<u>**ASSIGNMENT: 8**</u>

Title: Dynamic Routing Using Cisco Packet Tracer: RIP, OSPF, and BGP

INTRODUCTION: Dynamic routing protocols such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol) are integral components of modern computer networking, facilitating the automatic exchange of routing information among routers to determine optimal paths to network destinations. RIP, with its distance-vector algorithm, is suited for smaller networks, while OSPF, employing the link-state algorithm, offers scalability and faster convergence, making it ideal for larger and more complex networks. On the other hand, BGP, a path-vector protocol, enables routing between different autonomous systems on the Internet, providing flexibility and scalability to maintain global connectivity. Together, these dynamic routing protocols underpin the efficiency and reliability of network communication, catering to diverse network architectures and requirements.

RIP : 8.a To understand the concept and operation of Routing Information Protocol (RIP)

Requirements
- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 2 No
- Router – 2 Nos
- Cat-5 LAN cable

Procedure
- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router and apply clock rate as per the table.
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory
RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain, but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exists: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn’t advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1. RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth. RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

```
R1(config)#
R1(config)#int fa0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shut

R1(config-if)#
R1(config-if)#int serial 0/0/0
R1(config-if)#ip add 20.0.0.1 255.0.0.0
R1(config-if)#no shut
```

```
R2(config)#
R2(config)#int fa0/0
R2(config-if)#ip add 30.0.0.1 255.0.0.0
R2(config-if)#no shut

R2(config-if)#
R2(config-if)#int serial 0/0/0
R2(config-if)#ip add 20.0.0.2 255.0.0.0
R2(config-if)#no shut
```

IP configuration on PCs

Click PC->Desktop->IP Configuration. On each PC assign these addresses:

PC1: IP address: 10.0.0.2   Subnet mask 255.0.0.0 Default Gateway 10.0.0.1

PC2: IP address: 30.0.0.2   Subnet mask 255.0.0.0 Default Gateway 30.0.0.1

And now:

3. Configure **RIPv2** on the routers

Router 1

```
R1(config)#

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 20.0.0.0
```

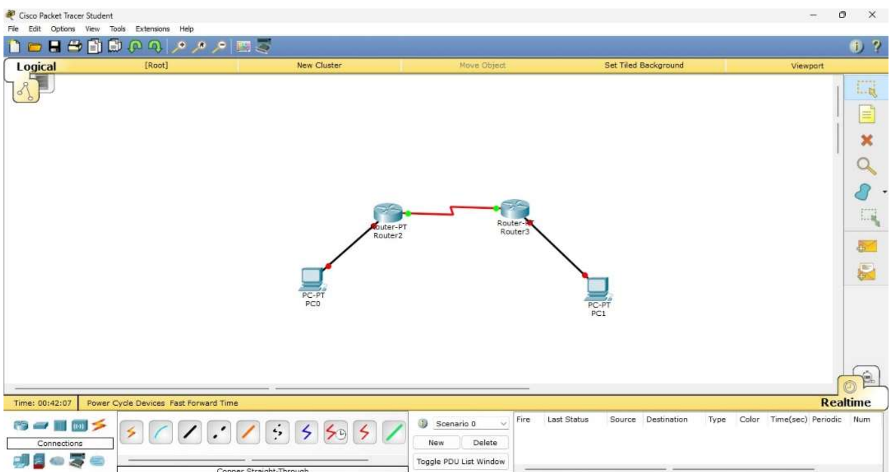
Router 2

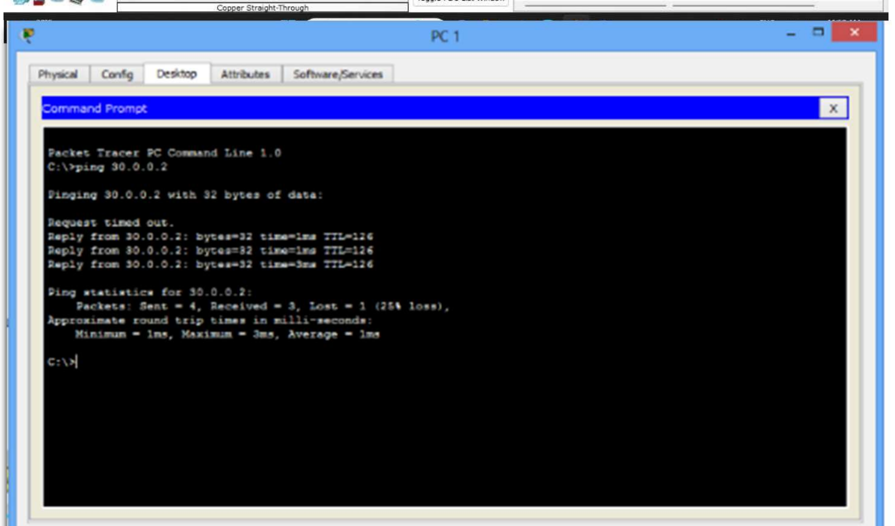
```
R2(config)#

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 20.0.0.0
R2(config-router)#network 30.0.0.0
```

As you can see,to configure rip on each router,we enable enable RIP using *router rip* command then advertise the networks directly connected to the router interfaces using *network* command.That’s all for RIP configuration.

4. We’ll now verify RIP configuration.To verify that RIP is indeed advertising routes, we can use the *show ip route* command on **R1.**





OSPF: 8.b Configuration of Open shortest Path First (OSPF) Algorithm : To construct multiple router networks and understand the operation of OSPF Protocol.

Requirements

- Windows pc – 3 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 3 No
- Router – 3 Nos
- Cat-5 LAN cable

Procedure

- Open the CISCO Packet tracer software.
- Drag and drop 5 pcs using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner.
- Select Routers and Give the IP address for serial ports of router and apply clock rate.
- Add HWIC -2T Peripheral to all routers, type CLI's for all routers.
- Make the connections using Straight through Ethernet cables.
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

Commands to Configuring OSPF:

(config)# router ospf<process ID>

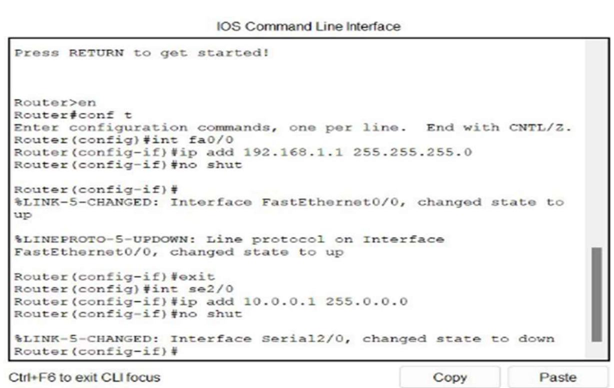
(config-router)# network<network ID><wildcard mask>area<area ID>

Implement the OSPF Single Area Network:

Step 1: Initialize the interface and host with IP addresses and default gateway respectively:

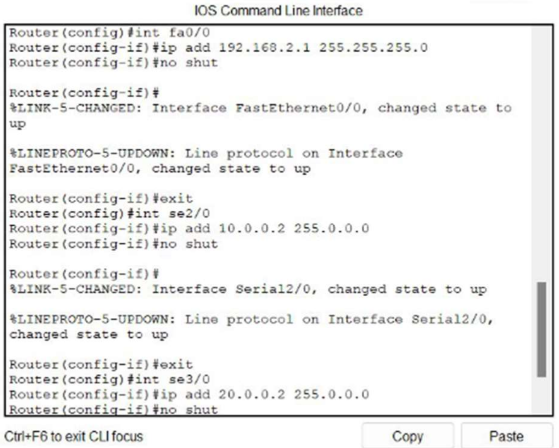
- Network topology consists of 3 Host, 3 Interfaces, and 3 switches
  - HOST1: IP 192.168.1.2, Default gateway: 192.168.1.1
  - HOST2: IP 192.168.2.2, Default gateway: 192.168.2.1
  - HOST3: IP 192.168.3.2, Default gateway: 192.168.3.1

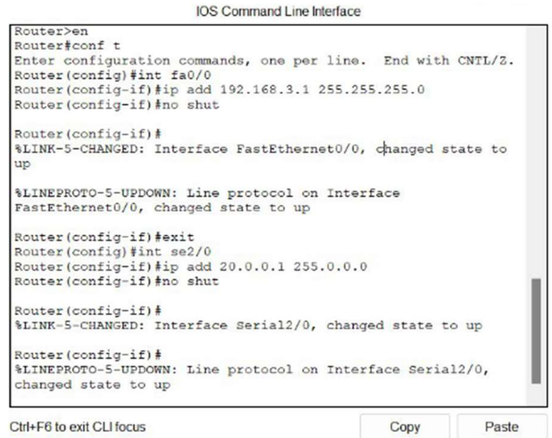
As we can see we have configured interface 1 (Router0) with Host 1 which is PC0 and the Serial port.



Step 2: Configuring the Interface 2 which is router1.

Step 3: Configuring the Interface 3 which is router2.



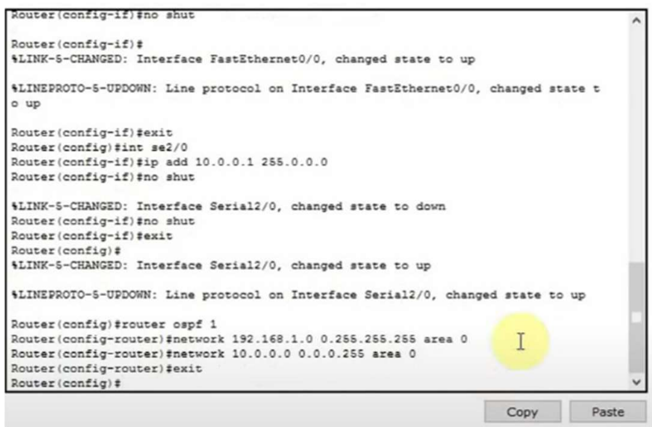


Now comes the main part now we have to configure the OSPF implementation:

Step 1: Configure the Router0 and create router OSPF1 and then add network id with wildcard mask.
Router(config)#router ospf 1

Router(config-router)#network 192.168.1.0 0.255.255.255 area 0

Router(config-router)#network 10.0.0.0 0.0.0.255 area 0

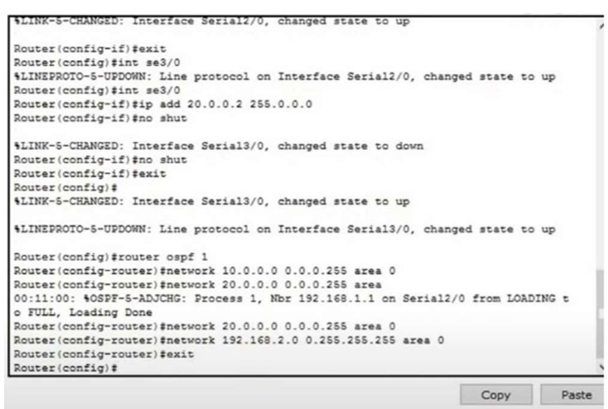


Step2: Configure the Router1 and create router OSPF 1 and then add network id with wildcard mask.
Router(config)#router ospf 1

Router(config-router)#network 10.0.0.0 0.0.0.255 area 0

Router(config-router)#network 20.0.0.0 0.0.0.255 area 0

Router(config-router)#network 192.168.2.0 0.255.255.255 area 0

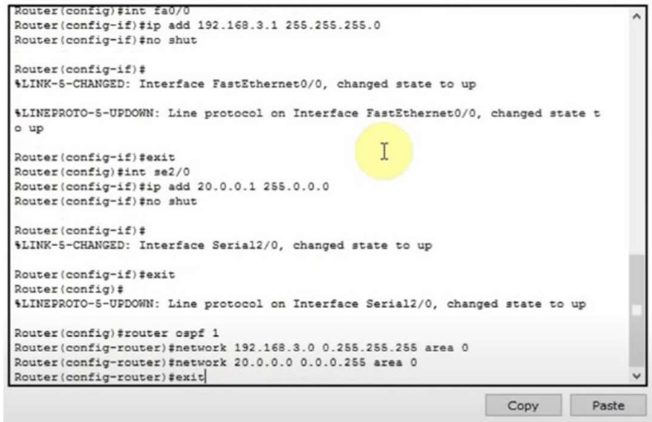


Step 3: Configure the Router2 and create router OSPF 1 and then add network id with wildcard mask.

Router(config)#router ospf 1

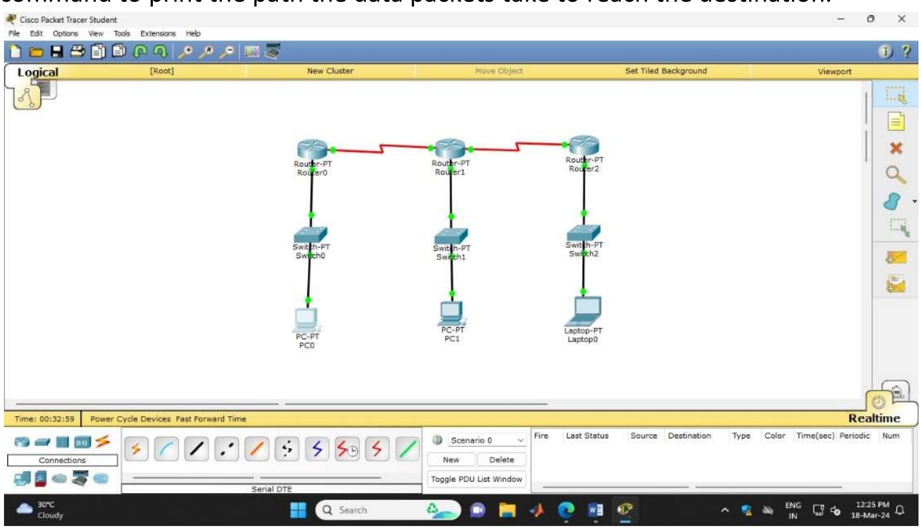
Router(config-router)#network 192.168.3.0 0.255.255.255 area 0

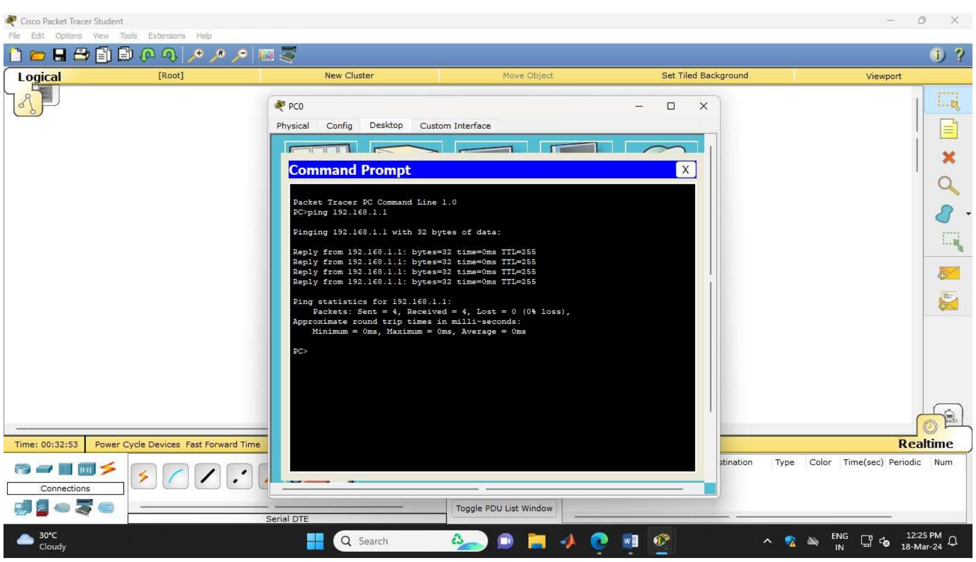
Router(config-router)#network 255.0.0.0 0.0.0.255 area 0



Verifying the OSPF routing

OSPF shares routing information only with neighbors. We use the **show ip ospf neighbor** command to verify OSPF neighbors. The following image shows the output of this command on R1.verify the OSPF configuration on all routers. Send **ping** requests from PC to Server. If it gets replies, it verifies the OSPF configuration. We can also use the **tracert** command to print the path the data packets take to reach the destination.





BGP: 8.c Configure BGP using packet tracer

BGP (Border Gateway Protocol) is the core routing protocol of the Internet. It is described as a path vector protocol as BGP does not use traditional IGP (OSPF, EIGRP, RIP) metrics, but makes routing decisions based on path, network policies and/or rulesets. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). Here three AS are there 1, 71 and 79 respectively. Configure accordingly using three routers.

Step 1:Draw BGP Topology Diagram.

Step 2: Assign ip address on each device as mentioned in Diagram.

Step 3: bgp configuration on Router R1:

```
R1(config)#router bgp 1

R1(config-router)#neighbor 172.16.0.2 remote-as 71

R1(config-router)#network 10.0.0.0 mask 255.0.0.0

R1(config-router)#exit

R1(config)#do write

Building configuration...[OK]

R1(config)#
```

Step 4: bgp configuration on Router R2:

```
R2(config)#router bgp 71

R2(config-router)#neighbor 172.16.0.1 remote-as 1

R2(config-router)#neighbor 172.14.0.2 remote-as 79

R2(config-router)#network 40.0.0.0 mask 255.0.0.0

R2(config-router)#exit

R2(config)#do write

Building configuration...[OK]

R2(config)#
```

Step 5: bgp configuration on Router R3:

```
R3(config)#router bgp 79

R3(config-router)#neighbor 172.14.0.1 remote-as 71

R3(config-router)#network 40.0.0.0 mask 255.0.0.0

R3(config-router)#exit

R3(config)#do write

Building configuration...[OK
```

Step 6: bgp configuration Testing and troubleshooting.

```
PC>ipconfig

PC>ping 10.0.0.2
```

Step 7: check bgp route on router R1:

```
R1#show ip route
```

Step 8: Check whether bgp protocols configure or not on Routre R1:

```
R1#show ip protocols
```

Step 9: Show BGP Status

```
R1#show ip bgp summary
```

Show bgp neighbors status:

```
R1#show ip bgp neighbors
```

Similarly we check bgp route on Router R2:

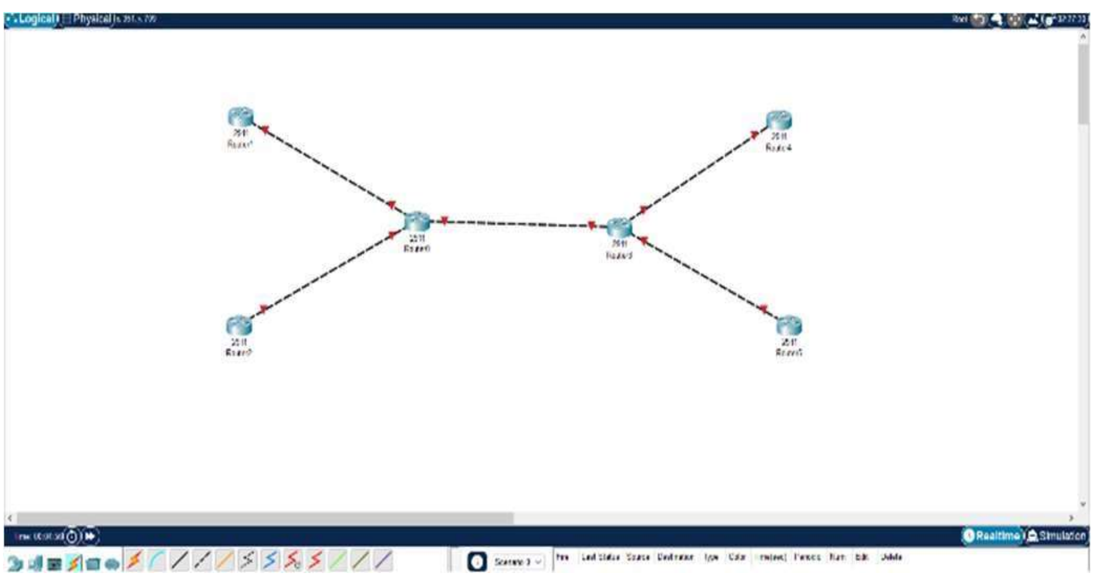
```
R2#show ip route

R2#show ip protocols
```

Similarly check bgp route on Router R3:

```
R3#show ip route

R3#show ip protocols
```



ASSIGNMENT: 9

Title: Packet Tracer Simulation - TCP and UDP Communications

Objectives:

Part 1: Generate Network Traffic in Simulation Mode

Part 2: Examine the Functionality of the TCP and UDP Protocols

Background:

This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail. Simulation mode provides the ability to view the functionality of the different protocols.

As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each ofthe protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC.

This activity provides an opportunity to explore the functionality of the TCP and UDP protocols, multiplexing and the function of port numbers in determining which local application requested the data or is sending the data.

Part 1: Generate Network Traffic in Simulation Mode

Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following tasks task to reduce the amount of network traffic viewed in the simulation.

a. Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ping 192.168.0.2** command. This will take a few seconds as every device on the networkresponds to **MultiServer**.

c. Close the **MultiServer** window.

Step 2: Generate web (HTTP) traffic.

a. Switch to Simulation mode.

b. Click **HTTP Client** and click the **Desktop** tab > **Web Browser**.

c. In the URL field, enter **192.168.0.2** and click **Go**. Envelopes (PDUs) will appear in the simulation window.

d. Minimize, but do not close, the **HTTP Client** configuration window.

Step 3: Generate FTP traffic.

a. Click **FTP Client** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.

c. Minimize, but do not close, the **FTP Client** configuration window.

Step 4: Generate DNS traffic.

a. Click **DNS Client** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

c. Minimize, but do not close, the **DNS Client** configuration window.

Step 5: Generate Email traffic.

a. Click **E-Mail Client** and click the **Desktop** tab > **E Mail** tool.

b. Click **Compose** and enter the following information:

1) **To:** png.edu.in

2) **Subject:** Personalize the subject line

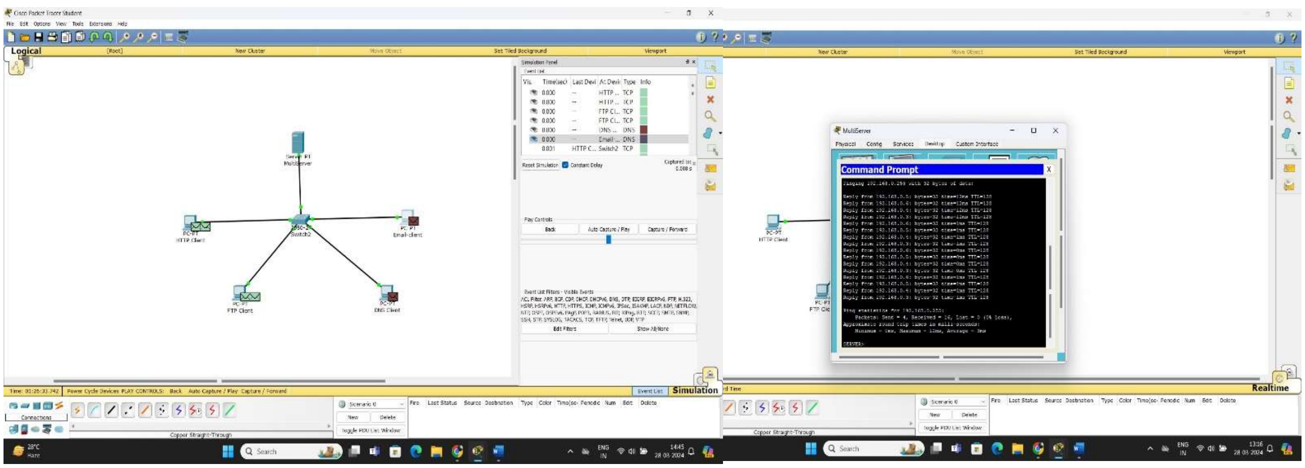
3) **E-Mail Body:** Personalize the Email

c. Click **Send**.

d. Minimize, but do not close, the **E-Mail Client** configuration window.

Step 6: Verify that the traffic is generated and ready for simulation.

Every client computer should have PDUs listed in the Simulation Panel.



TCP Service Table						
Service Name	Type	Local IP Address	Local Port	Remote IP Address	Remote Port	State
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen
HTTP		10.10.100.106	80	10.10.100.105	54284	Time wait
HTTP		10.10.100.106	80	10.10.100.105	54352	Established
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen

UDP Service Table				
Service Name	Type	Local IP Address	Local Port	Application Instance
	UDP	All	123	1
SNMP	UDP	All	161	1
	UDP6	All	546	1
Bonjour	UDP6	All	5353	1