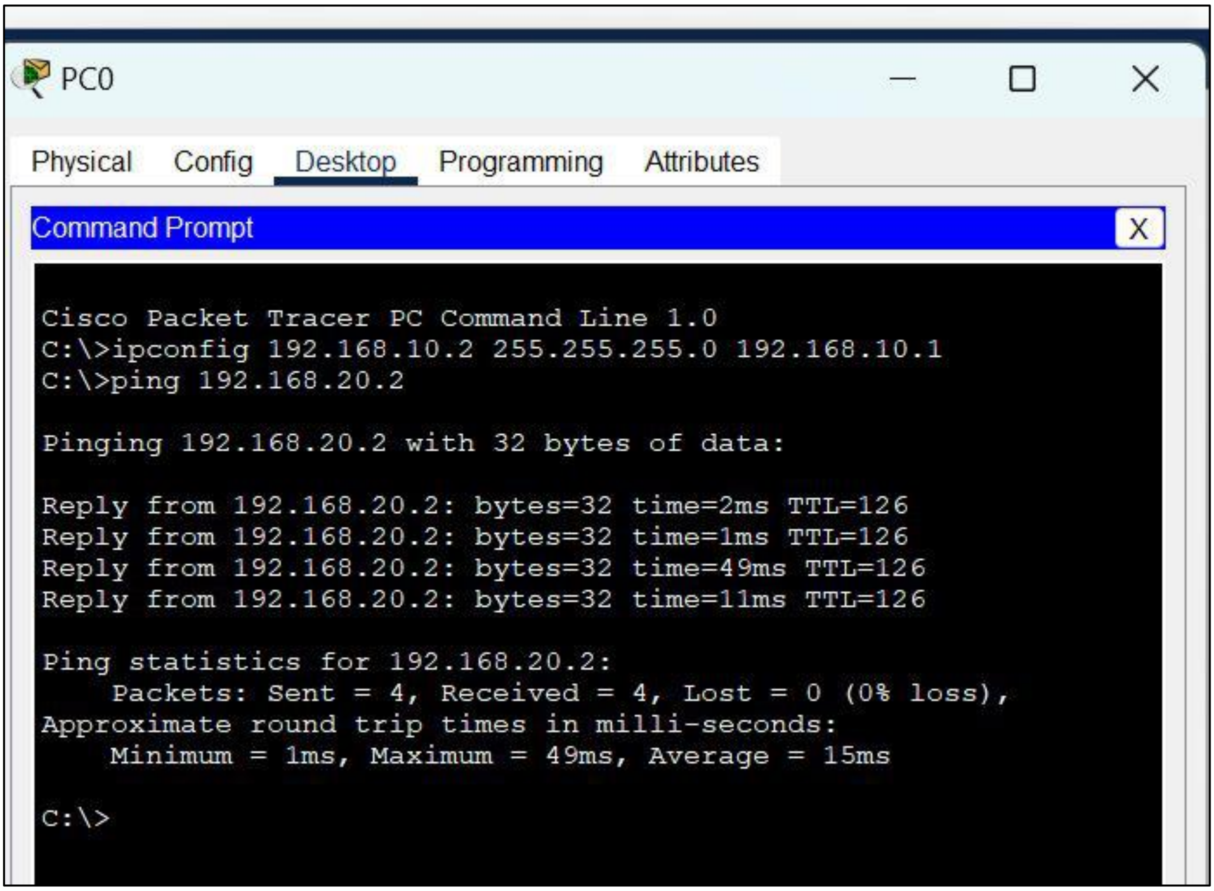
RIP Routes for Router2 are given below:

Router(config)#network 192.168.30.0

Router(config)#network 11.0.0.0

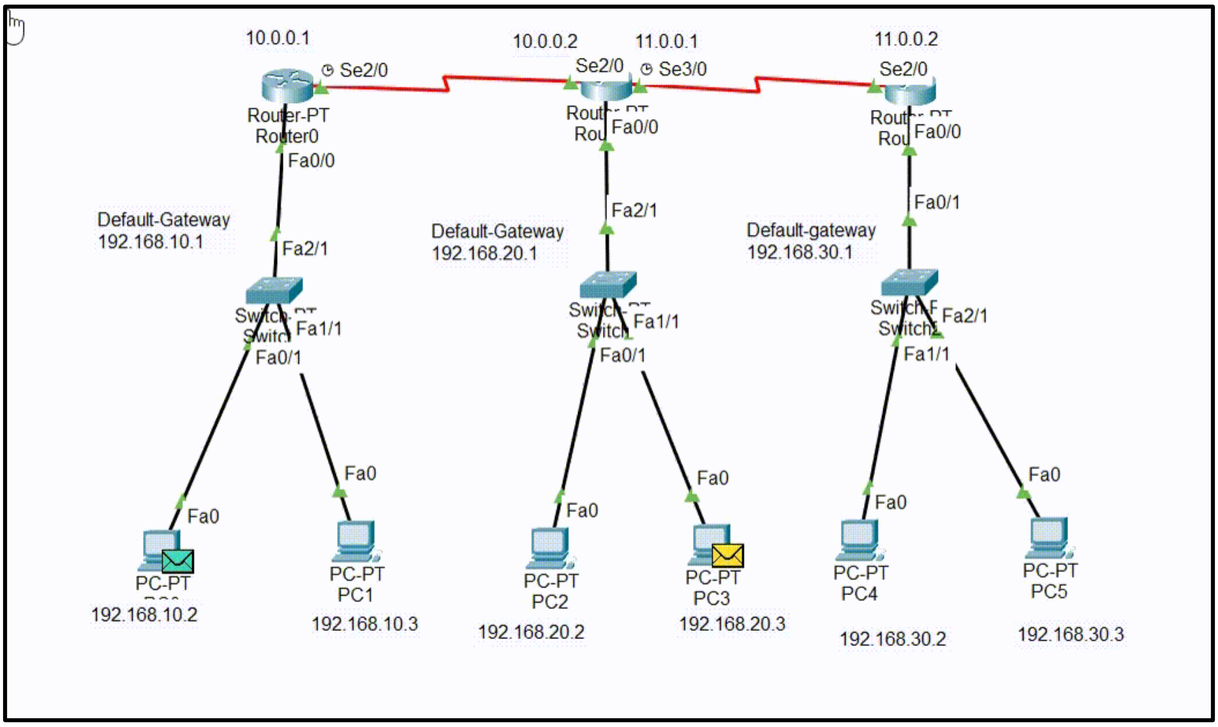
Step 5: Verifying the network by pinging the IP address of any PC.

- 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:



● **Conclusion**: Thus, we have studied about **RIP protocol graphical** simulation using packet trace

Name: Priyush B. Khobragade

PRN: 211112018

Batch: 03

EXPERMINT: 08

●Aim: - -Installation and configuration of Wire shark.

●Theory:

Wireshark

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Features:

The following are some of the many features wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.

Uses of Wireshark:

Wireshark can be used in the following ways:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.