NETWORK AND NETWORKING DEVICES WORKSHOP

Practical File

Course Code : INITC19

Submitted By –

Name: Rohit Kumar

Roll no.: 2020UIN3322

Branch: ITNS

Semester: 6th

Academic Year: 2022-23

INDEX

PRACTICAL-1

To familiarize with the Lab Network Topology. Locating different interfaces, routers and switches. Studying different pools of IP addresses.

Router- A Router is a networking device that forwards data packets between computer networks. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads address information in the packet to determine which port the packet will be sent. For example, a router provides you with internet access by connecting your LAN with the Internet. When a packet arrives at a Router, it examines the destination IP address of a received packet and makes routing decisions accordingly. Routers use Routing Tables to determine which interface the packet will be sent. A routing table lists all networks for which routes are known. Each router's routing table is unique and stored in the RAM of the device.

In a lab network topology, different **routers** can include:

1. Basic Router: A basic router is a device that connects multiple networks together, and it is responsible for forwarding data packets between those networks. They are typically located in a central location, such as a data center or a network closet, and are usually connected to multiple networks through interfaces. They can be managed through a web-based interface, or through a command-line interface, such as Telnet or SSH session.
2. Advanced Router: An advanced router is a router that has more advanced routing capabilities than a basic router. They can be used to segment large networks into smaller subnets and also provide features like VPN, QoS, and Firewall. They are typically located in a central location, such as a data center or a network closet, and are usually connected to multiple networks through interfaces. They can be managed through a web-based interface, or through a command-line interface, such as Telnet or SSH session.
3. Wireless Router: A wireless router is a router that includes a built-in wireless access point. It allows users to connect to the network wirelessly, eliminating the need for wired connections. They can also provide DHCP services and firewall protection. They are typically located in a central location, such as a data center or a network closet, and are usually connected to multiple networks through interfaces. They can be managed through a web-based interface, or through a command-line interface, such as Telnet or SSH session.
4. VPN Router: A VPN router is a router that includes built-in VPN capabilities. It allows remote users to connect to the network securely over the internet using a VPN connection. They are typically located in a central location, such as a data center or a network closet, and are usually connected to multiple networks through interfaces. They can be managed through a web-based interface, or through a command-line interface, such as Telnet or SSH session.

5. Multi-function Router: A multi-function router is a router that includes multiple features in one device, such as routing, VPN, firewall, and wireless capabilities. It allows users to have multiple functionalities with a single device, which is more cost-effective and easier to manage. They are typically located in a central location, such as a data center or a network closet, and are usually connected to multiple networks through interfaces. They can be managed through a web-based interface, or through a command-line interface, such as Telnet or SSH session.

In summary, different routers in a lab network topology can include basic routers, advanced routers, wireless routers, VPN routers, and multi-function routers. Each of these routers serves a unique purpose and can be used to connect different types of devices to the network, or to help in routing and switching of data packets.

Switches- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

In a lab network topology, different **switches** can include:

1. Unmanaged Switch: An unmanaged switch is a basic switch that does not have an interface for configuration. They are typically used in small networks where the number of devices is limited and the network is not complex. They can be used to connect different types of devices such as computers, printers, and servers, to the network. They are typically located in a central location, such as a network closet.
2. Managed Switch: A managed switch is a switch that has an interface for configuration. They are typically used in larger networks where the number of devices is high and the network is more complex. They can be used to connect different types of devices such as computers, printers, and servers, to the network. They can also be used to segment large networks into smaller subnets, and provide features like VLAN, QoS, and Link Aggregation. They are typically located in a central location, such as a network closet.
3. Layer 2 Switch: A layer 2 switch is a switch that operates at the Data Link Layer of the OSI model. They are typically used in smaller networks where the number of devices is limited and the network is not complex. They can be used to connect different types of devices such as computers, printers, and servers, to the network. They are typically located in a central location, such as a network closet.
4. Layer 3 Switch: A layer 3 switch is a switch that operates at both the Data Link Layer and the Network Layer of the OSI model. They are typically used in larger networks where the number

of devices is high and the network is more complex. They can be used to connect different types of devices such as computers, printers, and servers, to the network. They can also be used to segment large networks into smaller subnets and provide routing capabilities. They are typically located in a central location, such as a network closet.

5. Stackable Switch: A stackable switch is a switch that can be stacked with other switches to form a single logical switch. This allows for increased port density and easier management. They are typically used in larger networks where the number of devices is high and the network is more complex. They can be used to connect different types of devices such as computers, printers, and servers, to the network. They are typically located in a central location, such as a network closet.

In summary, different switches in a lab network topology can include unmanaged switches, managed switches, layer 2 switches, layer 3 switches and stackable switch. Each of these switches serves a unique purpose and can be used to connect different types of devices to the network and to help in the routing and switching of data packets.

IP address -All the computers of the world in the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called IP Address or Internet Protocol Address.

#DIFFERENT POOLS OF IP ADDRESSES

There are several different pools of IP addresses that are used for different purposes. These include:

1. IPv4 addresses: IPv4 is the most widely used version of IP addresses, it uses 32-bit addresses and is represented in a dot-decimal notation, such as 192.168.1.1. Each octet (or group of 8 bits) in an IPv4 address is represented by a decimal number between 0 and 255, separated by a dot. IPv4 addresses are divided into two parts: the network part and the host part. The network part identifies the network that the host is on, and the host part identifies the specific host within that network. This is done by using a subnet mask, which defines which portion of the address represents the network and which portion represents the host.
2. IPv6 addresses: IPv6 is the newer version of IP addresses, it uses 128-bit addresses and is represented in a colon-hexadecimal notation, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Each 16-bit block in an IPv6 address is represented by a hexadecimal number, separated by a colon. IPv6 addresses have a much larger address space than IPv4 addresses, which allows for many more devices to be connected to the internet.
3. Private IP addresses: These are IP addresses that are not publicly routable on the internet, but can be used within a private network. They are often used for internal networks, such as in homes or businesses. Examples of private IP addresses include 192.168.x.x and 10.x.x.x.

4. Public IP addresses: These are IP addresses that are publicly routable on the internet. They are assigned by internet service providers (ISPs) and are used to identify devices that need to connect to the internet. Public IP addresses are unique and can be used to identify a specific device on the internet.
5. Special-purpose IP addresses: These are IP addresses that are reserved for special uses. Examples include multicast addresses, loopback addresses, and link-local addresses.
6. Reserved IP addresses: There are certain ranges of IP addresses that are reserved for specific uses, such as for testing, research, or other special purposes. These ranges are not intended for general use and are not assigned to specific organizations or individuals.
7. Dynamic IP addresses: These are IP addresses that are assigned to a device on a network on an as-needed basis. They are commonly used in residential and business networks to conserve IP addresses. This is done by assigning a device a new IP address each time it connects to the network, rather than reserving a static IP address for it.

It's important to note that the availability of IP addresses is limited, and many organizations and individuals are working to conserve IP addresses and transition to IPv6 as IPv4 addresses are becoming scarce.

In a lab network topology, **different interfaces** can include:

1. Ethernet interfaces: These are physical interfaces that use the Ethernet protocol to transmit data. They are typically connected to other devices using Ethernet cables, and are usually labeled with the type of interface, such as "Ethernet" or "Gigabit Ethernet." Ethernet interfaces can be used to connect devices such as computers, servers, and switches to the network.
2. Serial interfaces: These are physical interfaces that use serial communication to transmit data. They are typically used to connect devices such as routers and modems, and can be used to establish a point-to-point connection between two devices. Serial interfaces are typically labeled with the type of interface, such as "Serial" or "RS-232."
3. Wireless interfaces: These are virtual interfaces that use wireless communication to transmit data. They can be used to connect devices such as laptops, smartphones, and tablets to the network. Wireless interfaces can be accessed through software, such as a command-line interface or a web-based interface, and are typically labeled with the type of interface, such as "Wi-Fi" or "Bluetooth."
4. Virtual interfaces: These are virtual interfaces that can be created within a device, such as a router or switch, to provide additional functionality. Examples of virtual interfaces can include VLANs, VPNs, or virtual NICs. These interfaces can be accessed through software, such as a command-line interface or a web-based interface.
5. Management interfaces: These are interfaces that are used to manage and configure devices on the network. Examples include web-based interfaces and command-line interfaces such as Telnet or SSH. These interfaces can be used to access the device's settings, monitor its performance, and troubleshoot issues.

In summary, different interfaces in a lab network topology can include Ethernet interfaces, serial interfaces, wireless interfaces, virtual interfaces, and management interfaces. Each of these interfaces serves a unique purpose and can be used to connect different types of devices to the network.

PRACTICAL-2

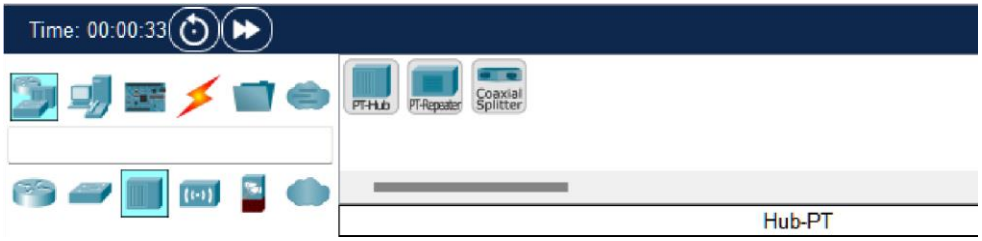
Establish a LAN Configuration using:

I. Hub:

Procedure:

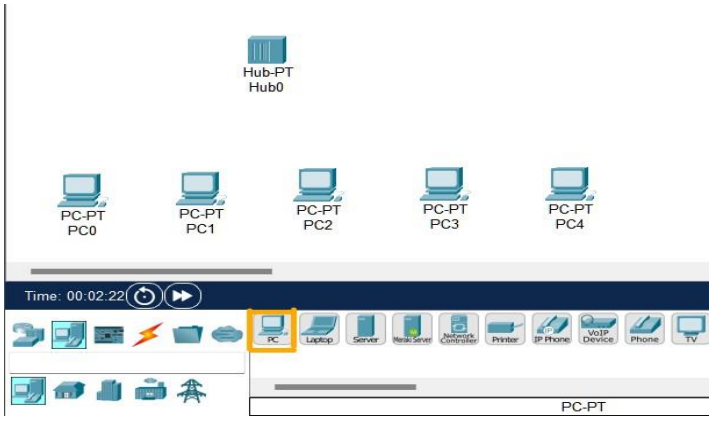
1.) Open Cisco Packet Tracer.

2.) Click on Network devices option from the bottom left corner and select Hub among various networkdevices.

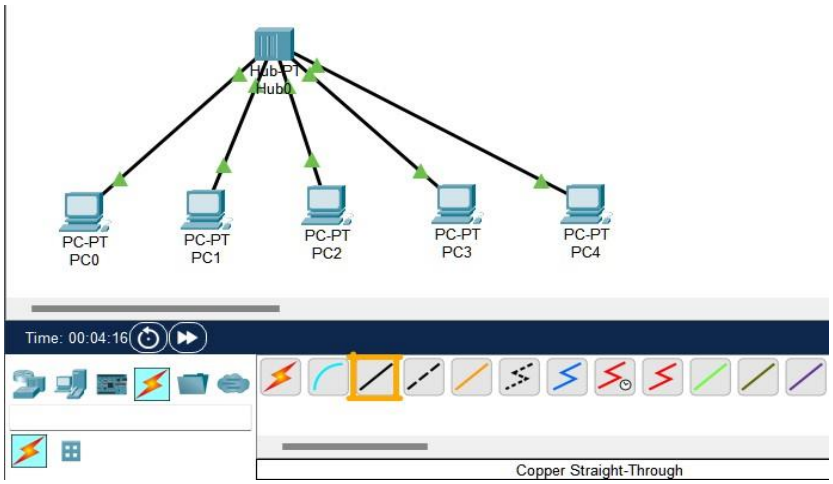


3.) Select PT-Hub from available options.

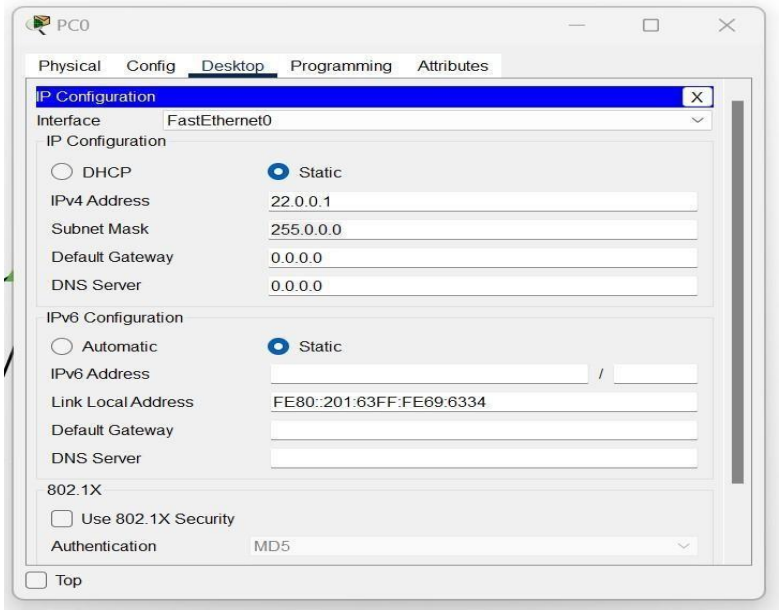
4.) Click on End Devices and select PCs from available options.



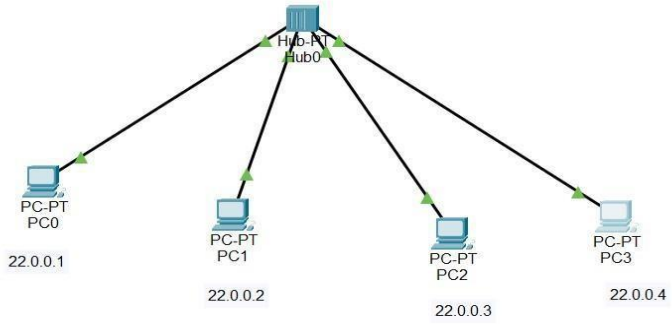
5.) Click on Connections and select “Copper Straight-Through” cable to connect these devices.



6.) Assign IP addresses to the computers. We get “IP Configuration” option by clicking on any computer and selecting “Desktop” option from the top ribbon.

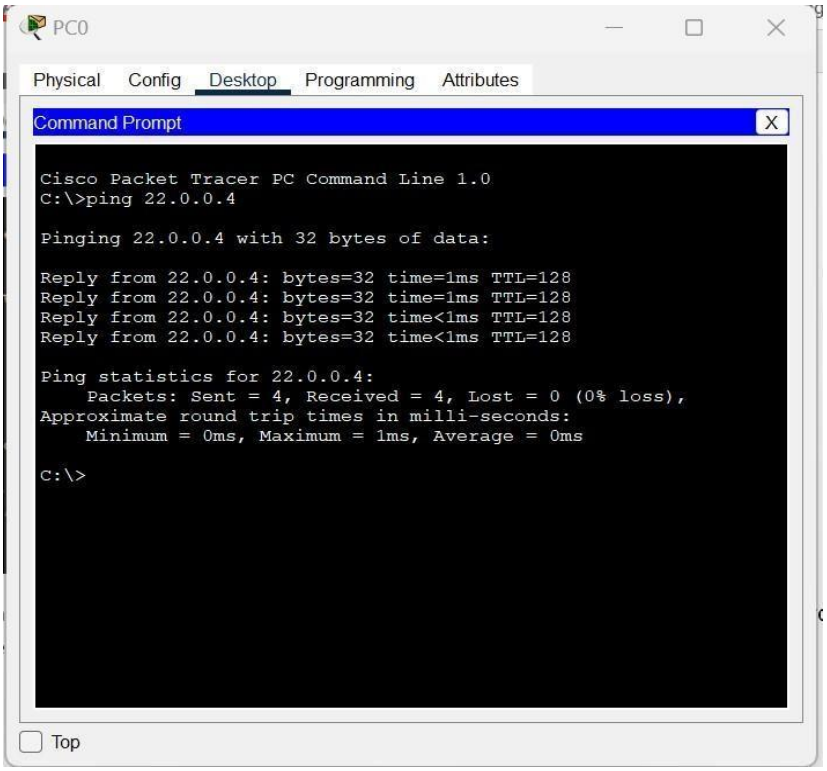


7.) Repeat step-6 and assign IP address to all the PCs.

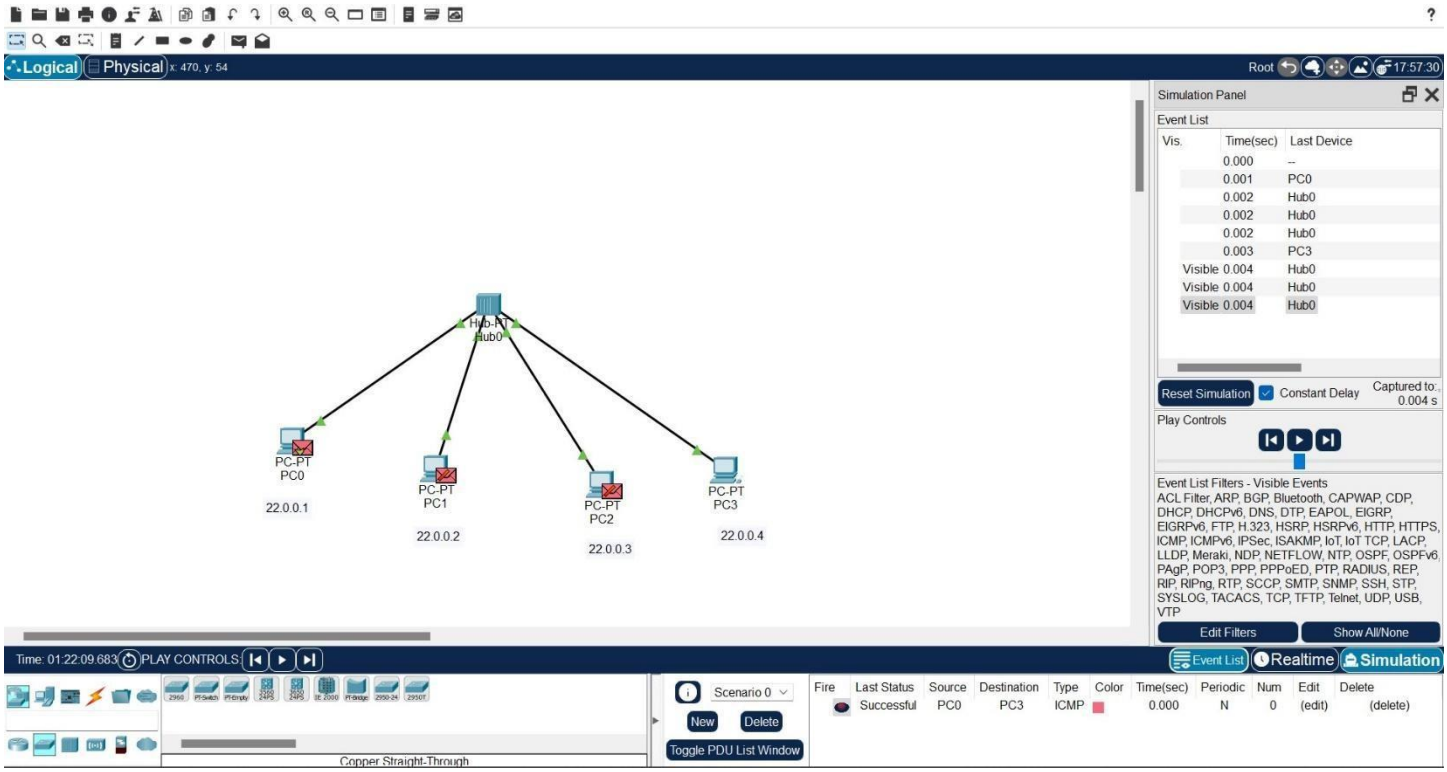


8.) To check whether the PCs are connected to each other, we use PING command.

Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded).



9.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which youwant to send the message to the destination computer, then Run the Simulation.

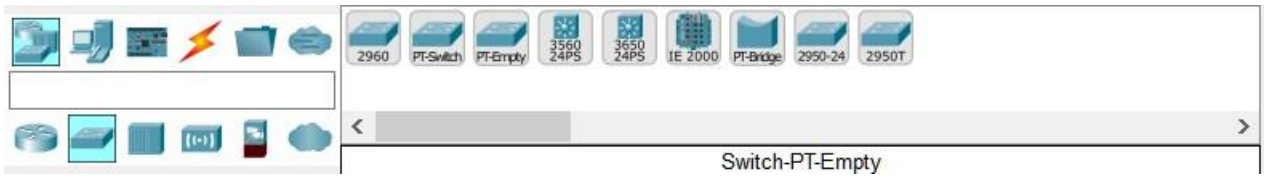


II. Switch:

Procedure:

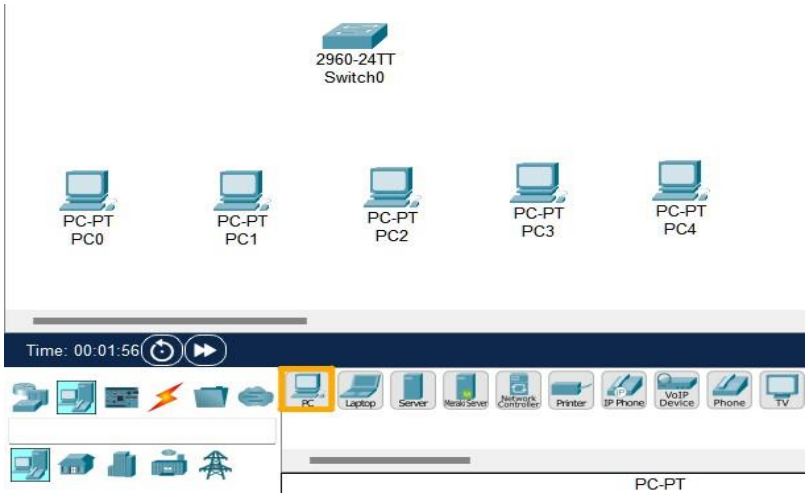
1.) Open Cisco Packet Tracer.

2.) Click on Network devices option from the bottom left corner and select Switch among various networkdevices.

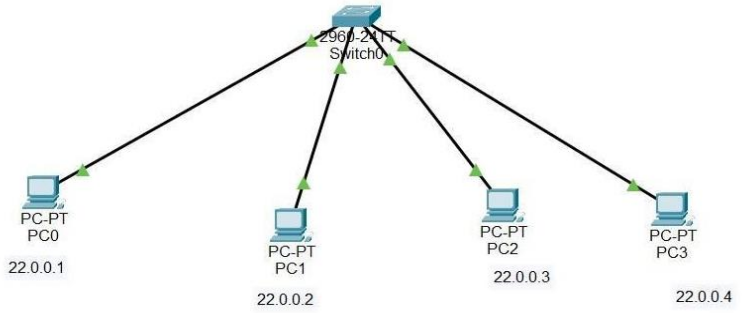


3.) Select 2960 switch from available options.

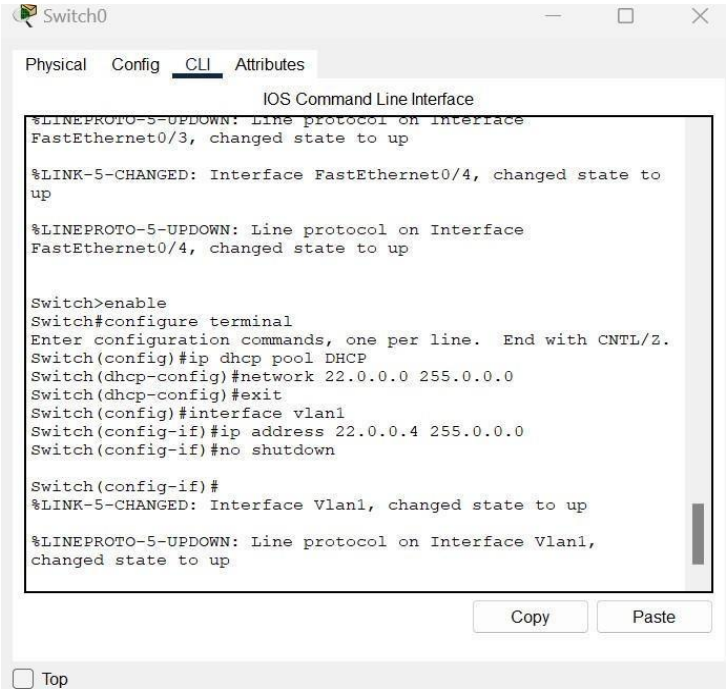
4.) Click on End Devices and select PCs from available options.



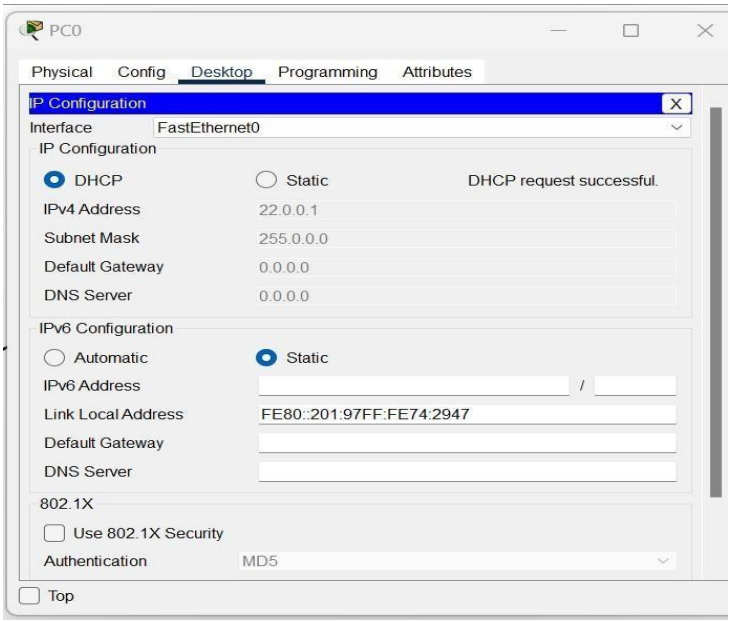
5.) Click on Connections and select “Copper Straight-Through” cable to connect these devices via FastEthernetInterface.



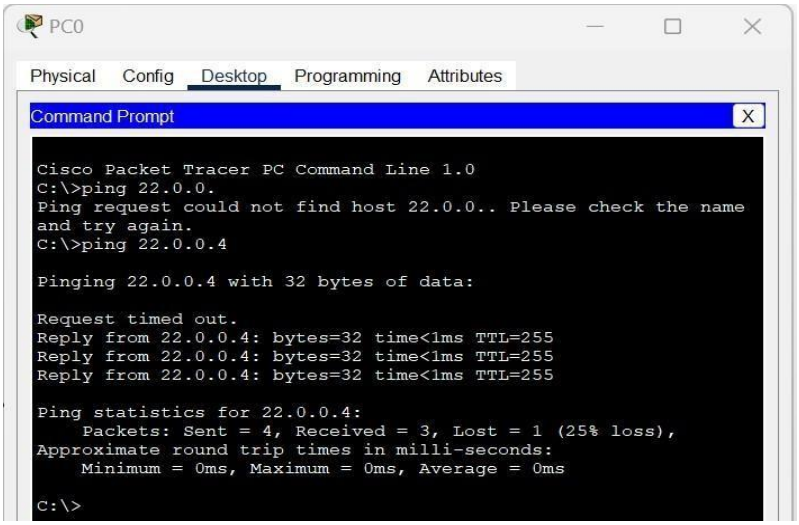
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of switch and write the following commands in order to assign the network to the connected devices.



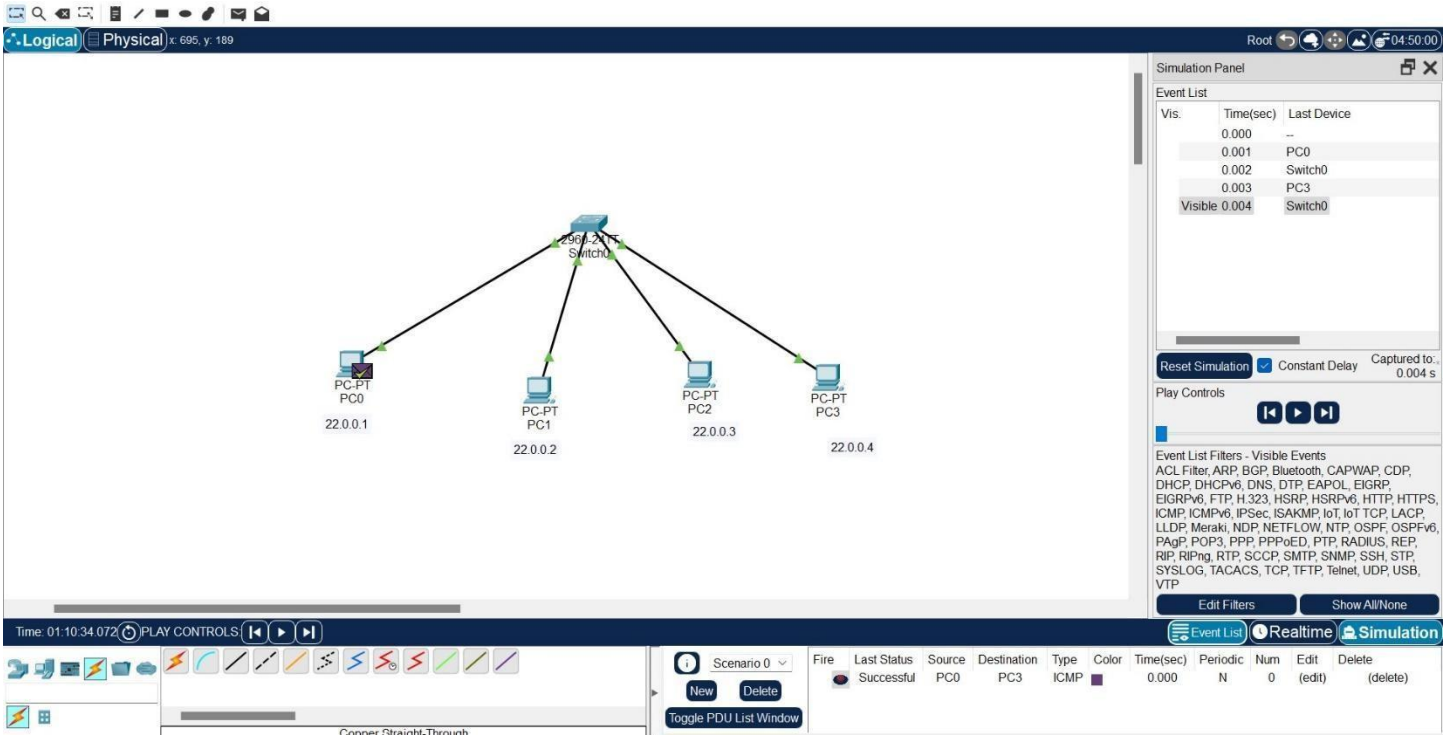
7.) Go to every PC's Desktop, click IP configuration and select DHCP. Repeat this step for all PC's.



8.) To check whether the PCs are connected to each other, we use PING command.Click on any computer and then go to "Desktop" and select "Command Prompt", then type "ping *IP address of any other computer*" (*excluded).



9.) Click on "Add Simple PDU" option from the top ribbon and then selecting the computer from which youwant to send the message to the destination computer, then Run the Simulation.



III. Router:

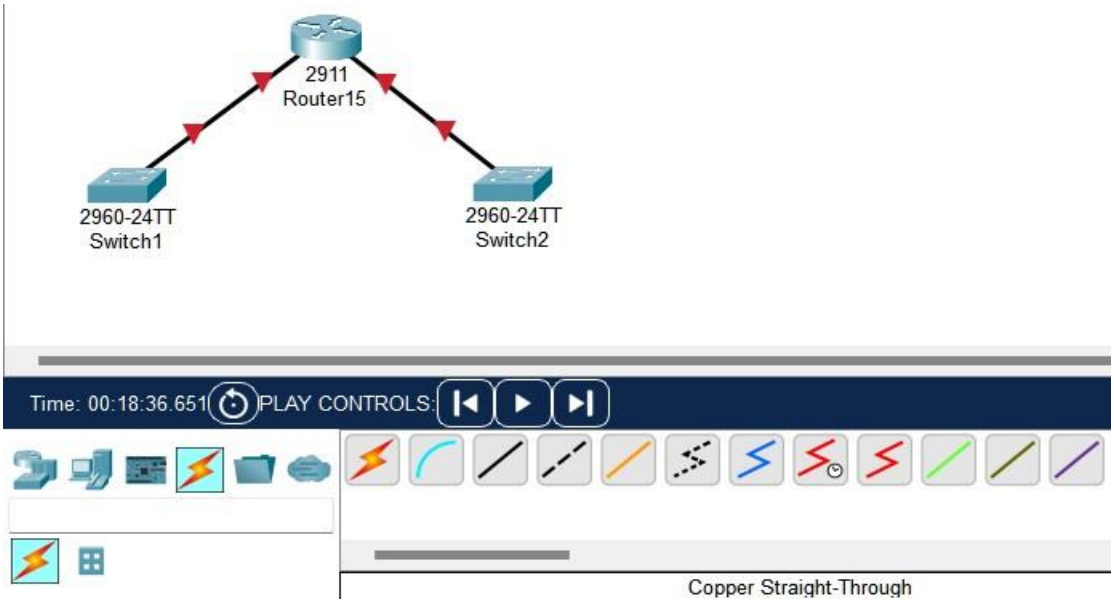
Procedure:

1.) Open Cisco Packet Tracer.

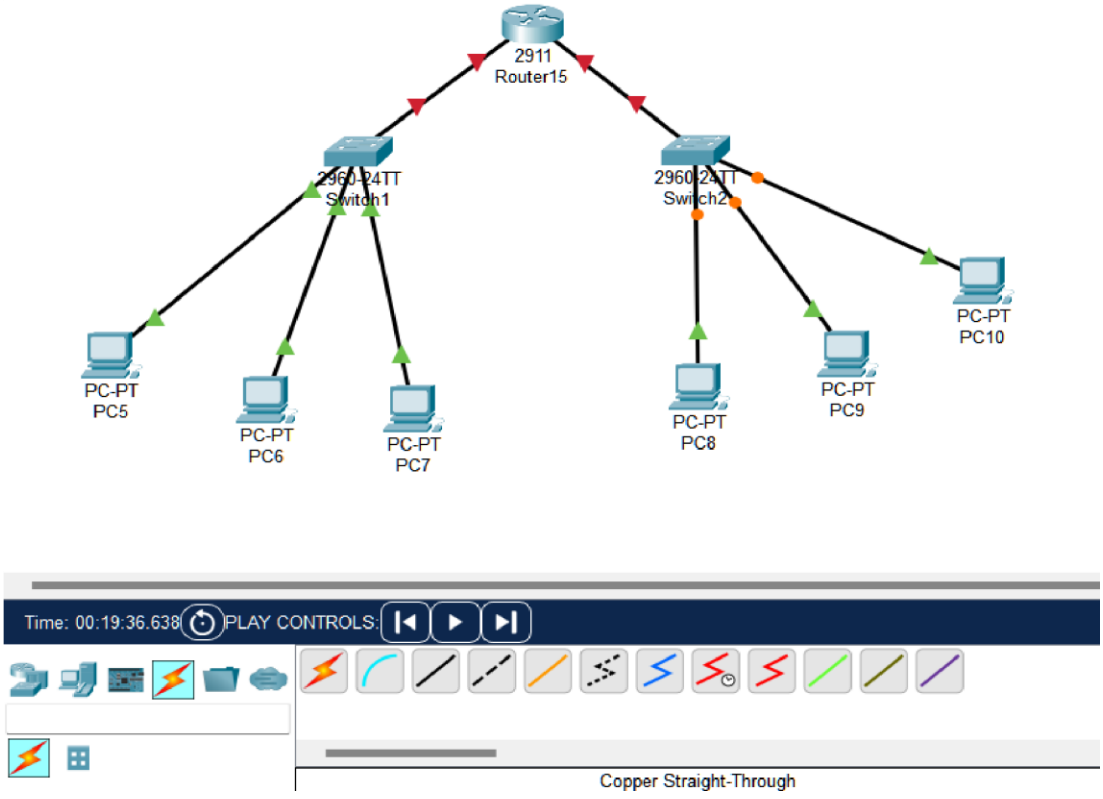
2.) Click on Network devices option from the bottom left corner and select Router among various networkdevices.

3.) Select “2911” Router from available options.

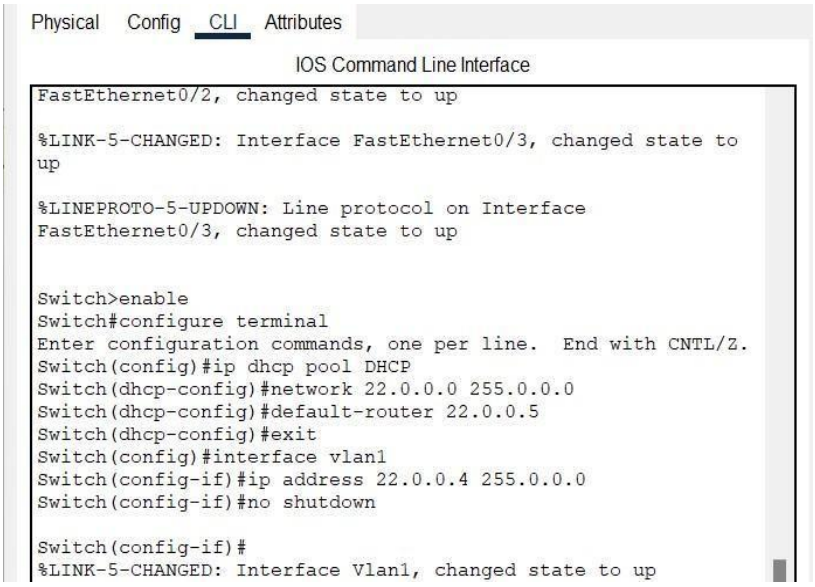
4.) Click on Network devices option from the bottom left corner and select two “2960” Switches amongvarious network devices, and connect them with router using “Copper Straight-Through”.



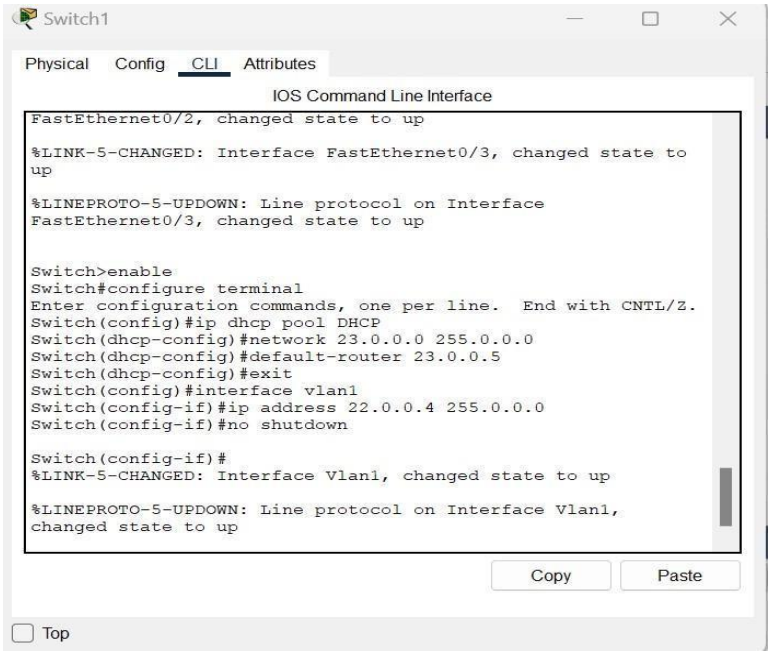
5.) Click on End Devices and select PCs from available options. Click on Connections and select “CopperStraight-Through” cable to connect PCs with Switches via FastEthernet Interface.



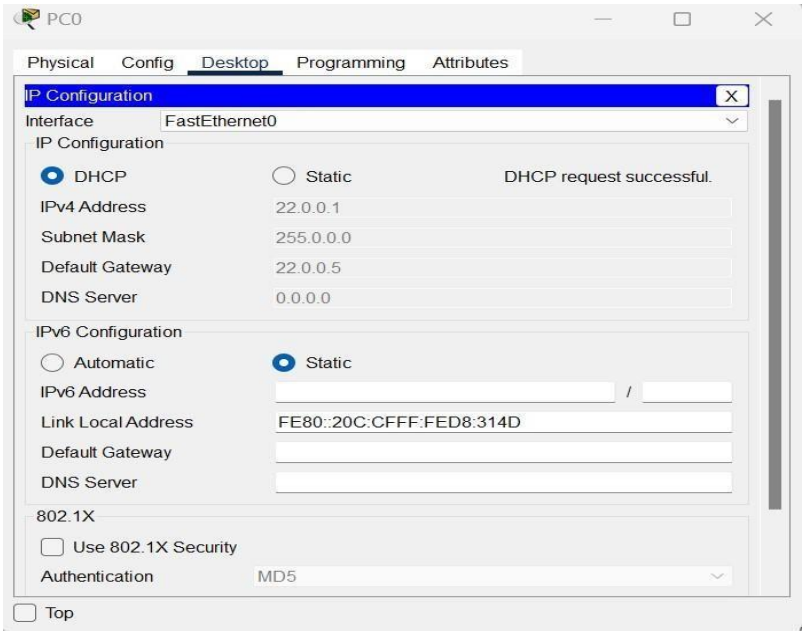
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of switch0 and write the following commands in order to assign the dynamic IP address to the connected devices of network 22.0.0.0 whose default router IP address is 22.0.0.5



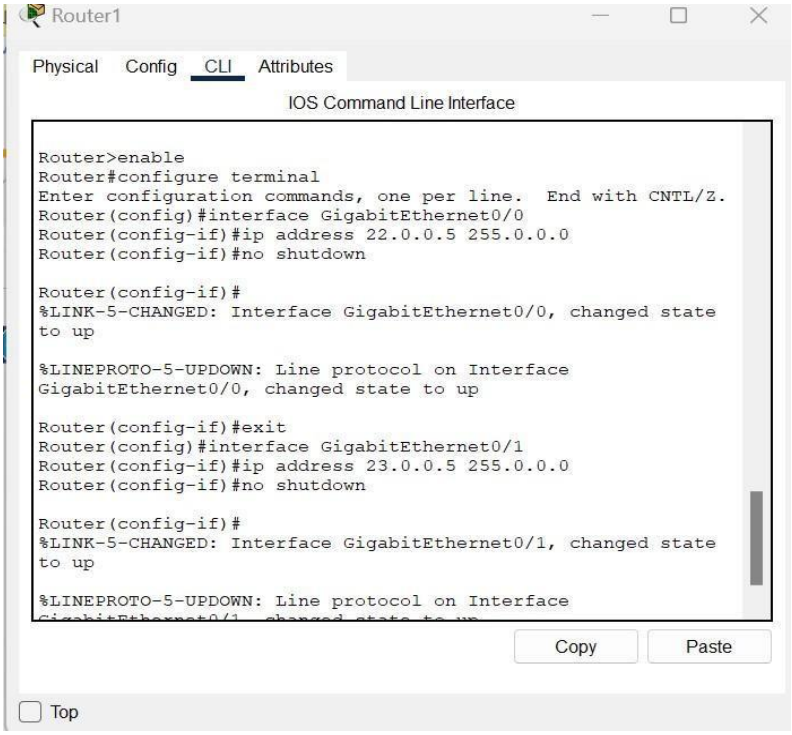
Similarly, go to CLI of switch1 and repeat the same process for the connected devices of network 23.0.0.0 whose default router IP address is 23.0.0.5



7.) Go to every PC's Desktop, click IP configuration and select DHCP. Repeat this step for all PC's.



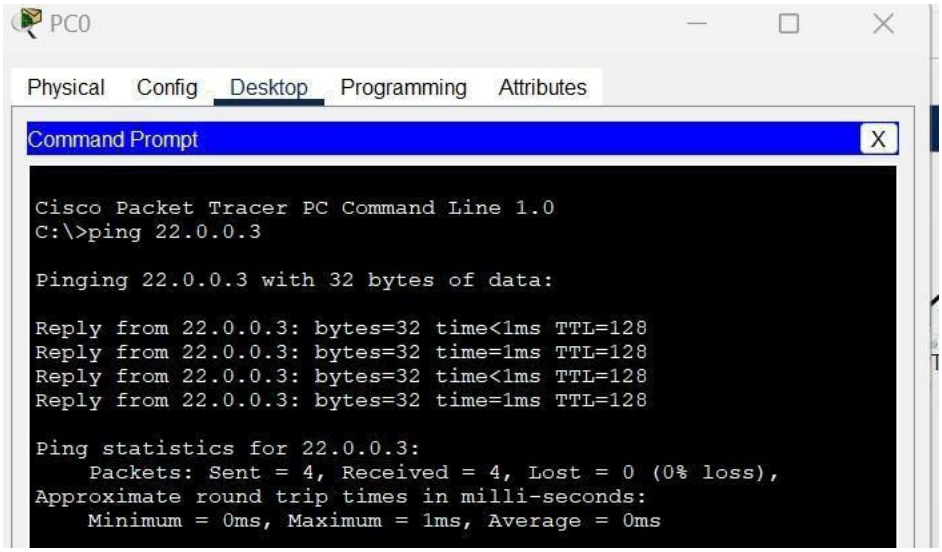
8.) Click on Router and Go to CLI. Write the commands shown below to connect router to the network 22.0.0.0 via the Gigabit Ethernet 0/0 cable and network 23.0.0.0 via the Gigabit Ethernet 0/1 cable.



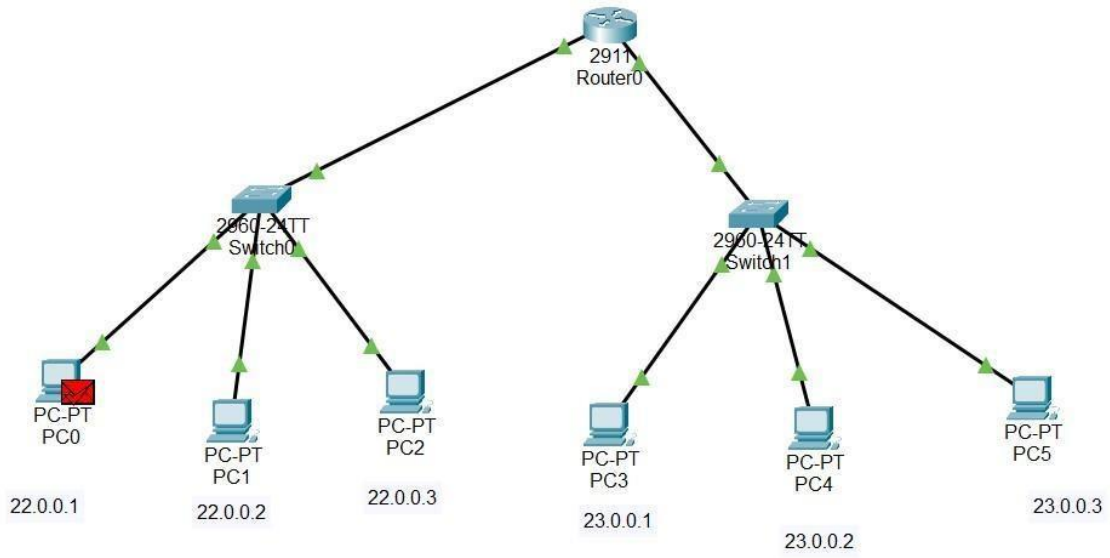
9.) To check whether the PCs are connected to each other, we use PING command.

Click on any computer and then go to "Desktop" and select "Command Prompt", then type

“ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



10.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which youwant to send the message to the destination computer, then Run the Simulation.

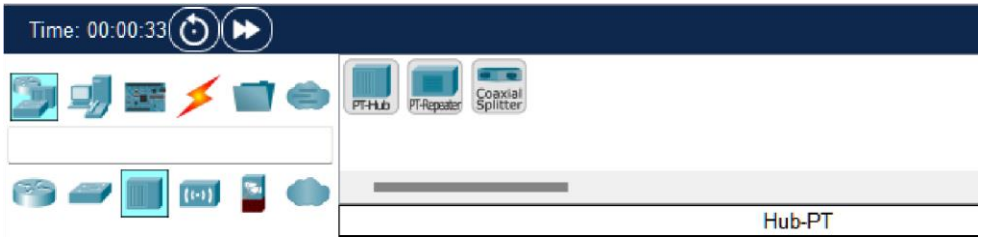


IV. Repeater:

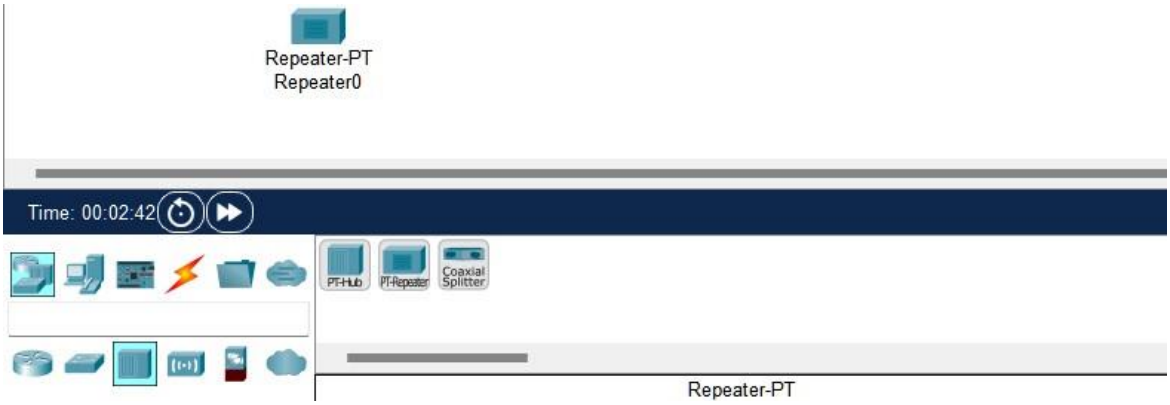
Procedure:

1.) Open Cisco Packet Tracer.

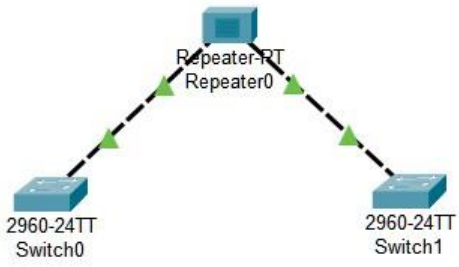
2.) Click on Network devices option from the bottom left corner and select Hub among various networkdevices.

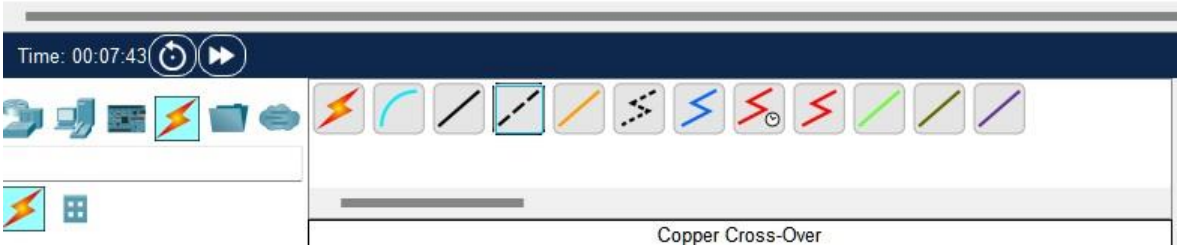


3.) Select PT-Repeater from available options.

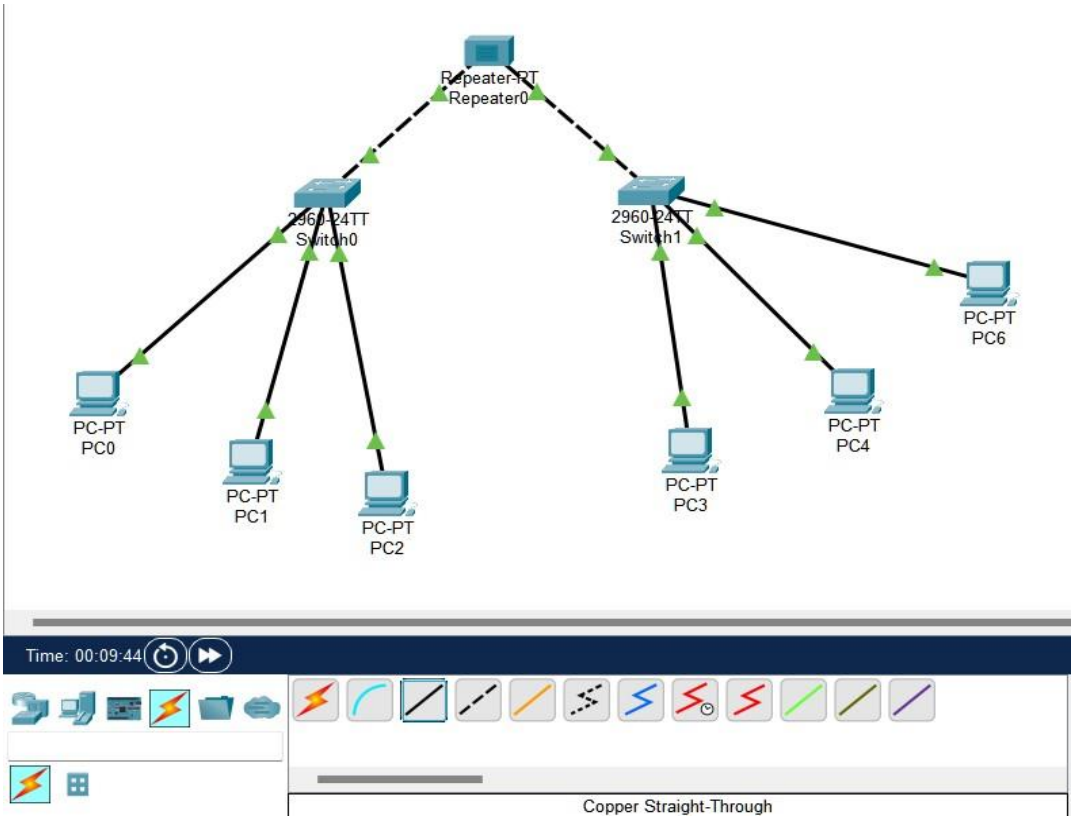


4.) Click on Network devices option from the bottom left corner and select two “2960” Switches amongvarious network devices, and connect them with router using “Copper Cross-Over”.

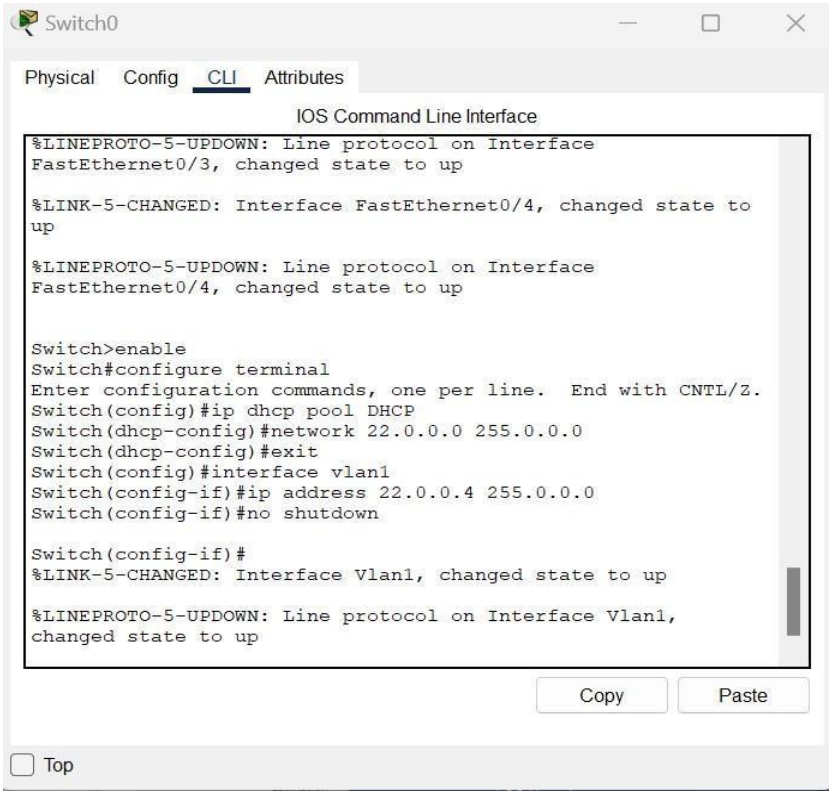




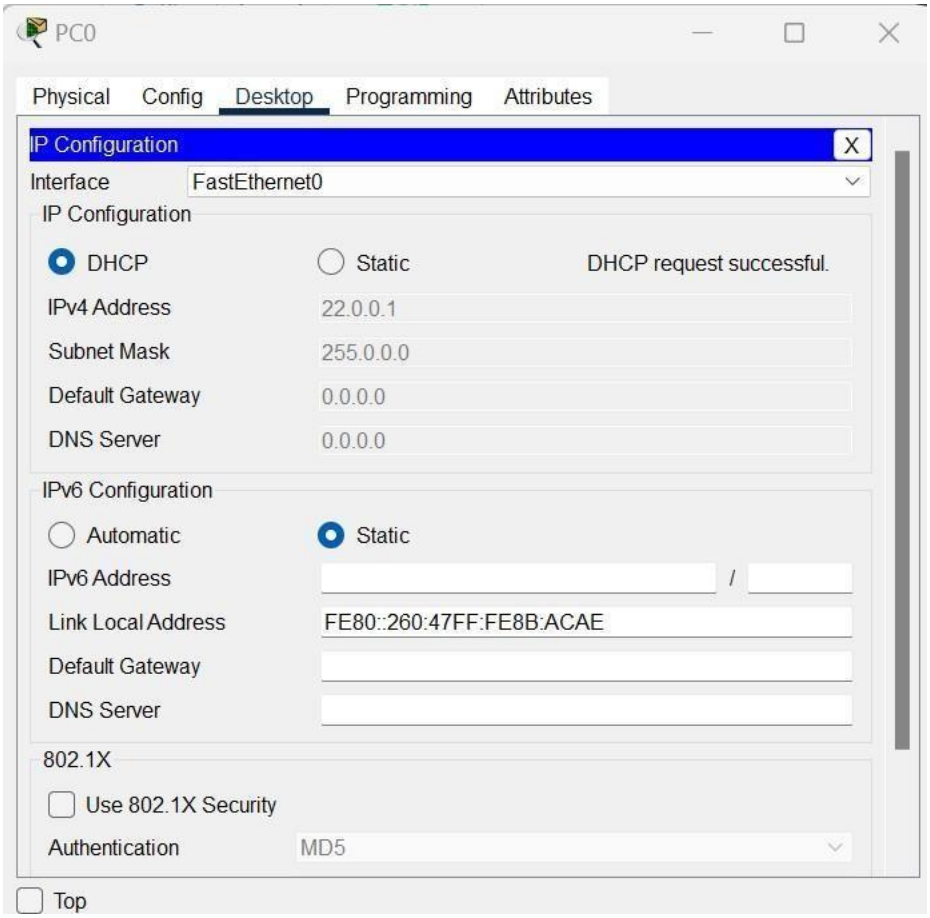
5.) Click on End Devices and select PCs from available options. Click on Connections and select “CopperStraight-Through” cable to connect PCs with Switches via FastEthernet Interface.



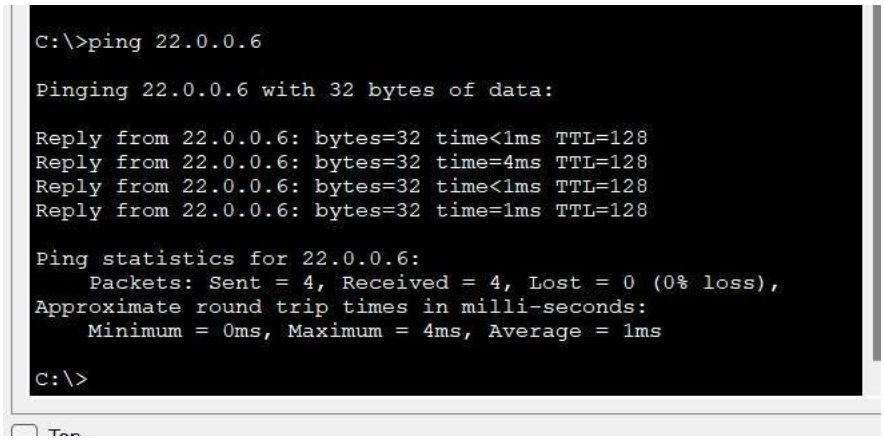
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of switch0 and write the following commands in order to assign the network to the connected devices.



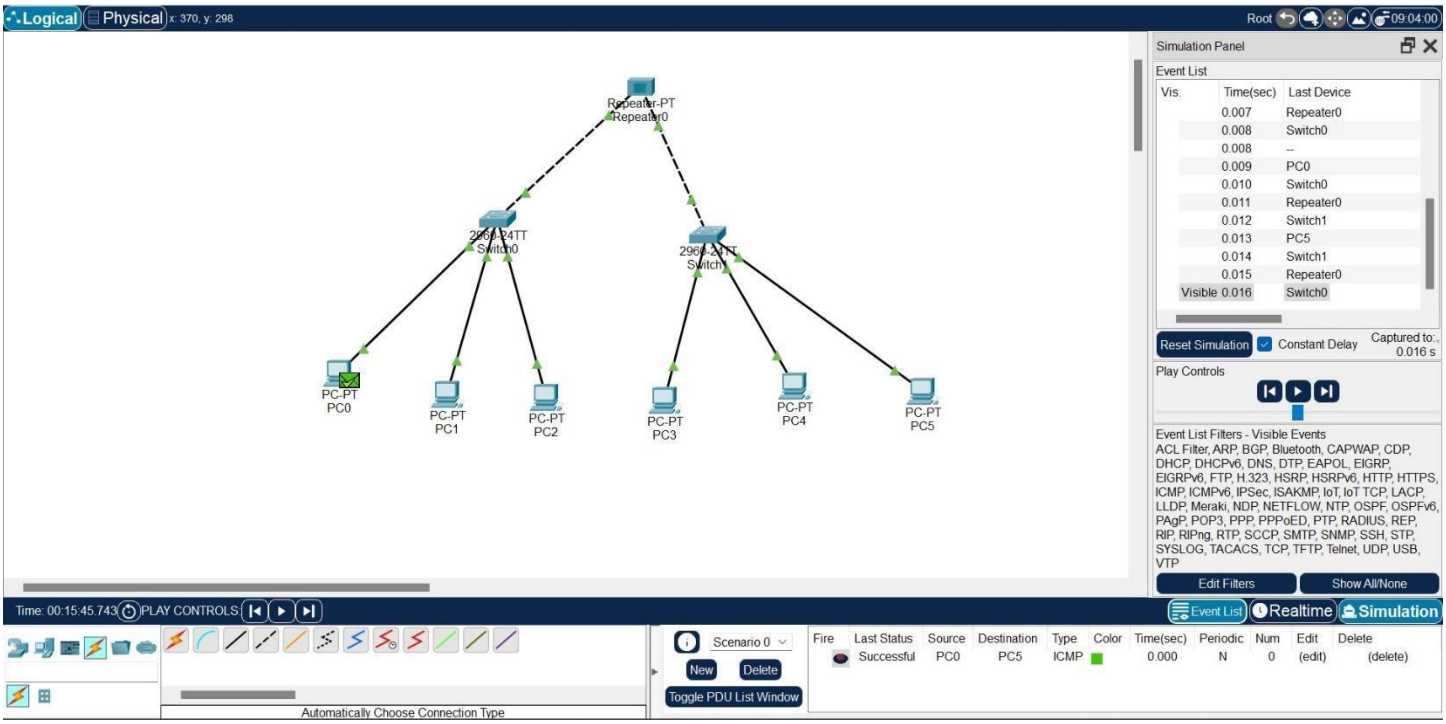
7.) Go to every PC's Desktop, click IP configuration and select DHCP. Repeat this step for all PC's.



9.) To check whether the PCs are connected to each other, we use PING command. Click on any computer andthen go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



10.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which youwant to send the message to the destination computer, then Run the Simulation.

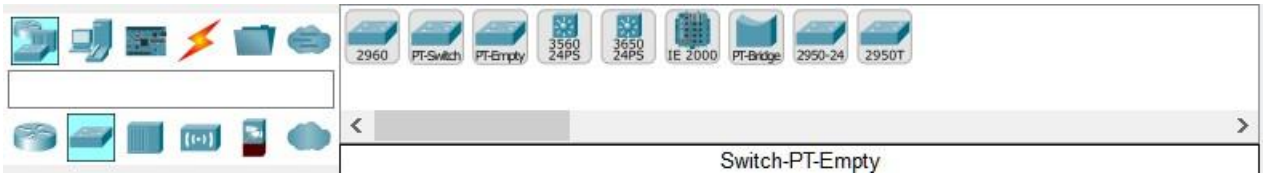


V. Bridge:

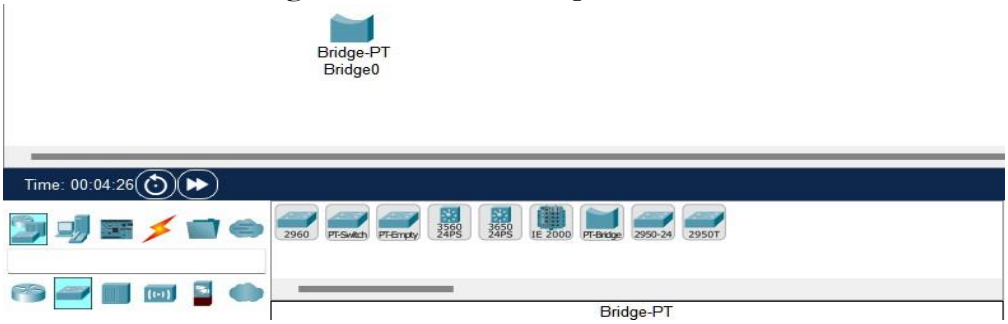
Procedure:

1.) Open Cisco Packet Tracer.

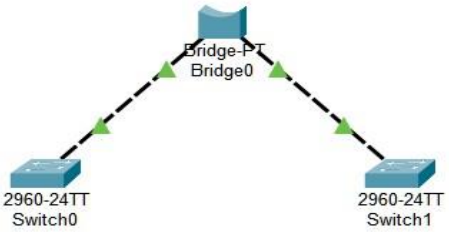
2.) Click on Network devices option from the bottom left corner and select Switch among various networkdevices.

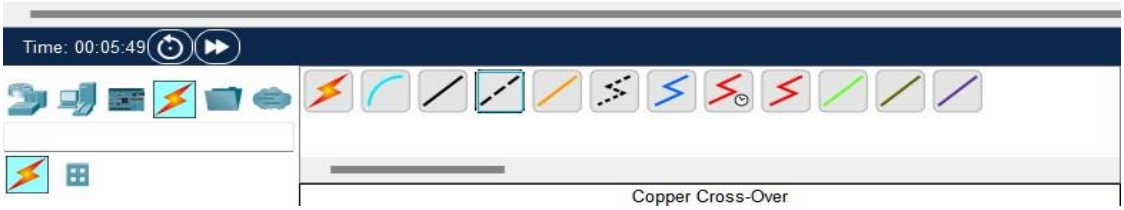


3.) Select PT-Bridge from available options.

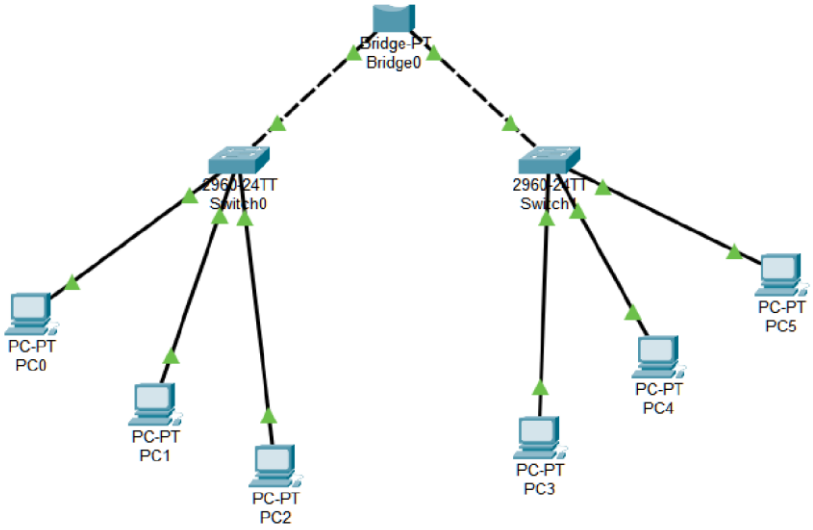


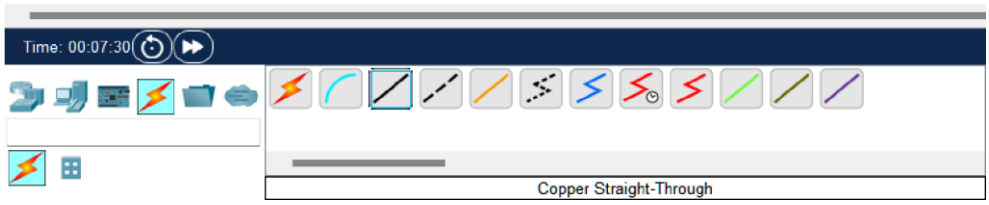
4.) Click on Network devices option from the bottom left corner and select two “2960” Switches amongvarious network devices, and connect them with router using “Copper Cross-Over”.



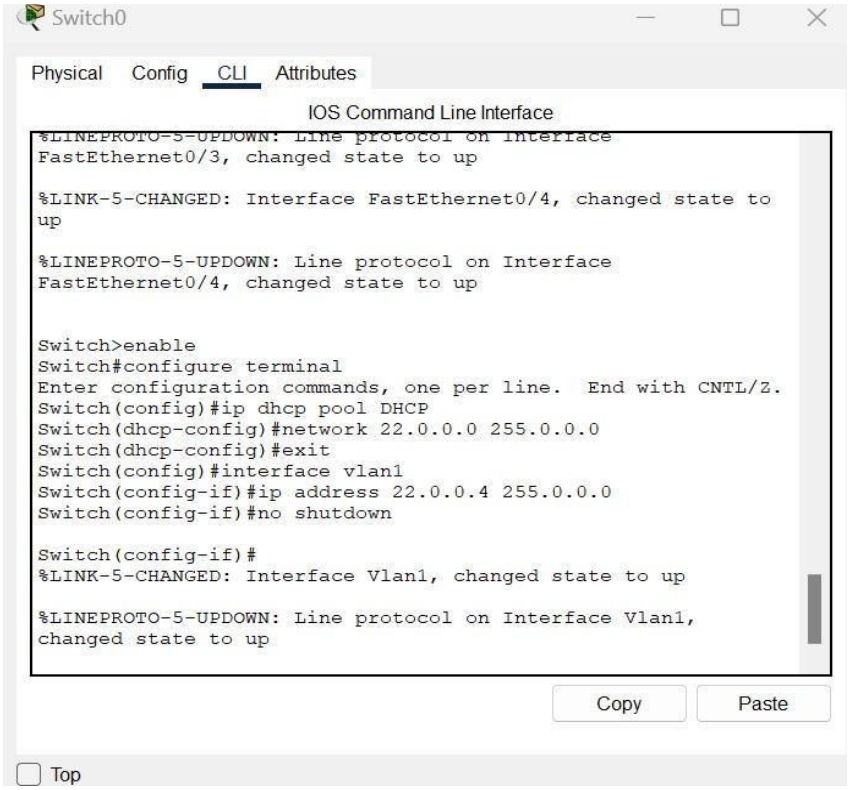


5.) Click on End Devices and select PCs from available options. Click on Connections and select “CopperStraight-Through” cable to connect PCs with Switches via FastEthernet Interface.

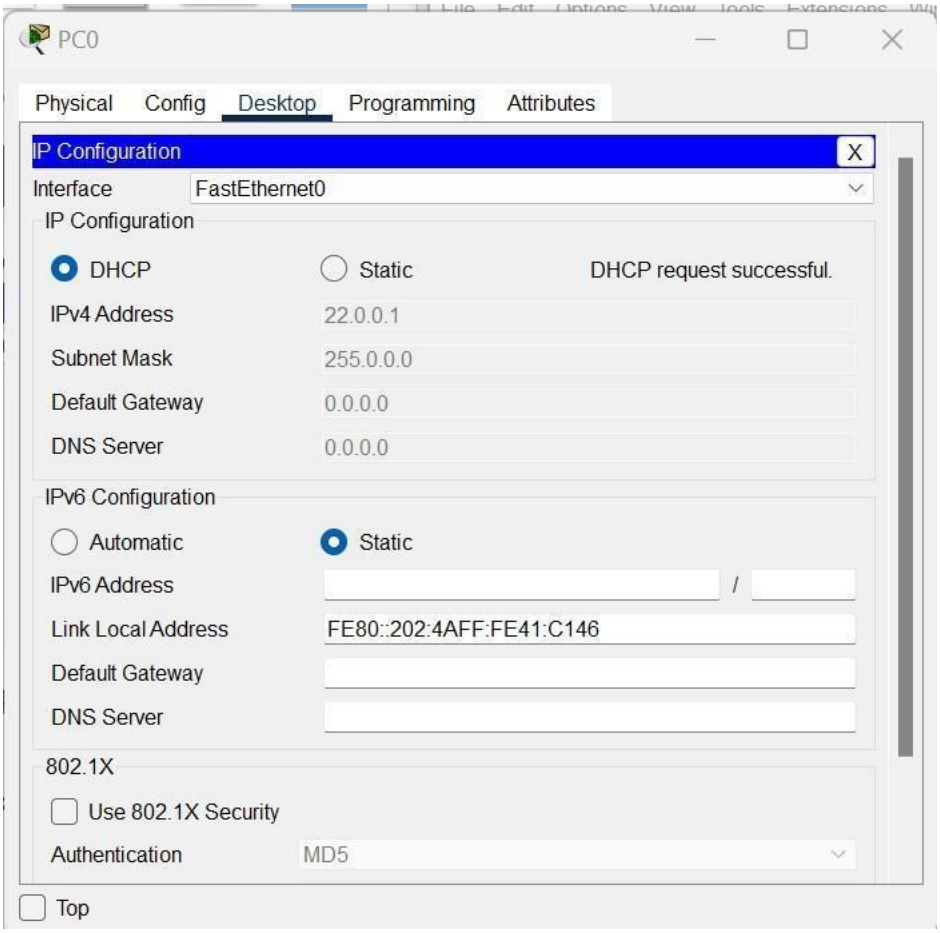




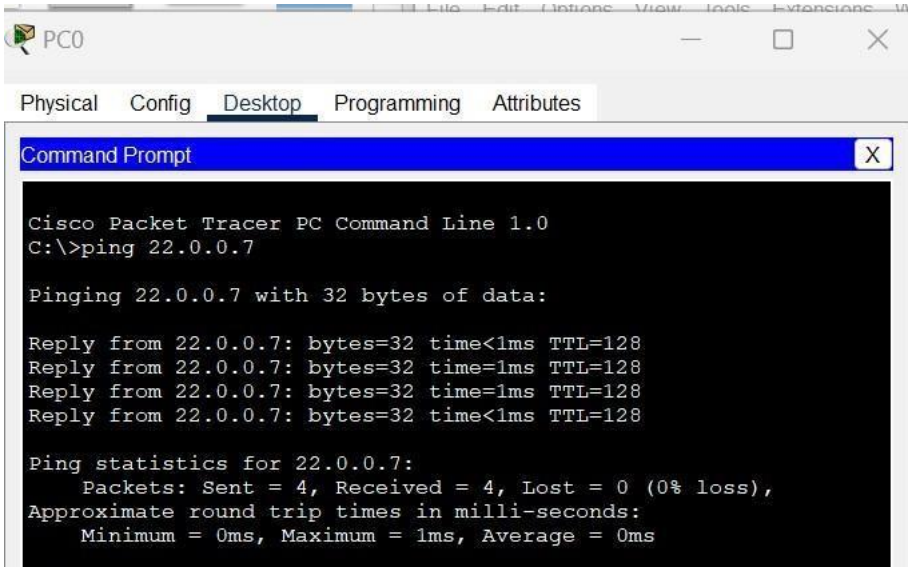
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of switch0 and writethe following commands in order to assign the network to the connected devices.



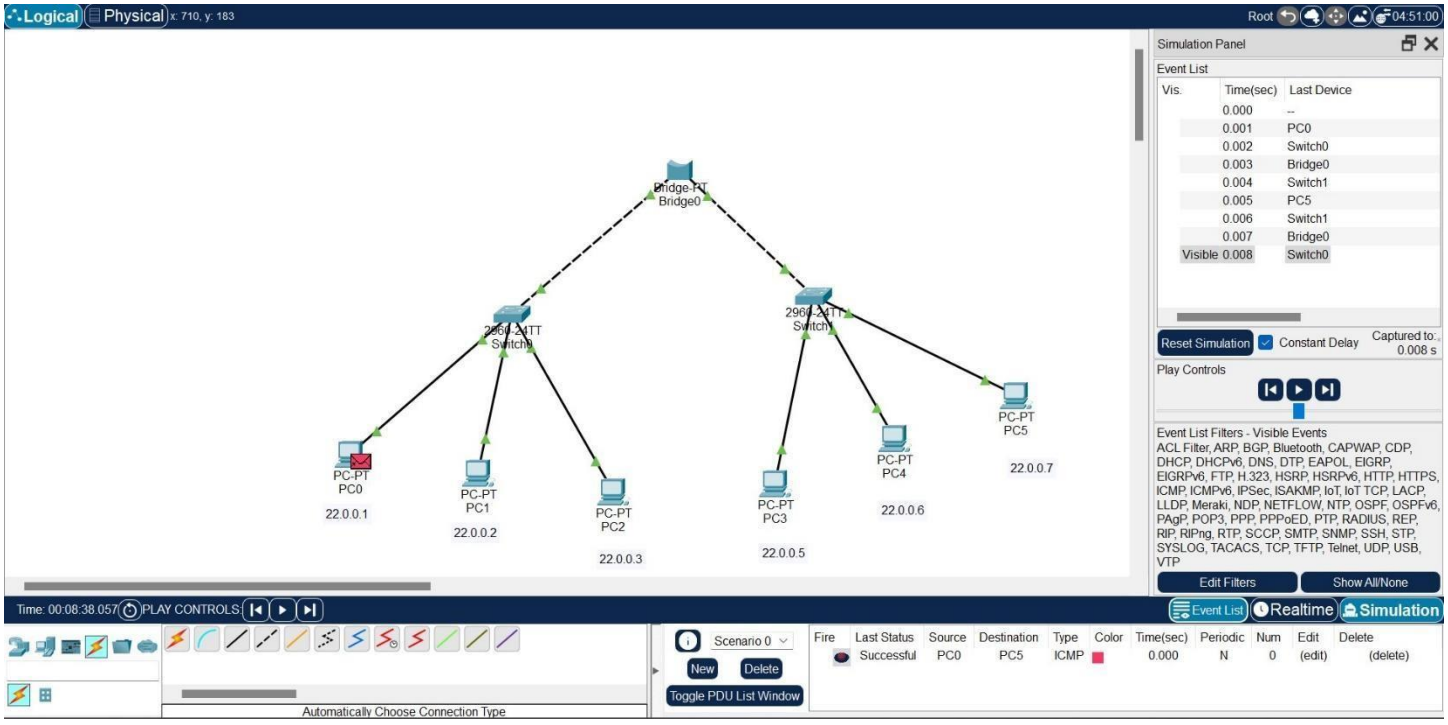
7.) Go to every PC's Desktop, click IP configuration and select DHCP. Repeat this step for all PC's.



9.) To check whether the PCs are connected to each other, we use PING command. Click on any computer andthen go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



10.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which youwant to send the message to the destination computer, then Run the Simulation.



PRACTICAL-3

Document a basic network using hub, switch and router in one network.

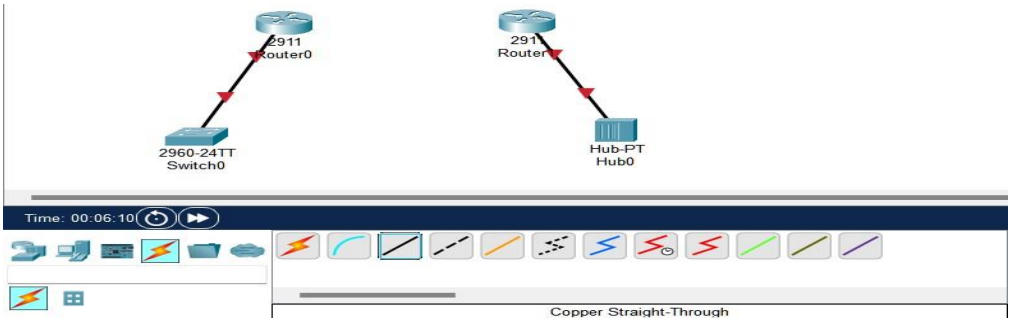
Procedure:

1.) Open Cisco Packet Tracer.

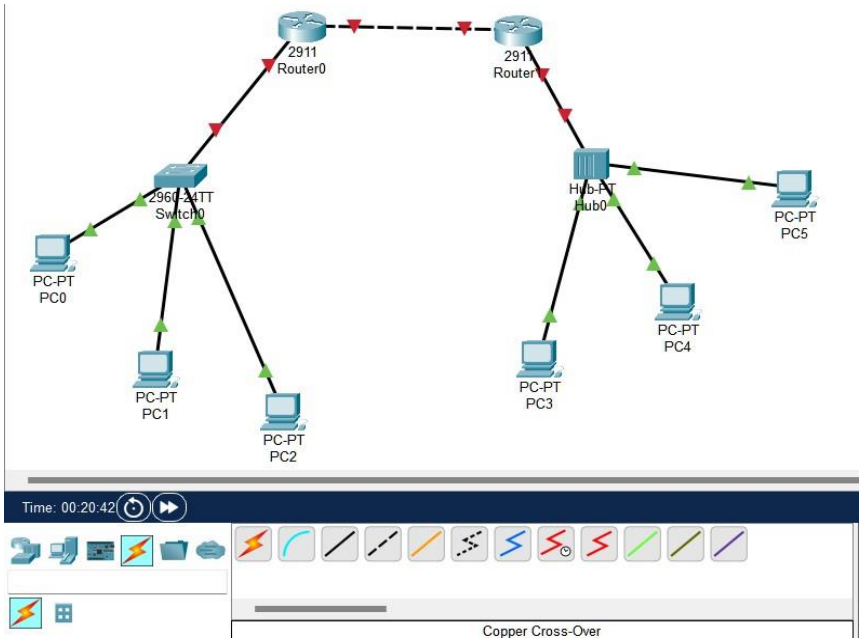
2.) Click on Network devices option from the bottom left corner and select Router among various network devices.

3.) Select two “2911” Routers from available options.

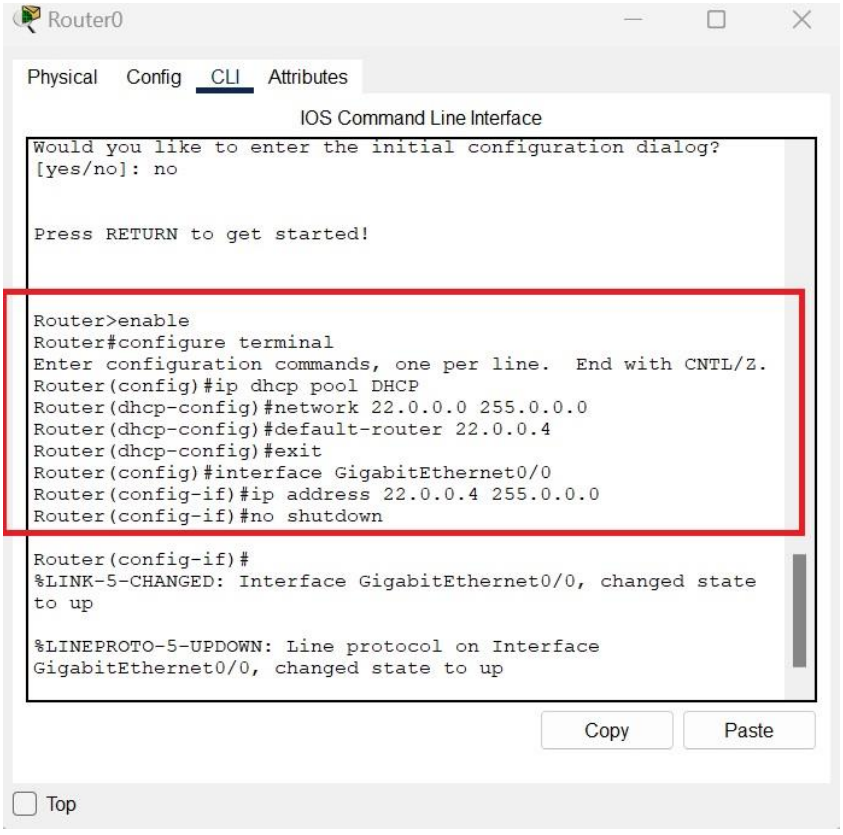
4.) Click on Network devices option from the bottom left corner and select one “2960” Switch and one PT-Hub among various network devices, and connect them with router using “Copper Straight-Through”.



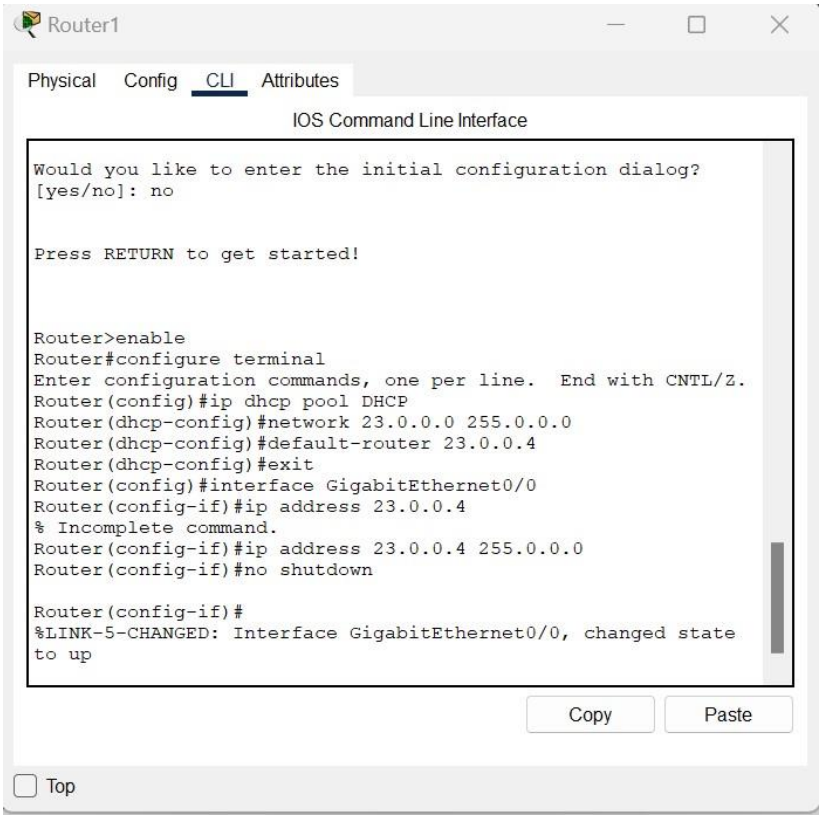
5.) Click on End Devices and select PCs from available options. Click on Connections and select “Copper Straight-Through” cable to connect PCs with Switches via GigabitEthernet Interface. And connect the routers with each other using “Copper-Cross over “cable via GigabitEthernet interface.



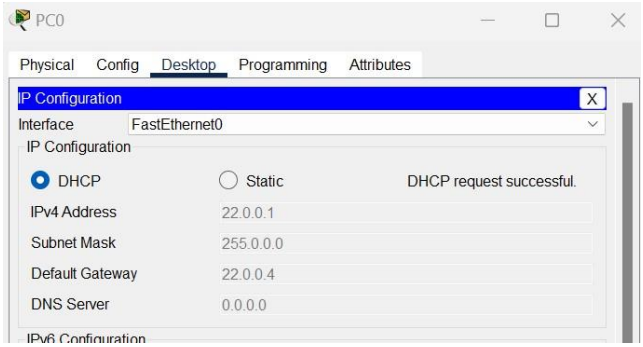
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of Router0 and write the following commands in order to assign the IP address to the connected devices with default gateway as Router0 with IP address 22.0.0.4



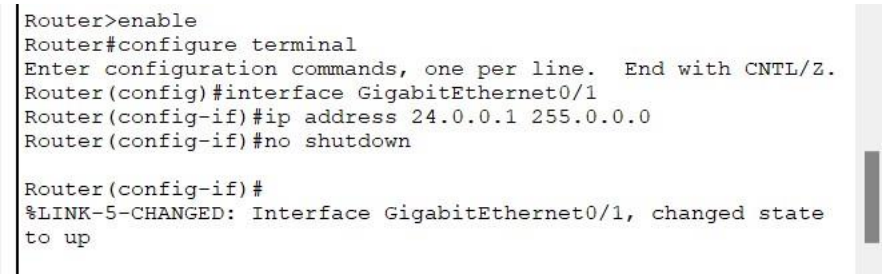
Repeat the process for Router1 and assign the IP address to the connected devices with default gateway as Router1 with IP address 23.0.0.4



7.) Go to every PC's Desktop, click IP configuration and select DHCP to assign the IP address dynamically using DHCP protocol. Repeat this step for all PC's.



8.) Now, to connect the two routers with each other. Go to Router0 and run the following commands in order to assign the IP address to the Router0 which is going to connect to Router1 via the interface GigabitEthernet0/1. Assign 24.0.0.1 address to router0.

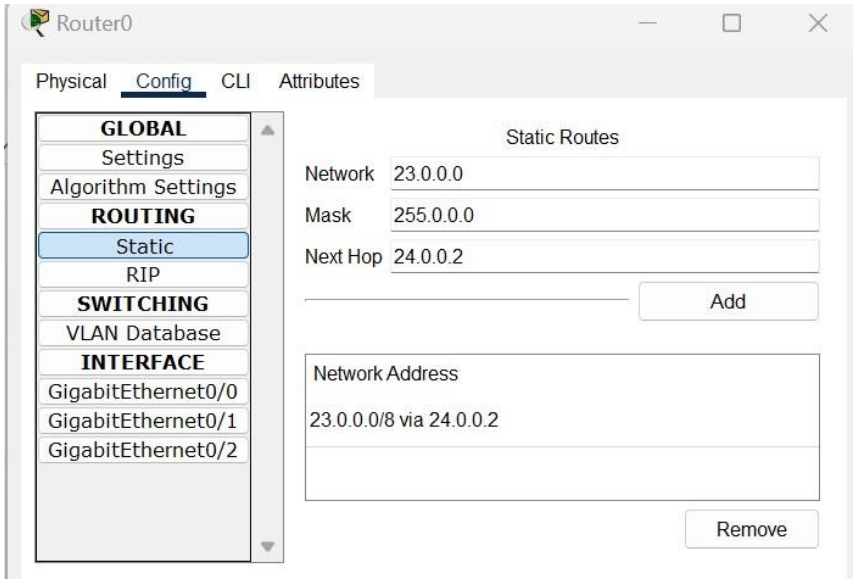


Similarly, Go to Router1 to perform the same operation in order to connect Router1 to Router0. Assign 24.0.0.2 address to Router1.

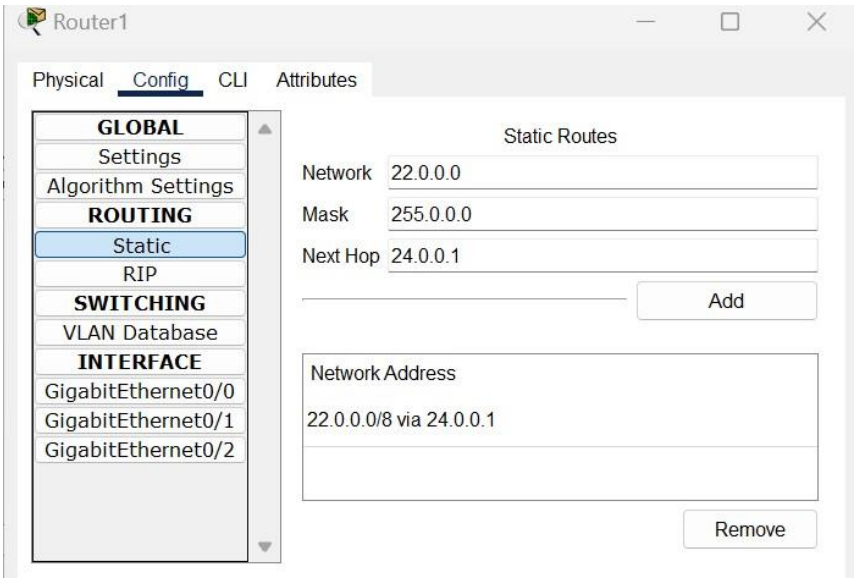
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 24.0.0.2 255.0.0.0
Router(config-if)#no shutdown

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

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

9.) Add the next hop in Router0 by selecting “Static” in routing option which is present in “config” section under Router0.

Enter the network and its subnet mask where you want to send the packet and Router1 IP address (24.0.0.2) in next hop because the packet is going to transmit via Router1.



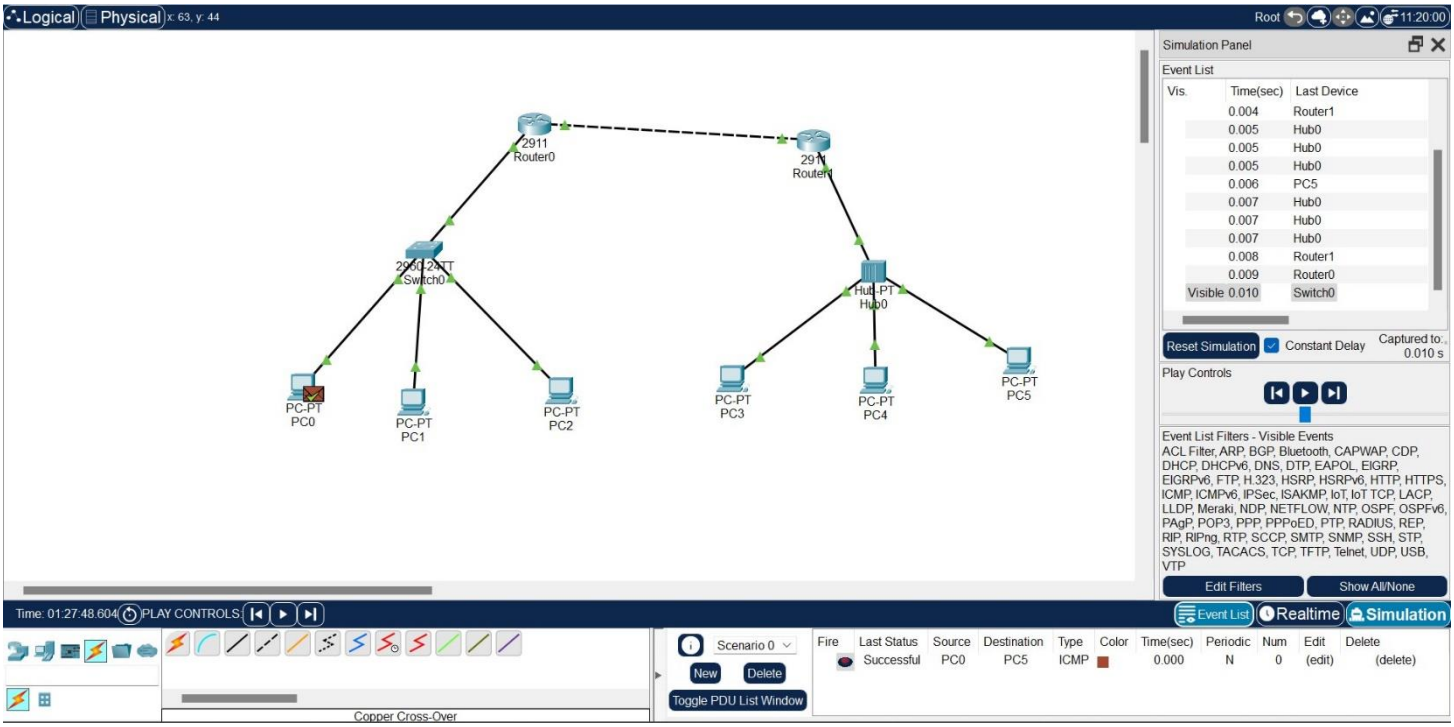
Repeat the process for Router1.



10.) To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

```
C:\>ping 23.0.0.1

Pinging 23.0.0.1 with 32 bytes of data:

Reply from 23.0.0.1: bytes=32 time<1ms TTL=126
Reply from 23.0.0.1: bytes=32 time<1ms TTL=126
Reply from 23.0.0.1: bytes=32 time=12ms TTL=126
Reply from 23.0.0.1: bytes=32 time<1ms TTL=126

Ping statistics for 23.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

10.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



PRACTICAL-4

Document a basic network using 3 routers in a LAN configuration.

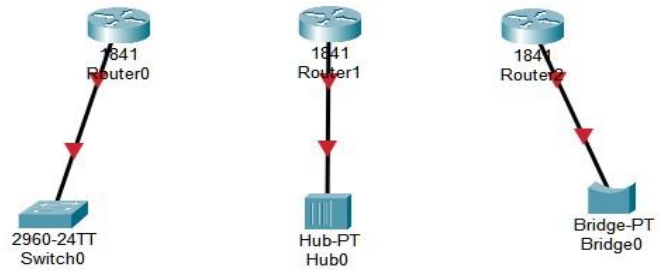
Procedure:-

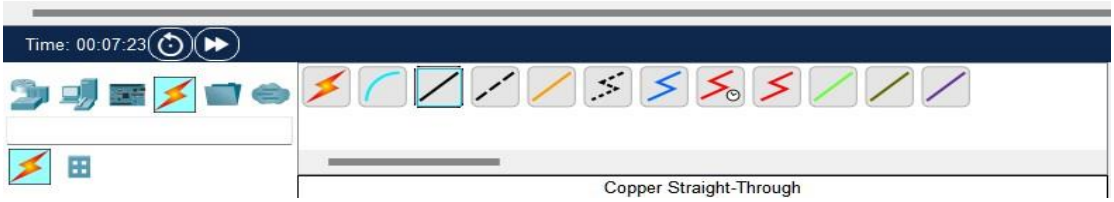
1.) Open Cisco Packet Tracer.

2.) Click on Network devices option from the bottom left corner and select Router among various network devices.

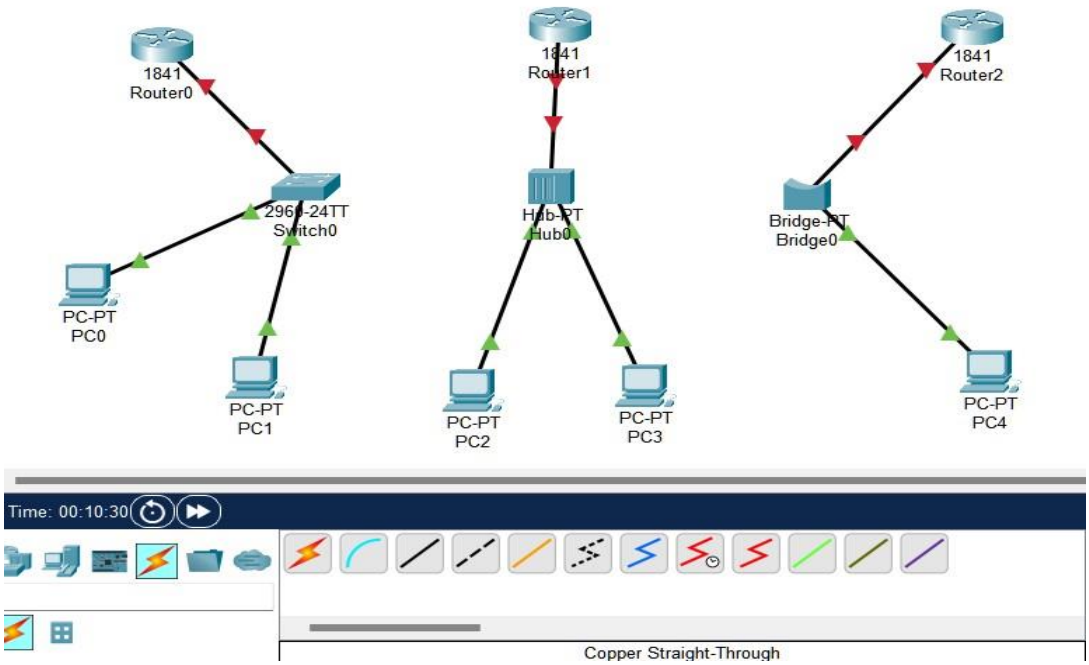
3.) Select three “1841” Routers from available options.

4.) Click on Network devices option from the bottom left corner and select one “2960” , one PT-Hub and one PT-Bridge among various network devices, and connect them with router using “Copper Straight-Through”.

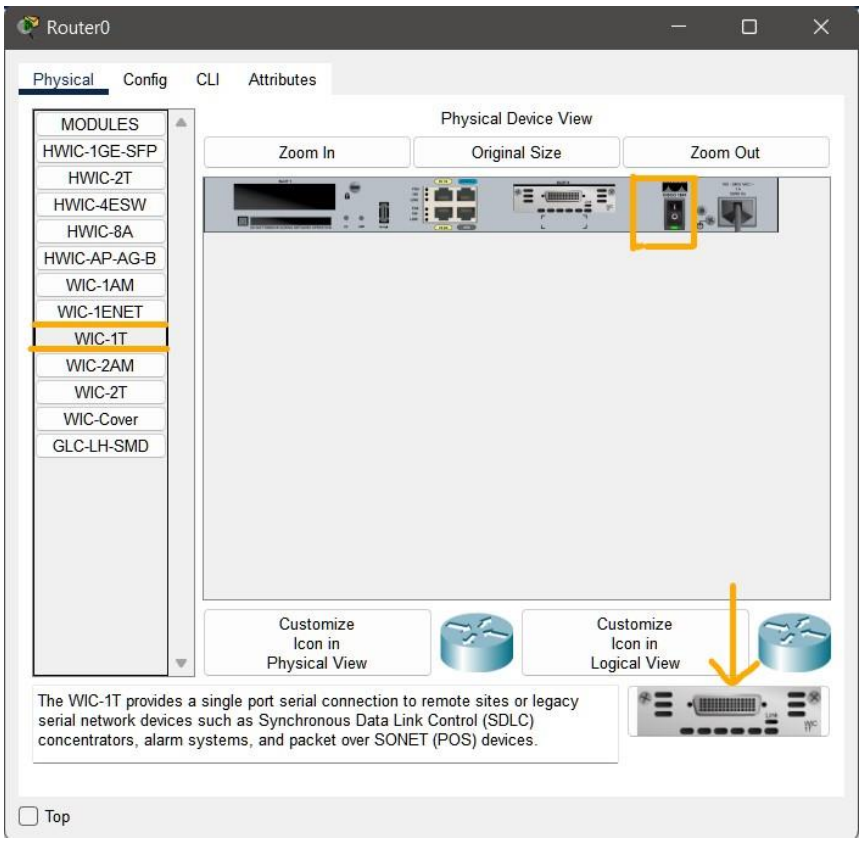




5.) Click on End Devices and select PCs from available options. Click on Connections and select “Copper Straight-Through” cable to connect PCs with Switches via GigabitEthernet Interface.

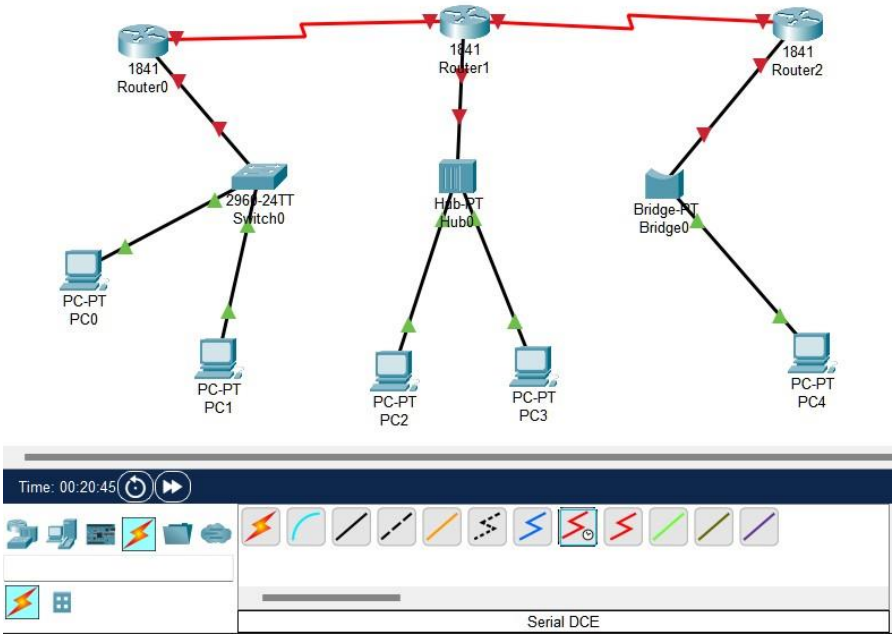


6.) To connect the router, click on them; select “Physical” option from the top ribbon then turn off the router from the button given in picture, then select “WIC-1T” and drag it to the empty slots in the router, then turn on the Router. Repeat the process for the second and third router.

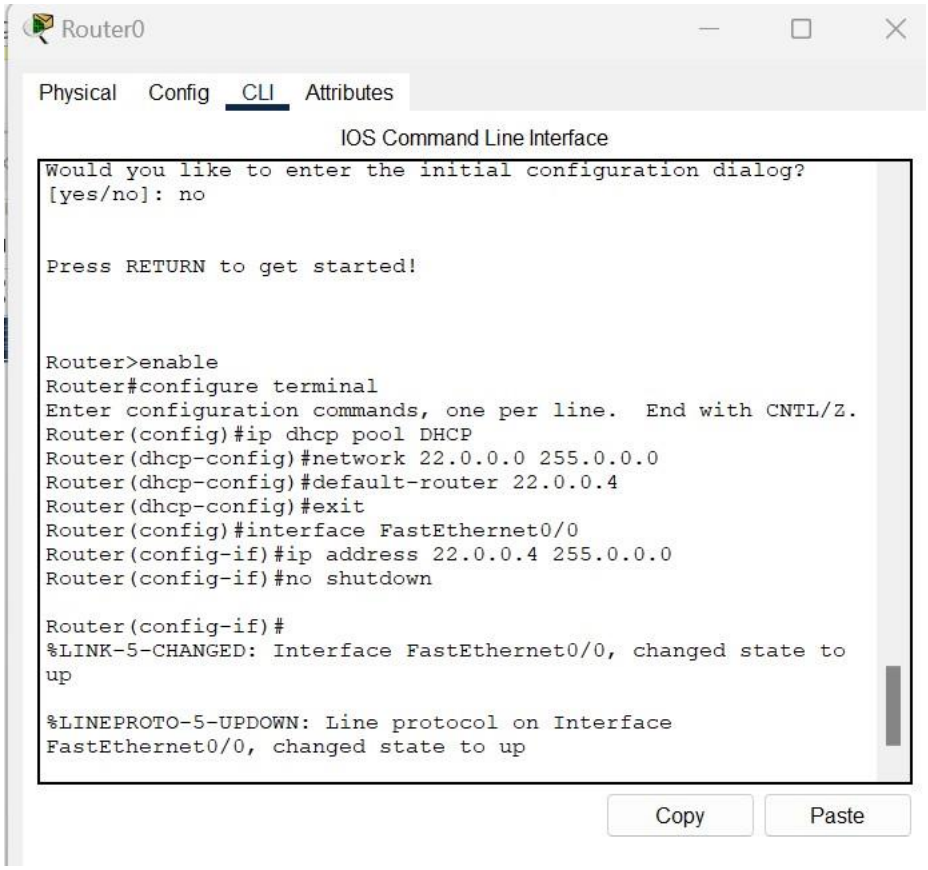


NOTE: Use 2 WIC-1T port in the second router as we have to connect it with 2 routers.

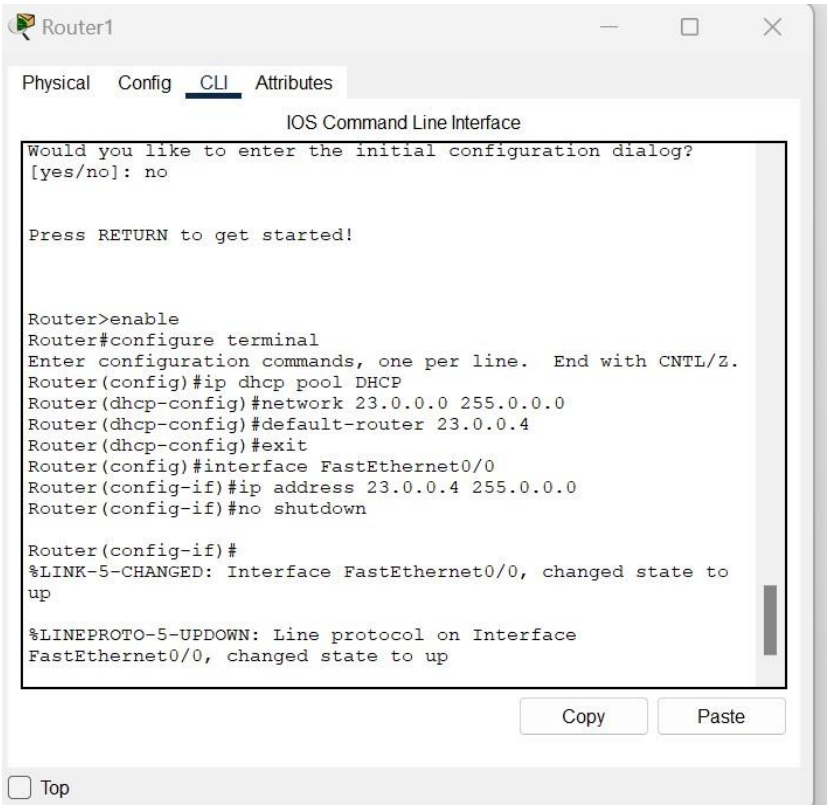
10.) Select “Serial DCE” wire from the Connections to connect the routers. Click on one router and select Serial port and then click on other router and select Serial port.



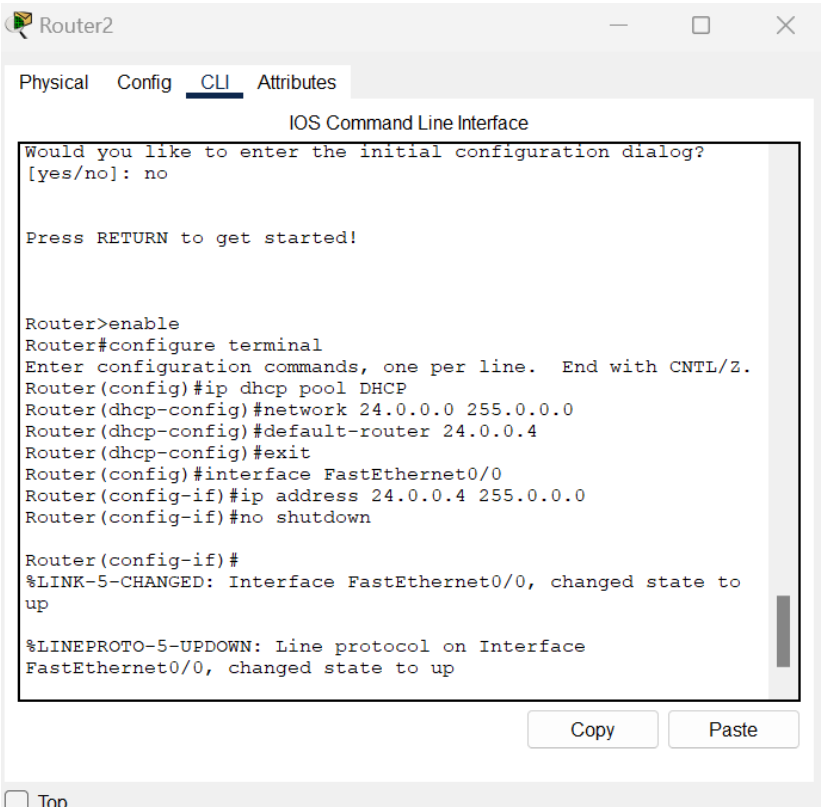
6.) Assign IP addresses to the computers dynamically by using DHCP protocol. Go to CLI of Router0 and write the following commands in order to assign the IP address to the connected devices with default gateway as Router0 with IP address 22.0.0.4



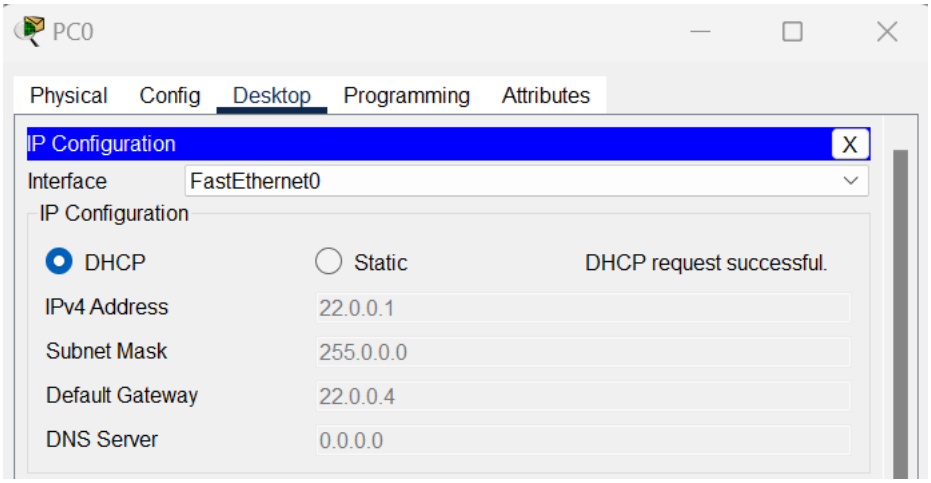
Repeat the process for Router1 and assign the IP address to the connected devices with default gateway as Router1 with IP address 23.0.0.4



Repeat the process for Router2 and assign the IP address to the connected devices with default gateway as Router3 with IP address 24.0.0.4



7.) Go to every PC's Desktop, click IP configuration and select DHCP to assign the IP address dynamically using DHCP protocol. Repeat this step for all PC's.



8.) Now, to connect the two routers with each other. Go to Router0 and run the following commands in order to assign the IP address to the Router0 which is going to connect to Router1 via the interface Serial0/0/0. Assign 20.0.0.1 address to router0.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial0/0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
```

Similarly, Go to Router1 to perform the same operation in order to connect Router1 to Router0. Assign 20.0.0.2 address to Router1.

```
Router(config)#interface serial0/1/0
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

Now, To Connect Router1 with Router2, go to router 1 and assign IP address of 21.0.0.1.

```
Router(config)#interface serial0/0/0
Router(config-if)#ip address 21.0.0.1 255.0.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
```

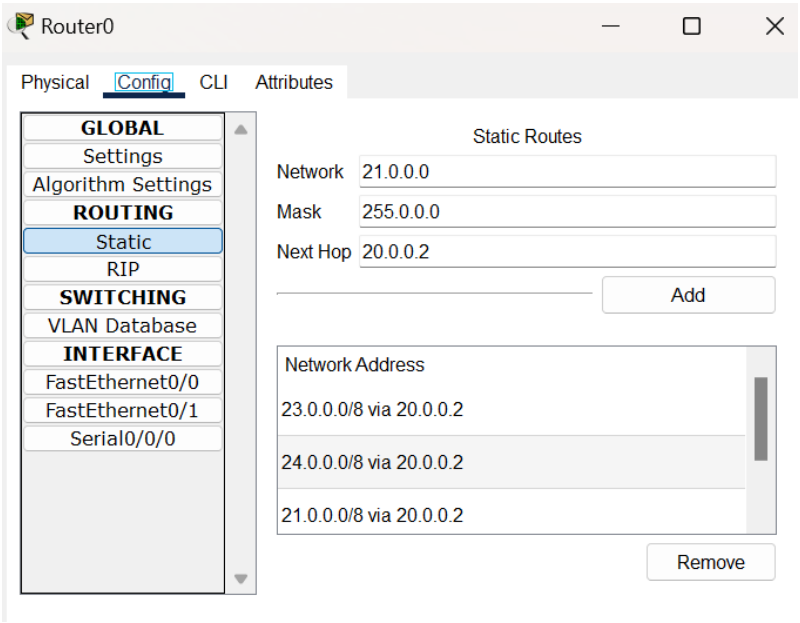
Similarly, Go to Router2 and assign IP address of 21.0.0.2.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 21.0.0.2 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

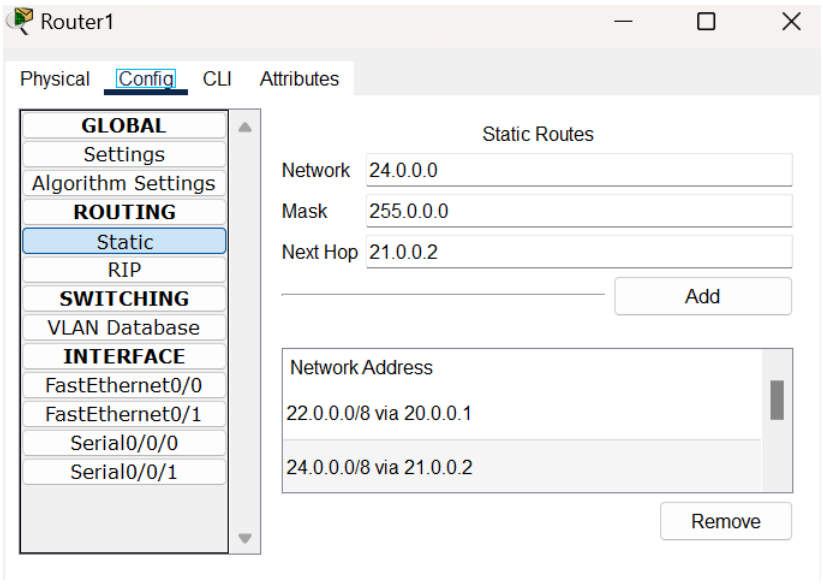
9.) Add the next hop in Router0 by selecting “Static” in routing option which is present in “config” section under Router0.

Enter the network connected to hub(23.0.0.0) and its subnet mask and Router1 IP address (20.0.0.2) in next hop because the packet is going to transmit via Router1.

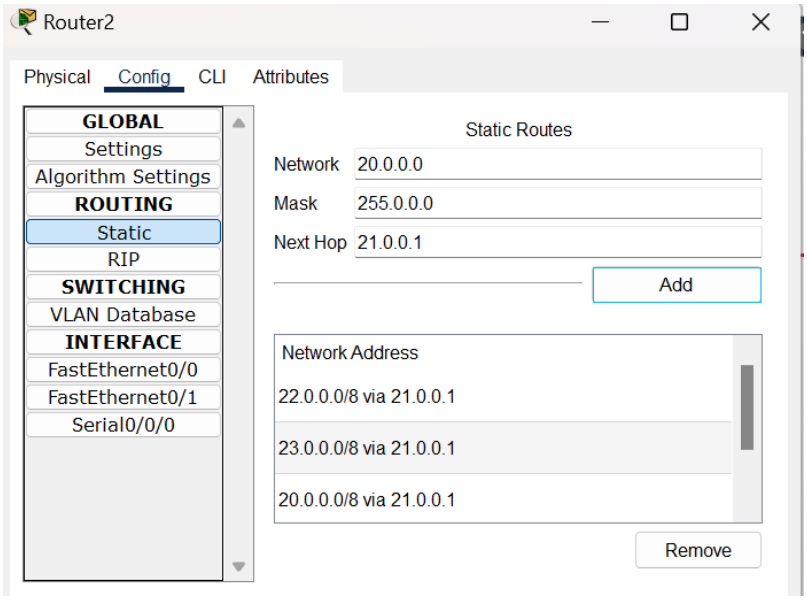
Repeat the process, enter all other networks as shown below :



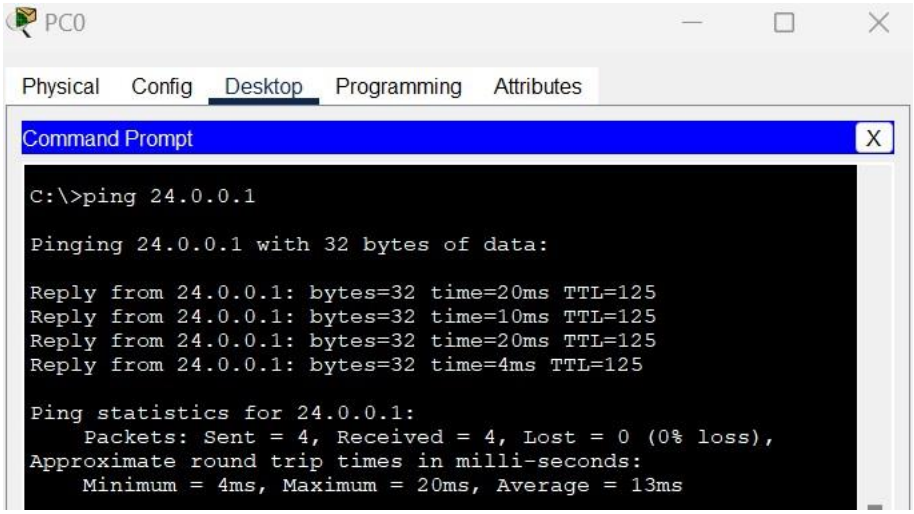
Repeat the process for Router1.



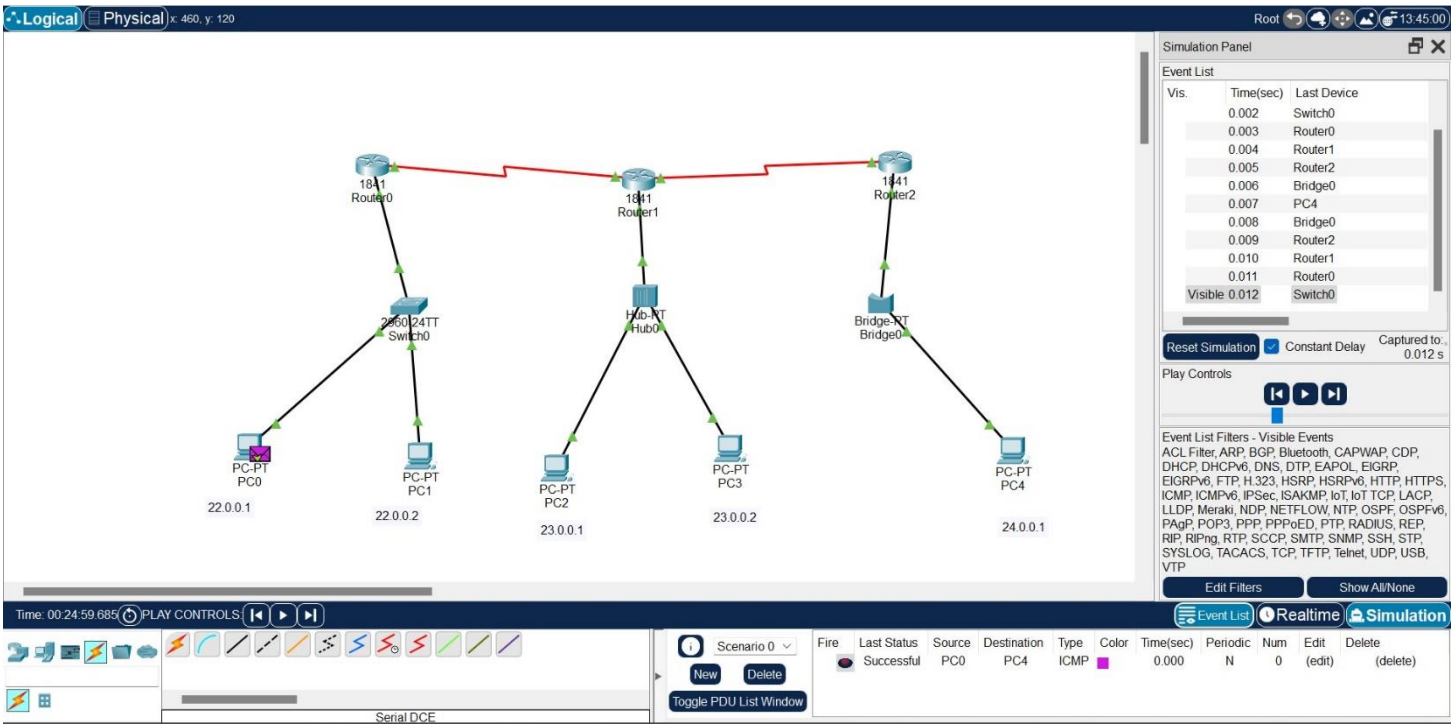
Repeat the process for Router2.



10.) To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



10.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.


Logical
Physical
x: 460, y: 120
Root
13:45:00
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.002 Switch0
0.003 Router0
0.004 Router1
0.005 Router2
0.006 Bridge0
0.007 PC4
0.008 Bridge0
0.009 Router2
0.010 Router1
0.011 Router0
Visible 0.012 Switch0
Reset Simulation
Constant Delay
Captured to:
0.012 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
1841 Router0
1841 Router1
1841 Router2
2960-24TT Switch0
Hub-PT Hub0
Bridge-PT Bridge0
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
22.0.0.1
22.0.0.2
23.0.0.1
23.0.0.2
24.0.0.1
Time: 00:24:59.685
PLAY CONTROLS:
Event List
Realtime
Simulation
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Successful
PC0
PC4
ICMP
0.000
N
0
(edit)
(delete)

PRACTICAL-5

Implement static routing in a network.

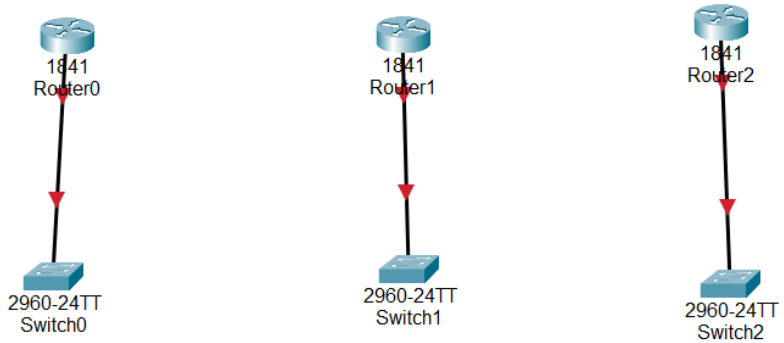
Procedure:-

1.) Open Cisco Packet Tracer.

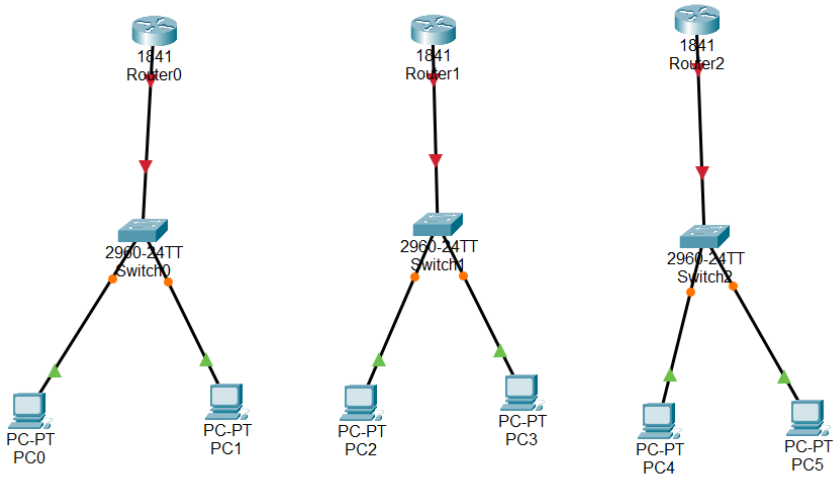
2.) Click on Network devices option from the bottom left corner and select Router among various network devices.

3.) Select three “1841” Routers from available options.

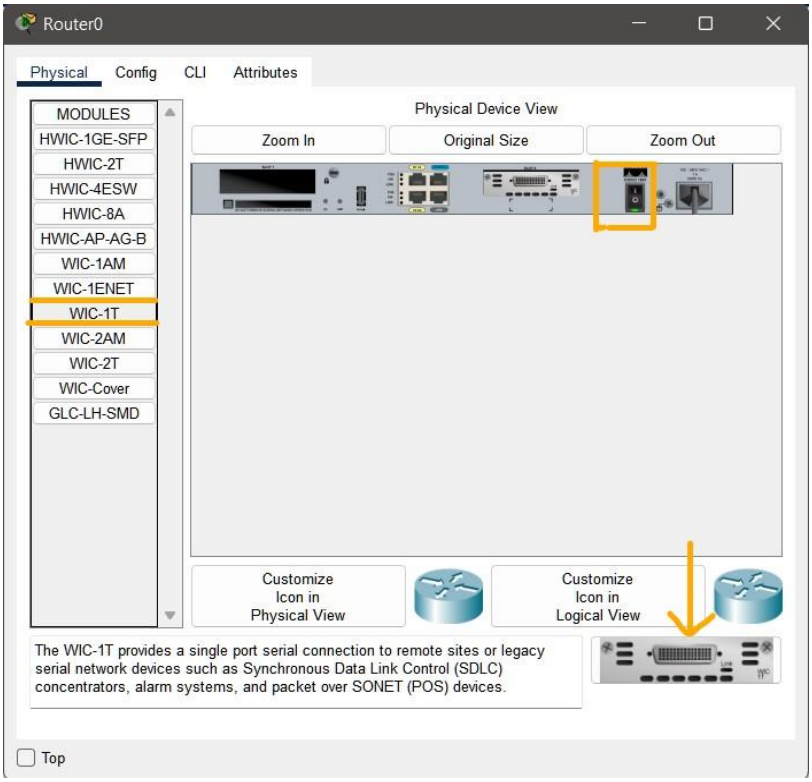
4.) Click on Network devices option from the bottom left corner and select three “2960” switch and connect them with router using “Copper Straight-Through”.



5.) Click on End Devices and select PCs from available options. Click on Connections and select “Copper Straight-Through” cable to connect PCs with Switches via GigabitEthernet Interface.

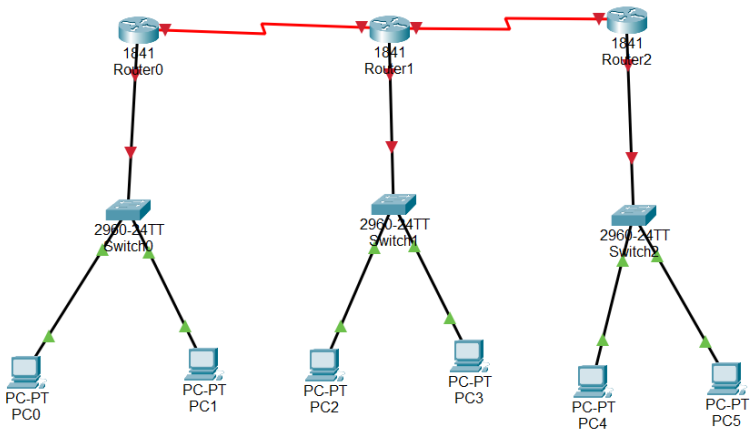


6.) To connect the router, click on them; select “Physical” option from the top ribbon then turn off the router from the button given in picture, then select “WIC-1T” and drag it to the empty slots in the router, then turn on the Router. Repeat the process for the second and third router.

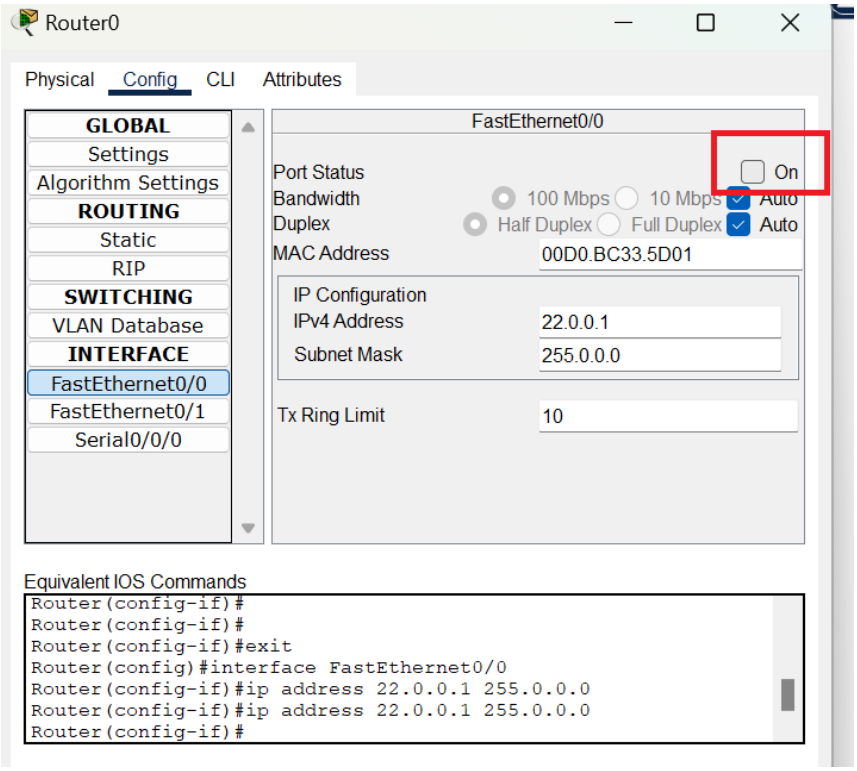


NOTE: Use WIC-2T port in the second router as we have to connect it with 2 routers.

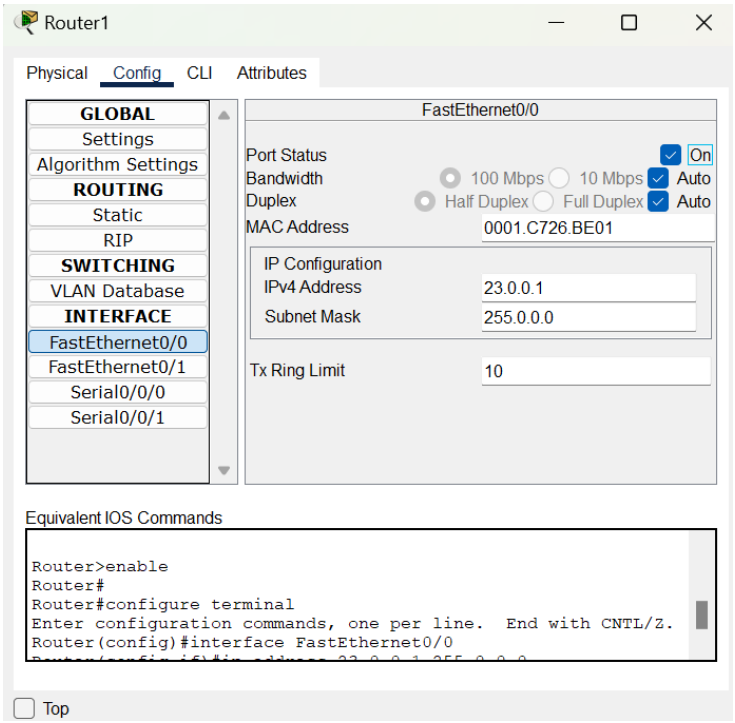
7.) Select “Serial DCE” wire from the Connections to connect the routers. Click on one router and select Serial port and then click on other router and select Serial port.



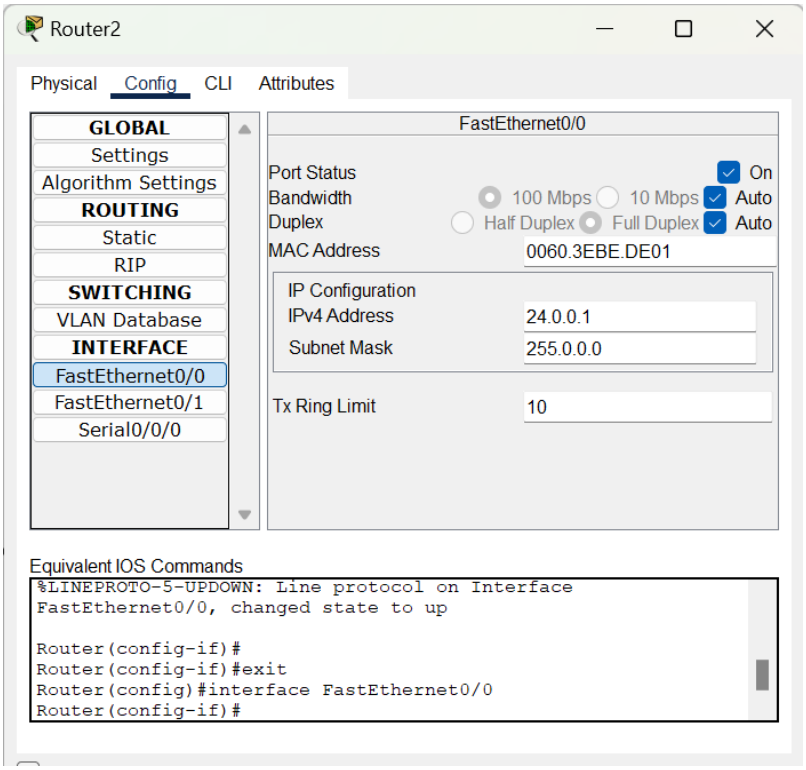
8.) Go to Config of Router0,then click on FastEthernet0/0 and write ipv4 address as 22.0.0.1 then click on "On" to assign the IP address to the connected devices with default gateway as Router0 with IP address 22.0.0.1



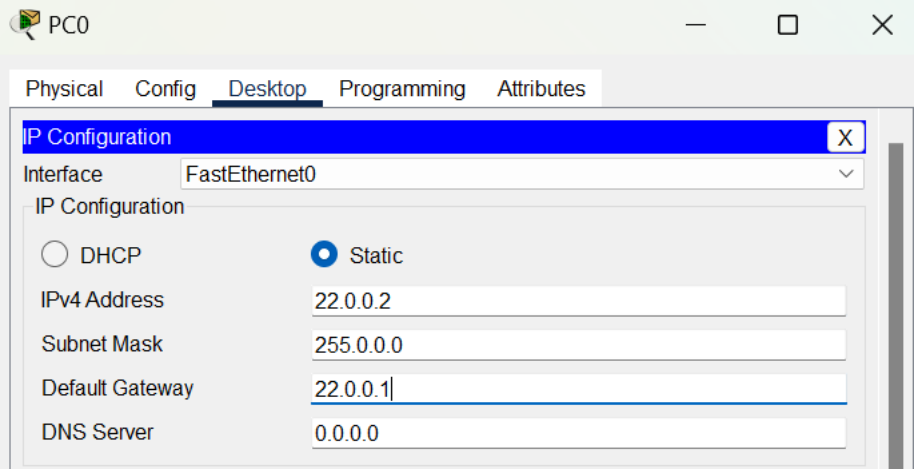
Repeat the process for Router1 and assign the IP address to the connected devices with default gateway as Router1 with IP address 23.0.0.1



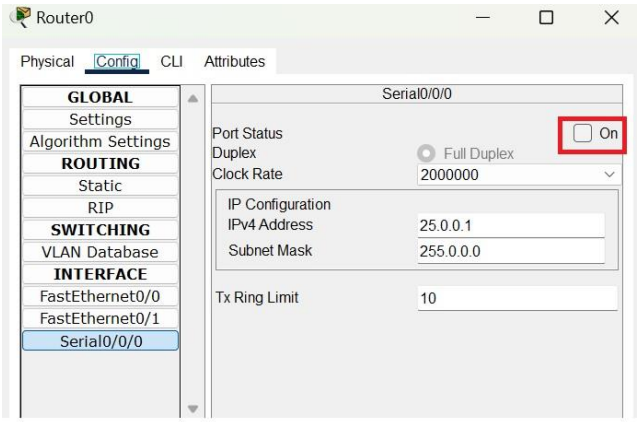
Repeat the process for Router2 and assign the IP address to the connected devices with default gateway as Router3 with IP address 24.0.0.1.



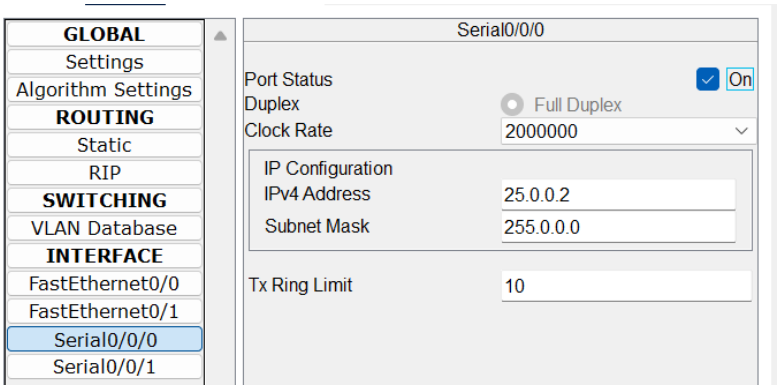
9).Go to every PC's Desktop, click IP configuration and select static to assign the IP address statically and type ip address of router in default gateway column of pc. Repeat this step for all PC's.



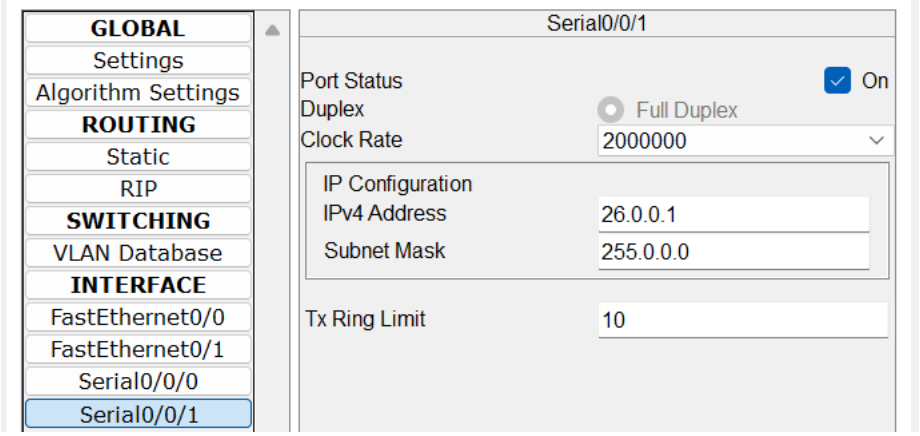
10).Now, to connect the two routers with each other. Go to Router0,then click on config and then on serial0/0/0,then type the ip address as 25.0.0.1 and click on "On" button in order to assign the IP address to the Router0 which is going to connect to Router1 via the interface Serial0/0/0.



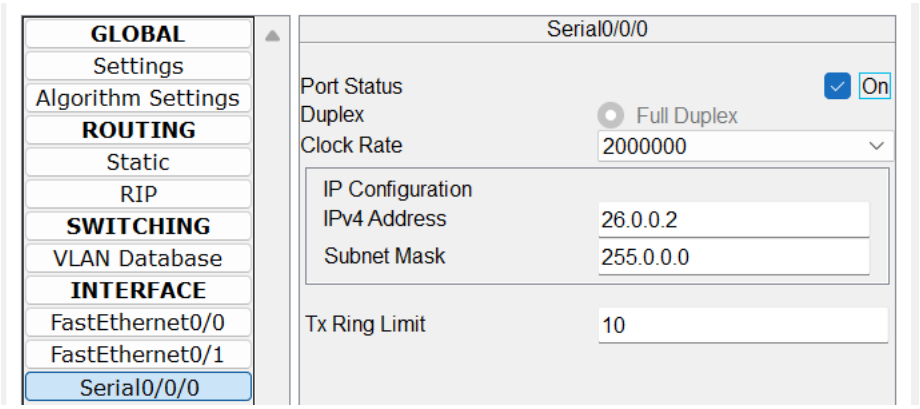
Similarly, Go to Router1 to perform the same operation in order to connect Router1 to Router0. Assign 25.0.0.2 address to Router1.



Now, To Connect Router1 with Router2, go to router 1 and assign IP address of 26.0.0.1.



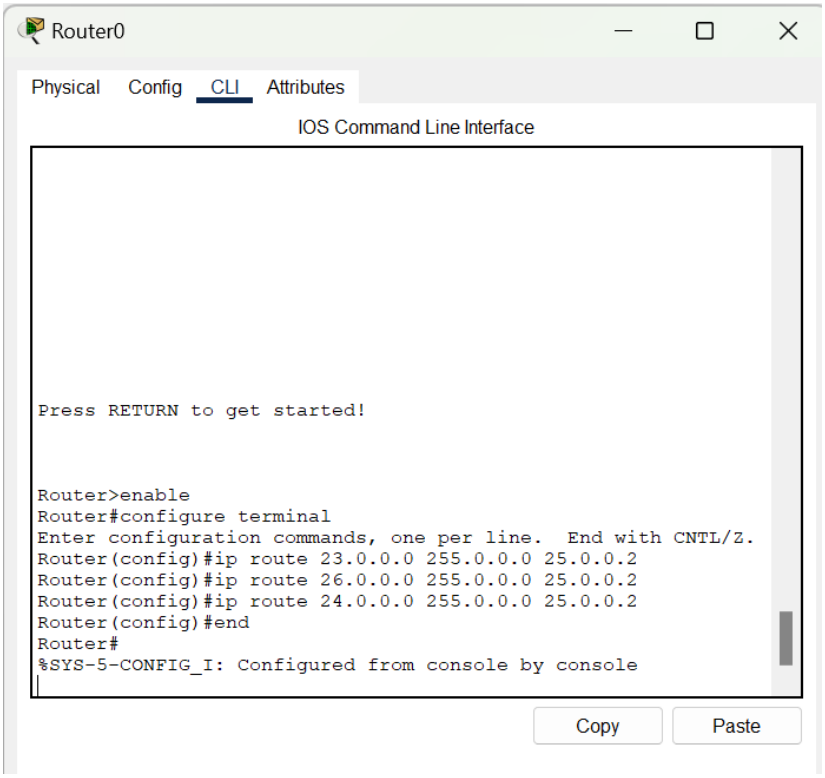
Similarly, Go to Router2 and assign IP address of 26.0.0.2.



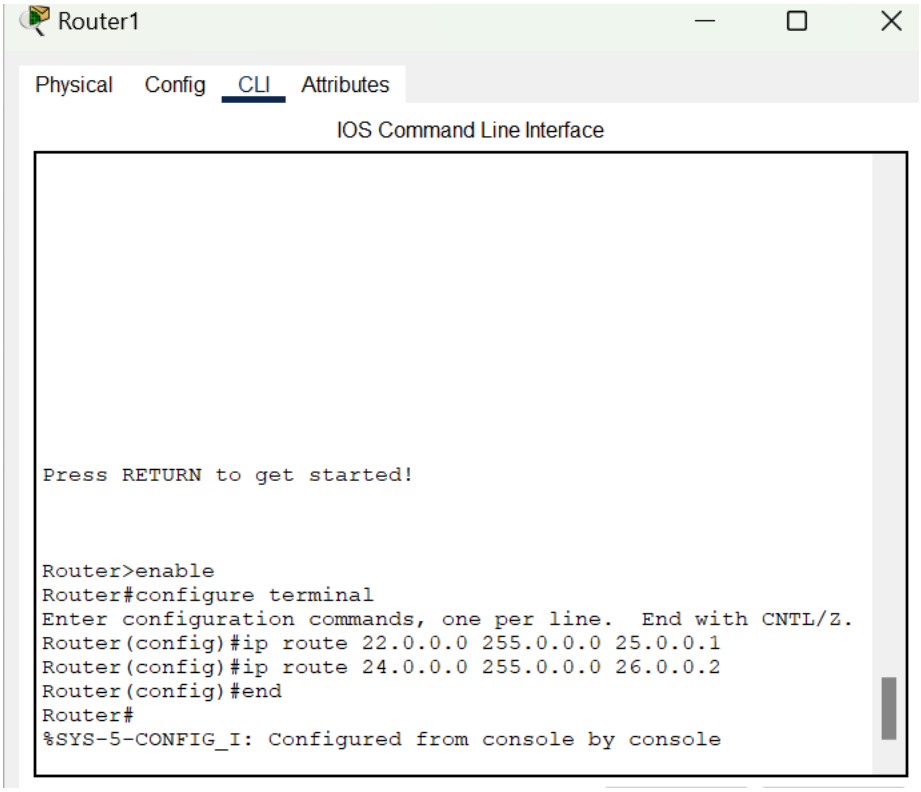
11) To add a next hop to a route using the CLI(statically), follow these steps :

1. select the router you want to configure.
2. In the command line interface (CLI) of the router, enter "enable" mode by typing "enable" and hitting enter.
3. Type "configure terminal" and hit enter to enter configuration mode.
4. Type "ip route [destination network address] [subnet mask] [next hop IP address]" to add a static route to the routing table.
5. Type "end" to save the changes and exit configuration mode.

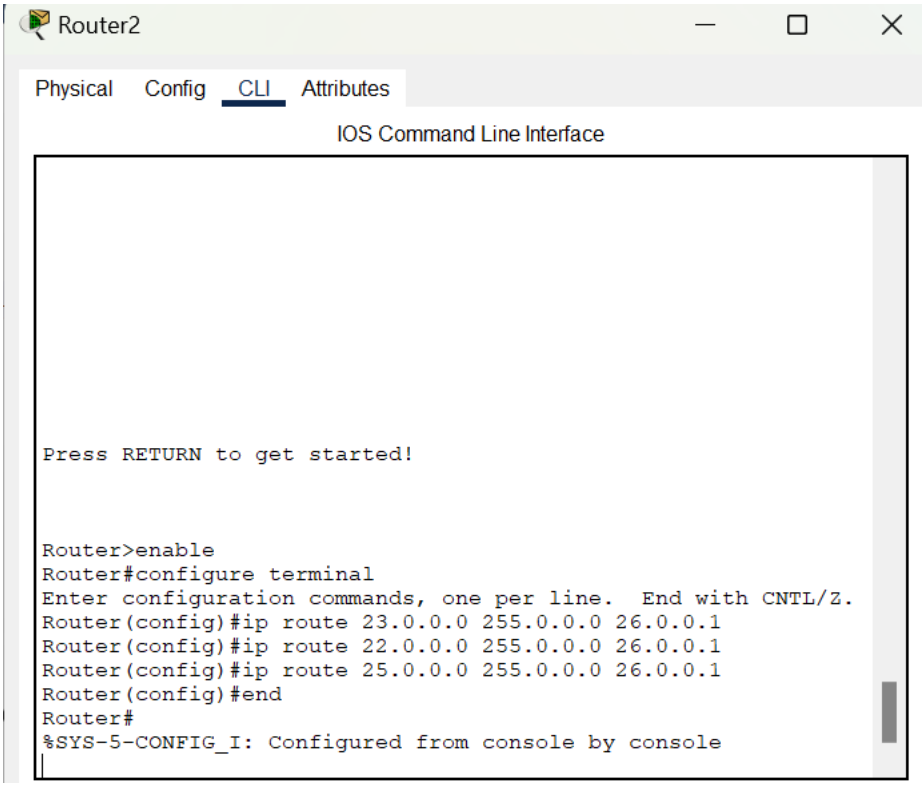
Go to cli of router1 and type these command to add next hop



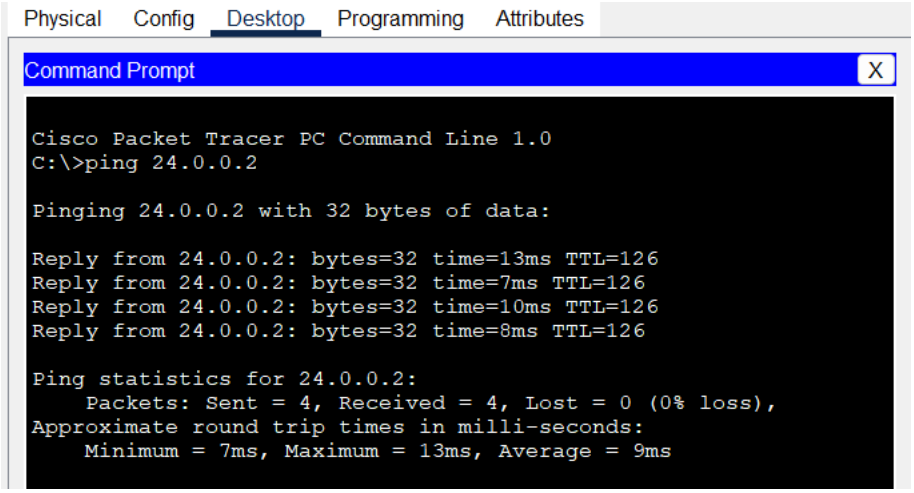
Repeat the process for Router1.



Repeat the process for Router2.

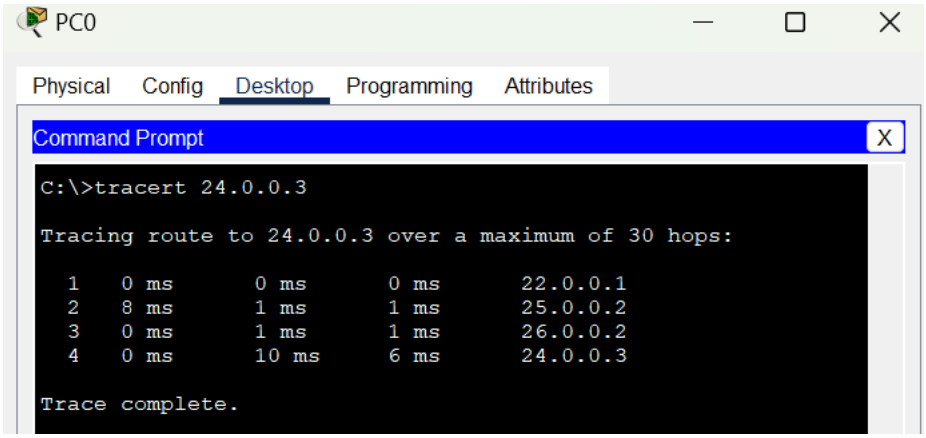


12).To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

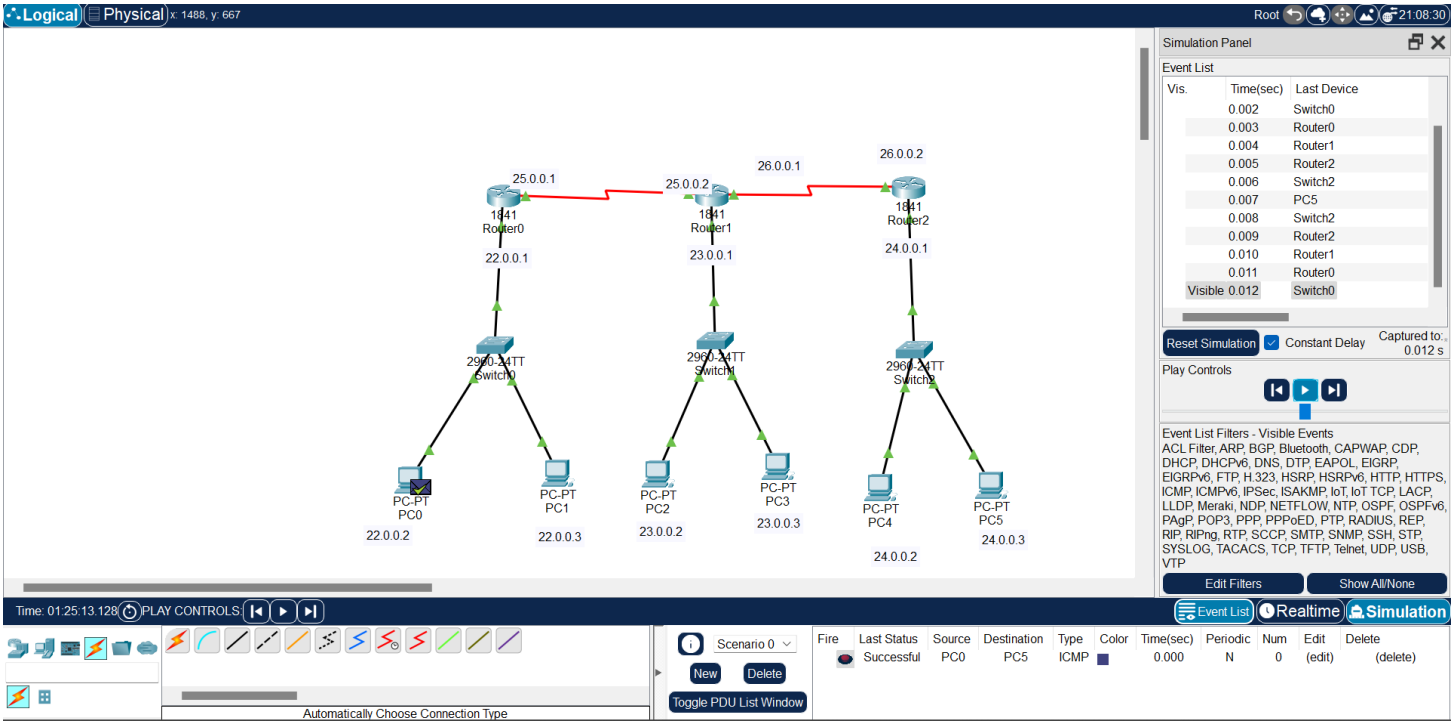


13).For tracing the routes taken by packets to reach from one pc to another . Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “tracert *IP address of any other computer*”

(*excluded). Then it will display the path taken by the packets from the source device to the destination ,including the ip addresses of each hop and the time it takes for the packet to reach each hop.



14.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



PRACTICAL-6

Implement dynamic routing in a network.

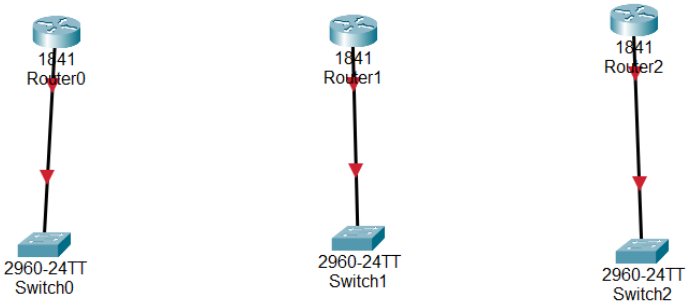
Procedure:-

1.) Open Cisco Packet Tracer.

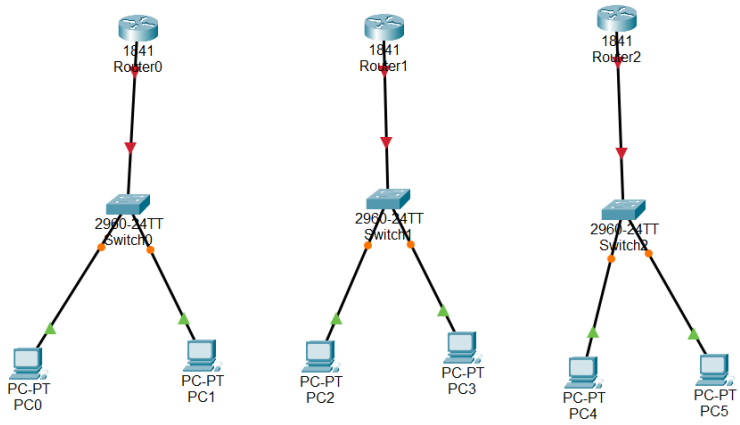
2.) Click on Network devices option from the bottom left corner and select Router among various network devices.

3.) Select three “1841” Routers from available options.

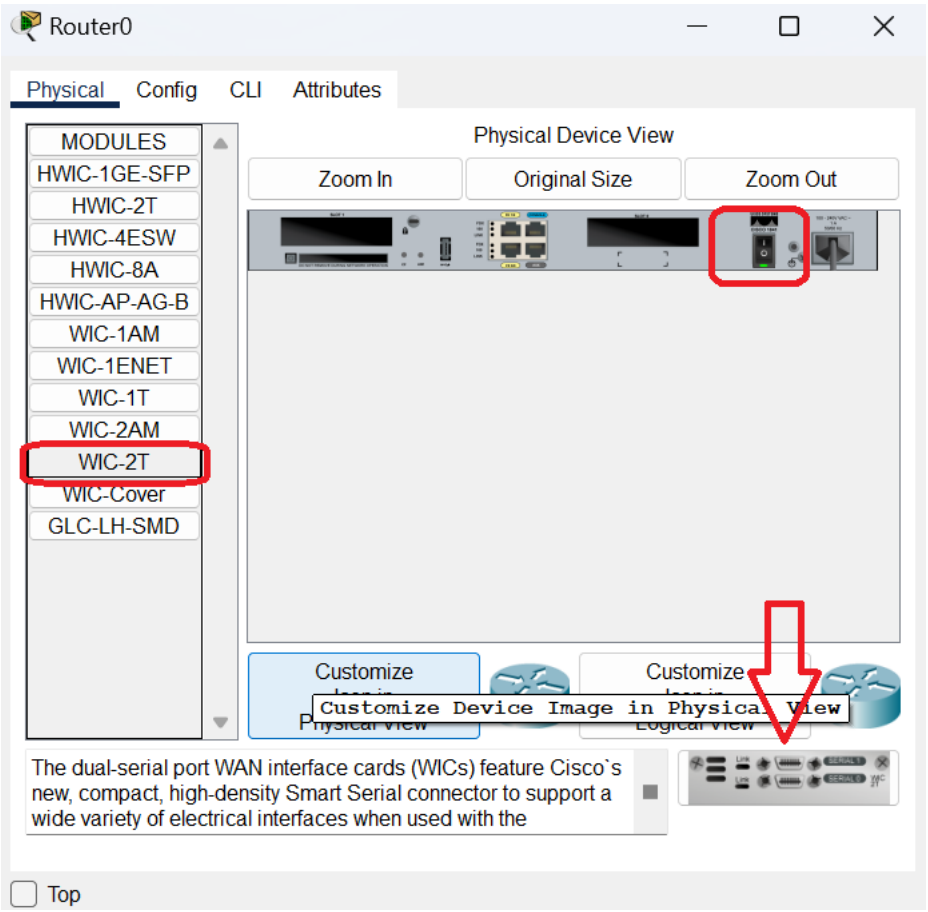
4.) Click on Network devices option from the bottom left corner and select three “2960” switch and connect them with router using “Copper Straight-Through”.



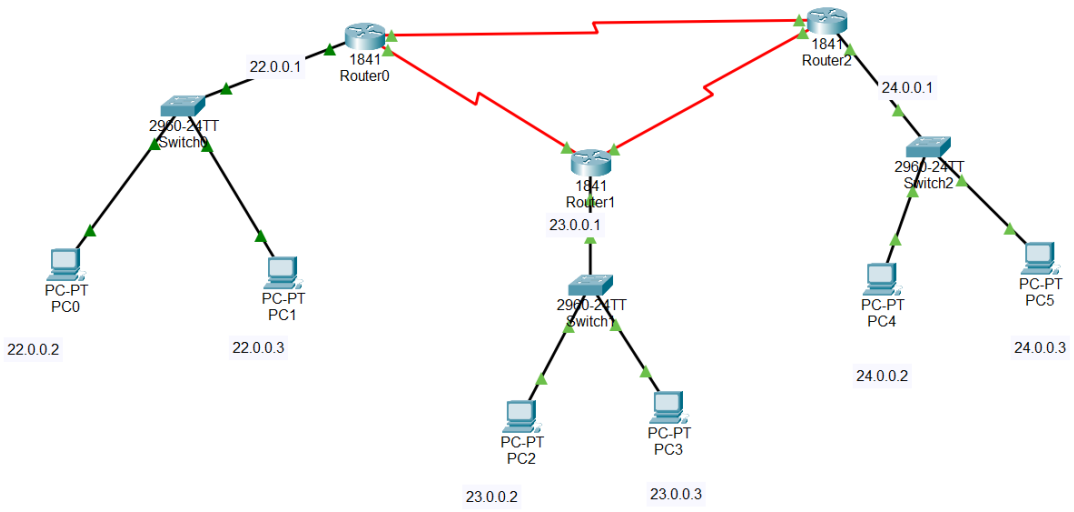
5.) Click on End Devices and select PCs from available options. Click on Connections and select "Copper Straight-Through" cable to connect PCs with Switches via GigabitEthernet Interface.



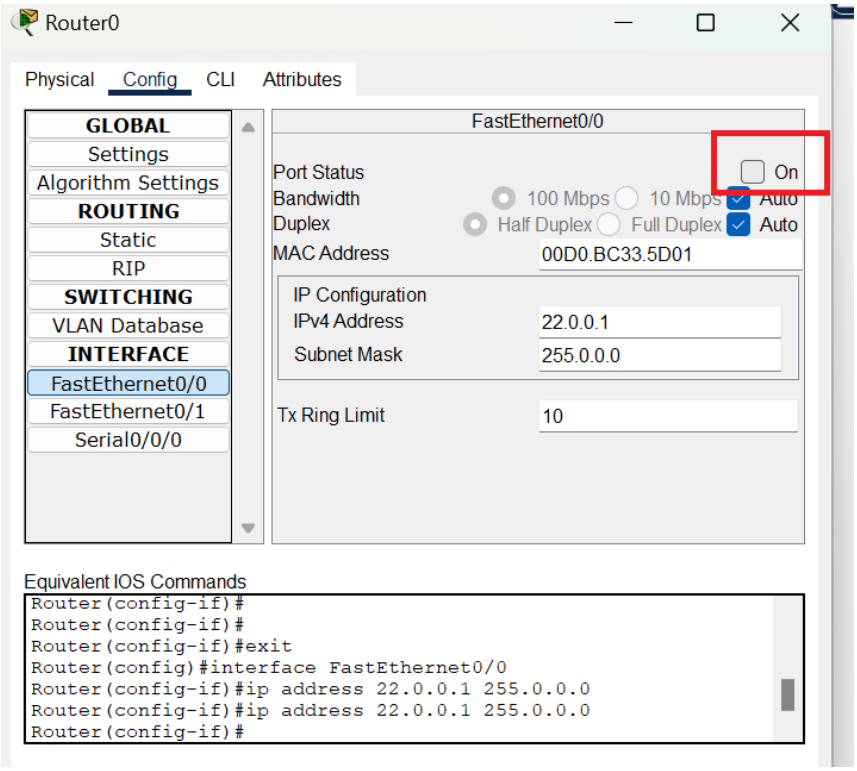
7.) To connect the router, click on them; select "Physical" option from the top ribbon then turn off the router from the button given in picture, then select "WIC-2T" and drag it to the empty slots in the router, then turn on the Router. Repeat the process for the second and third router.



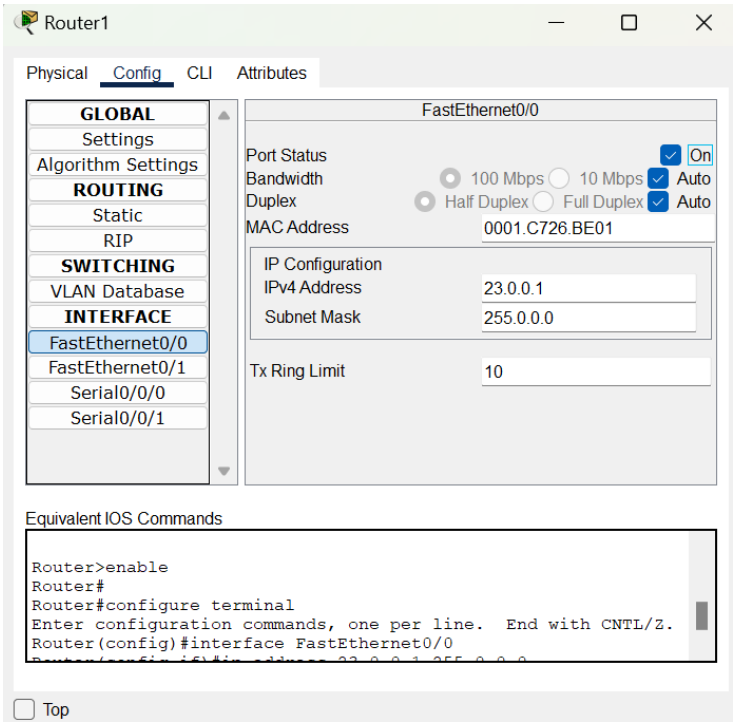
7.) Select “Serial DCE” wire from the Connections to connect the routers. Click on one router and select Serial port and then click on other router and select Serial port.



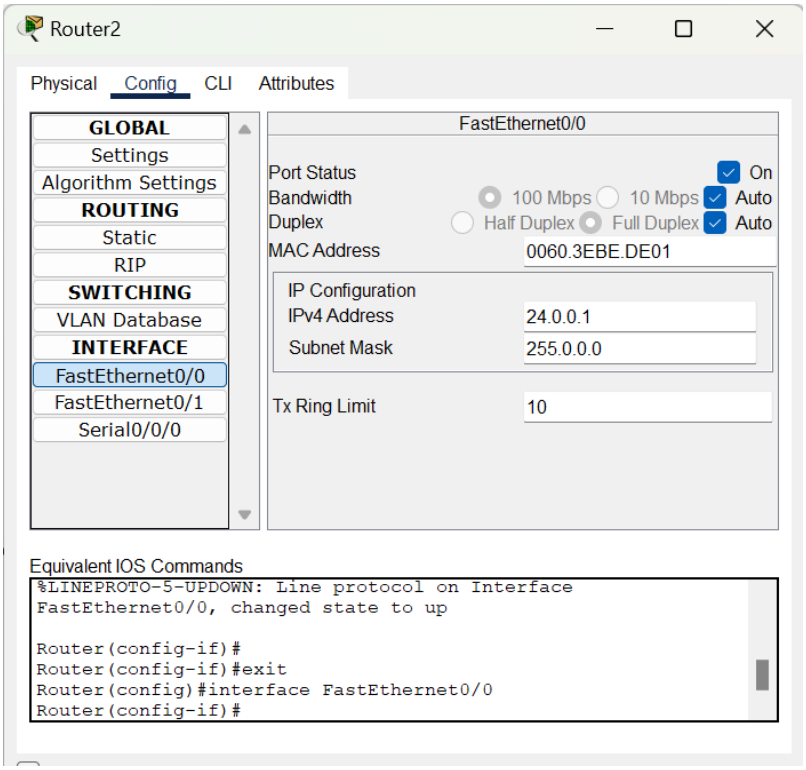
8.) Go to Config of Router0,then click on FastEthernet0/0 and write ipv4 address as 22.0.0.1 then click on "On" to assign the IP address to the connected devices with default gateway as Router0 with IP address 22.0.0.1



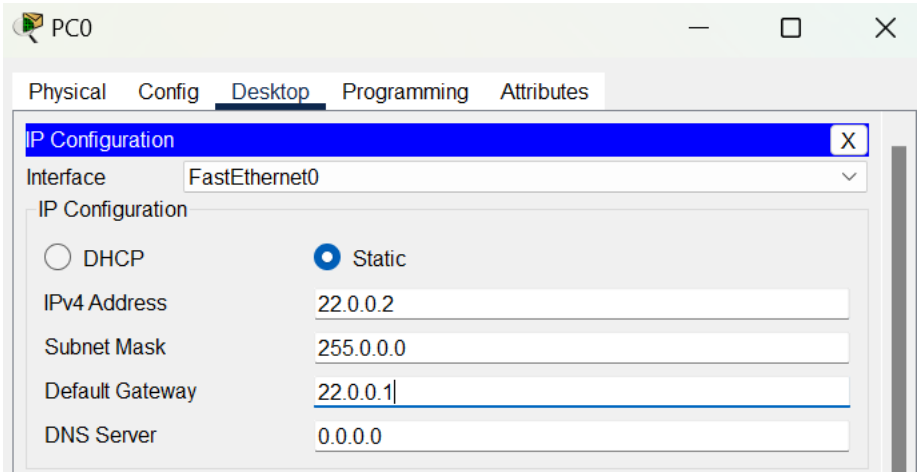
Repeat the process for Router1 and assign the IP address to the connected devices with default gateway as Router1 with IP address 23.0.0.1



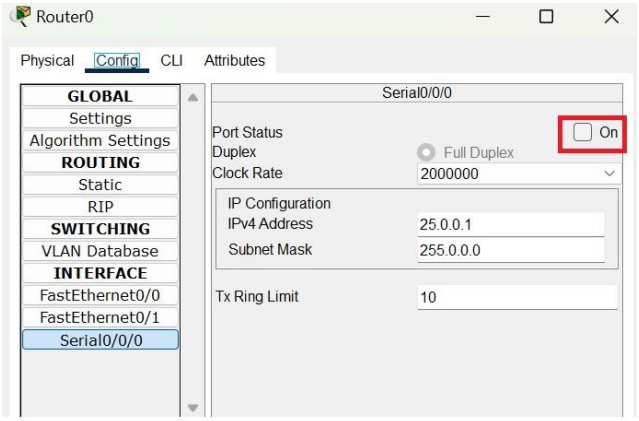
Repeat the process for Router2 and assign the IP address to the connected devices with default gateway as Router3 with IP address 24.0.0.1.



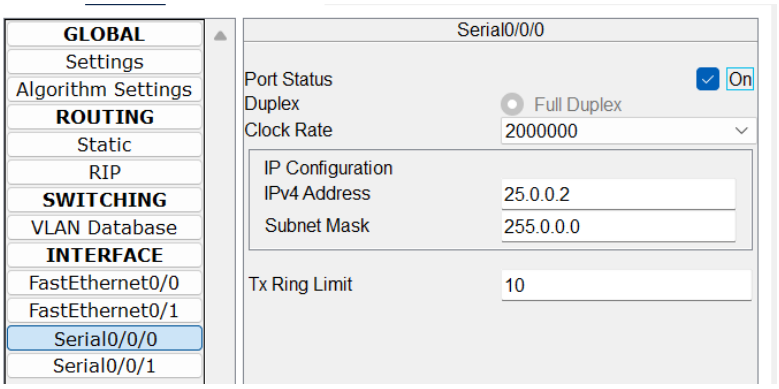
9).Go to every PC's Desktop, click IP configuration and select static to assign the IP address statically and type ip address of router in default gateway column of pc. Repeat this step for all PC's.



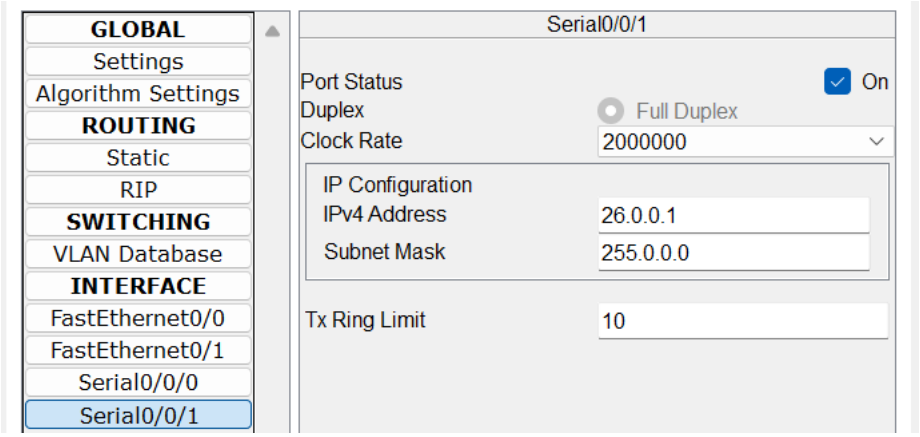
10).Now, to connect the two routers with each other. Go to Router0,then click on config and then on serial0/0/0,then type the ip address as 25.0.0.1 and click on "On" button in order to assign the IP address to the Router0 which is going to connect to Router1 via the interface Serial0/0/0.



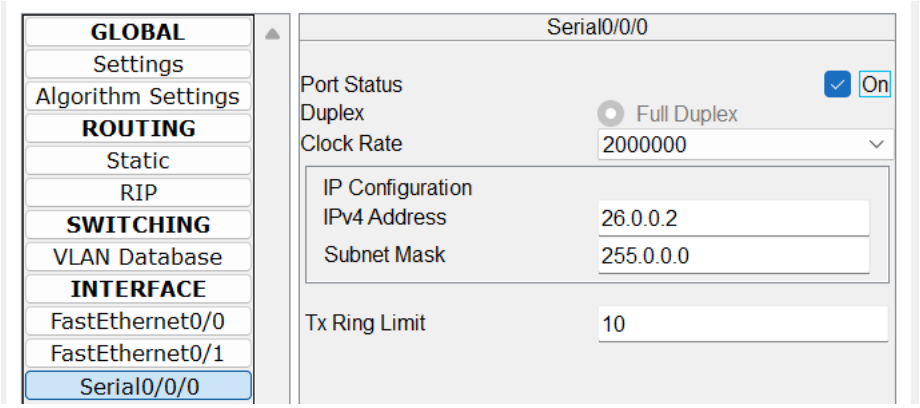
Similarly, Go to Router1 to perform the same operation in order to connect Router1 to Router0. Assign 25.0.0.2 address to Router1.



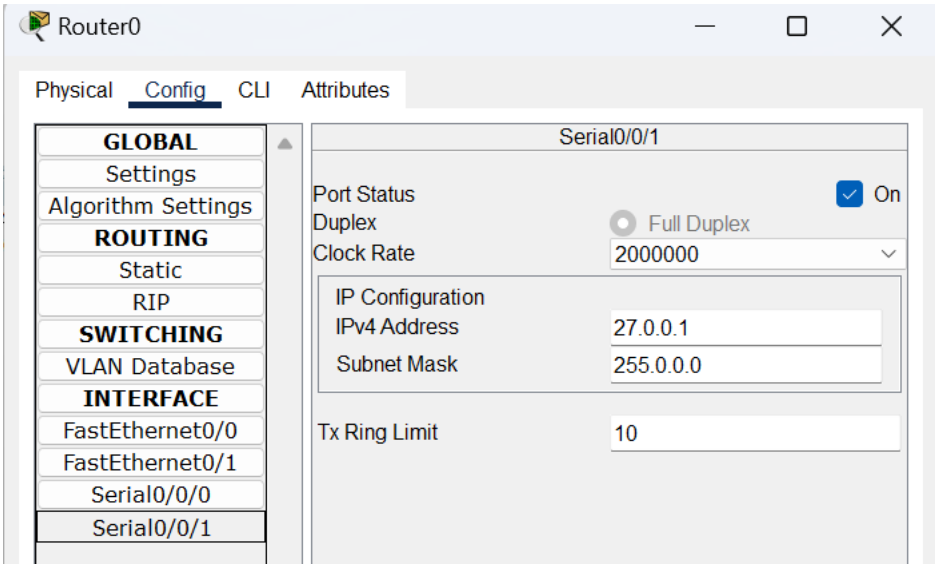
Now, To Connect Router1 with Router2, go to router 1 and assign IP address of 26.0.0.1.



Similarly, Go to Router2 and assign IP address of 26.0.0.2.



Now, To connect router 0 and router 2,go to router 0 and click on serial0/0/1 then assign ip address of 27.0.0.1.



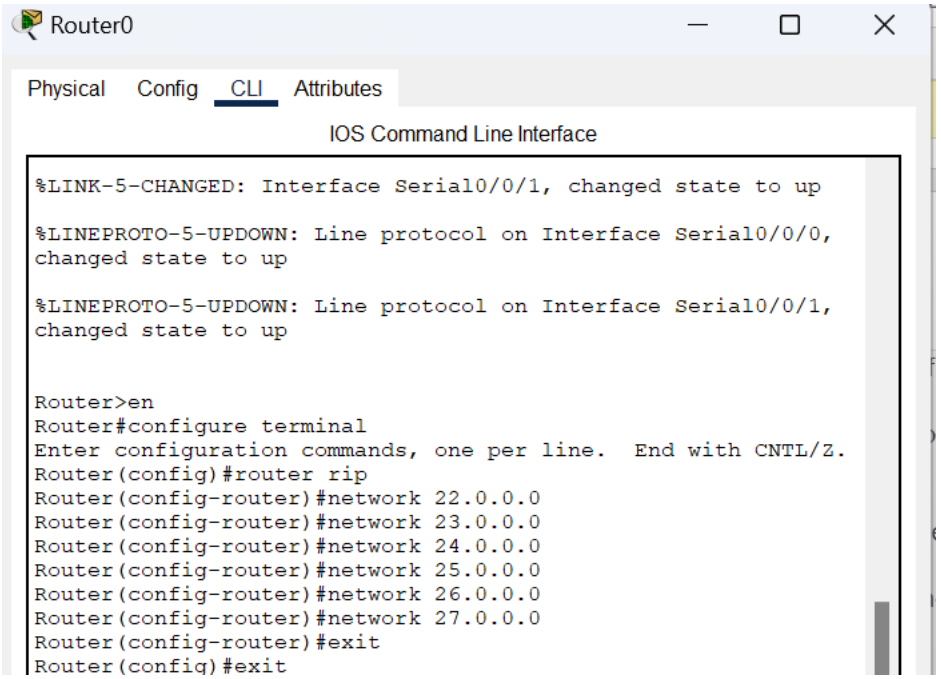
Similarly ,go to router 0 and click on serial0/0/1 then assign ip address of 27.0.0.2

11) After configuring all of the devices we need to assing the routes to the routers.

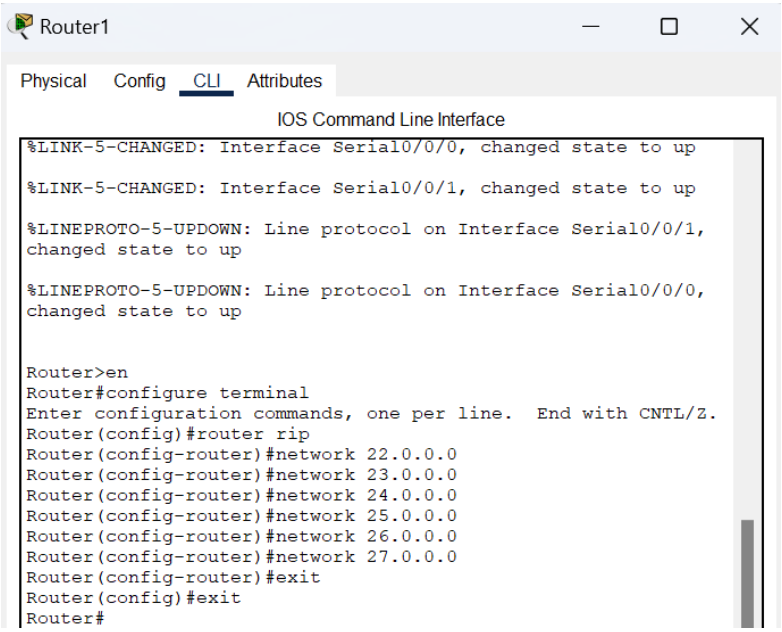
To assign Rip routes to particular router :

- Click on the router that you want to configure and click on the CLI tab at the bottom of the window.
- Type "enable" to enter privileged mode and then type "configure terminal" to enter global configuration mode.
- Type "router rip" to enter the RIP configuration mode.
- Type "network <network-address>" to enable RIP on the interface connected to the specified network. Repeat this step for each interface that you want to enable RIP on.
- Type "exit" to exit the RIP configuration mode and return to the global configuration mode.
- Type "exit" again to return to privileged mode.
- Type "copy running-config startup-config" to save the configuration.

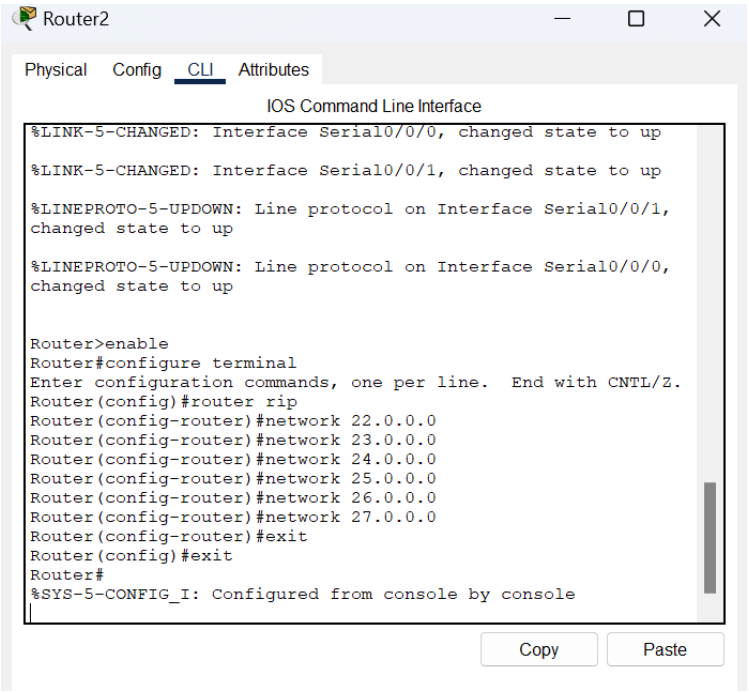
Go to cli of router1 and type these command to add routes to router 1



Repeat the process for Router1.



Repeat the process for Router2.



12).To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

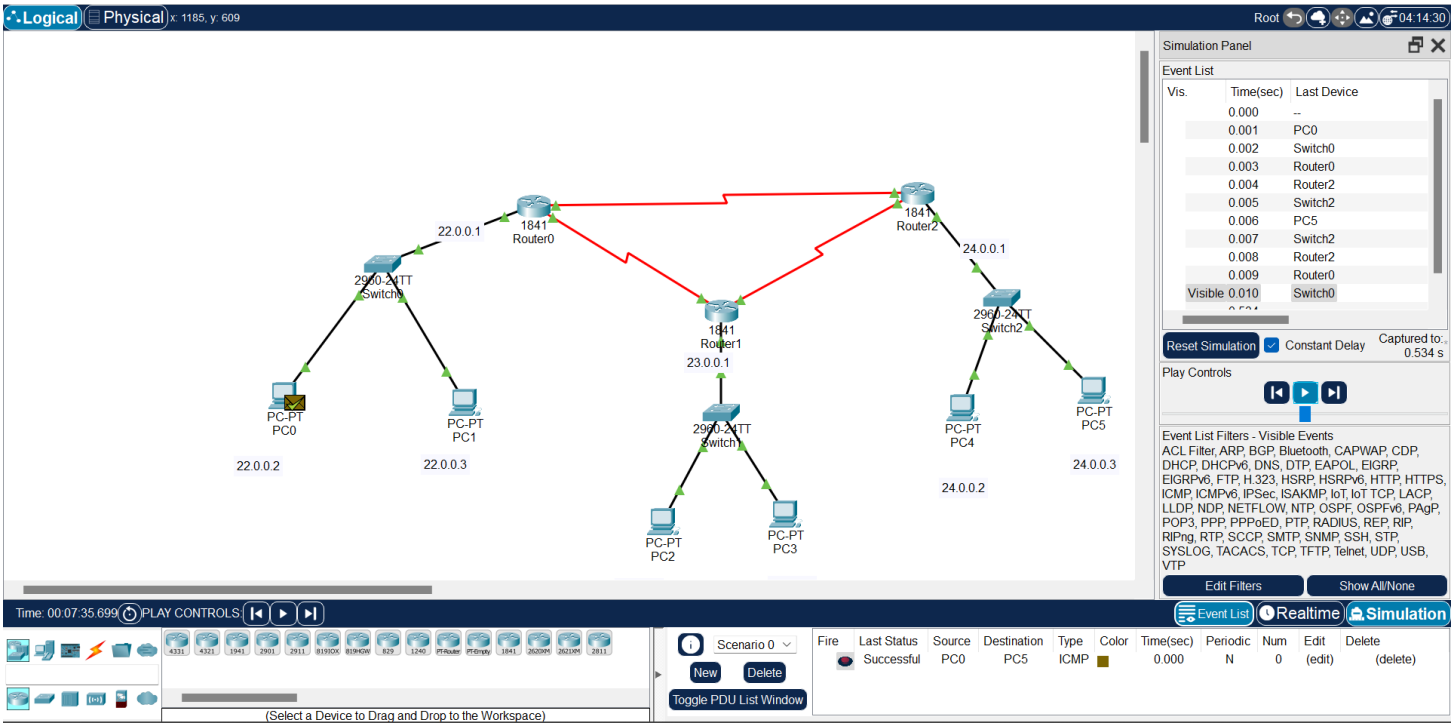
```
C:\>ping 24.0.0.3

Pinging 24.0.0.3 with 32 bytes of data:

Reply from 24.0.0.3: bytes=32 time=23ms TTL=126
Reply from 24.0.0.3: bytes=32 time=11ms TTL=126
Reply from 24.0.0.3: bytes=32 time=3ms TTL=126
Reply from 24.0.0.3: bytes=32 time=1ms TTL=126

Ping statistics for 24.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 23ms, Average = 9ms

C:\>
```

Top

13).For tracing the routes taken by packets to reach from one pc to another . Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “tracert *IP address of any other computer*” (*excluded). Then it will display the path taken by the packets from the source device to the destination ,including the ip addresses of each hop and the time it takes for the packet to reach each hop.

```
C:\>tracert 24.0.0.3

Tracing route to 24.0.0.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      22.0.0.1
  2    0 ms      5 ms      1 ms      27.0.0.2
  3    0 ms      0 ms      1 ms      24.0.0.3

Trace complete.
```

14.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



PRACTICAL-7

Explore the working of netstat, ping and traceroute command. Debugging the network to find down links.

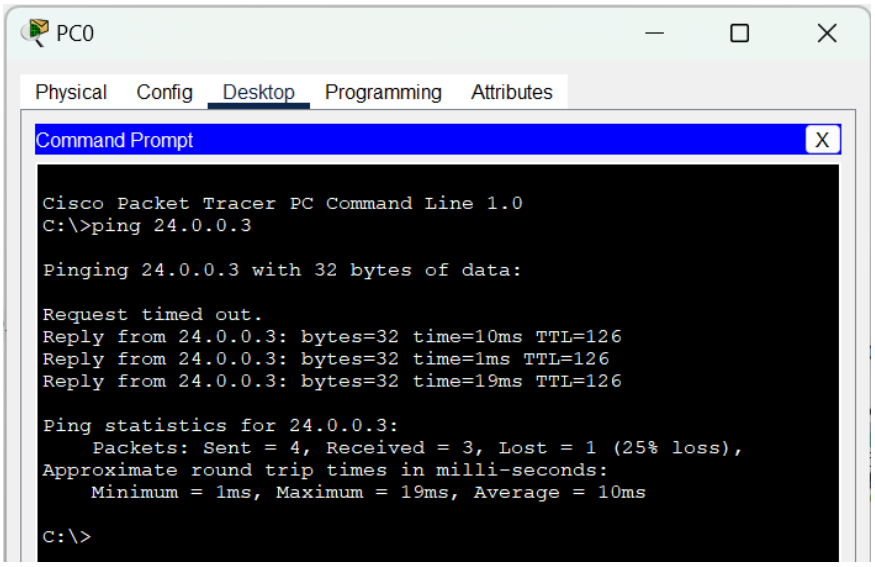
I. PING:

Ping uses ICMP (Internet Control Message Protocol) Echo messages to see if a remote host is active or inactive, how long a round trip message takes to reach the target host and return, and any packet loss. It sends a request and waits for a reply (which it receives if the destination responds back within the timeout period).It's basically a quick, easy way to verify that you can reach a destination on the internet.

To use the ping command in Packet Tracer, follow these steps:

- Open the command prompt or terminal.
- Type the ping command followed by the destination host or IP address.
- Press Enter to run the command.
- Review the output to see the response time, packet loss, and other statistics.

Lets use this command on practical 6 network .After using this command we get the output as given below :



II. TRACEROUTE:

Traceroute is one of the most common utilities built into most operating systems. It is useful for diagnosing network connections. It shows the path of a packet going from your host/computer through each of the individual routes that handle the packet and time required for it to go from one router to another up to the final host/destination.

How it works

When you start the traceroute command, it sends a packet (using the Internet Control Message Protocol or ICMP) with a time limit value (known as the 'time to live' - TTL). The first packet has a TTL of 1, the second packet has a TTL of 2, etc. Increasing TTL in such a manner, it resends the packet so that you can reach the first, the second and other routers on the way to the destination. When a router receives the packet, it sends a Time Exceeded message, which provides an opportunity to determine the time required for the hop to the router. Each time a packet is passed to a new router, the TTL is decreased by 1. When it reaches 0, the packet is discarded, and the router returns an error message.

Traceroute determines that the packet has reached the destination by including a port number that is outside the normal range. When it's reached, the **Port Unreachable** message is sent in return, which defines the time length of the final hop. Traceroute provides you with the information hop by hop. Each hop is determined three times. When a website is unreachable or slow, traceroute allows you to see where the connection fails or has delays.

To use the traceroute command in Packet Tracer, follow these steps:

- Open the command prompt or terminal.
- Type the tracert command followed by the destination host or IP address.
- Press Enter to run the command.
- Review the output to see the route that packets take and the IP addresses of routers along the path.

Lets use this command on practical 6 network .After using this command we get the output as given below :

```
C:\>tracert 24.0.0.3

Tracing route to 24.0.0.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      22.0.0.1
  2    0 ms      0 ms     13 ms      27.0.0.2
  3    1 ms      0 ms      0 ms      24.0.0.3

Trace complete.

C:\>
```

III. NETSTAT:

Netstat (Network Statistics) is a command-line tool used to display and analyze network connections and their corresponding protocols (TCP or UDP), IP addresses, and port numbers. It can be used to diagnose network connectivity issues, monitor network traffic, and identify security issues.

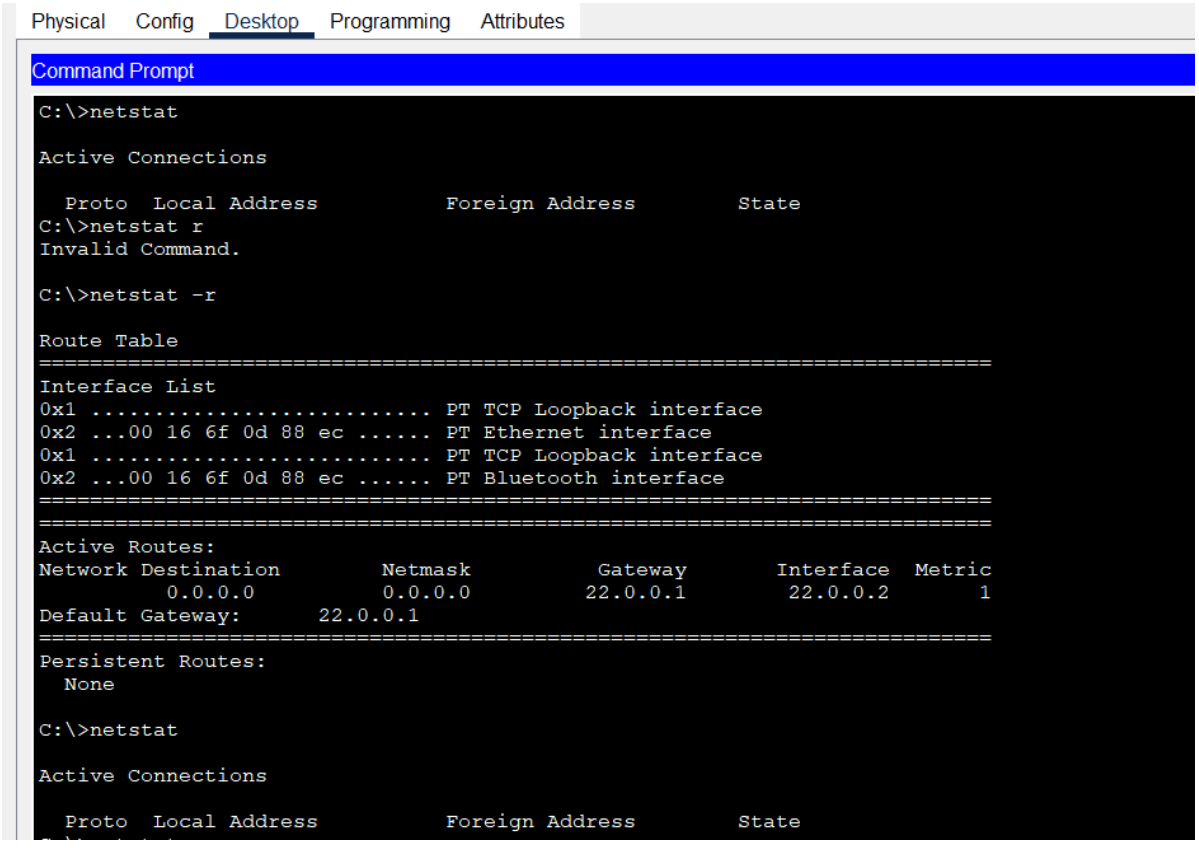
The netstat command can show active connections, listening ports, routing tables, and multicast group memberships. It can also display statistics for each protocol, such as the number of packets sent and received, errors, and discards.

Netstat is available on most operating systems, including Windows, Linux, and macOS. It is a powerful tool for network administrators, developers, and security analysts to troubleshoot network issues and monitor network performance.

To use the netstat command in Packet Tracer, follow these steps:

- Open the command prompt or terminal.
- Type the netstat command followed by any options or arguments you want to use.
- Press Enter to run the command.
- Review the output to see active network connections, protocols, addresses, and ports.

Lets use this command on practical 6 network .After using this command we get the output as given below :



PRACTICAL-8

Establish a VLAN configuration.

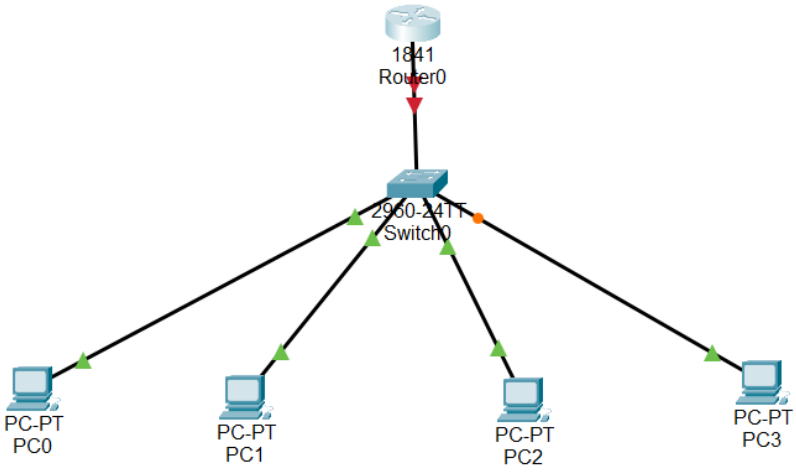
Procedure:-

1.) Open Cisco Packet Tracer.

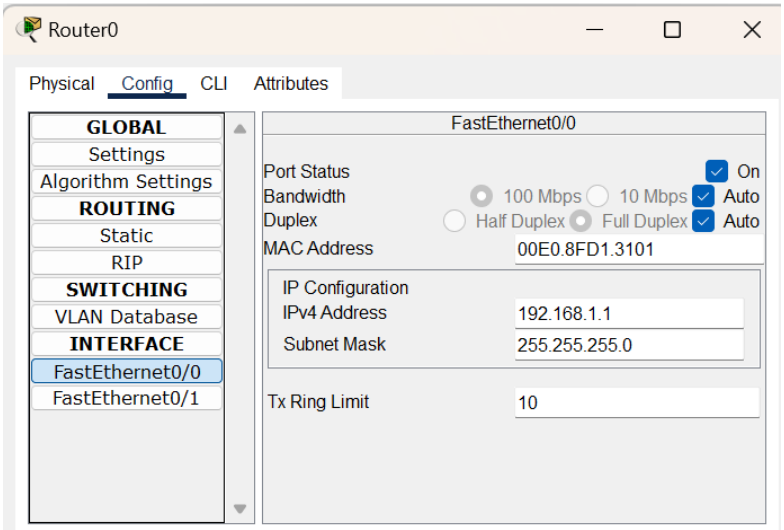
2.) Click on Network devices option from the bottom left corner and select Router among various network devices. Select one "1841" router from the available options .

3.) Click on Network devices option from the bottom left corner and select one “2960” switch.

4.) Click on End Devices and select four PCs from available options. Click on Connections and connect them.

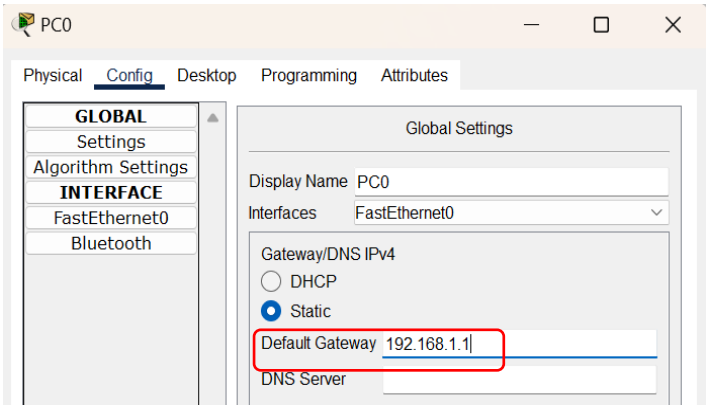


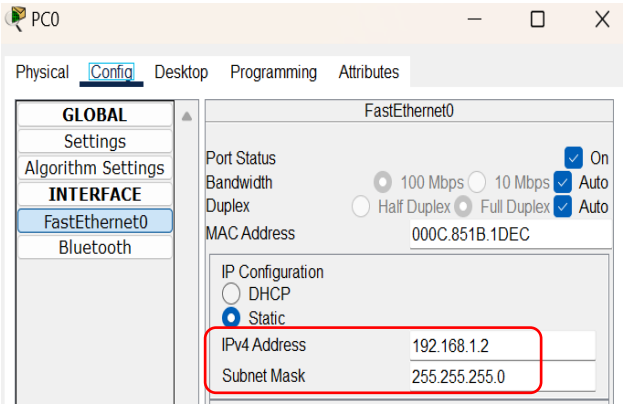
5.) Go to Config of Router0,then click on FastEthernet0/0 and write ipv4 address as 192.168.1.1 then click on "On" to assign the IP address to the connected devices with default gateway of Router0 with IP address 192.168.1.1.



6.) Set the gateway of pc0 and pc1 to 192.168.1.1

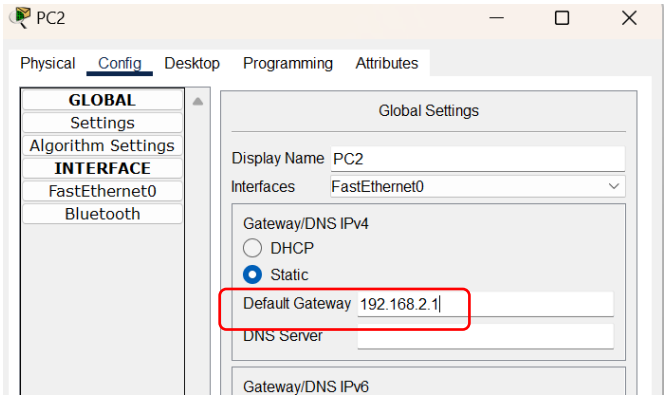
- Set ip of pc0 to 192.168.1.2.
- Set ip of pc1 to 192.168.1.3.

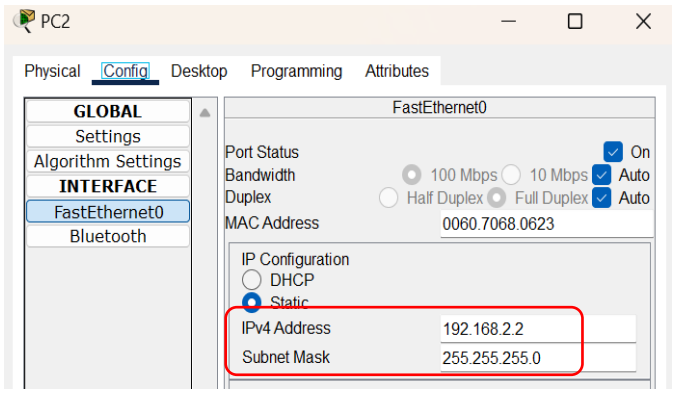




7.) Set the gateway of pc2 and pc3 to 192.168.2.1

- 192.168.2.1 is our VLAN gateway.
- Set ip of pc2 to 192.168.2.2
- Set ip of pc3 to 192.168.2.3

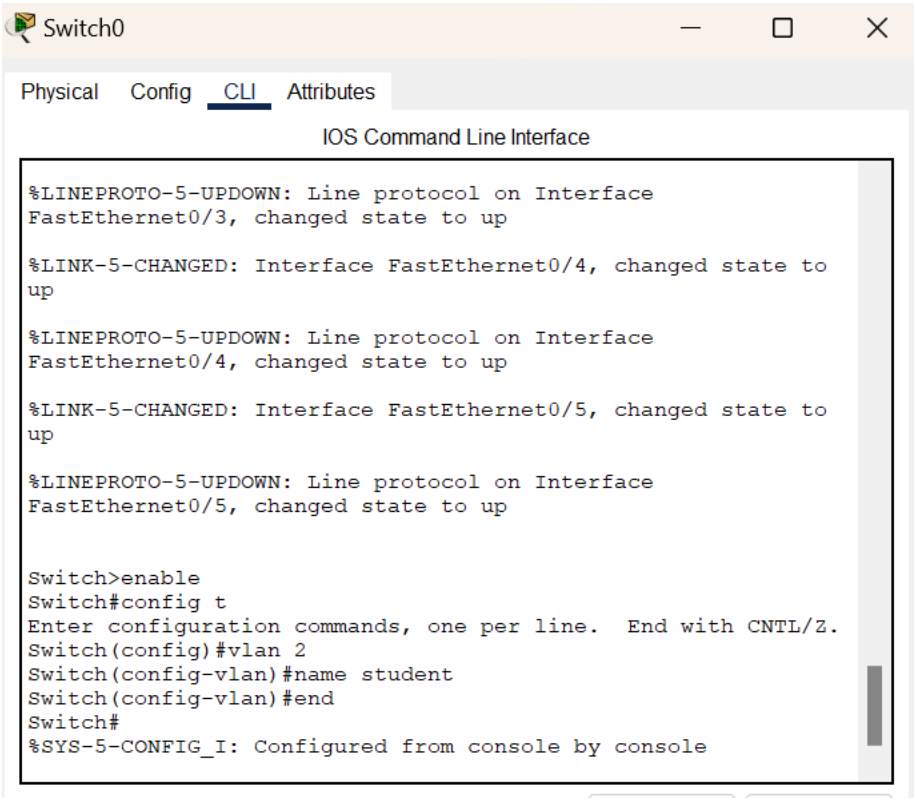




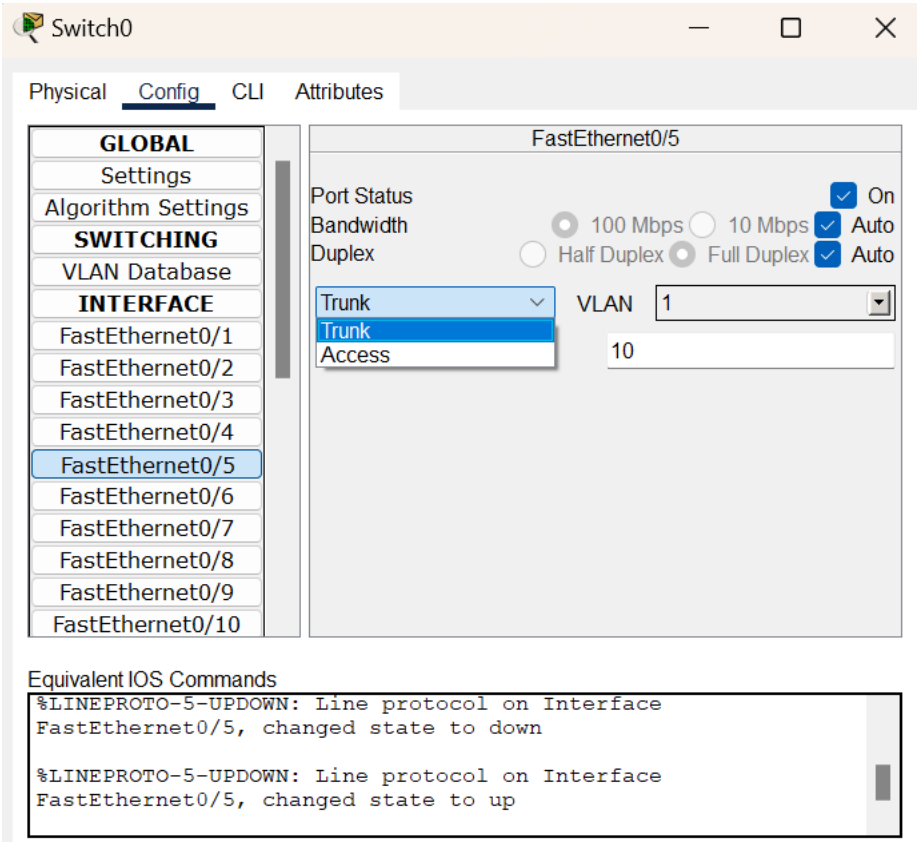
8.) Add {number: 2, name: student } to the VLAN database on the switch.

To add a VLAN to the VLAN database of a Cisco switch using the CLI command in Cisco Packet Tracer, you can follow these steps:

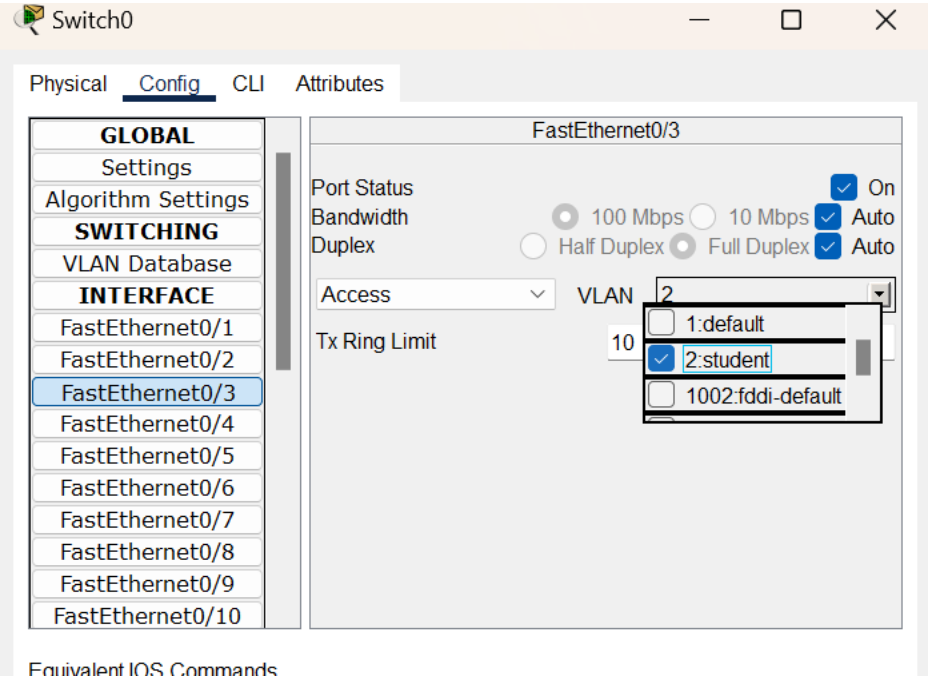
1. Open the CLI console of the switch by clicking on it and then selecting "CLI" from the bottom panel.
2. Enter privileged EXEC mode by typing "enable".
3. Enter global configuration mode by typing "configure terminal".
4. Create the VLAN by typing "vlan <vlan_id>" where <vlan_id> is the number of the VLAN you want to create. For example, to create VLAN 10, type "vlan 10".
5. Assign a name to the VLAN by typing "name <vlan_name>" where <vlan_name> is the name you want to give to the VLAN. For example, to name VLAN 10 as "Sales", type "name Sales".
6. Exit global configuration mode by typing "end".



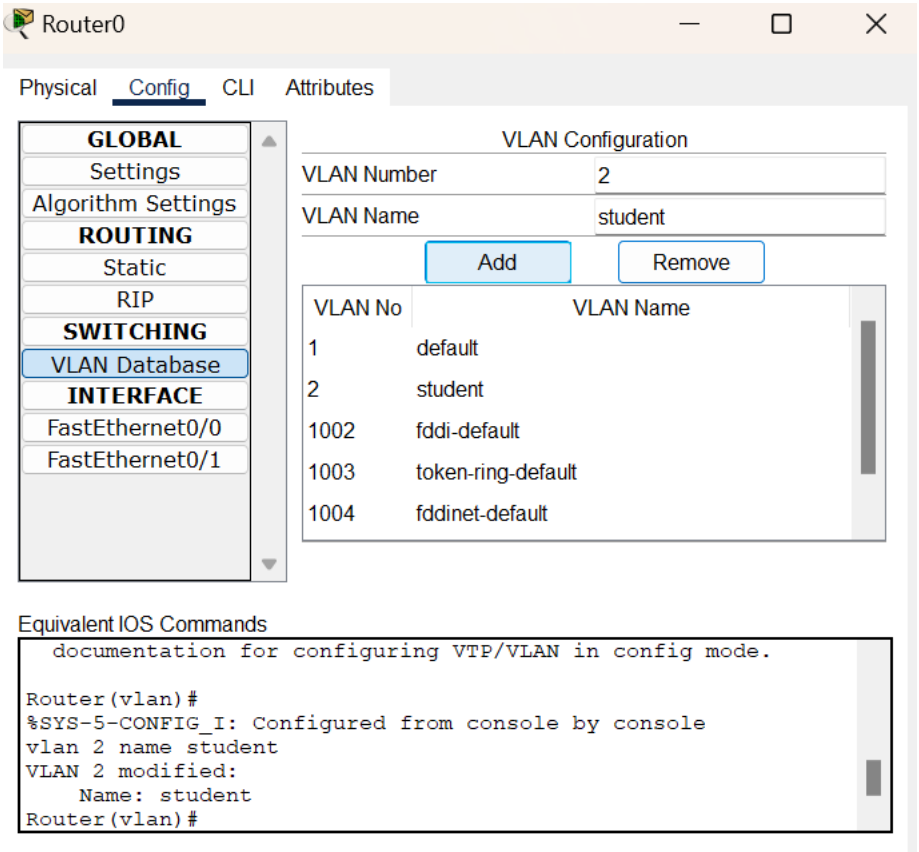
9.) Check the port number of the port connected to the router from the switch and set its type to Trunk.



10.) Change the vlan of ports of the switch connected to pc2 and pc3 to {number: 2, name: student }.

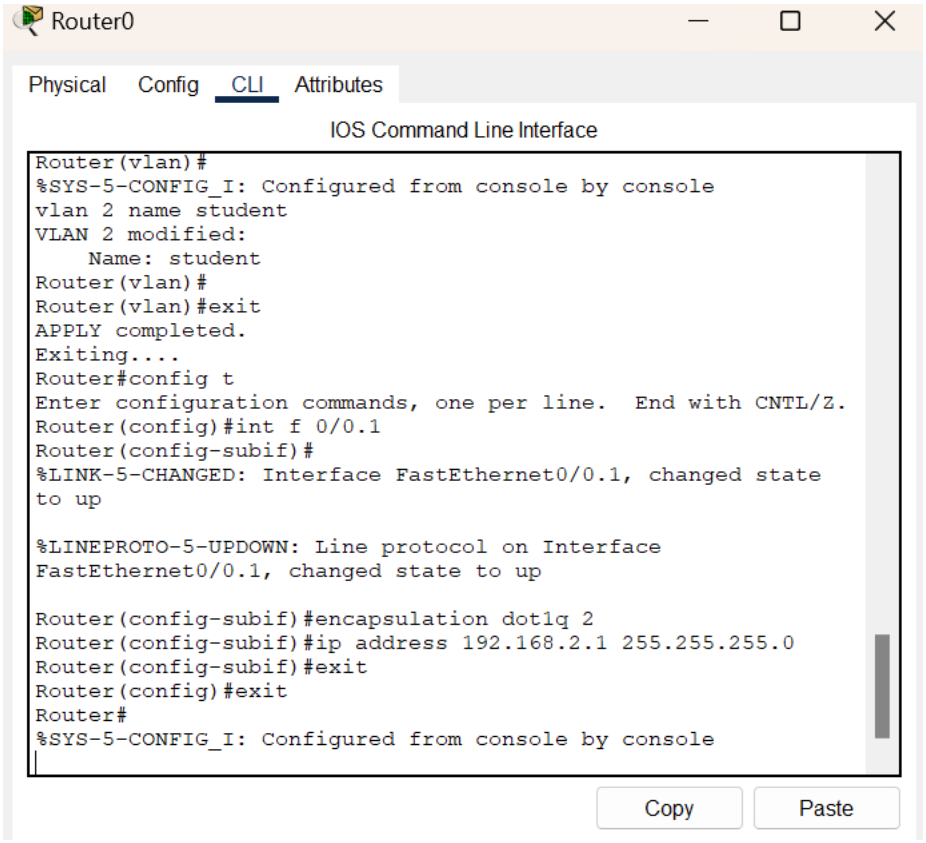


11.) Add {number: 20, name: student } to the VLAN database on the router.

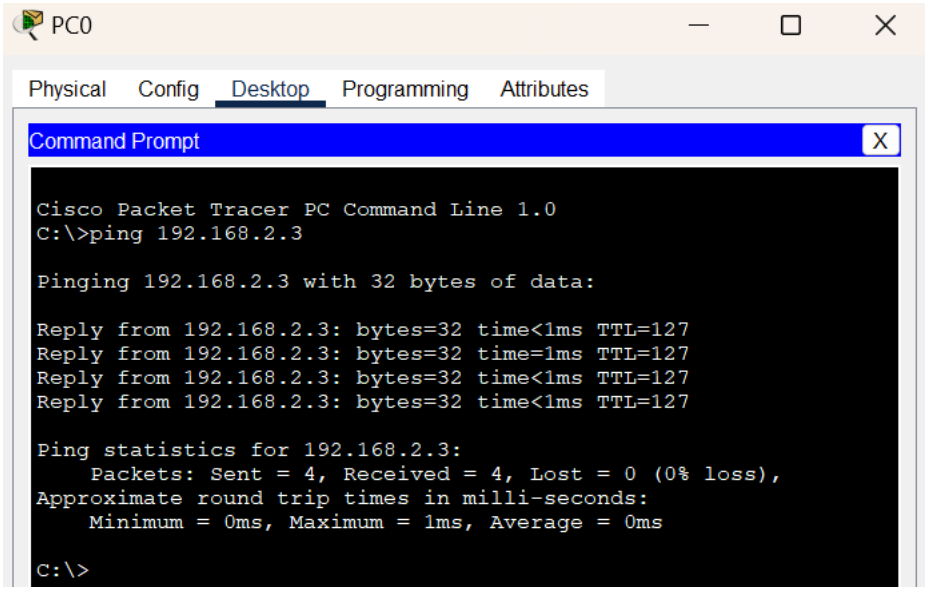


12.) Go to router CLI and run the following commands:

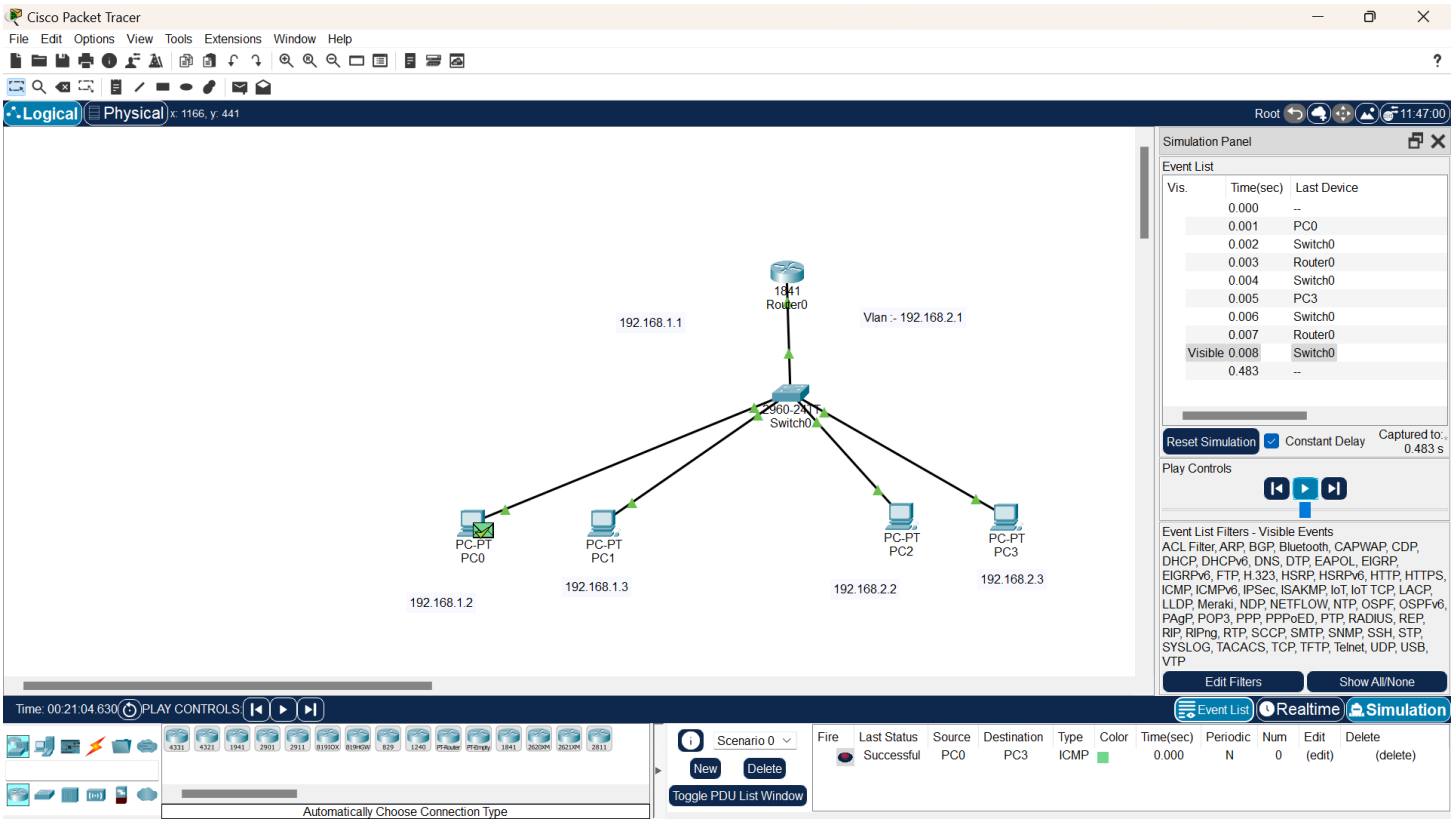
- config t
- int f 0/0
- encapsulation dot1q 2
- ip address 192.168.2.1 255.255.255.0
- exit
- exit



13). To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

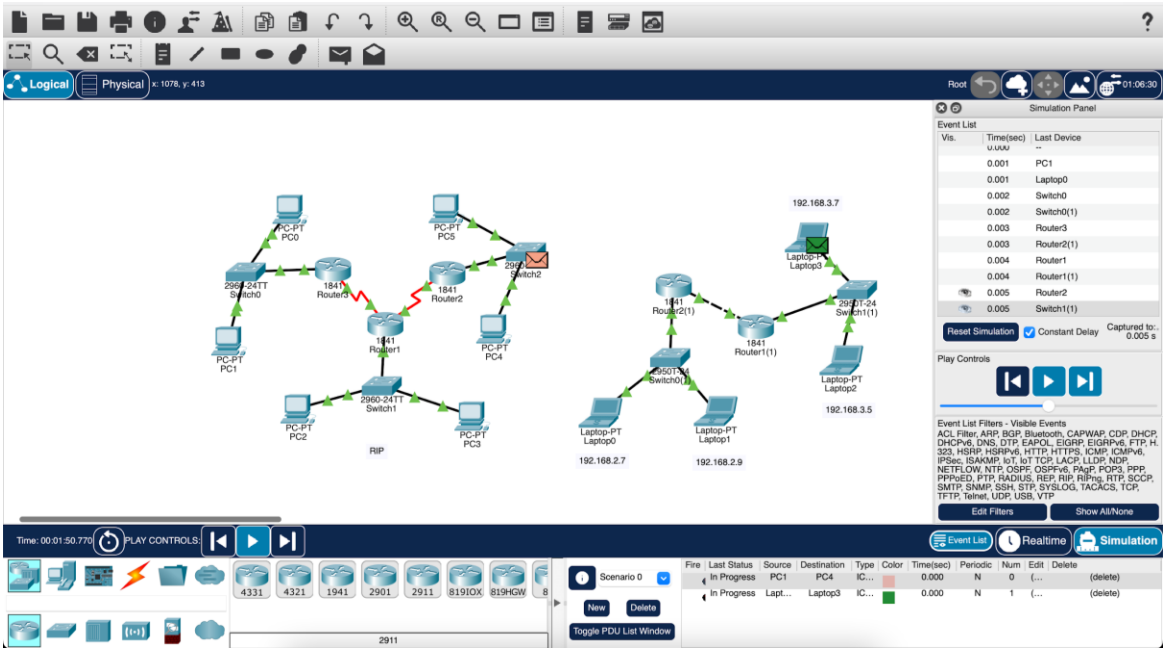


14.) Click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



PRACTICAL-9

Observe the working of IP protocol. Exploring the routing tables for different routers.



Commands

RIP

```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    11.0.0.0/8 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/1] via 10.0.0.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R    192.168.3.0/24 [120/1] via 11.0.0.2, 00:00:25, Serial0/0/1
```

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        192.168.2.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            10.0.0.2        YES manual up                    up
Serial0/0/1            11.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Static

```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S    192.168.3.0/24 [1/0] via 192.168.1.4

Router#
```

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        192.168.2.3     YES manual up                    up
FastEthernet0/1        192.168.1.2     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

PRACTICAL-10

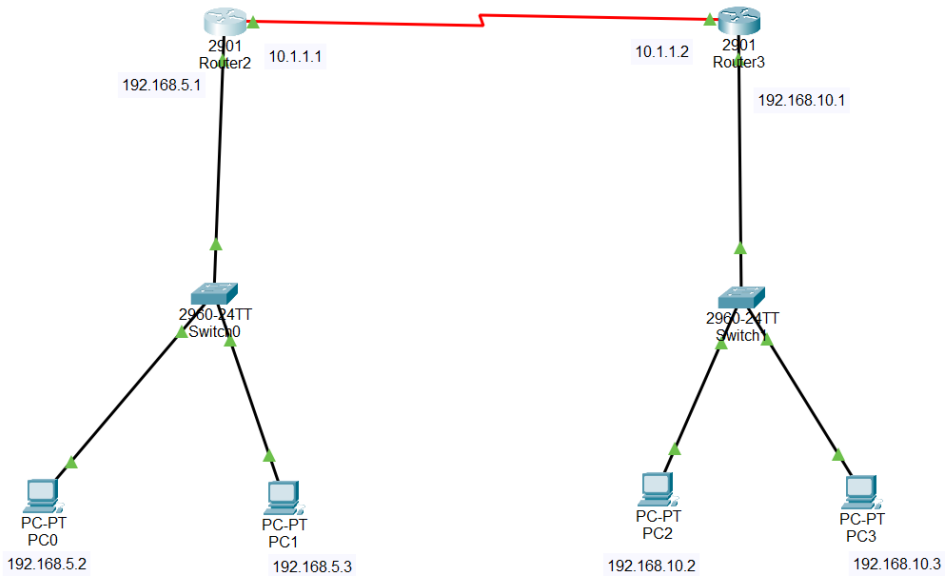
Implement routing protocols:

1.) RIP v1 and RIP v2 protocol

a)RIPv1 Protocol

Procedure :-

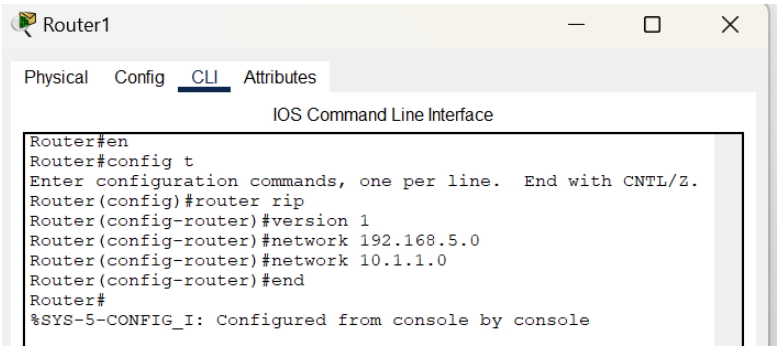
I. open cisco packet tracer and create network configuration as shown below :



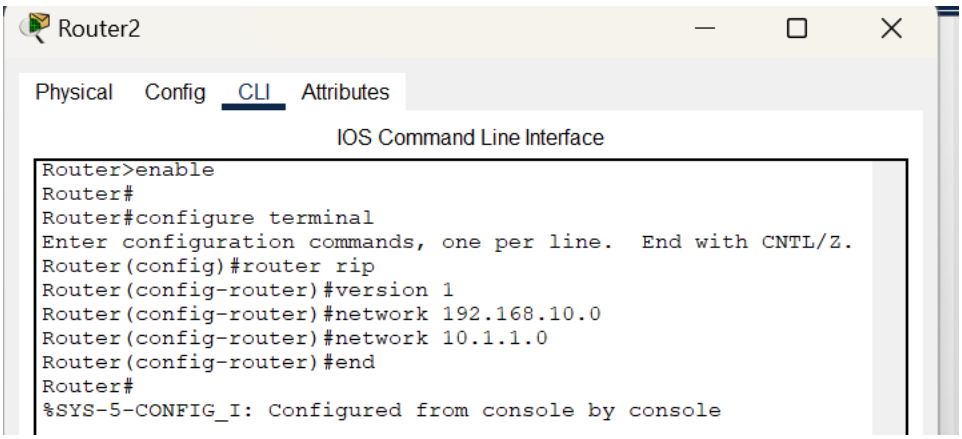
II. Enable RIP v2 on both routers using the following commands in the CLI:

- ✓ Router(config)# router rip
- ✓ Router(config-router)# version 1
- ✓ Router(config-router)# network x.x.x.x

(The "network" command adds the specified networks to the routing process.)

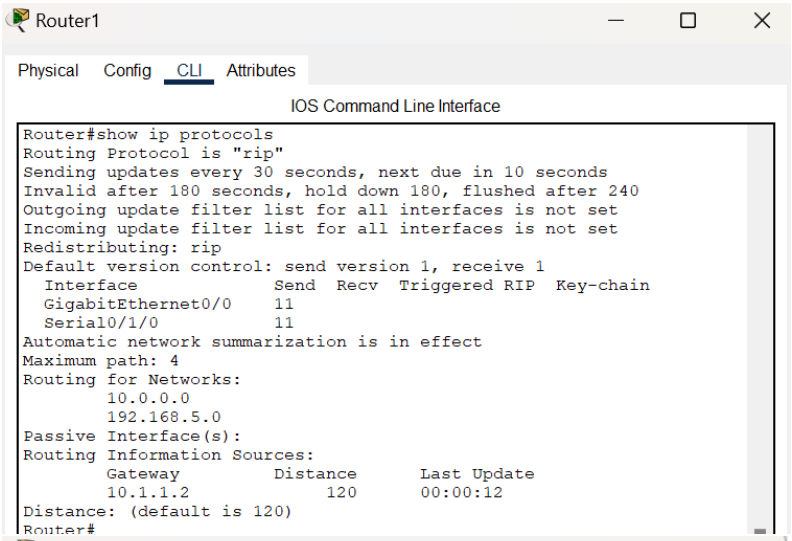


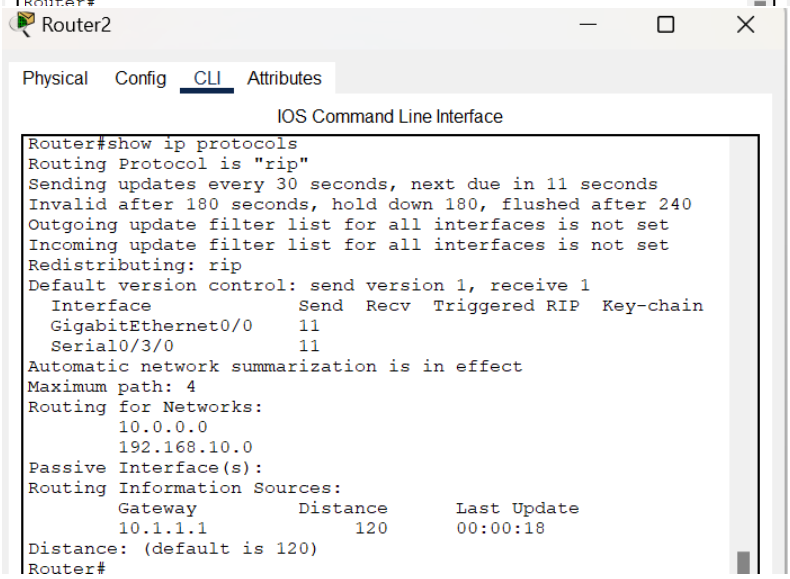
Similary write the above commands in second router



III. Verify that RIP version 1 is enabled on both routers by typing the following command in the CLI:

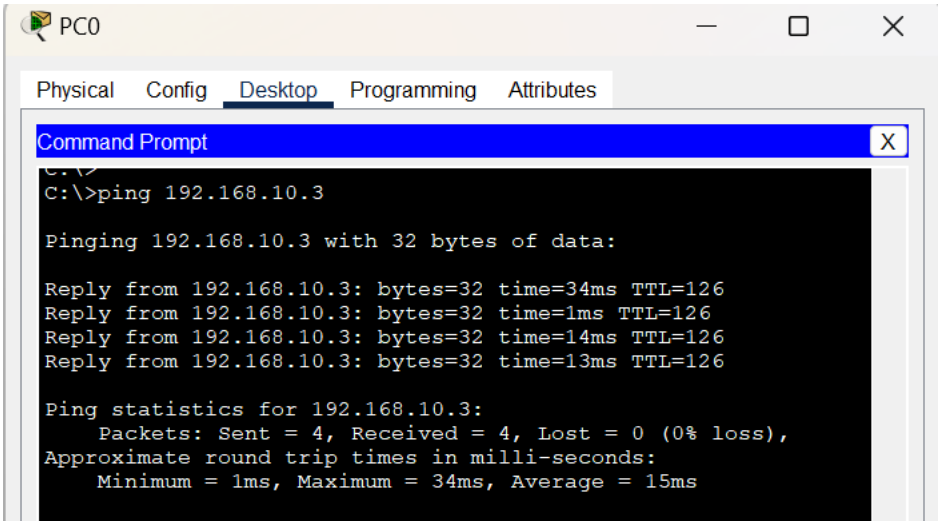
- ✓ show ip protocols



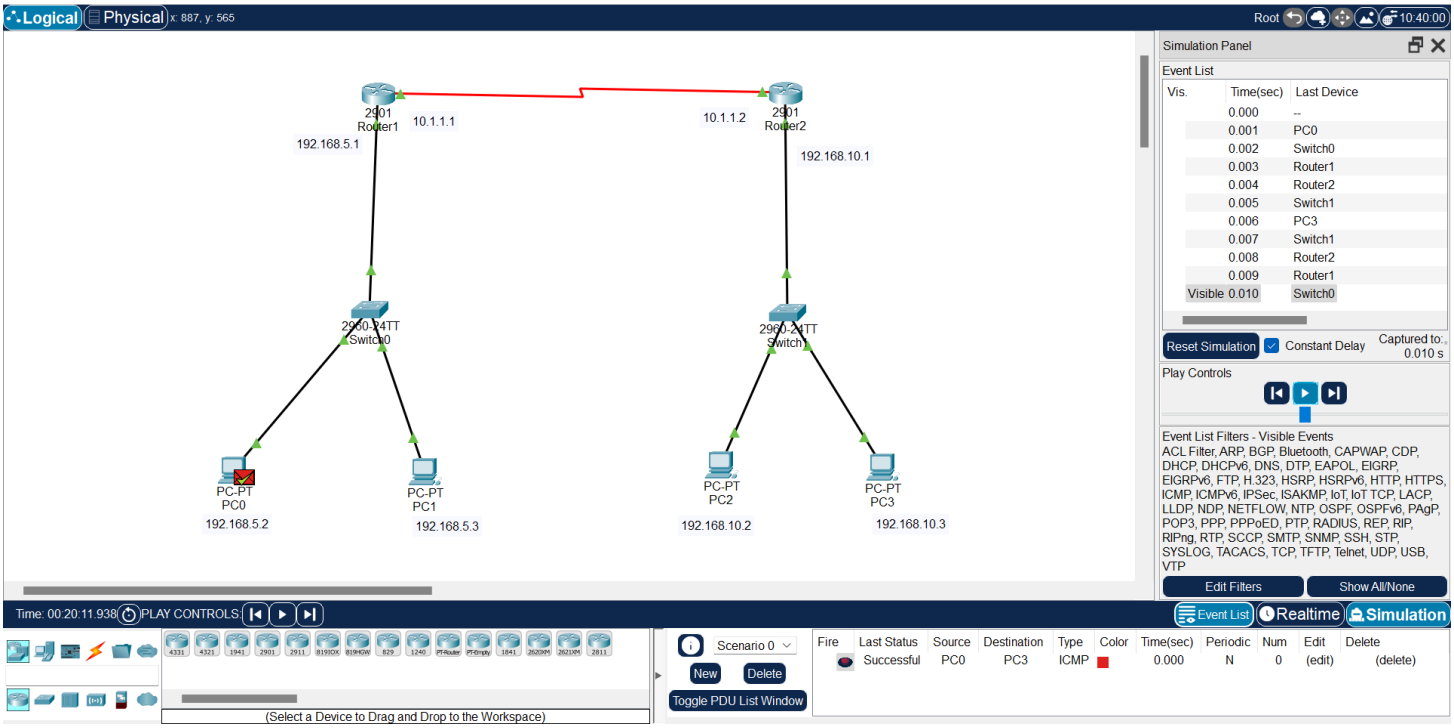


(This command will display the routing protocols currently enabled on the router. You should see send and receive version as 1 .)

IV. To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



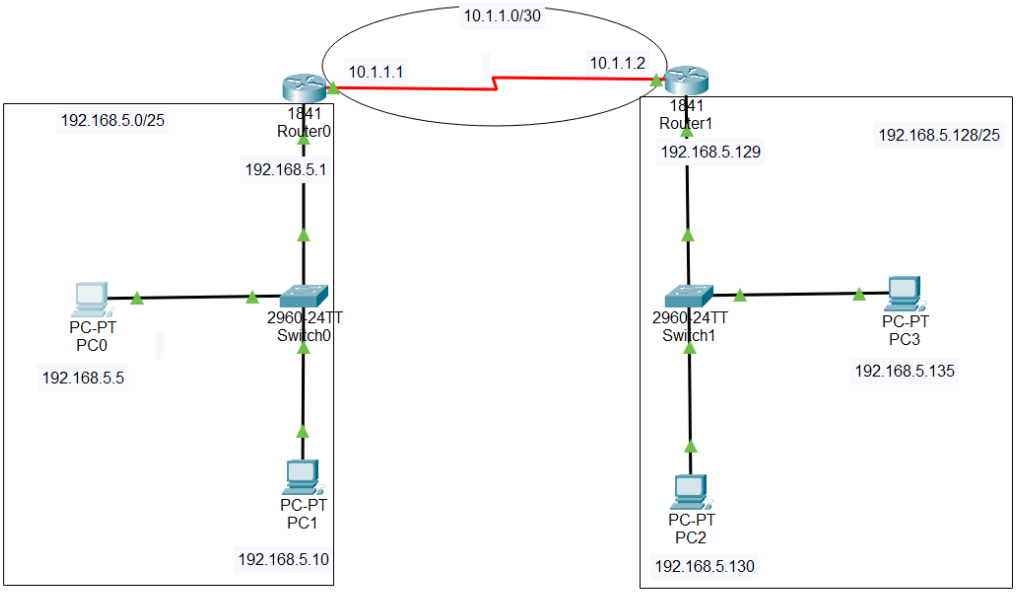
V. Finally to check the connectivity ,click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



b)RIPv2 Protocol

Procedure :-

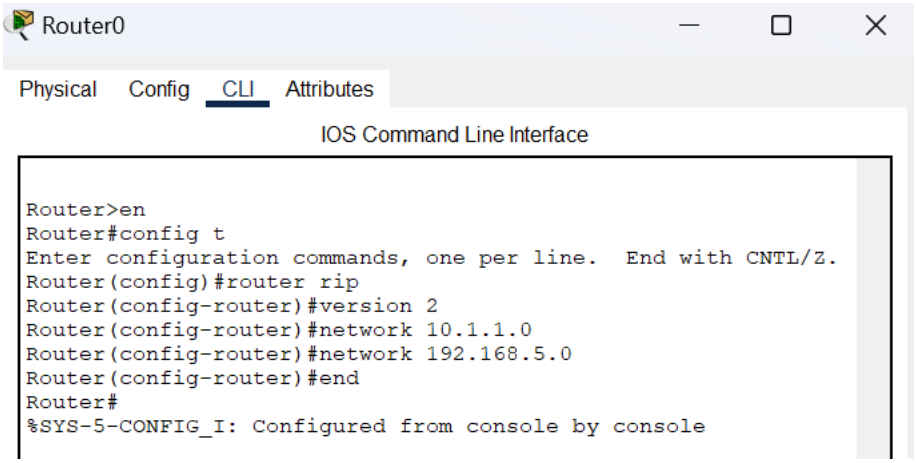
I. open cisco packet tracer and create network configuration as shown below :



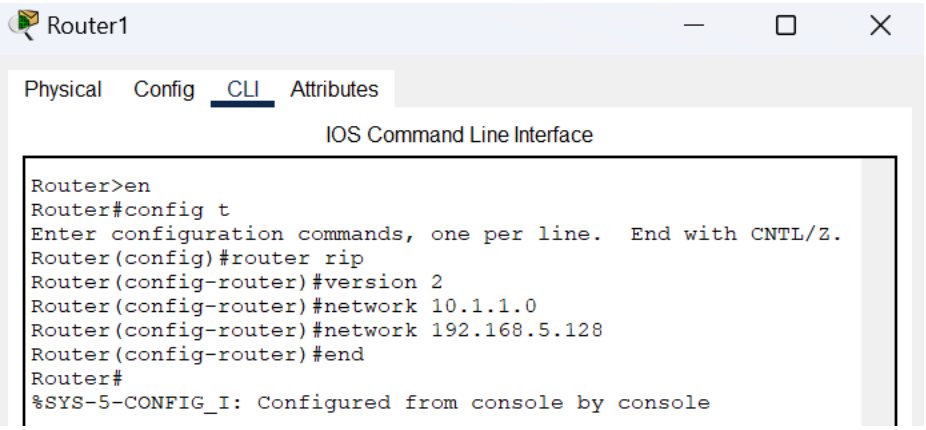
II. Enable RIP v2 on both routers using the following commands in the CLI:

- ✓ Router(config)# router rip
- ✓ Router(config-router)# version 2
- ✓ Router(config-router)# network x.x.x.x

(The "network" command adds the specified networks to the routing process.)

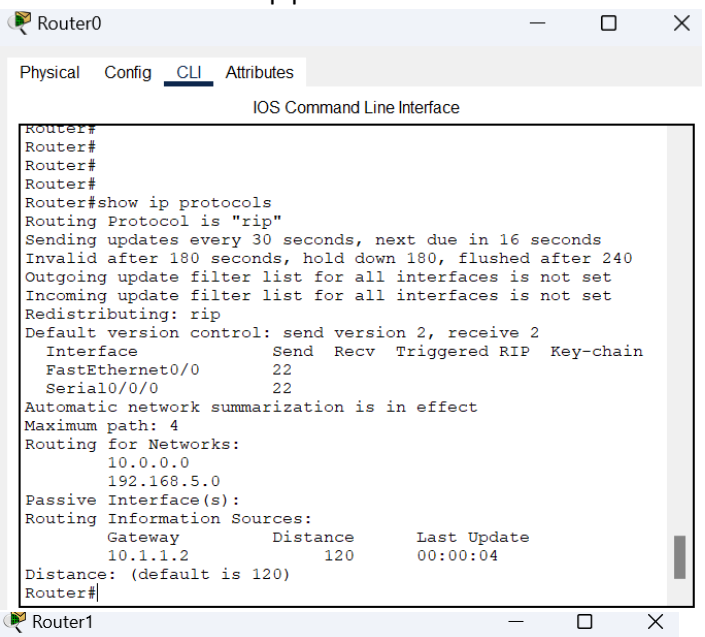


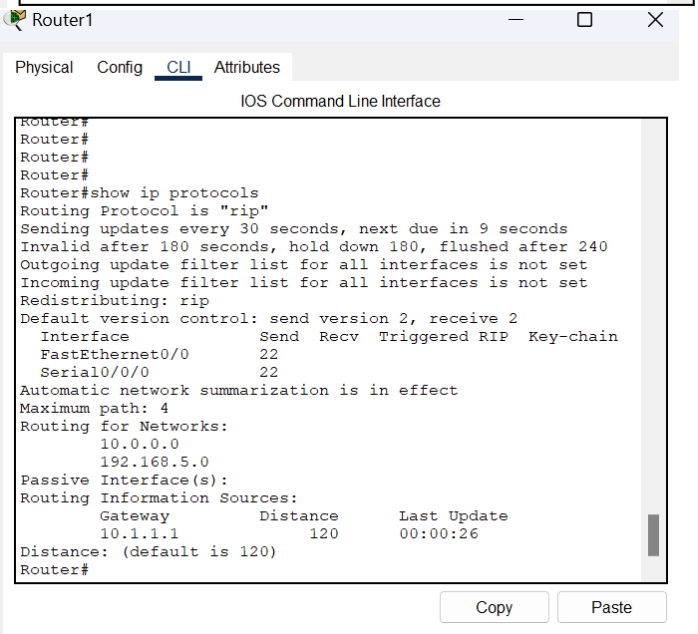
Similary write the above commands in second router



III. Verify that RIP version 2 is enabled on both routers by typing the following command in the CLI:

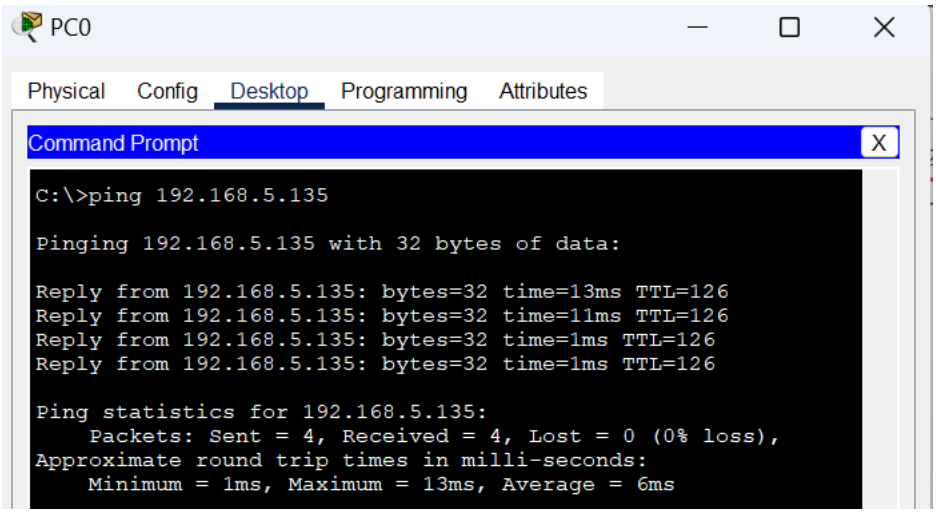
- ✓ show ip protocols





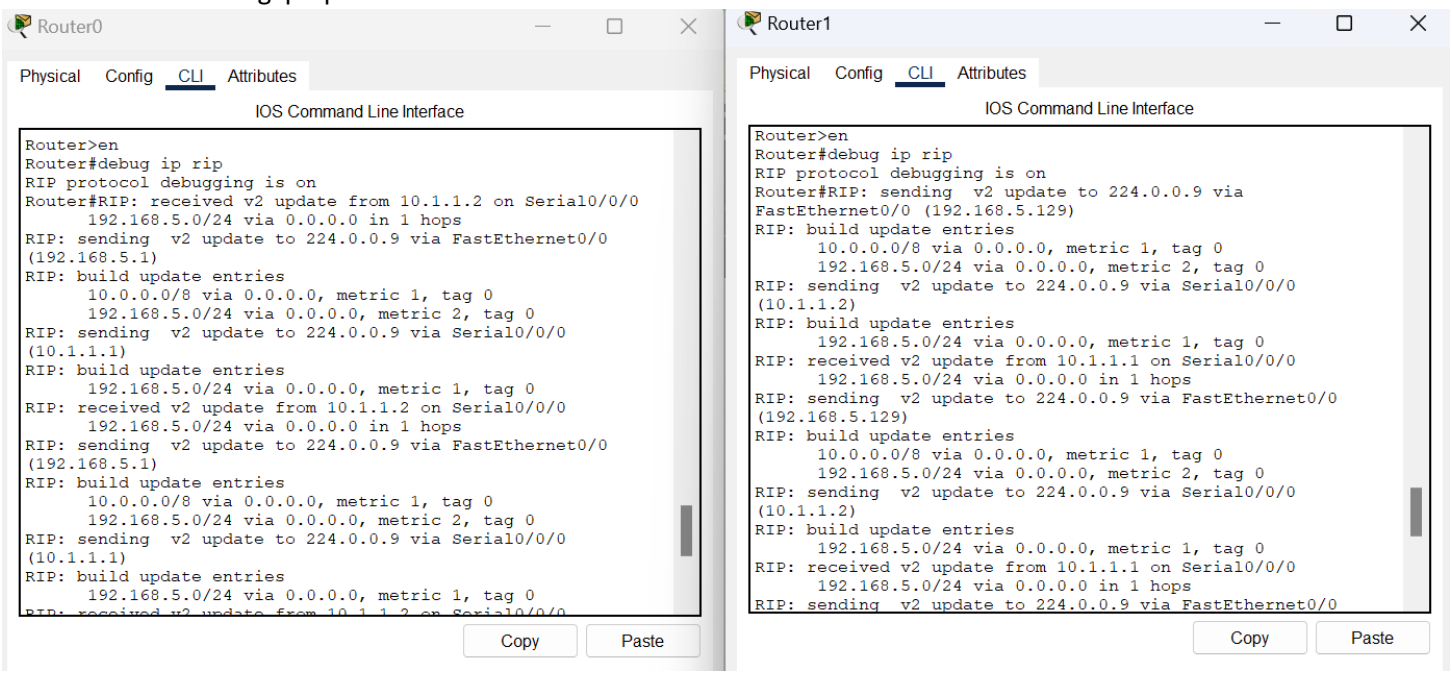
(This command will display the routing protocols currently enabled on the router. You should see RIP v2 listed as one of the routing protocols.)

IV. To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

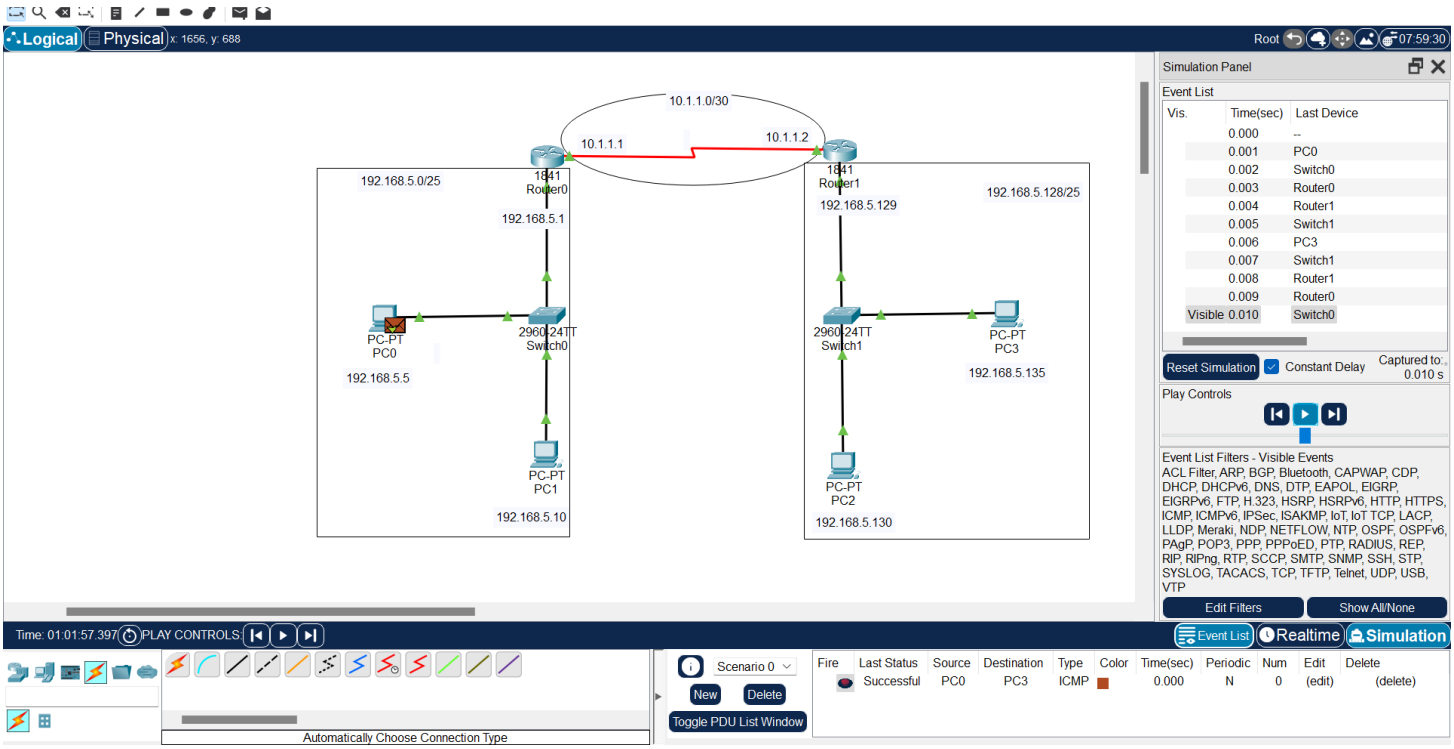


V. To verify that supernets are being sent and received use the following commands

- ✓ Show ip route
- ✓ Debug ip rip



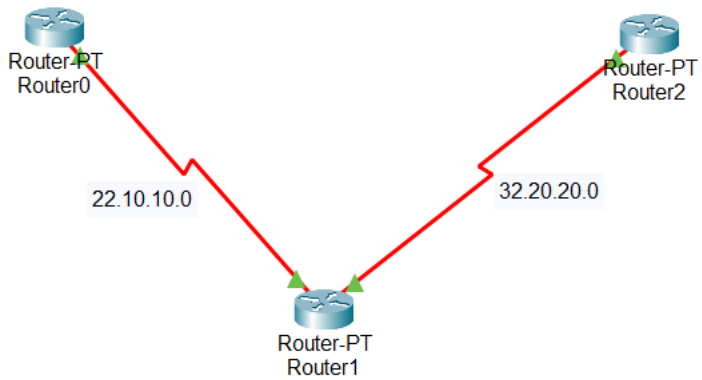
VI. Finally to check the connectivity ,click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



2.) BGP protocol

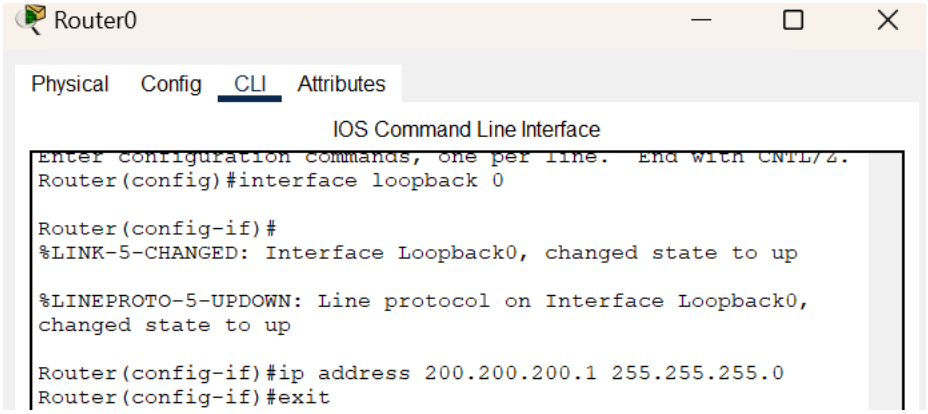
Procedure :-

i. open cisco packet tracer and create a network topology and assign ip addresses to the interfaces of routers as shown below :



ii. Configure loopback interfaces on router0 participating in the BGP networkThis is done using the following commands in globalconfiguration mode:

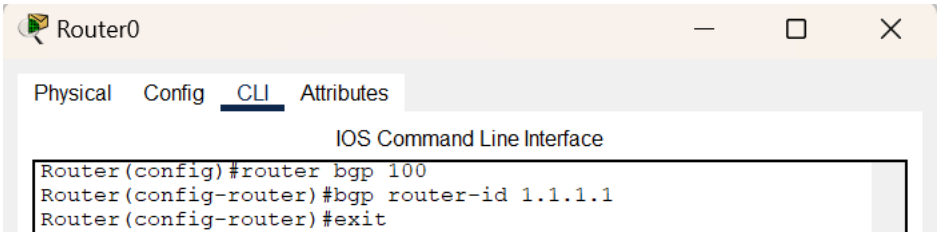
- ✓ Router(config)# interface loopback <interface-number>
- ✓ Router(config-if)# ip address <IP-address> <subnet-mask>



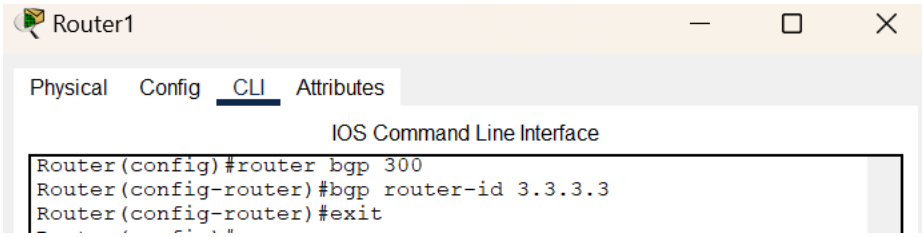
iii. Configure BGP Autonomous system number and router id on each router by using the following commands in the CLI:

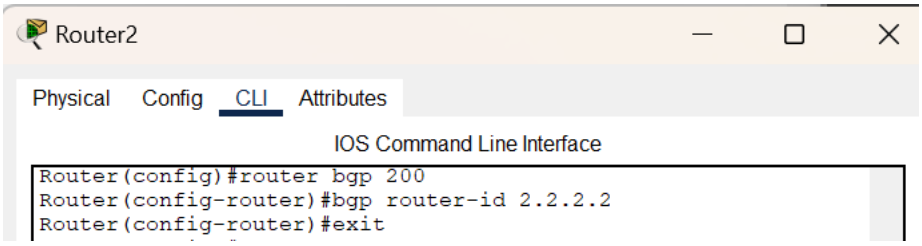
- ✓ Router(config)# router bgp <AS-number>
- ✓ Router(config-router)# bgp router-id <IP-address>

#Replace [AS number] with the BGP autonomous system



Similarly do this for second and third router

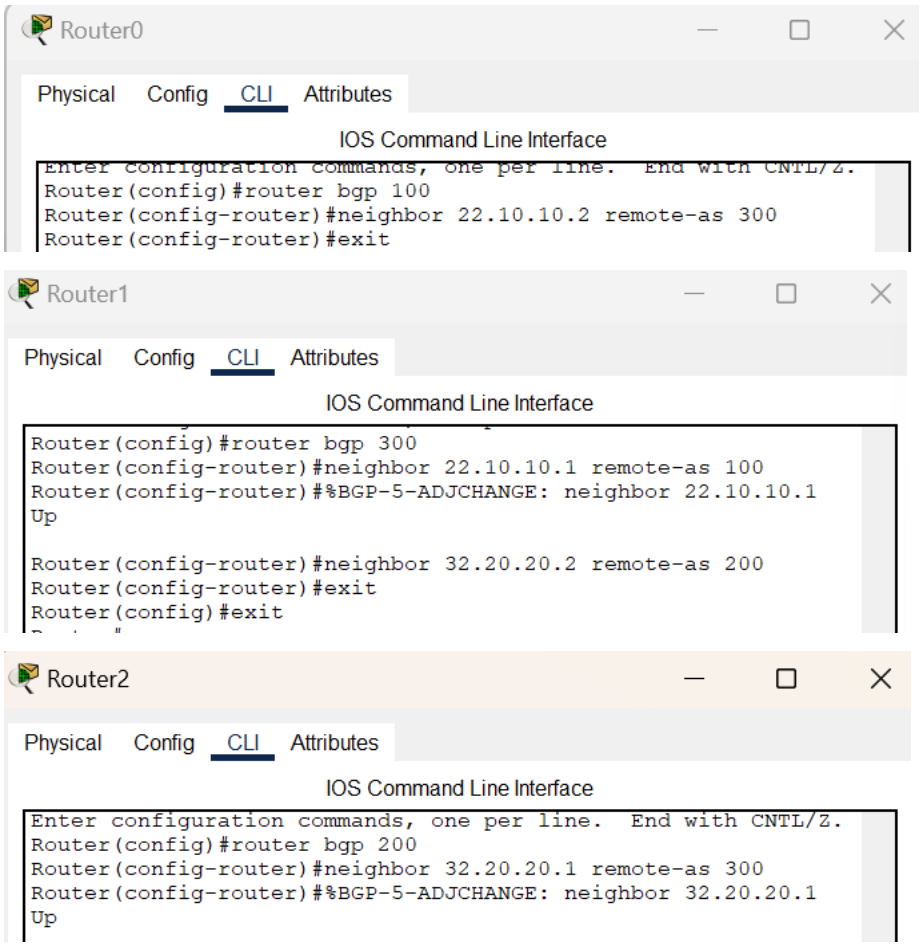




iv. Configure BGP neighbors for each router in the BGP network. This is done using the following command in router configuration mode:

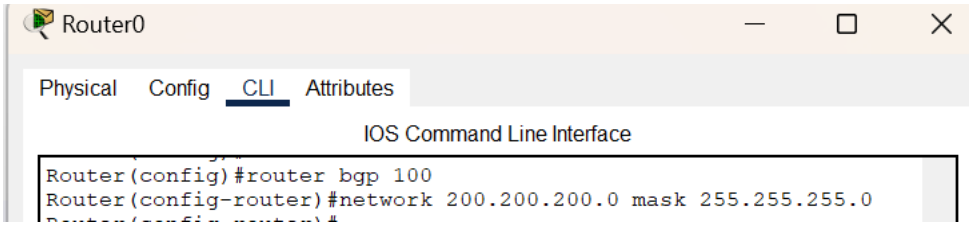
- ✓ Router(config-router)# neighbor <IP-address> remote-as <AS-number>

(Note that the "remote-as" parameter specifies the AS number of the neighbor router.)



v. Configure the router to advertise its own network prefixes to the BGP network. This is done using the following command in router configuration mode:

- ✓ Router(config-router)# network <network-address> mask <subnet-mask>



vi. Verify the BGP configuration by using the following commands in the CLI:

- ✓ Router# show ip bgp

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#show ip bgp
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 200.200.200.0/24  0.0.0.0                  0     0 32768 i

Router#
Router#
```

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#show ip bgp
BGP table version is 2, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 200.200.200.0/24  22.10.10.1               0     0     0 100 i

Router#
Router#
```

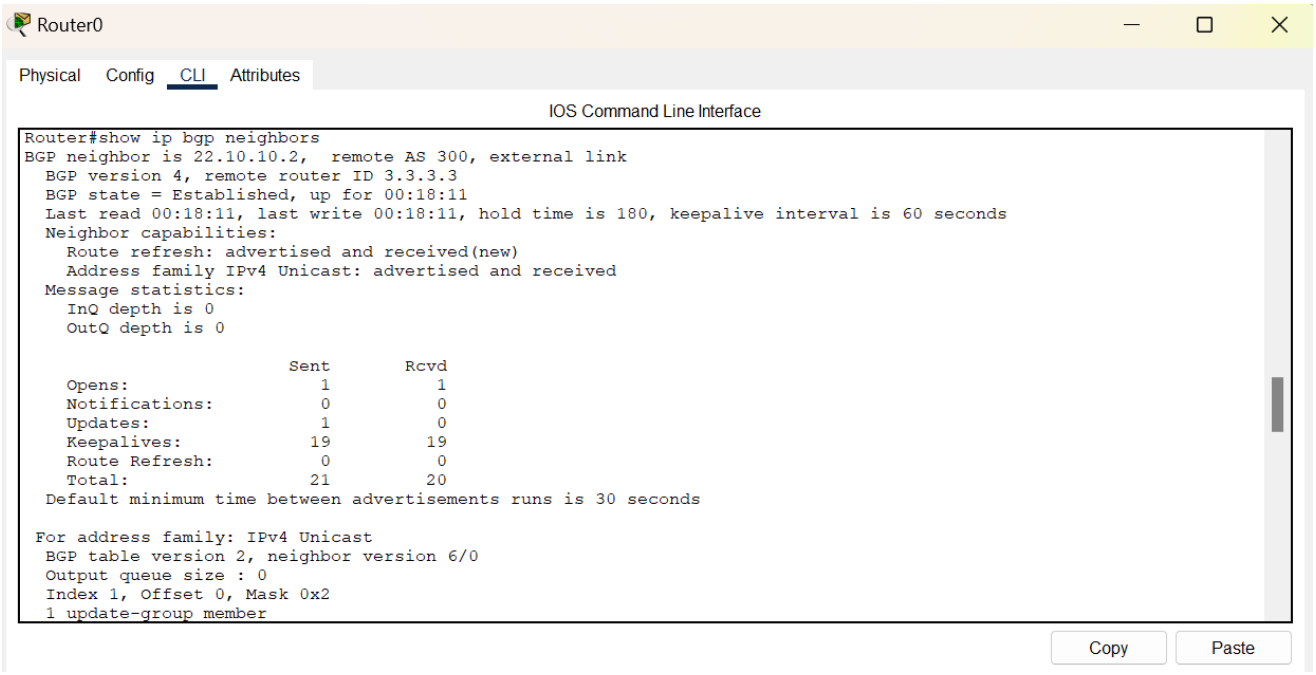
Router2

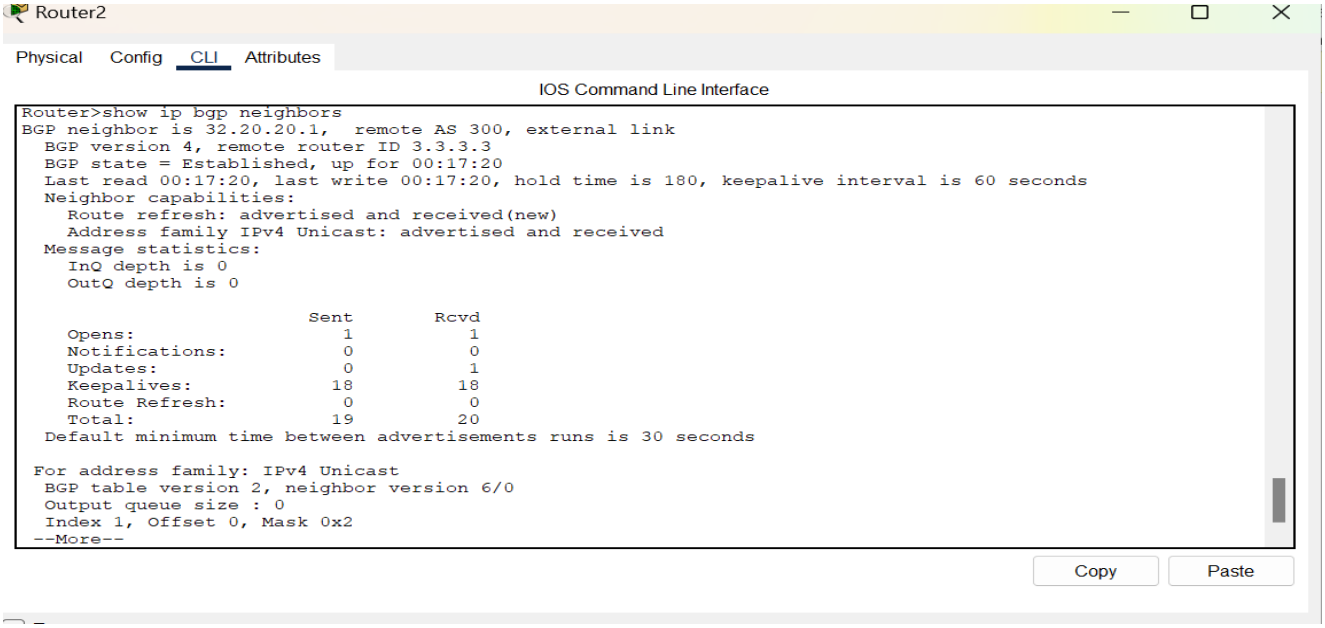
Physical Config CLI Attributes

IOS Command Line Interface

```
Router>show ip bgp
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 200.200.200.0/24  32.20.20.1               0     0     0 300 100 i

Router>
Router>
```

✓ Router# show ip bgp neighbors

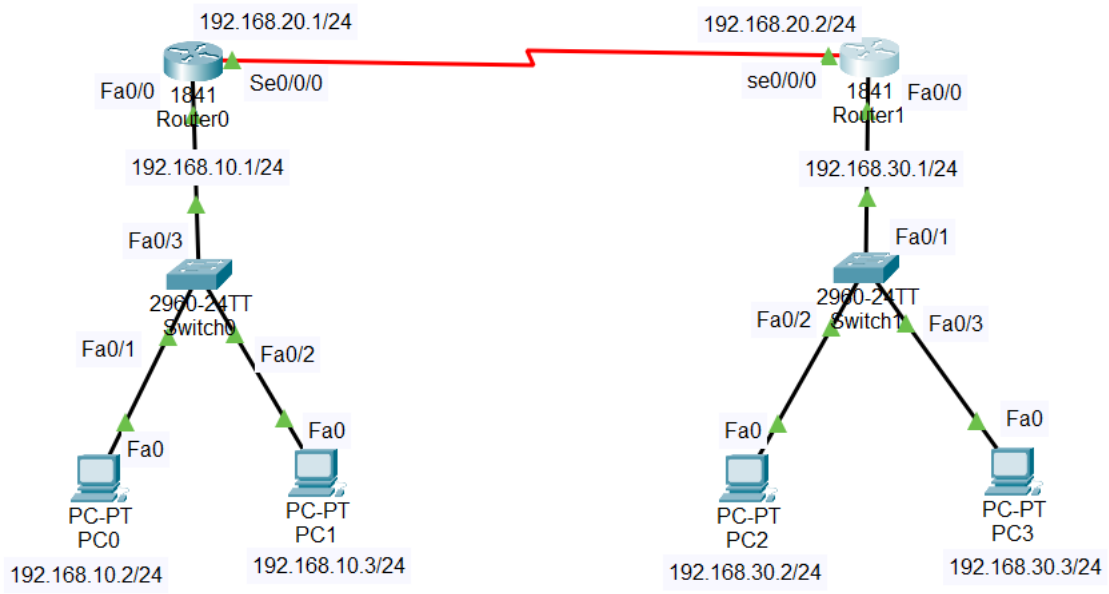




3.) EIGRP Protocol

Procedure :-

I. open cisco packet tracer and create a network topology and assign ip addresses to the routers and the pcs as shown below :

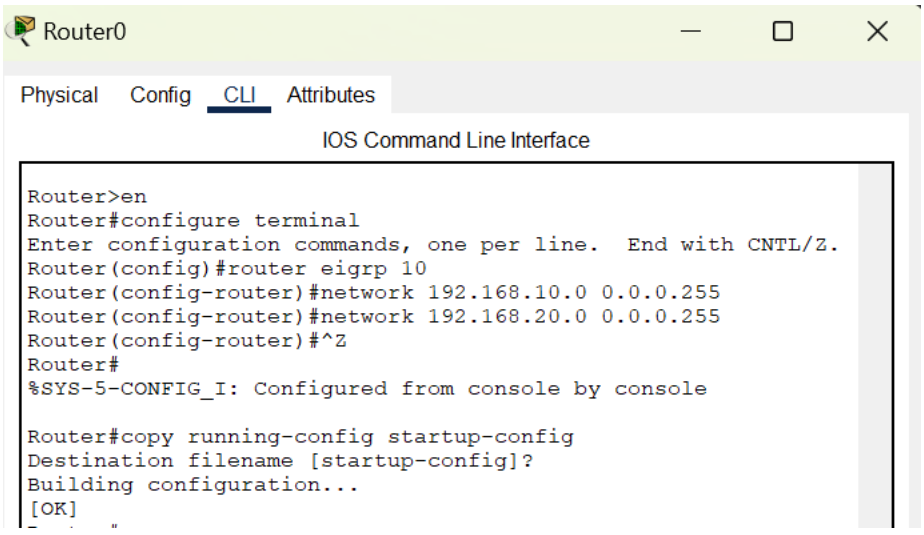


II. Enable EIGRP on each router by using the following commands in the CLI:

- ✓ Router(config)# router eigrp [AS number]
- ✓ Router(config-router)# network [network address] [wildcard-mask]

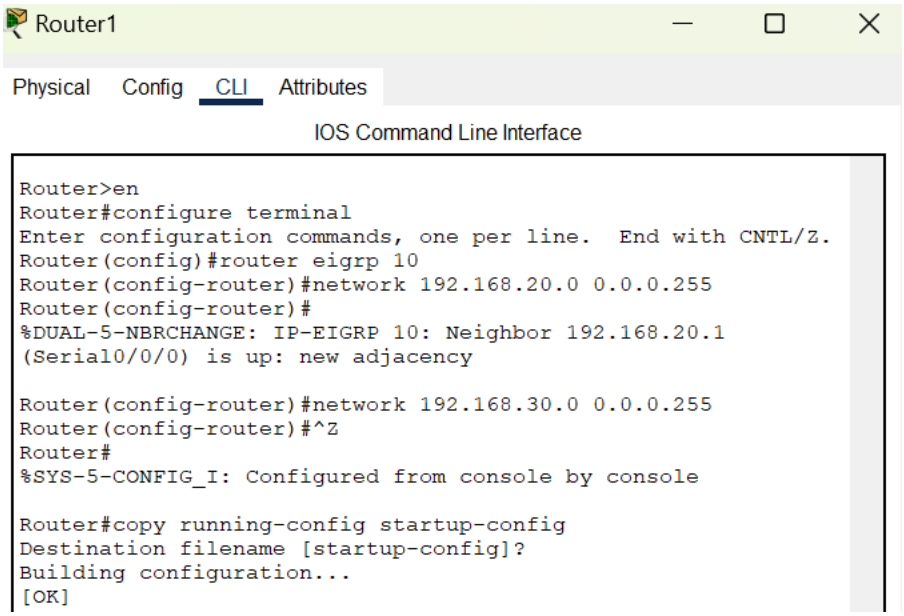
#Replace [AS number] with the EIGRP autonomous system number and [network address] with the network address you want to advertise.

#Network command with wildcard mask is used to configure eigrp to advertise specific subnets



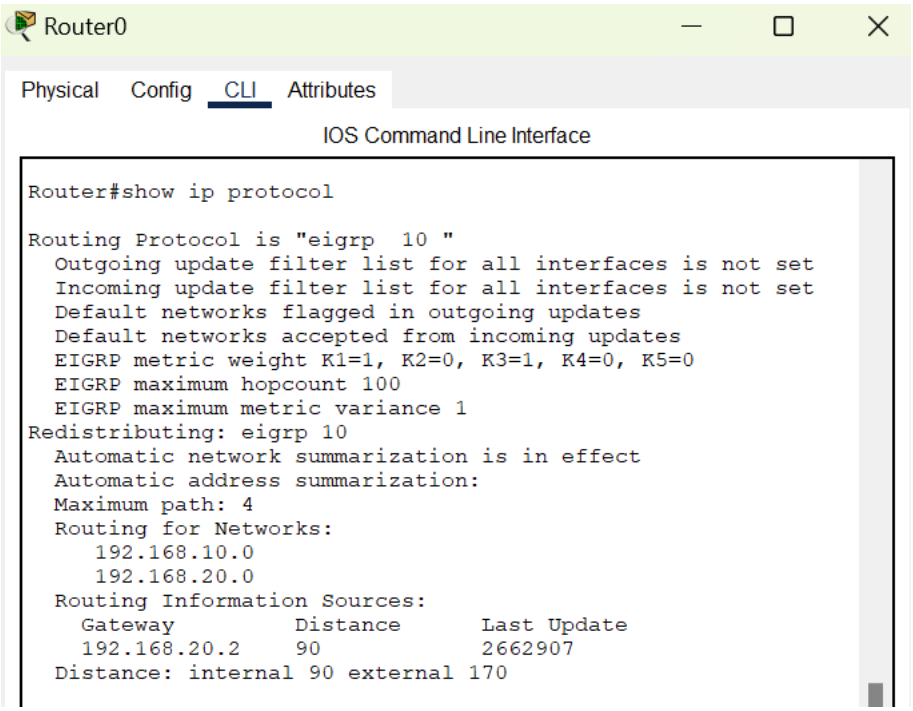
(copy running-config startup-config command is used to save the configuration)

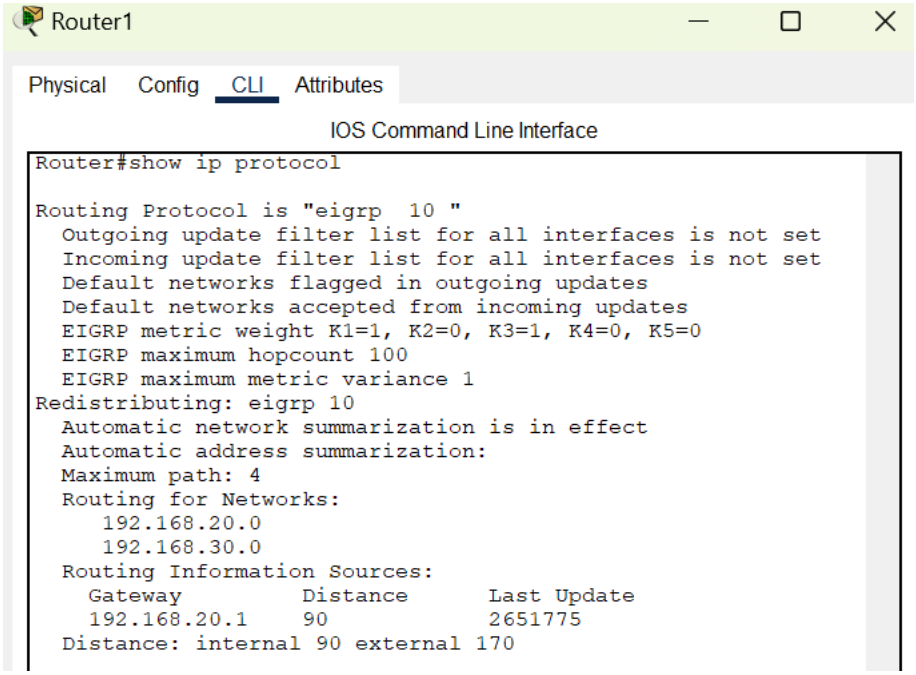
Similarly do this for second router



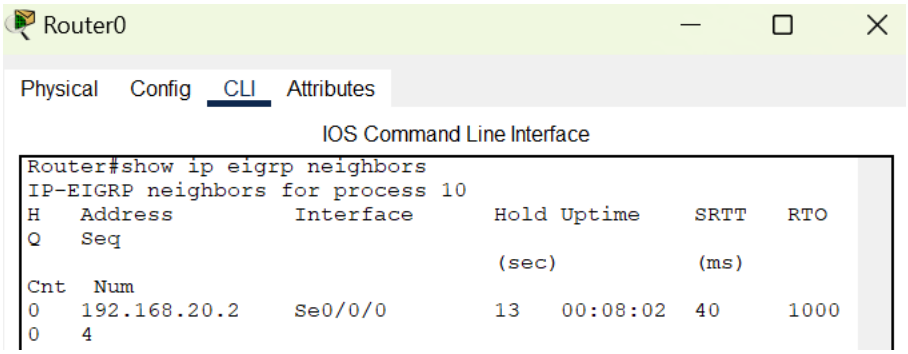
III. Verify the EIGRP configuration by using the following commands in the CLI:

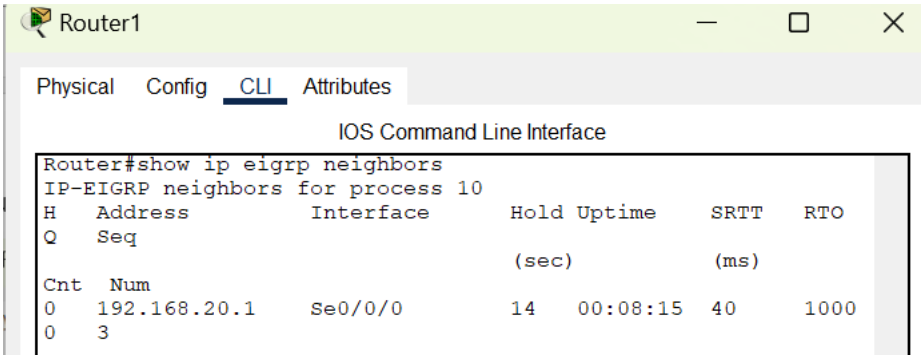
- ✓ Router# show ip protocols



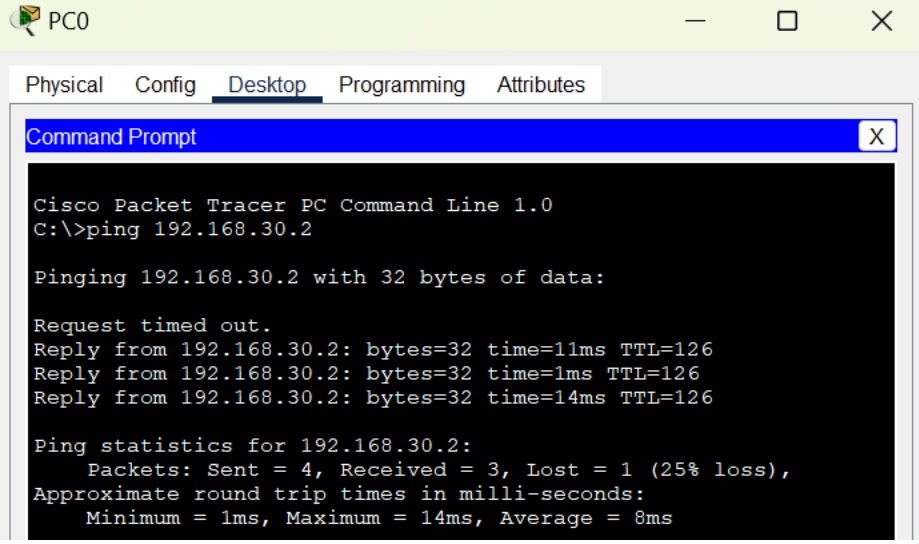


✓ Router# show ip eigrp neighbors

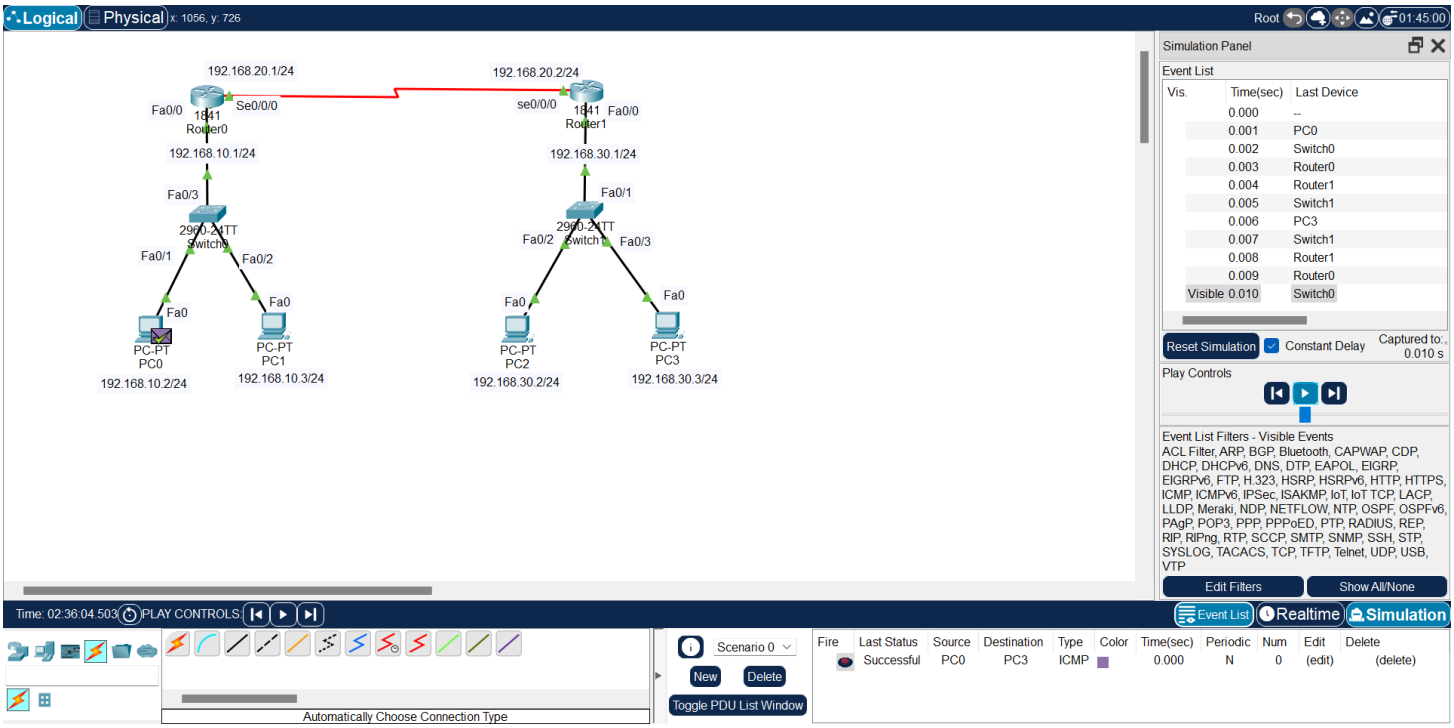




IV. To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.



V. Finally to check the connectivity ,click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.

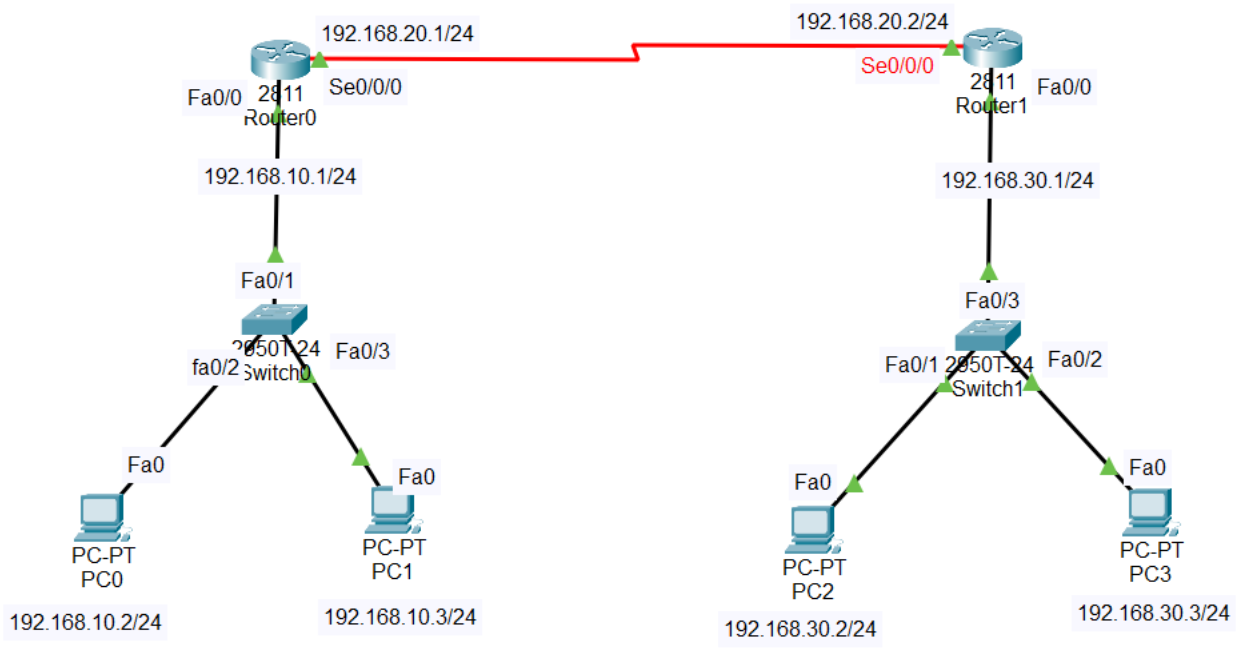


PRACTICAL-11

Implement the routing protocols in order to monitor traffic loads.

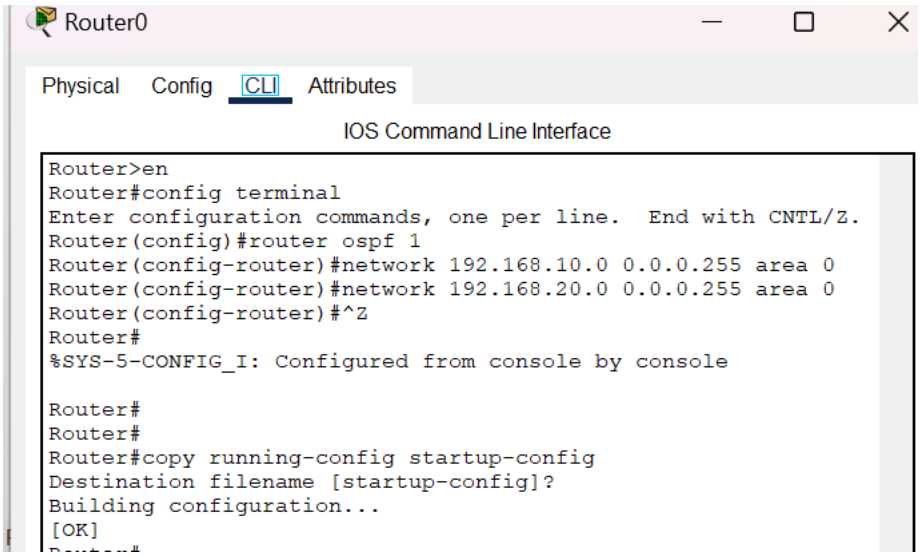
Procedure:-

1.) open cisco packet tracer and create a network topology and assign ip addresses to the routers and the pcs as shown below :

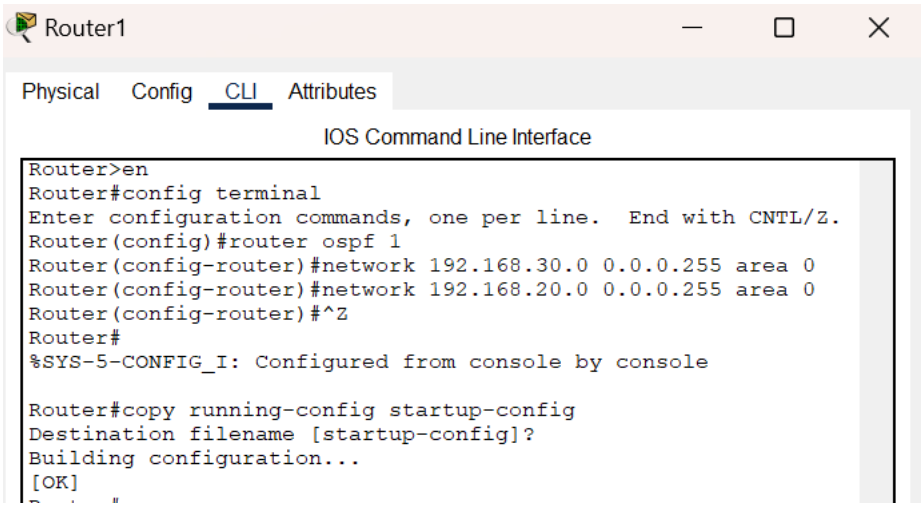


2.) Enable EIGRP on each router by using the following commands in the CLI:

- ✓ enter "enable" to enter privileged mode.
- ✓ Type "configure terminal" to enter global configuration mode.
- ✓ Type "router ospf 1" to enter OSPF configuration mode. 1 is the process ID.
- ✓ Type "network [ip address] [wildcard-mask] area [area-id]" to enable OSPF on the router's and assign it to Area with area-id.
- ✓ Repeat the same steps for the each interfaces on the router
- ✓ Exit the OSPF configuration mode by typing "exit" twice.
- ✓ Save the configuration by typing "copy running-config startup-config"

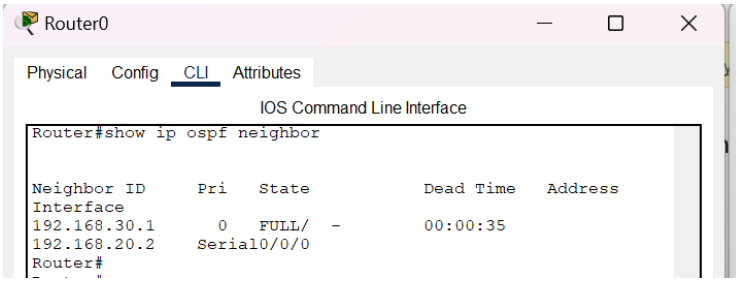


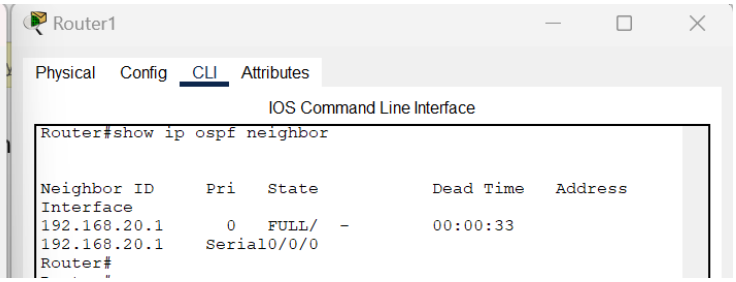
(similarly for router 1)



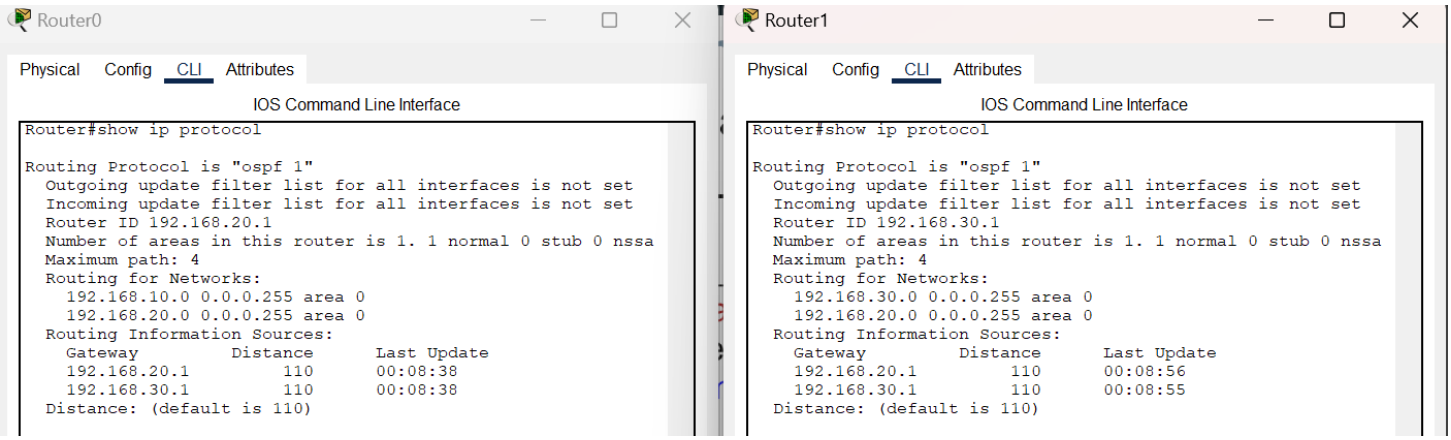
3.) Verify the ospf configuration by using the following commands in the CLI:

- ✓ Router# show ip ospf neighbor

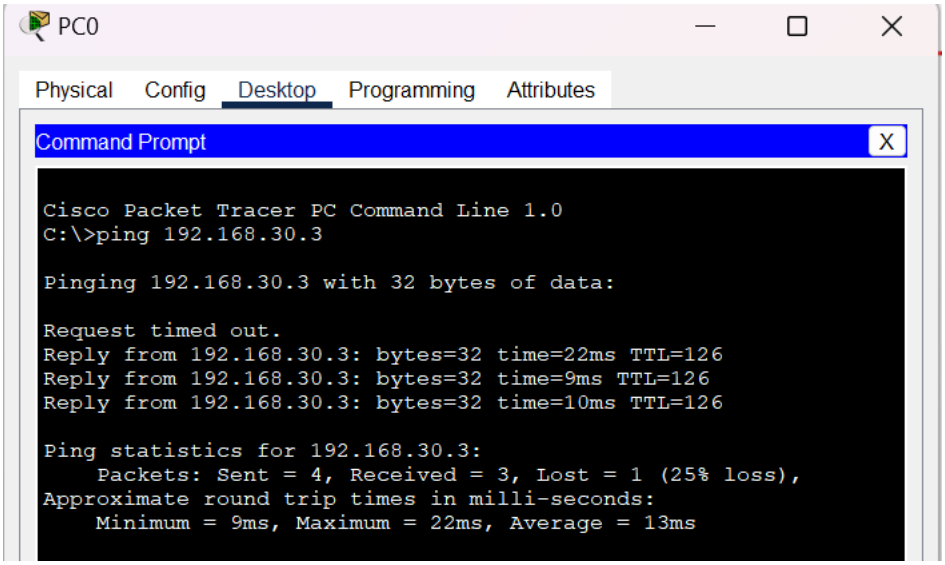




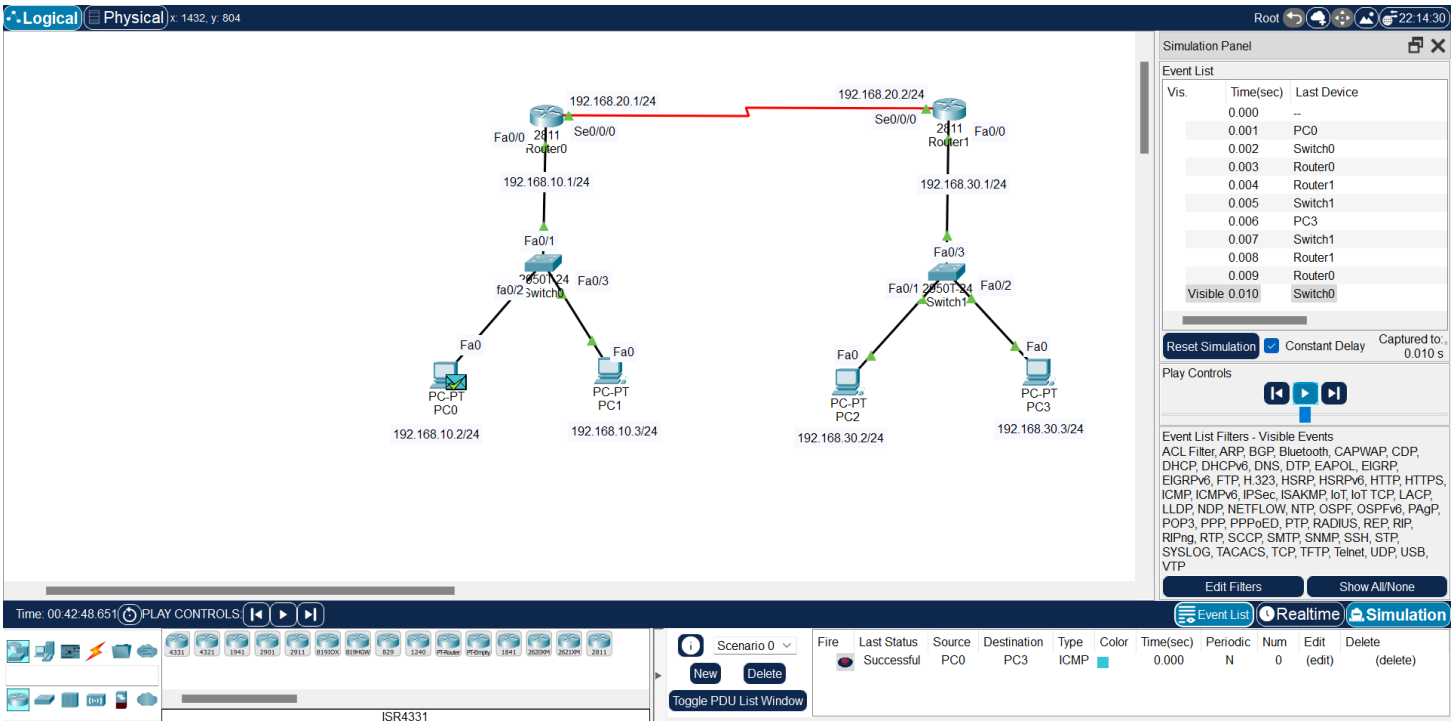
✓ Router# show ip protocol



4.)To check whether the PCs are connected to each other, we use PING command. Click on any computer and then go to “Desktop” and select “Command Prompt”, then type “ping *IP address of any other computer*” (*excluded). If all the packets are received (0 Lost) then the connection is successfully established.

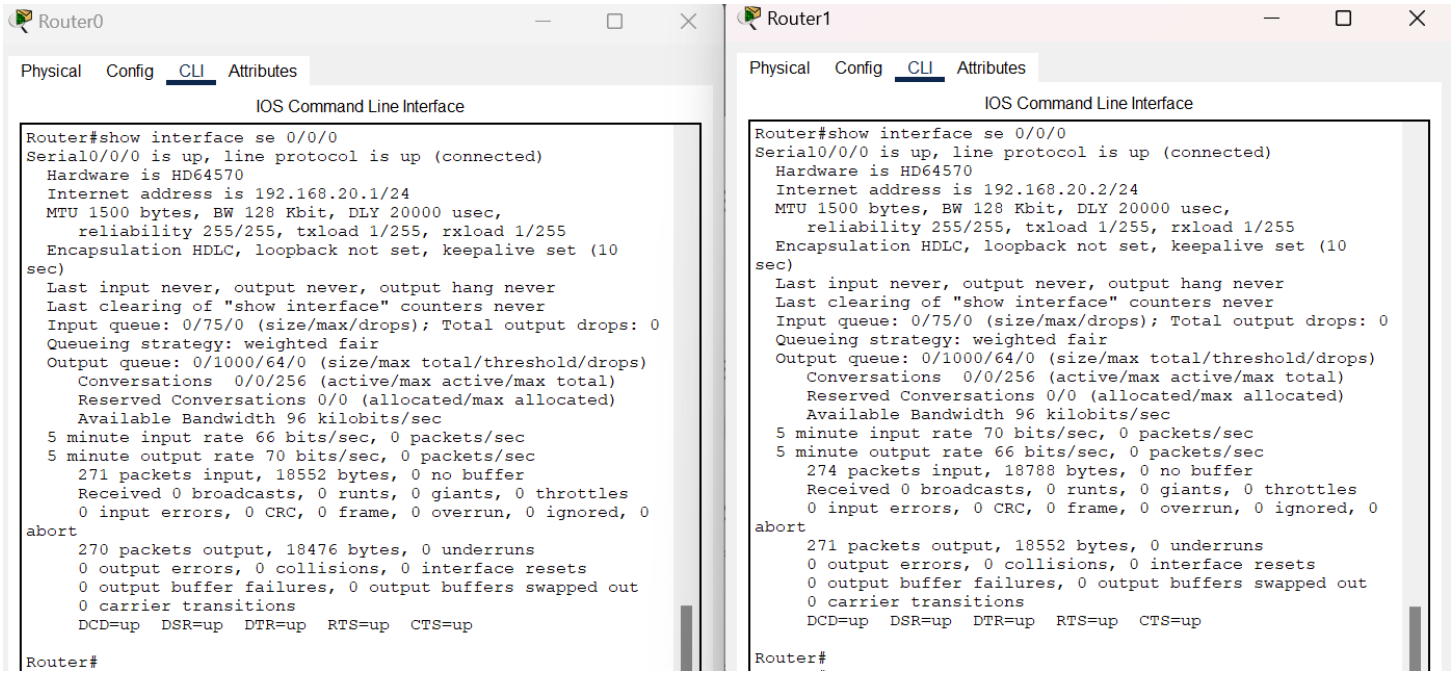


5.) Finally to check the connectivity ,click on “Add Simple PDU” option from the top ribbon and then selecting the computer from which you want to send the message to the destination computer, then Run the Simulation.



6.)Monitor the traffic load on each interface by using this command :

- ✓ Show interface [interface name]



That's it! By following these steps, you should be able to successfully implement OSPF in Cisco Packet Tracer and monitor the traffic loads on your network.

PRACTICAL-12

Set-up a TFTP server to back-up IOS images.

Theory :-

TFTP Server is used for simple file transfer (typically for boot-loading remote devices).

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files. The TFTP protocol supports only file send and receive operations. File delete, move, and rename are not supported. Due to its limitations, TFTP is a complement to the regular FTP and not a replacement. It is only used when its simplicity is important, and its lack of features is acceptable. The most common application is bootstrapping, although it can be used for other purposes as well.

IOS images in CPT

Cisco IOS (Internetwork Operating System) is a proprietary operating system that runs on Cisco Systems routers and switches. The core function of Cisco IOS is to enable data communications between network nodes.

In addition to routing and switching, Cisco IOS offers dozens of additional services that an administrator can use to improve the performance and security of network traffic. Such services include encryption, authentication, firewall capabilities, policy enforcement, deep packet inspection, Quality of Service (QoS), intelligent routing and proxy capability. In Cisco's Integrated Services Routers (ISRs), IOS can also support call processing and unified communications services.

Cisco IOS software releases are organized into what Cisco calls "families" and "trains." Each family shares the same code base and trains are how new IOS releases are delivered.

There are two types of IOS operating systems:

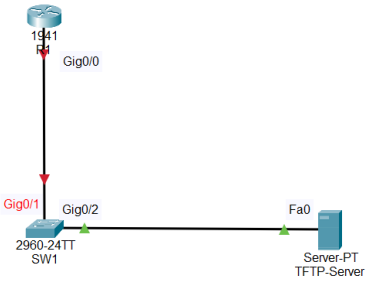
IOS XE - runs on top of a Linux kernel. IOS XE and IOS share a lot of the same code, but IOS XR is considered to be a completely different code base.

IOS XR - based on QNX a commercial Unix-like real-time operating system. IOS XR supports software-defined networking (SDN) and the embedded systems market.

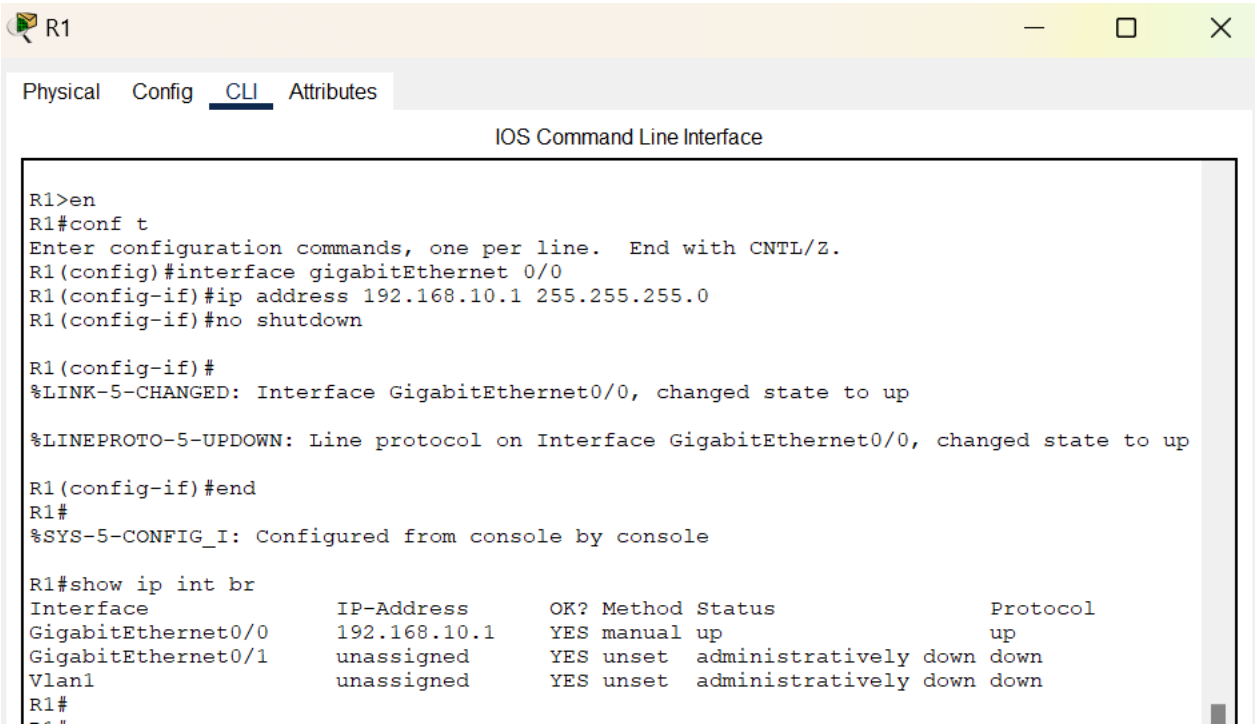
Procedure:-

1.) open cisco packet tracer and add a Cisco Router, Switch, and server to the Packet Tracer workspace

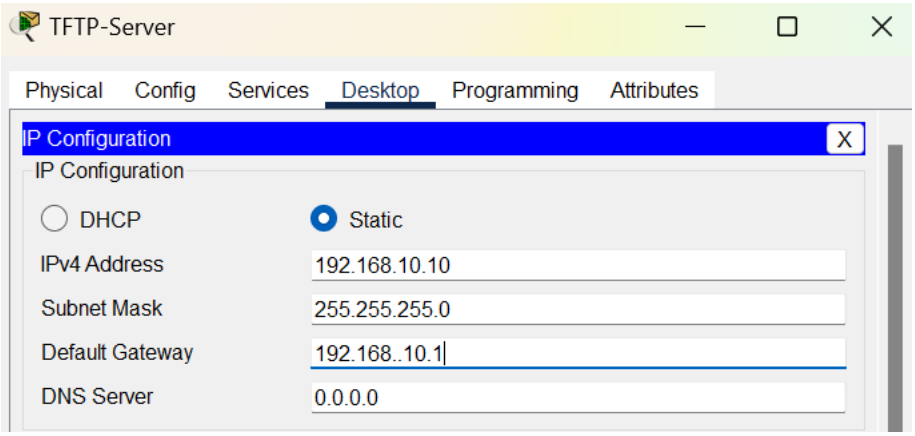
2.) Connect the added Router and server to the Switch using a Copper-straight Through cable as shown below :



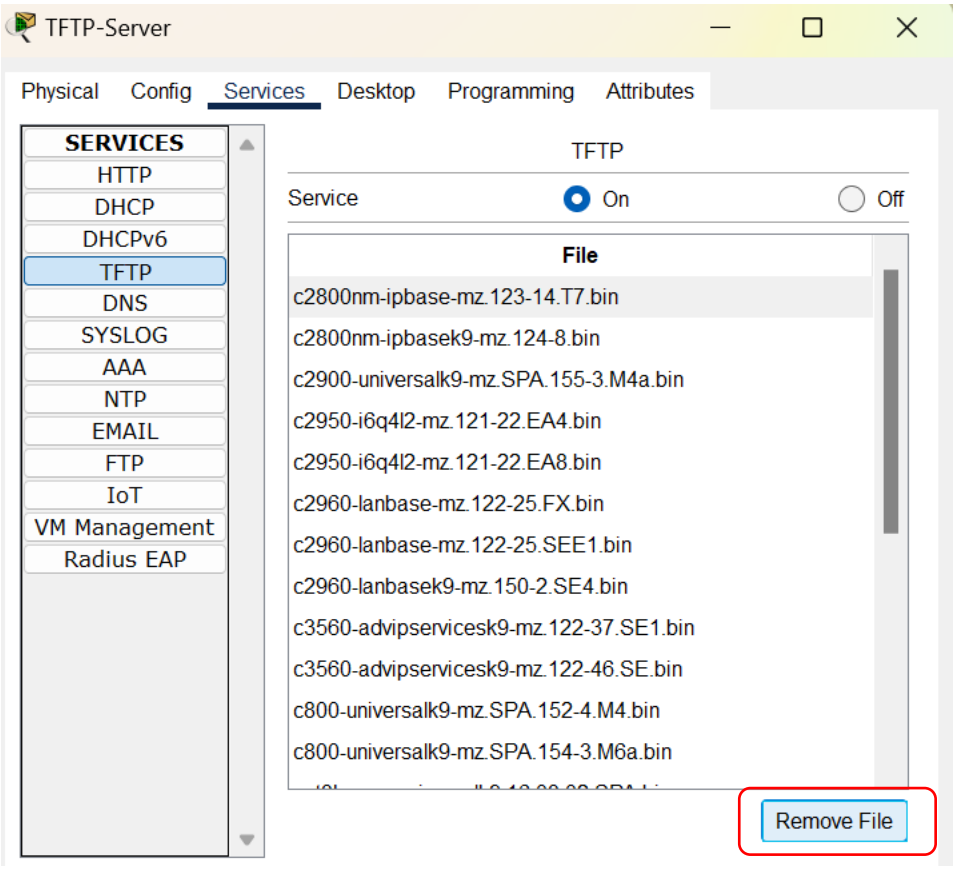
3.) Open the CLI command prompt of the router and assign an IP address to its interface connected to the Switch and open the port.



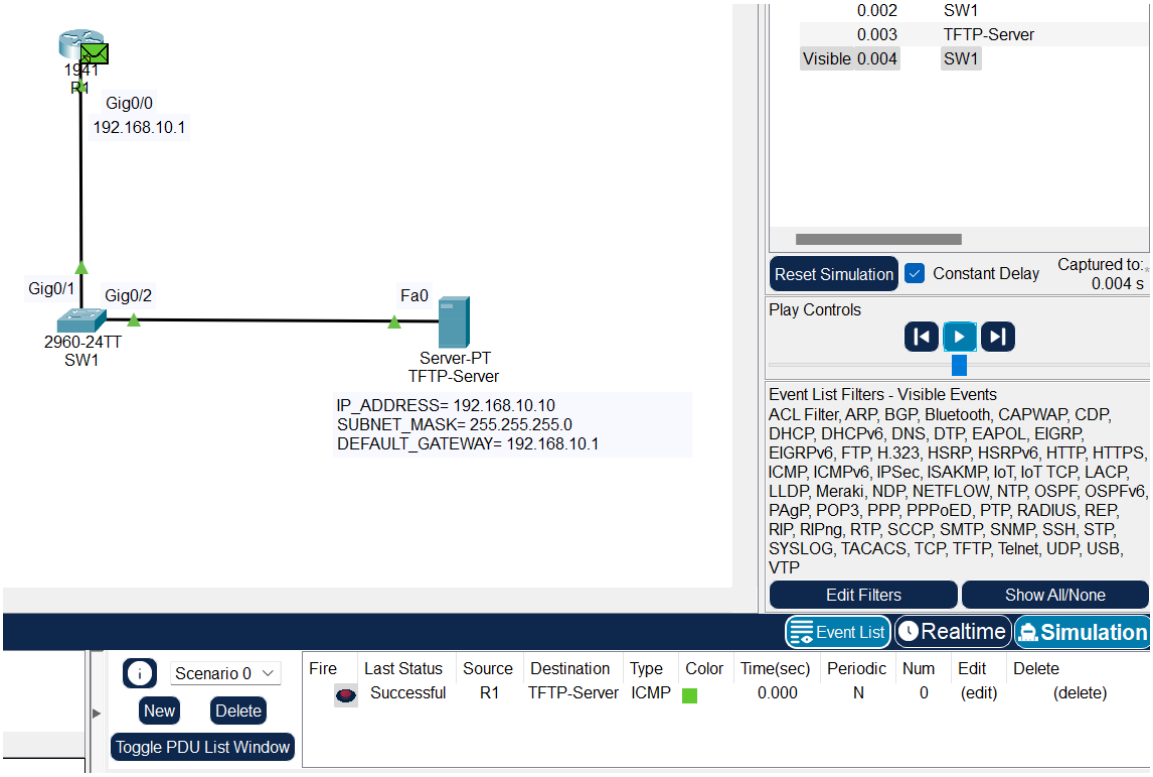
4.) Configure the TCP/IP settings of the interface connected to the Switch in the IP configuration of the #TFTP server.



5.) Click on the Services tab and enable TFTP service, and then delete all files on the server.



6.) Test the network connection between the server and the router. To do this click on "add simple pdu" and select router and tftp-server then run the simulation



7.) To upload the IOS image running on the router to the server, first run the show flash command in enable mode and learn the file name. Then, after executing the copy flash command, type the filename in the source filename field.

8.) In the next step, type the IP address of the server and press Enter.

9.) Press Enter without changing the filename in the Destination filename section.

10.) As a result of this process, IOS will be copied to the server. Check the folder on the server to verify the backup.

R1

Physical Config CLI Attributes

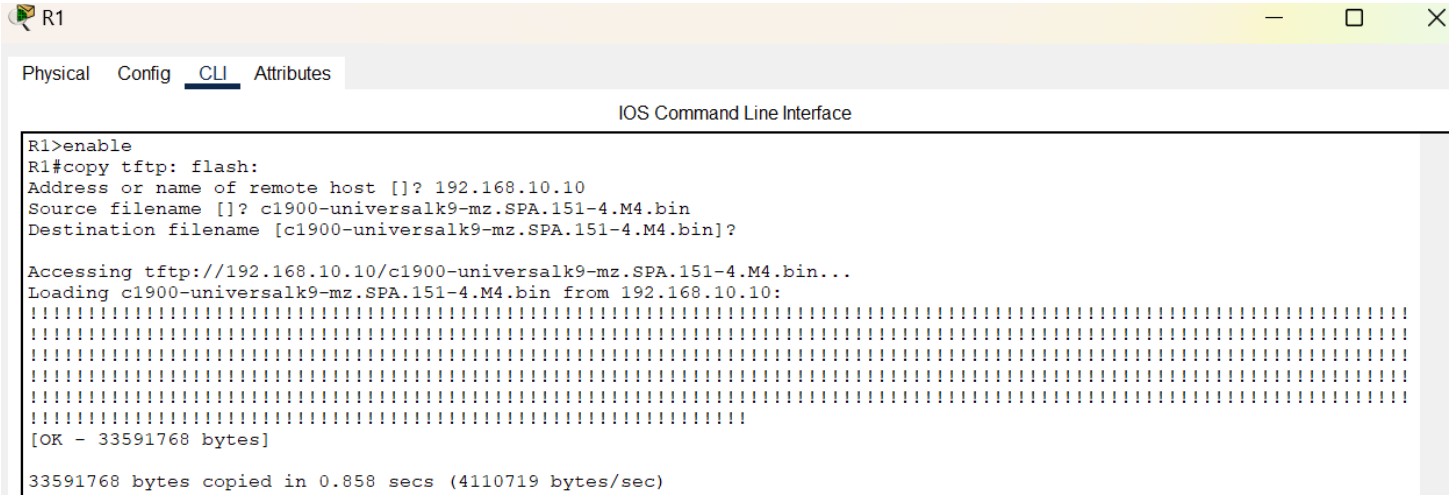
IOS Command Line Interface

```
R1>enable
R1#show flasH:

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R1#copy flash: tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 192.168.10.10
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?

Writing c1900-universalk9-mz.SPA.
151-4.M4.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 1.369 secs (2576330 bytes/sec)
```

Step 11: Now, to restore the ios image from the tftp server , first delete the IOS on the Router with the delete flash command.

```
R1#
R1#delete flash:
Delete filename []?c1900-universalk9-mz.SPA.151-4.M4.bin
Delete flash:/c1900-universalk9-mz.SPA.151-4.M4.bin? [confirm]

R1#show flash:

System flash directory:
File  Length   Name/status
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[255819 bytes used, 255488181 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

12.): Then in enable mode, execute the copy tftp flash command this time and write the IP address of the server as the remote address. In the Source filename section, type the name of the IOS file and press Enter.



13.) To verify the ios image is restored or not type the "show flash" and check the file is present or not