**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

**Course** **Name:** **Computer** **Network** **Page no: 1**

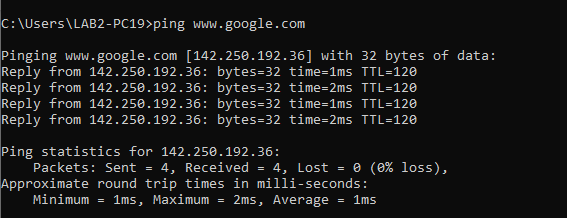
**Practical** **Number:-** **01**

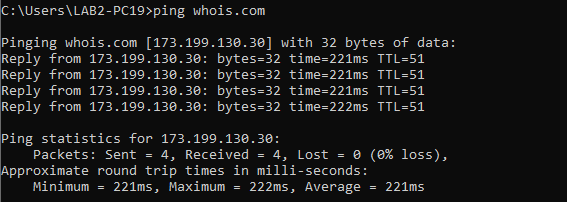
**Q.** **Use** **of** **network** **commands.**

1. **Ping** **Command:**
   * The ping command is used to test the ability of the source computer to reach a specified destination computer.
   * The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

**Command**: ping <ipaddress/url>

**Output:**





**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

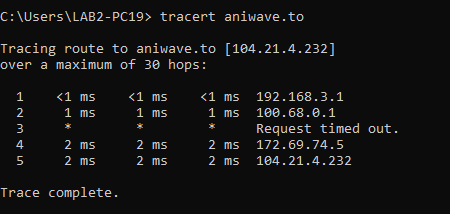
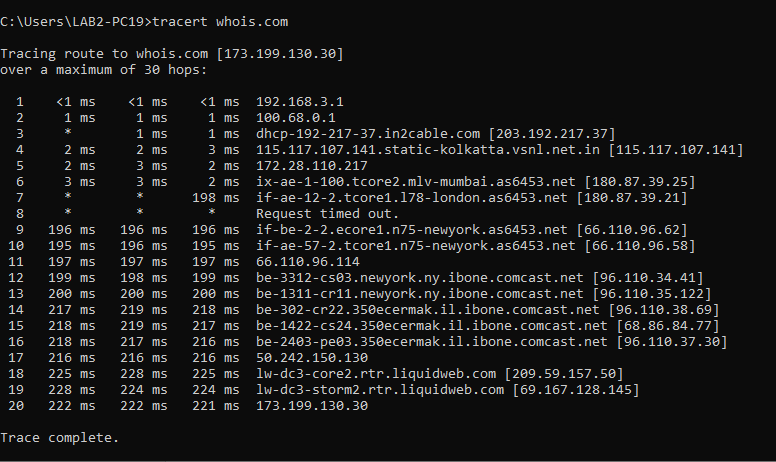
**Course** **Name:** **Computer** **Network** **Page no: 2**

**Practical** **Number:-** **01**

1. **Tracert** **command:**
   * Tracert is used to show several details about the path that a packet takes from the computer or device you or on to whatever destination you specify
   * Traceout is a command which can show you the path, a packet of information takes from your computer to one you specify.
   * It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.
   * In addition to this, it will tell you how long each hop from router to router is being taken.

**Command:** tracert <ipaddress/url>

**Output:**



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

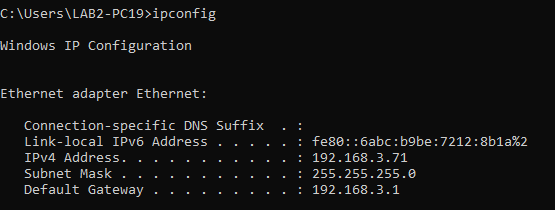
**Course** **Name:** **Computer** **Network** **Page no: 3**

**Practical** **Number:-** **01**

1. **Ipconfig** **command:**
   * IPconfig is a DOS utility that can be used from MSDOS and the windows command line to display the nework settings currently assigned and given by a network.
   * The command can be utilized to verify a network connection as well as to verify your settings.

**Command:** ipconfig

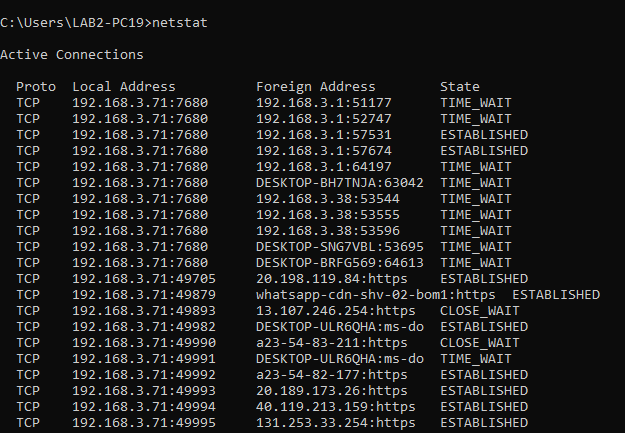
**Output:**



1. **Netstat** **command:**
   * The netstat command, meaning network statistics is used to display very detailed information about how your computer is communicating with other computers or network devices
   * Specifically, the netstat command can show details about individual network connections, overall and protocol specific networking statistics, and much more, all of which could help troubleshoot certain kind of networking issues.

**Command:** netsat

**Output:**



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

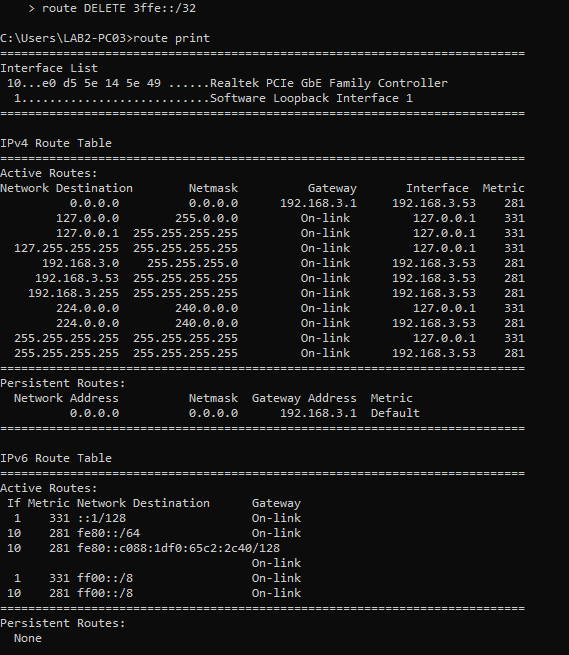
**Course** **Name:** **Computer** **Network** **Page no: 4**

**Practical** **Number:-** **01**

1. **Route** **Command:**
   * The route command allows you to make manual entries into the network routing tables.
   * The route command distinguishes between routes to hosts to networks by interpreting he network address of the destination variable, which can be specified either by symbolic name or numeric address.
   * The route command resolves all symbolic names into addresses, using either the /etc/hosts file or the network name server
   * One can: I PRINT prints a route
2. ADD adds a route
3. DELETE deletes a route
4. CHANGE modifies an existing route

**Command:** route print

**Output:**



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

**Course** **Name:** **Computer** **Network** **Page no: 5**

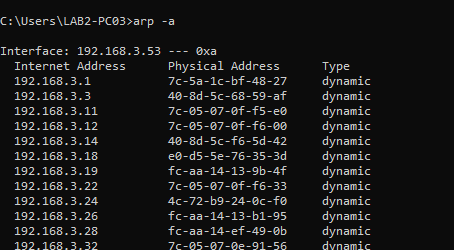
**Practical** **Number:-** **01**

1. **ARP** **command:**
   * ARP command is used to view and modify the arp (address resolution protocol) table entries on the local computer.
   * This may display all the known connections on your local area network segment (if they have been active and in the cache). The arp command is useful for viewing the arp cache and resolving address resolution problem.

**Command:** arp -a (to display the arp table)

**Example:** arp – a

**Output:**



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

**Course** **Name:** **Computer** **Network** **Page no: 6**

**Practical** **Number:-** **01**

**Q.** **Use** **of** **Wireshark**

* To scan and check the packet information of the following protocols:

1. HTTP
2. ICMP
3. TCP
4. SMTP
5. POP3

* Network Sniffing:
* Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet.
* Network Sniffers are programs that capture low-level package data that is transmitted over a network.
* An attacker can analyse this information to discover valuable information such as user ids and passwords.
* Network sniffing is the process of capturing data packets sent over a network.
* This can be done by the specialized software program or hardware equipment.
* Sniffing can be used to:
  + Capture sensitive data such as login credentials
  + Eavesdrop on chat messages
  + Capture files that have been transmitted over a network. The following are protocols that are vulnerable to sniffing:
  + Telnet
  + HTTP
  + ICMP
  + SMTP
  + NNTP
  + POP
  + FTP
  + IMAP

The above protocols are vulnerable if login details are sent in plain text.

* Network sniffing using Wireshark:
* Wireshark is a free and open-source packet analyser.
* It is used for network troubleshooting, analysis, software and communications protocol development and education.
* Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets.
* It runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.
* There is also a terminal-based (non-GUI) version called TShark.
* Wireshark is used to capture and analyse packets in network.
* It is also used as a sniffer, network protocol analyser, and network analyser.
* We can also apply specific filter on network traffic to get more filtered data packets.

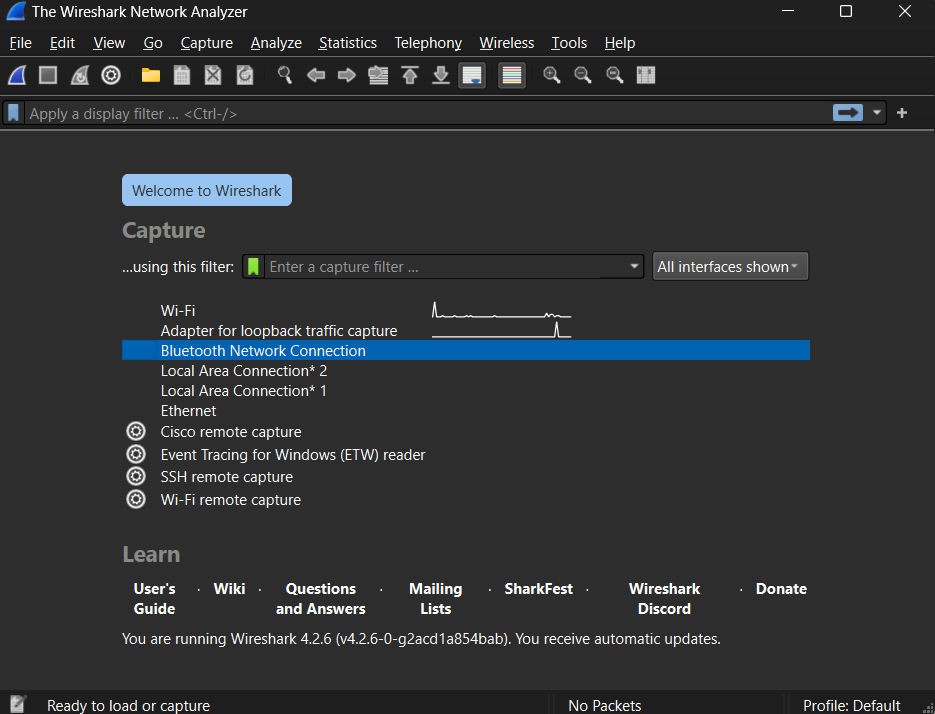
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

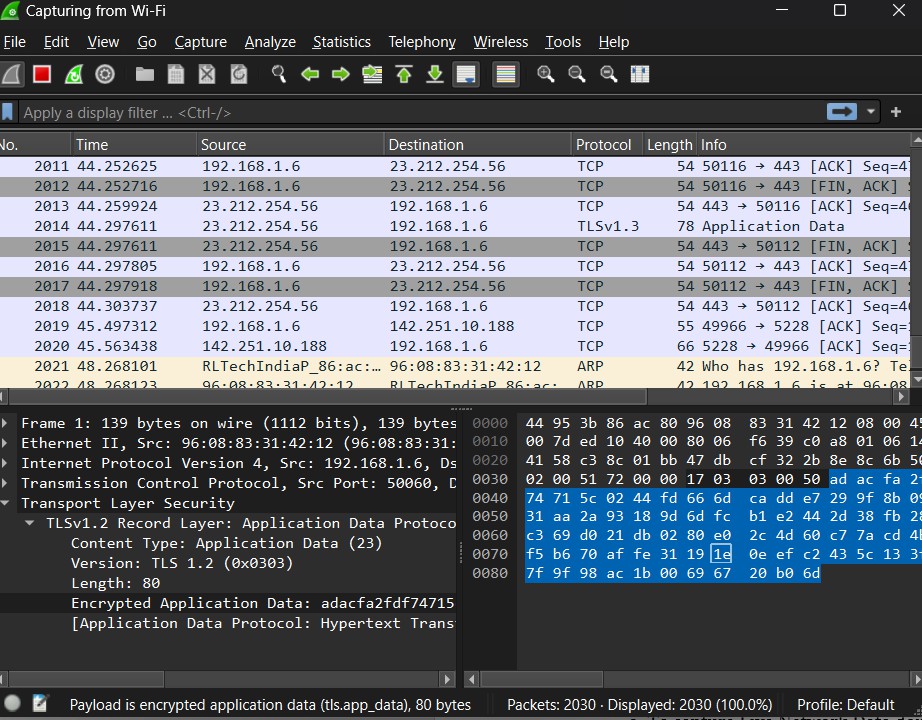
**Course** **Name:** **Computer** **Network** **Page no: 7**

**Practical** **Number:-** **01**

* 1. Wireshark User Interface:



* 1. Capturing Live Network Data:
     1. To capture Live Network Data double, click on any of the interface in the above UI screen.
     2. Once you double click on the interface you will start getting packet detail entering and leaving the network as shown below:



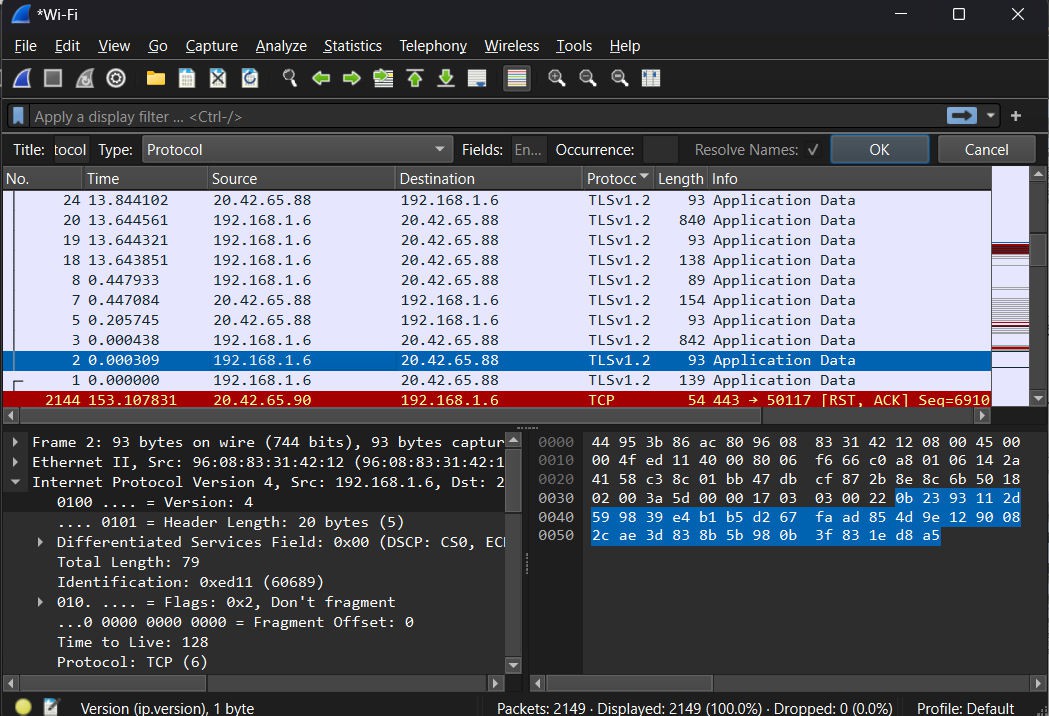
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 05-07-2024

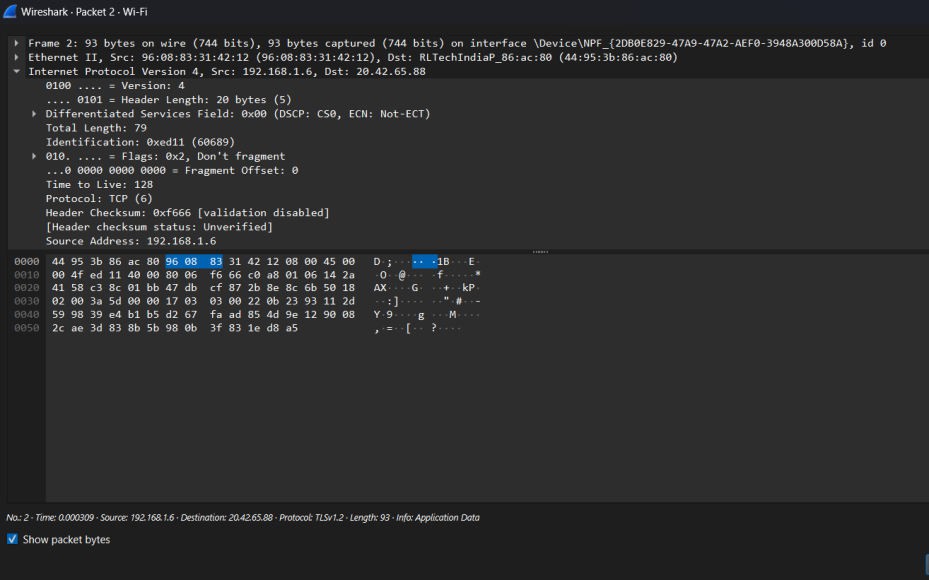
**Course** **Name:** **Computer** **Network** **Page no: 8**

**Practical** **Number:-** **01**

* + 1. Packet based on different coding scheme.



* 1. Viewing captured packets.
     1. Double click on any of the packet that you want to view. Another window will open, showing the details of the selected packet as shown below:



Class: SYIT Sem: III Roll No.: SYIT33 Date: 04/09/2024 Course Name: Computer Networks Page no: Practical Number:- 03

# Network Host:

A network address is a unique physical or logical address that distinguishes a network node or device over a computer or telecommunications network. The Network address is a numeric number or address that is assigned to any new device that seeks access to the network or is already part of the network.

# Network broadcast address:

A broadcast address is a special IP address that is used to send a message or packet to all devices on a network. Broadcast addresses are commonly used for network management tasks, such as sending out configuration updates or discovery requests.

# Host bits:

Host bits are the portion of an IP address that identify a specific host in a subnet. The subnet mask determines how much of the address is used for network bits and host bits**.**

# Number of hosts:

A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means.

# First address & last address:

The first part of an IP address is used as a network address, the last part as a host address

1. An address in a block is given as 180.8.17.9.Find the number of addesses in the block, the first address, and the last address.

# Solution:

The given address is a Class B address therefore n=16

# No. of addresses:

N=232-n

=232-16

=216

Class: SYIT Sem: III Roll No.: SYIT33 Date: 04/09/2024 Course Name: Computer Networks Page no: Practical Number:- 03

=65536

Therefore, the number of addresses are 65536 addresses.

# First addresses:

For class B address netid=16 Therefore network mass is 255.255.0.0

To find the first address we logically AND the given address with the network mask.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Given**  **address** | **180** | **8** | **17** | **9** |
| **Network**  **mask** | **255** | **255** | **0** | **0** |
| **AND**  **operation** | **180** | **8** | **0** | **0** |

Therefore, the first address is 180.8.0.0

# Last address:

To find the last address we logically OR the given address with the COMPLEMENT of the network mask.

Network mask= 255.255.0.0

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Mask | 255 | 255 | 0 | 0 |
| Complement Of mask | 0 | 0 | 255 | 255 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Given Address | 180 | 8 | 17 | 9 |
| Complement Of mask | 0 | 0 | 255 | 255 |
| OR operation | 180 | 8 | 255 | 255 |

Class: SYIT Sem: III Roll No.: SYIT33 Date: 04/09/2024 Course Name: Computer Networks Page no: Practical Number:- 03

Hence, we concluded that,

* 1. Network address: The first address is the network address: 180.8.0.0
  2. Network broadcast address: The last address is the network broadcast address 180.8.255.255
  3. Total number of host bits: 16
  4. Number of hosts: 65534(65536-2)

1. An address in a block is given as 130.34.12.64. Find the number of addesses in the block, the first address, and the last address.

# Solution:

The given address is a Class B address therefore n=16

# No. of addresses:

N=232-n

=232-16

=216

=65536

Therefore, the number of addresses are 65536 addresses.

# First addresses:

For class B address netid=16 Therefore network mass is 255.255.0.0

To find the first address we logically AND the given address with the network mask.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Given address** | **130** | **34** | **12** | **64** |
| **Network mask** | **255** | **255** | **0** | **0** |
| **AND operation** | **130** | **24** | **0** | **0** |

Therefore, the first address is 130.34.0.0

Class: SYIT Sem: III Roll No.: SYIT33 Date: 04/09/2024 Course Name: Computer Networks Page no: Practical Number:- 03

# Last address:

To find the last address we logically OR the given address with the COMPLEMENT of the network mask.

Network mask= 255.255.0.0

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Mask | 255 | 255 | 0 | 0 |
| Complement Of mask | 0 | 0 | 255 | 255 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Given Address | 130 | 34 | 12 | 64 |
| Complement Of mask | 0 | 0 | 255 | 255 |
| OR operation | 130 | 34 | 255 | 255 |

Hence, we concluded that,

1. Network address: The first address is the network address: 130.64.0.0
2. Network broadcast address: The last address is the network broadcast address 130.64.255.255
3. Total number of host bits: 16
4. Number of hosts: 65534(65536-2)

**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 04-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **04**

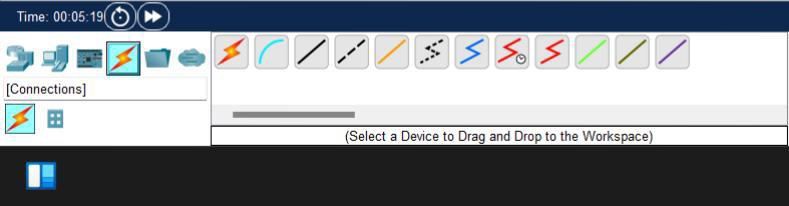
Q. Using Cisco Packet Tracer configure IP static routing.

Steps:

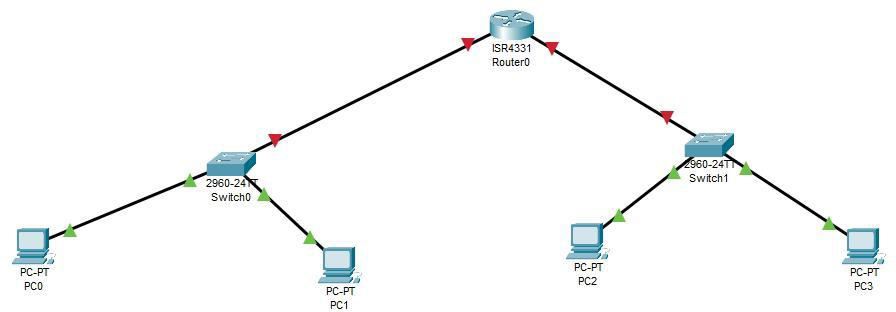
1. Open Cisco Packet Tracer and from Network Devices select one router, two switches and four end devices(4 PC’s) from End Devices and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



Your schema should look something like this:



1. If the red triangles on the wires turn green, it means that the there is a connection between the node. To create a proper connection we need to assign the IP address to the Gigabit Ethernet i.e configure the router ports. To do that double click on the Router > Conifg > Select the Gigabit Ethernet port you want to configure.

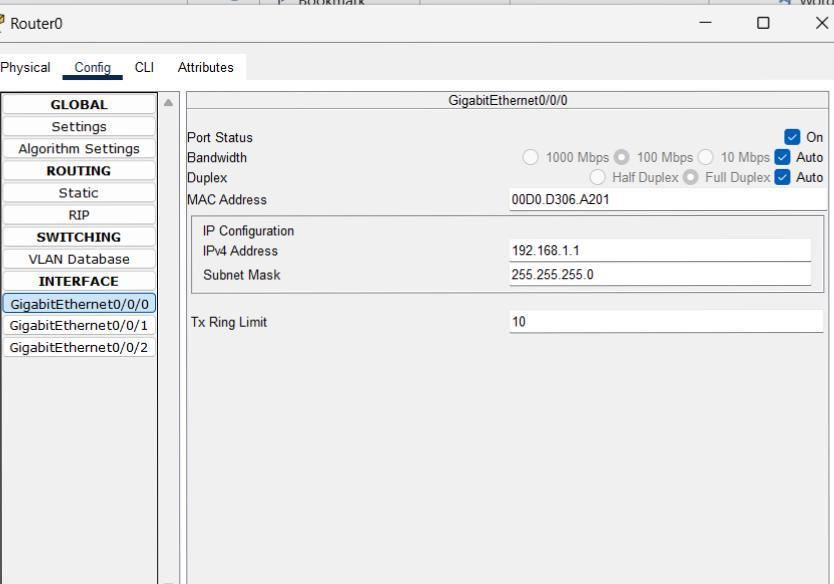
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 04-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

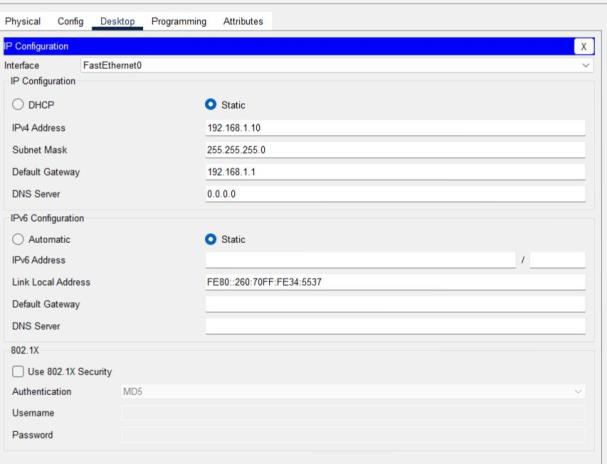
**Practical** **Number:-** **04**

Next, enter the IP address you want for your port. Make sure you tick the checkbox to turn on the port.



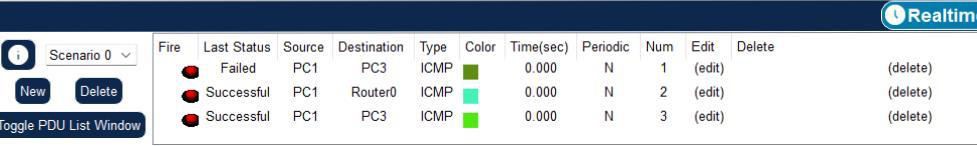
Similarly, assign a different IP address to the other port.

1. Next step is to assign IP address to the PC’s. Click on one PC > Desktop > IP configuration. Enter the IP address you want for your device, the subnet mask is automatically set and in the default gateway enter the IP assigned to the switch. Do the same to the other devices.



1. The connection Is now set properly. You can use the ‘Add sample PDU’ to check your connection. Select it and click on any one of the PC’s to make it the source and then click on any one of the PC’s to make it the destination.

You can check the status of your packet on the bottom-left corner



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 04-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **05**

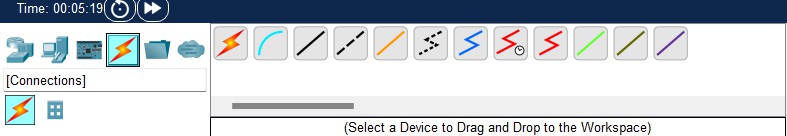
Q. Draw a network layout topology for different scenarios using Cisco packet tracer.

**Steps:**

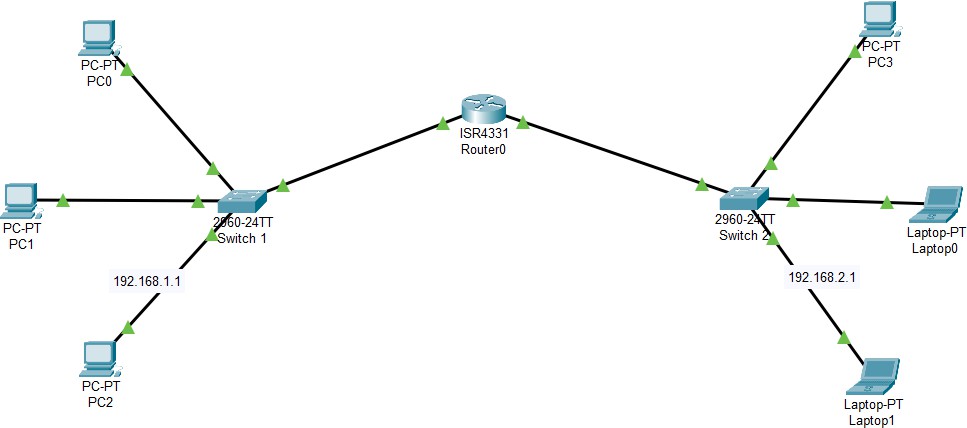
1. Open Cisco Packet Tracer and from Network Devices select one router, two switches and six end devices(4 PC’s & 2 laptop) from End Devices and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



1. Your schema should look something like this:



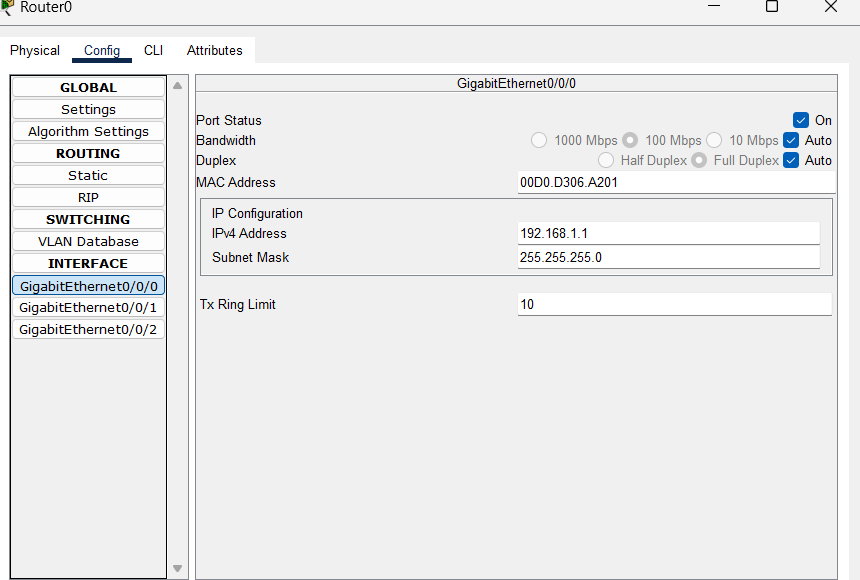
1. If the red triangles on the wires turn green, it means that the there is a connection between the node. To create a proper connection we need to assign the IP address to the Gigabit Ethernet i.e configure the router ports. To do that double click on the Router > Conifg > Select the Gigabit Ethernet port you want to configure.
2. Next, enter the IP address you want for your port. Make sure you tick the checkbox to turn on the port.

**Class:** **SYIT**

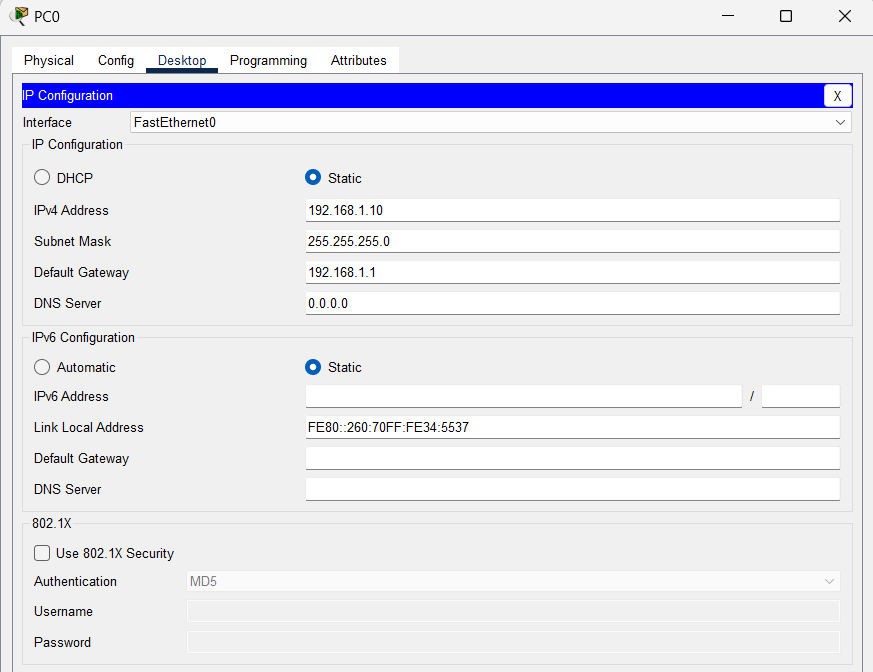
Sem: III Roll No.: SYIT33 Date : 04-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **05**



1. Similarly, assign a different IP address to the other port.
2. Next step is to assign IP address to the PC’s. Click on one PC > Desktop > IP configuration. Enter the IP address you want for your device, the subnet mask is automatically set and in the default gateway enter the IP assigned to the switch. Do the same to the other devices.



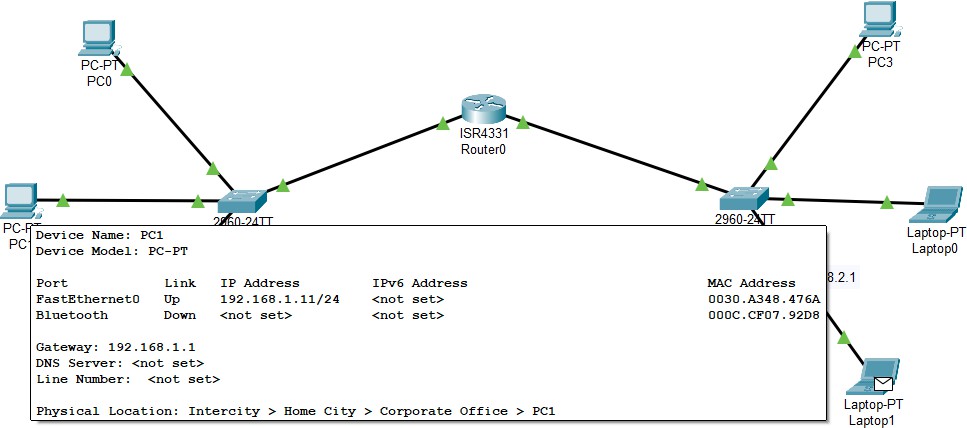
1. The connection Is now set properly. You can use the ‘Add sample PDU’ to check your connection. Select it and click on any one of the PC’s to make it the source and then click on any one of the PC’s to make it the destination.

**Class:** **SYIT**

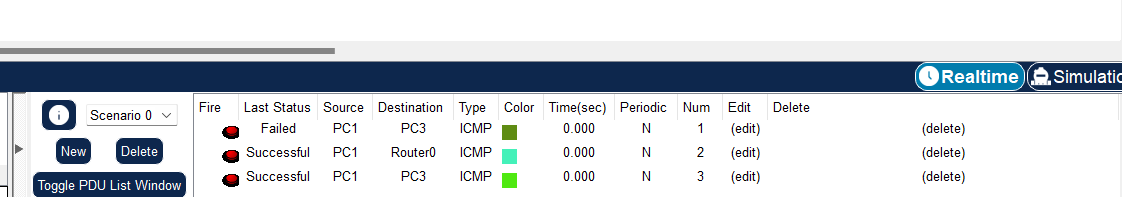
Sem: III Roll No.: SYIT33 Date : 04-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

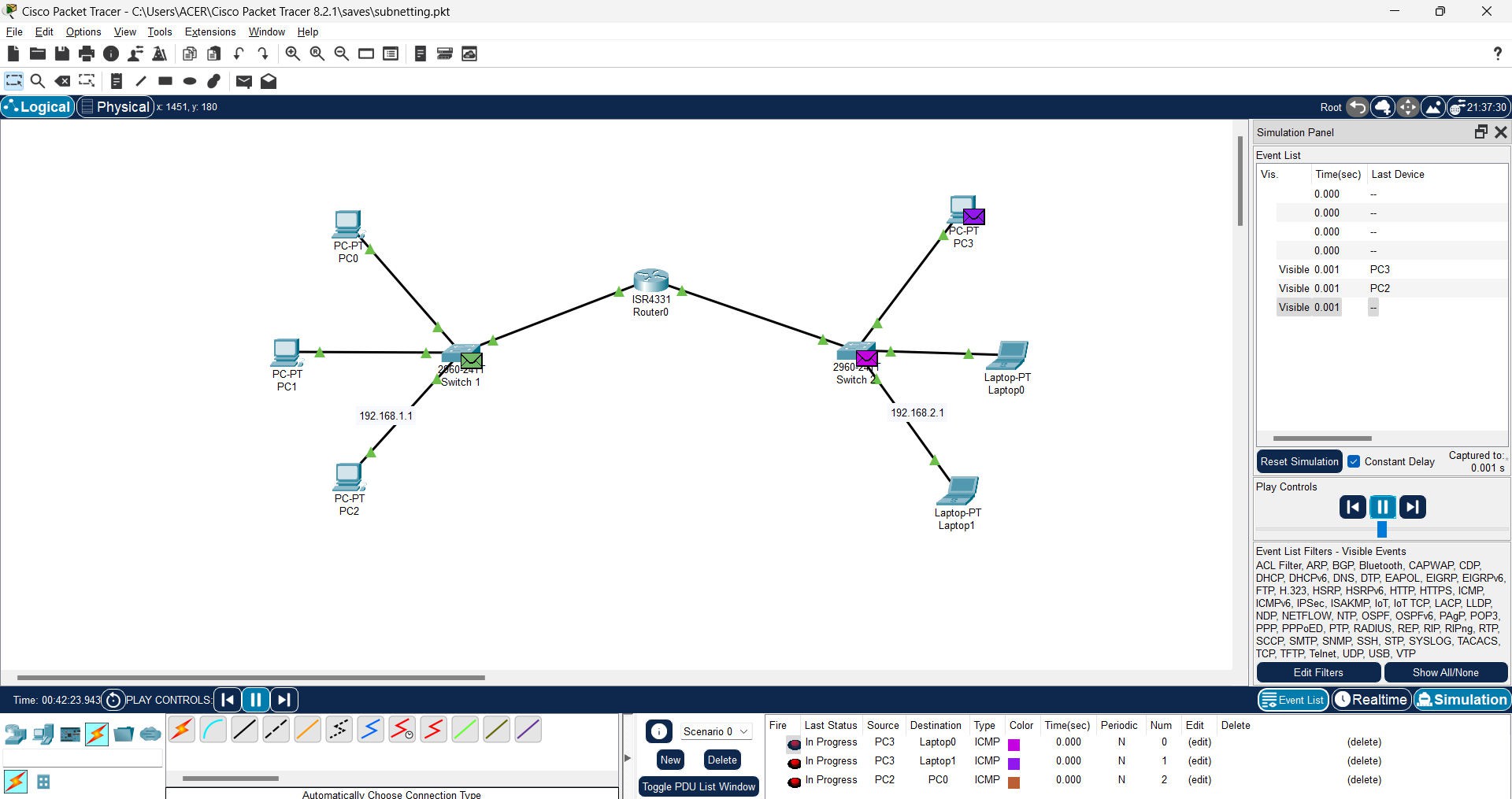
**Practical** **Number:-** **05**



1. On the bottom left corner you can know the status of your packet whether it was successful or it failed.



1. You can use Simulation to simulate the entire process of transmission of the packet from device to device. This feature can be useful if you want to know where exactly is the problem, if there is any.



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**

Q. Using Cisco Packet Tracer configure Static Routing.

What is static routing?

Static routing is a type of network routing where routes are manually configured by the network administrator. In static routing, specific paths are set for data to travel between devices or networks, based on predefined routes.

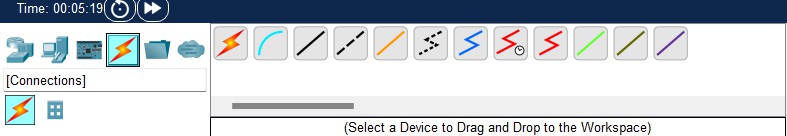
Unlike dynamic routing, static routes do not change unless manually updated, making it simple but less flexible. It's ideal for small or stable networks where traffic paths are predictable and don't need frequent updates.

Steps:

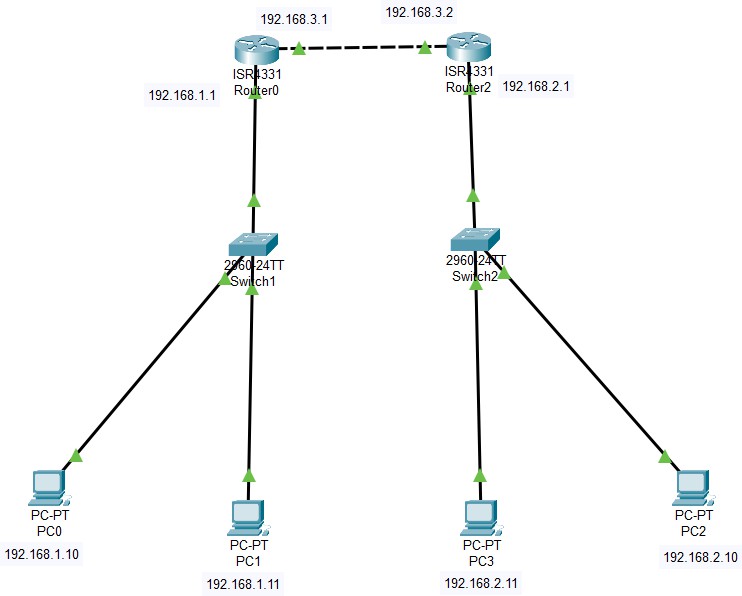
1. Open Cisco Packet Tracer and from Network Devices select one router, two switches and six end devices(4 PC’s & 2 laptop) from End Devices and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



1. Your schema should look something like this:



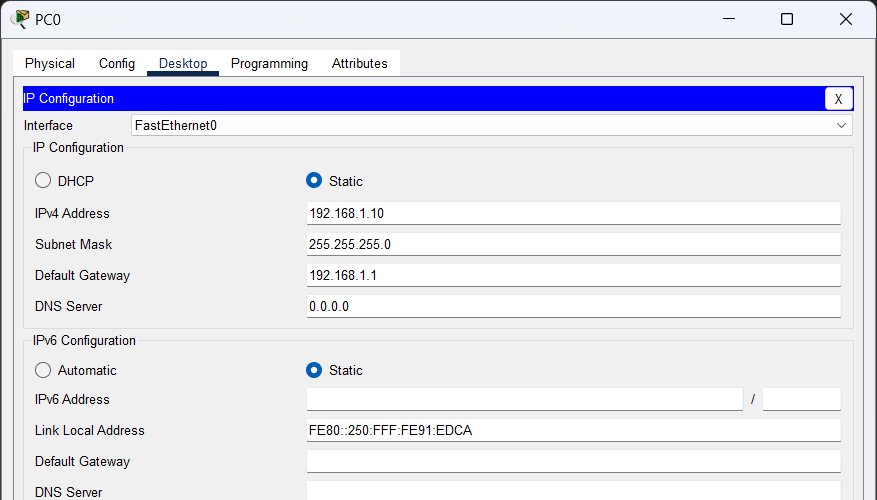
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 13-08-2024

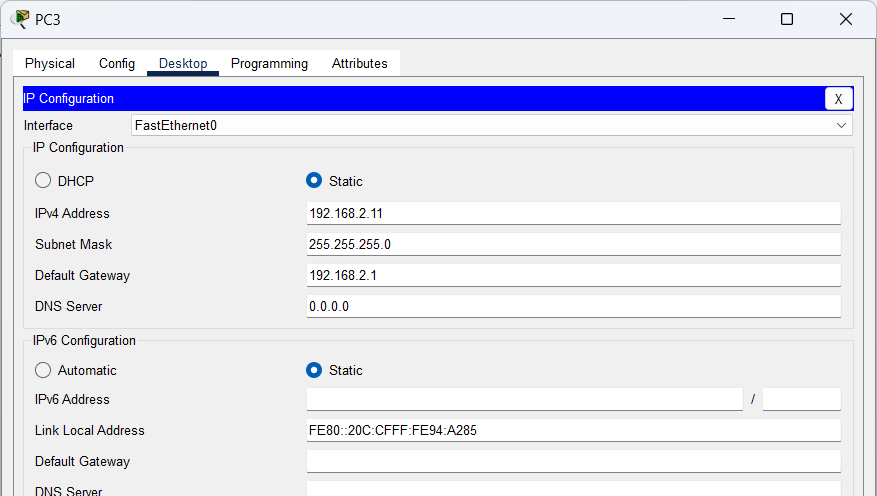
**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**

1. Now, manually configure the IP address for the PC’s and router. For PC’s connected to router 0, the default gateway should be 192.168.1.1



For devices connected to router 1, the default gateway should be 192.168.2.1



Assign the IP address accordingly.

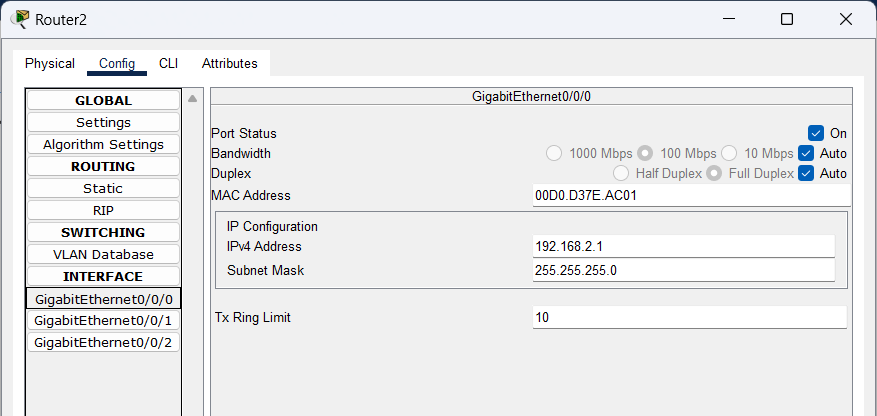
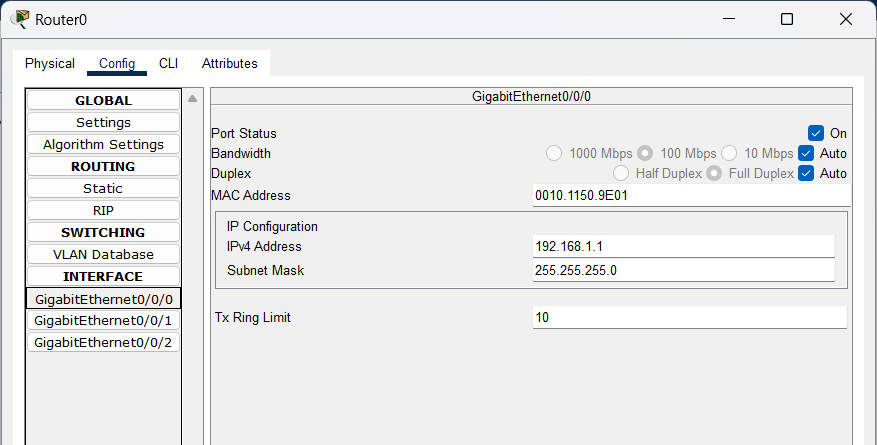
1. Next, Go to each Router interface and ensure you assign the correct IP addresses to the interfaces connected to the switches. Make sure to turn on the interfaces by clicking the checkmark. By default the switches would be connected through GigabitEthernet 0/0/0.

**Class:** **SYIT**

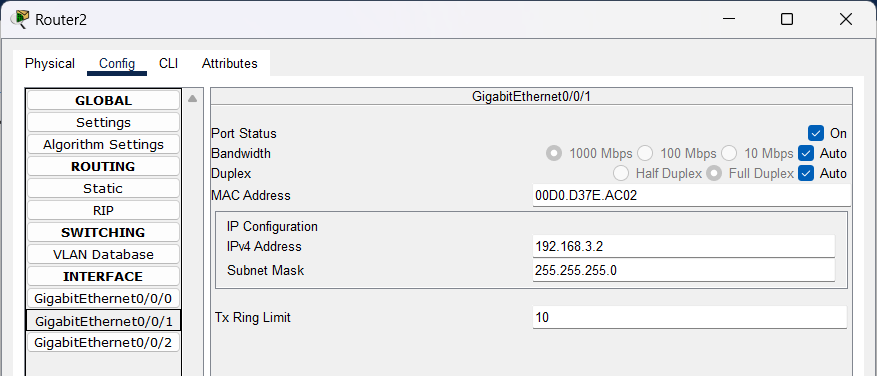
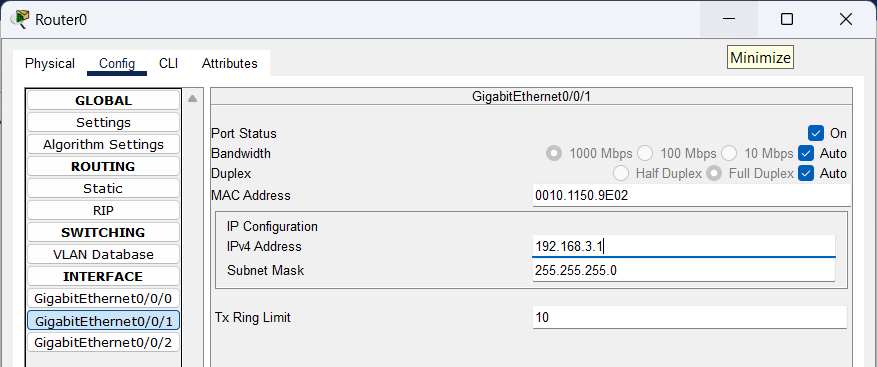
Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**



1. Now, setup GigabitEthernet 0/0/1, the connection between router 0 and router 1.



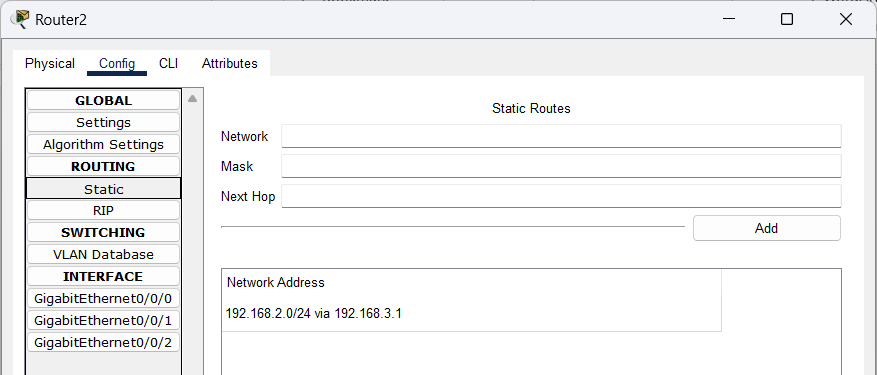
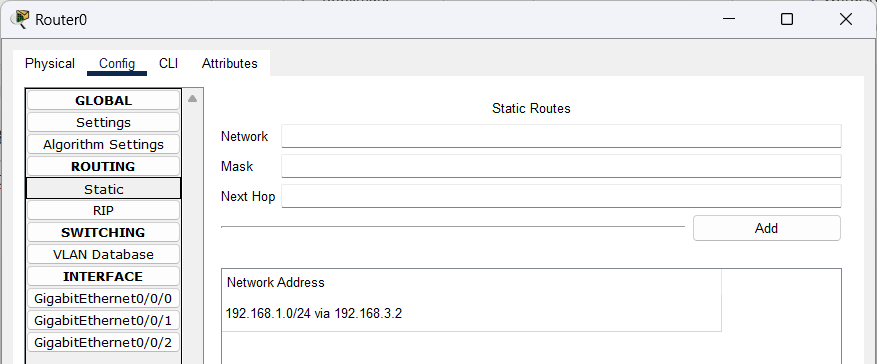
1. After configuring this connection, we can now setup the static routing addresses. In network enter the current network address of the router 192.168.1.0, mask as 255.255.255.0 and next hop as 192.168.3.2 (GigabitEthernet 0/0/1 address of router 1). Similarly do the same for router 1 and click add.

**Class:** **SYIT**

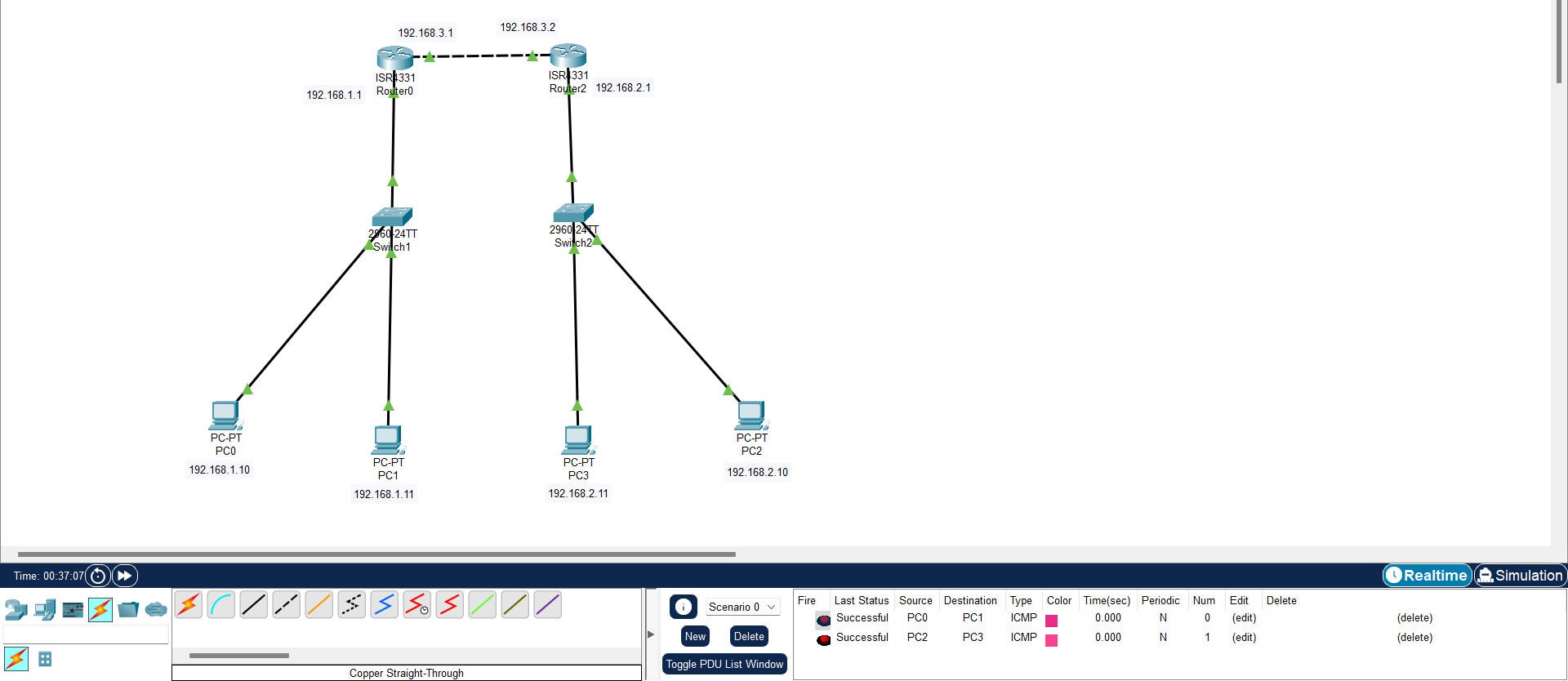
Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**



1. The two routers are now connected. You can use the PDU to test your connection, the result will be successful if the packet is delivered.



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**

Q. Using Cisco Packet Tracer configure IP Routing using RIP.

What is RIP routing?

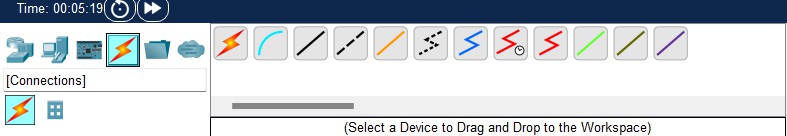
RIP (Routing Information Protocol) is a distance-vector routing protocol used to determine the best path for data to travel across a network. It is one of the oldest routing protocols and is mainly used in smaller, simpler networks.

Steps:

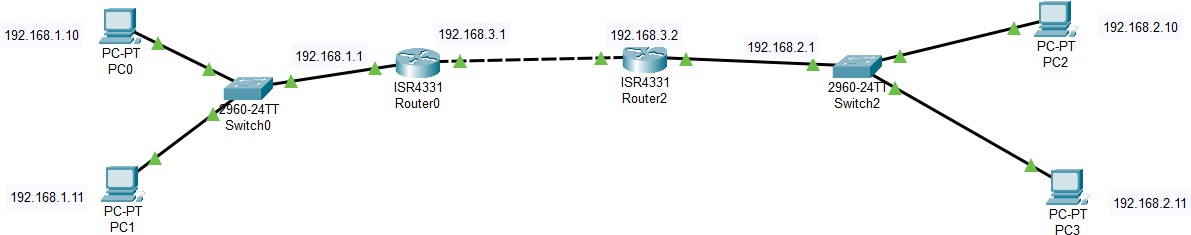
1. Open Cisco Packet Tracer and from Network Devices select one router, two switches and six end devices(4 PC’s & 2 laptop) from End Devices and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



1. Your schema should look something like this:



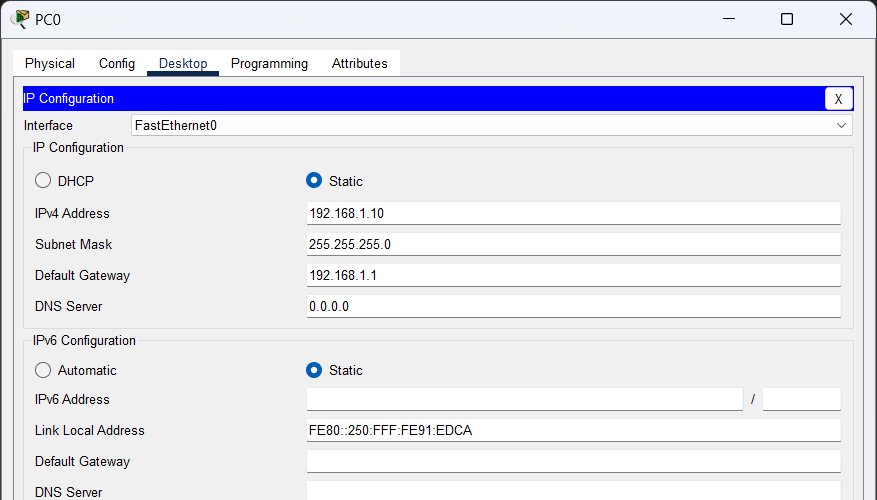
1. Now, manually configure the IP address for the PC’s and router. For PC’s connected to router 0, the default gateway should be 192.168.1.1

**Class:** **SYIT**

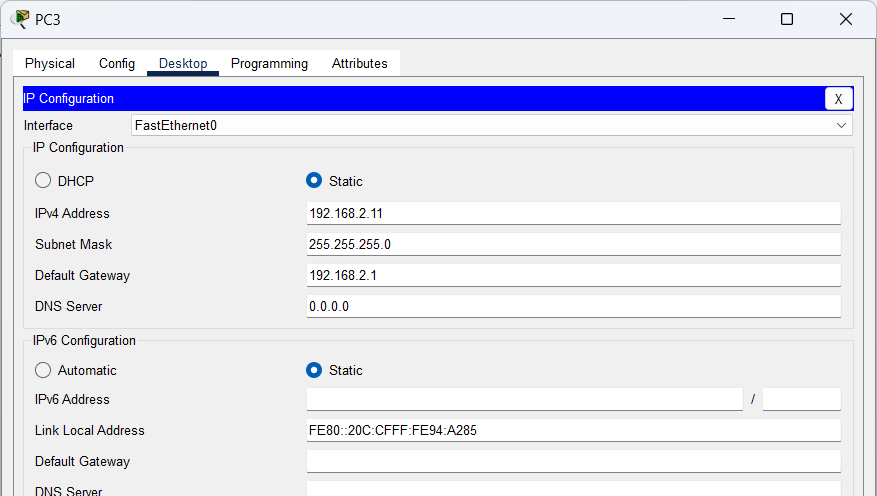
Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**

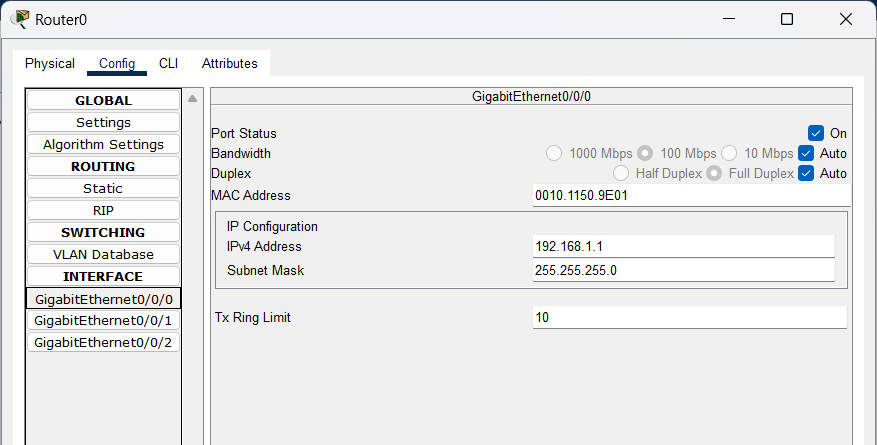


For devices connected to router 1, the default gateway should be 192.168.2.1



Assign the IP address accordingly.

1. Next, Go to each Router interface and ensure you assign the correct IP addresses to the interfaces connected to the switches. Make sure to turn on the interfaces by clicking the checkmark. By default the switches would be connected through GigabitEthernet 0/0/0.

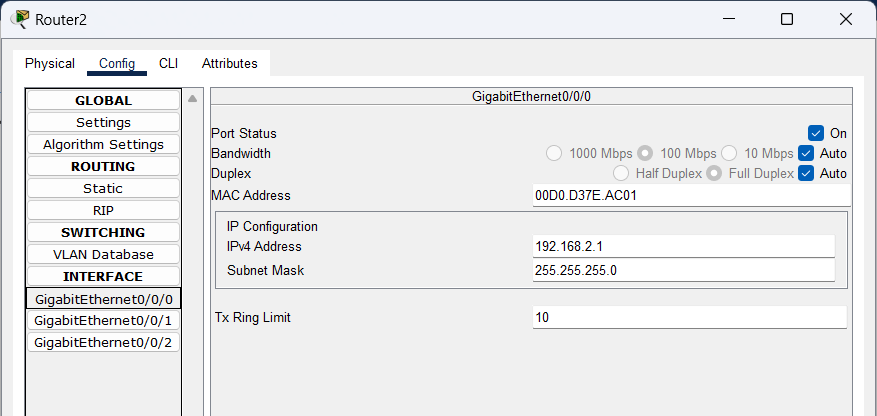


**Class:** **SYIT**

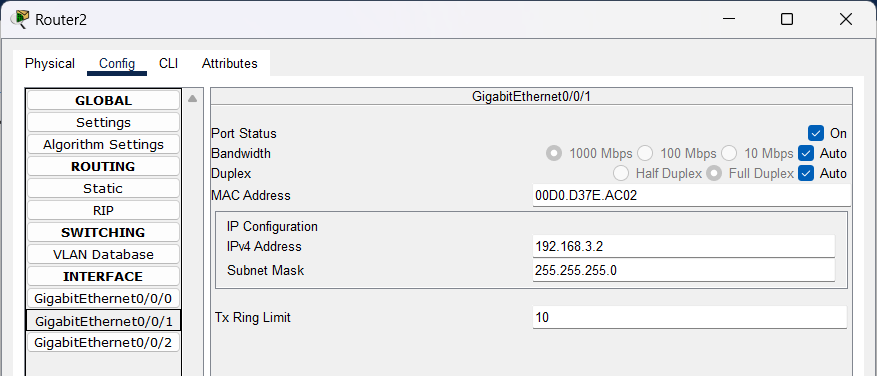
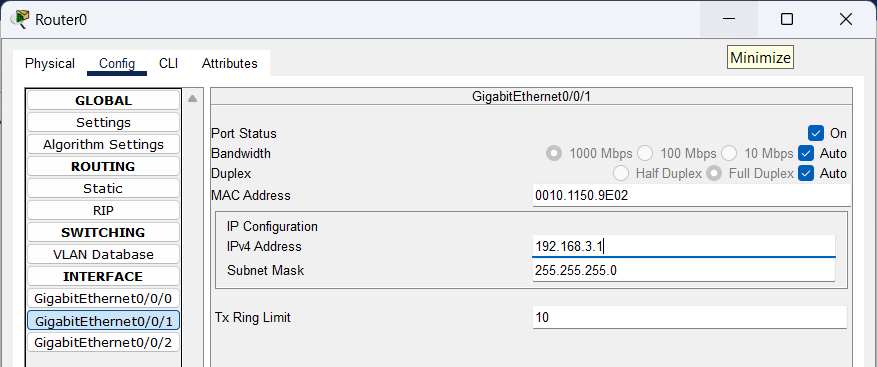
Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

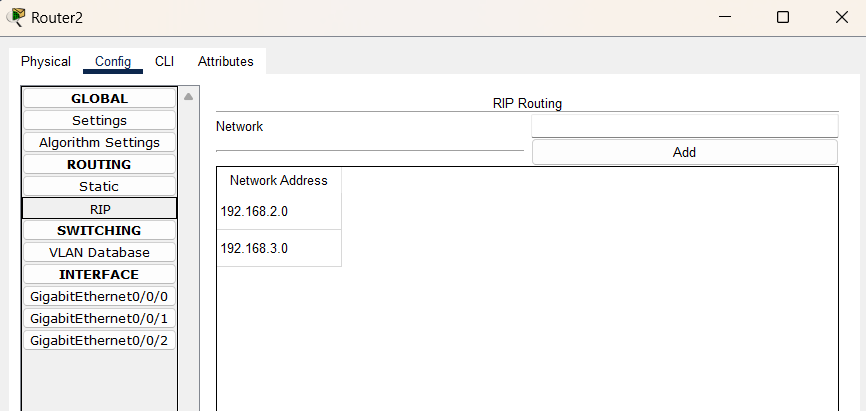
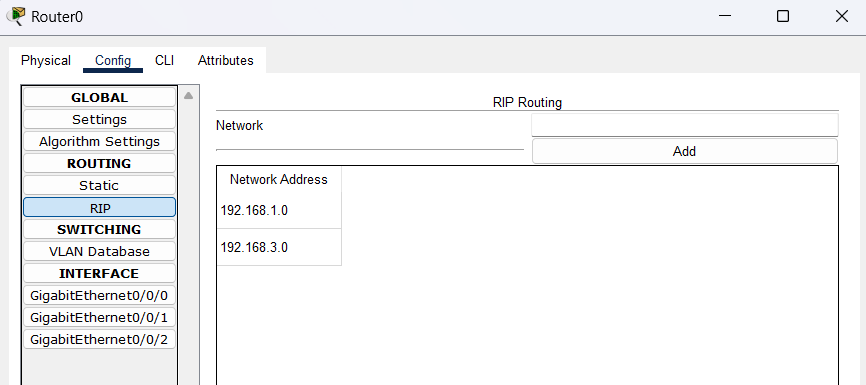
**Practical** **Number:-** **06**



1. Now, setup GigabitEthernet 0/0/1, the connection between router 0 and router 1.



1. After configuring this connection, we can now setup the RIP. Go to router 0 > config > RIP. Over there, enter the network address you want the data to route from. i.e the current network address 192.168.1.0 and the address of router 1’s interface i.e 192.168.3.0 Do the same for router 1.



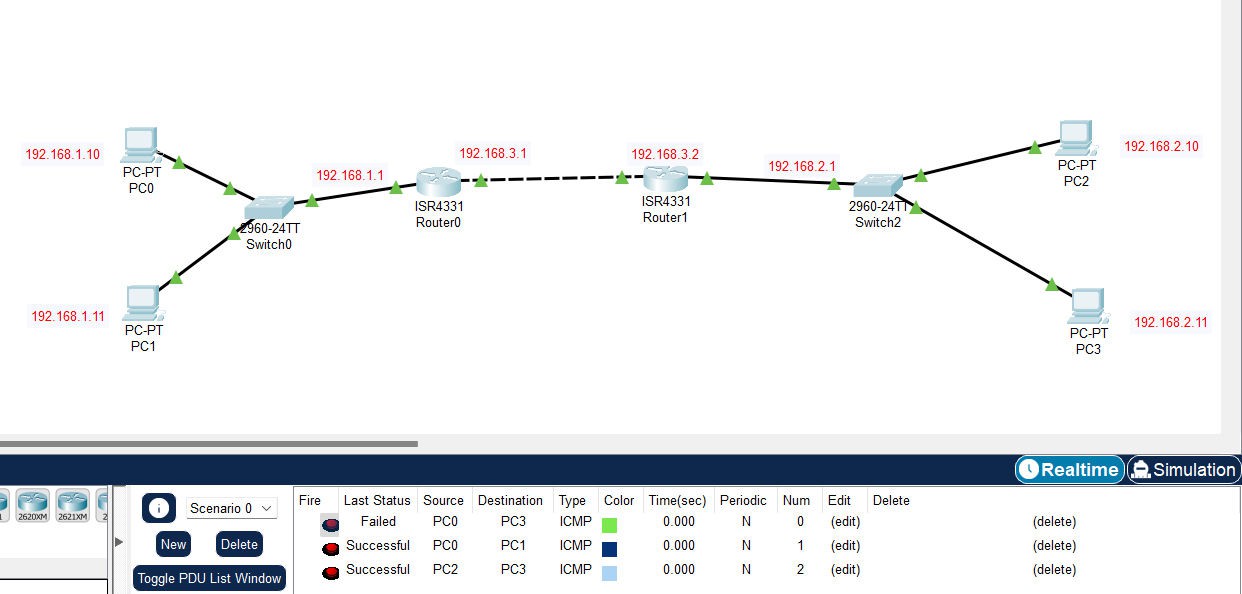
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 13-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **06**

1. The two routers are now connected. You can use the PDU to test your connection, the result will be successful if the packet is delivered.



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **08**

Q. Using Cisco Packet Tracer configure simple OSPF.

What is OSPF?

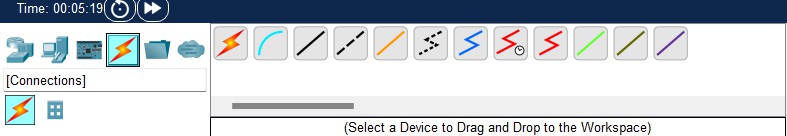
OSPF (Open Shortest Path First) is a routing protocol used in IP networks to find the best path for data to travel. It uses link-state information and calculates the shortest path to each destination based on the Dijkstra algorithm. OSPF is dynamic, meaning it automatically updates routing information when network changes occur. It is widely used in larger enterprise networks because it supports hierarchical network design and scales efficiently.

**Steps:**

1. Open Cisco Packet Tracer and from Network Devices select one router, two switches and six end devices(4 PC’s & 2 laptop) from End Devices and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



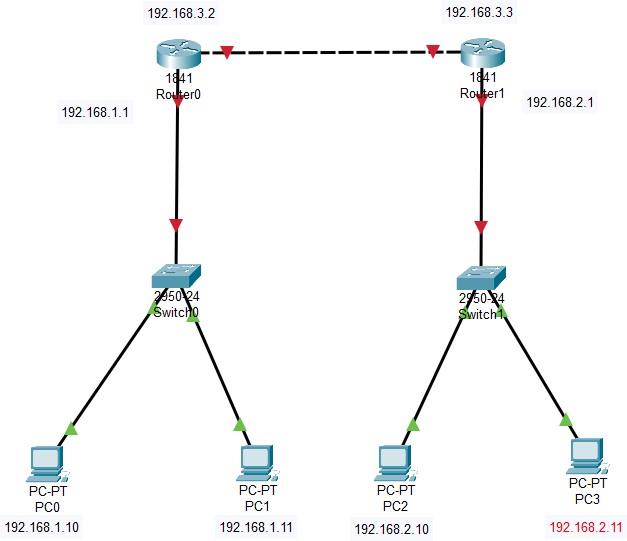
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-08-2024

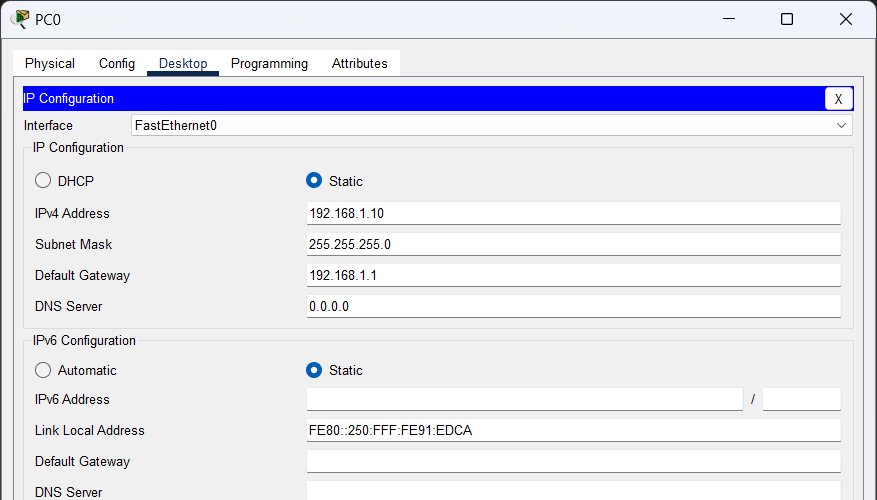
**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **08**

1. Your schema should look something like this:



1. Now, manually configure the IP address for the PC’s and router. For PC’s connected to router 0, the default gateway should be 192.168.1.1



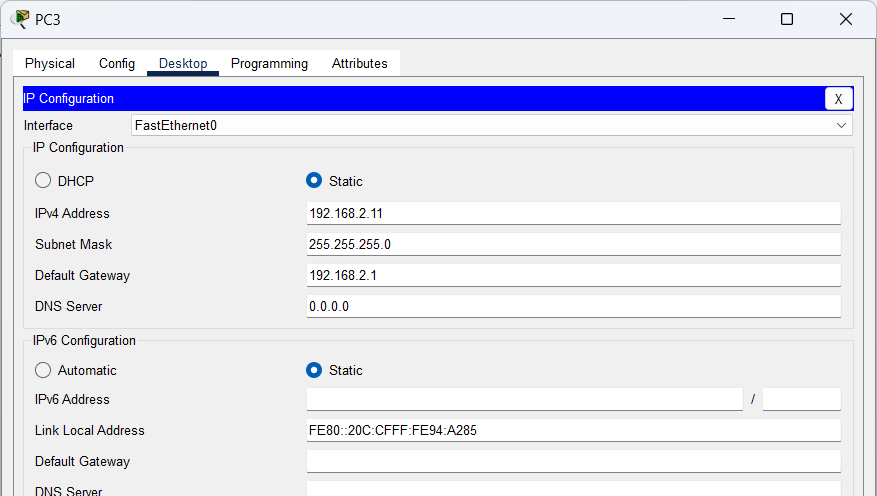
For devices connected to router 1, the default gateway should be 192.168.2.1

**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-08-2024

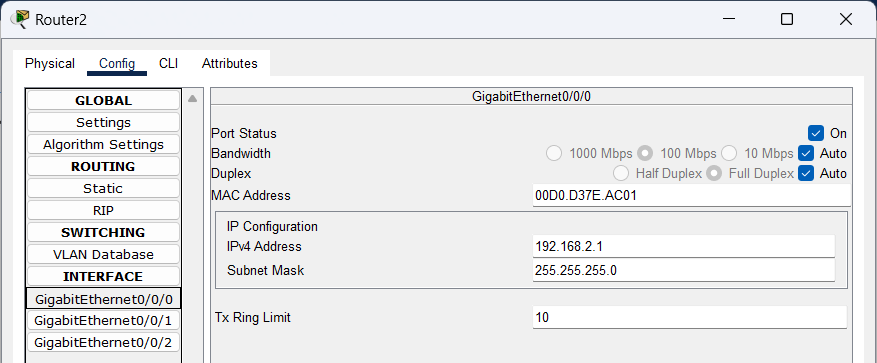
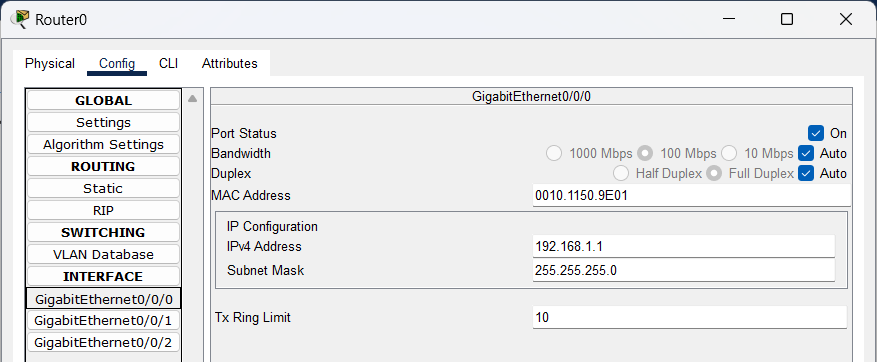
**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **08**

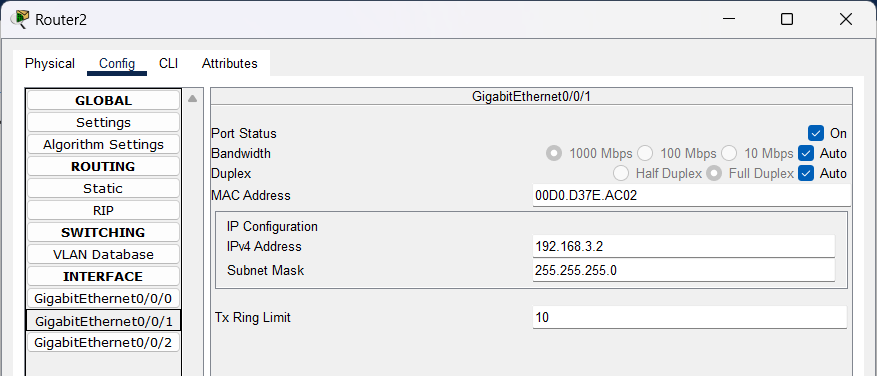
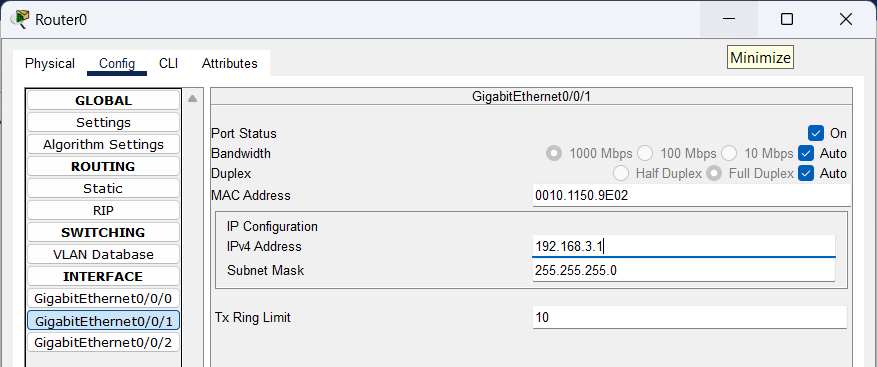


Assign the IP address accordingly.

1. Next, go to each Router interface and ensure you assign the correct IP addresses to the interfaces connected to the switches. Make sure to turn on the interfaces by clicking the checkmark. By default the switches would be connected through GigabitEthernet 0/0/0.



1. Now, setup GigabitEthernet 0/0/1, the connection between router 0 and router 1.



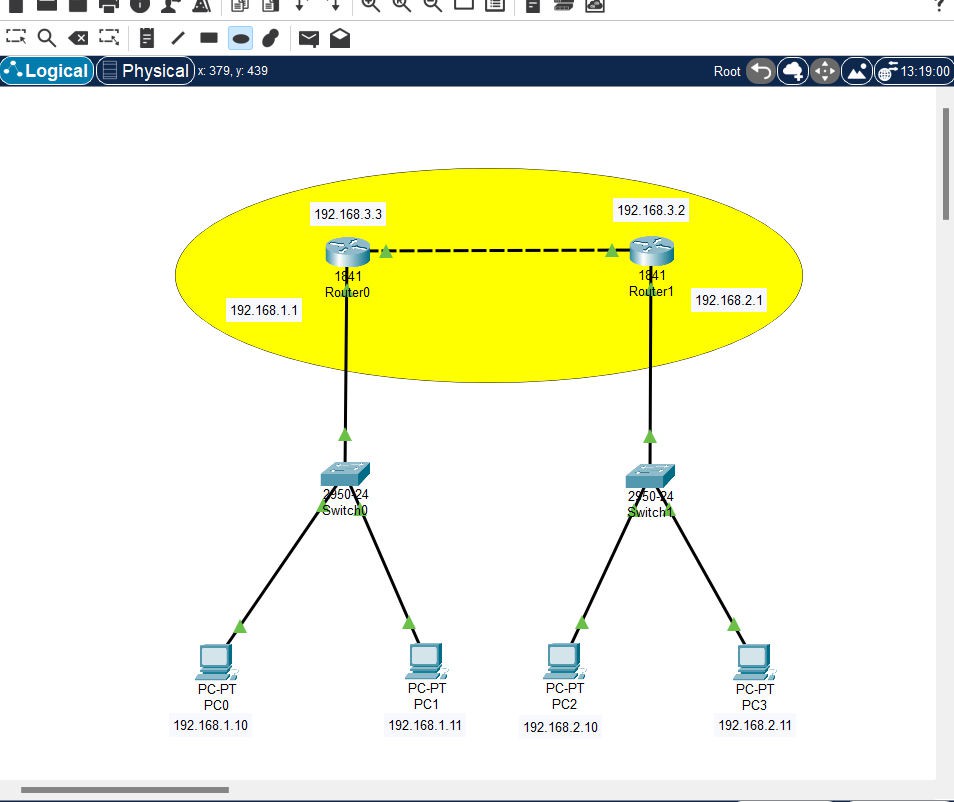
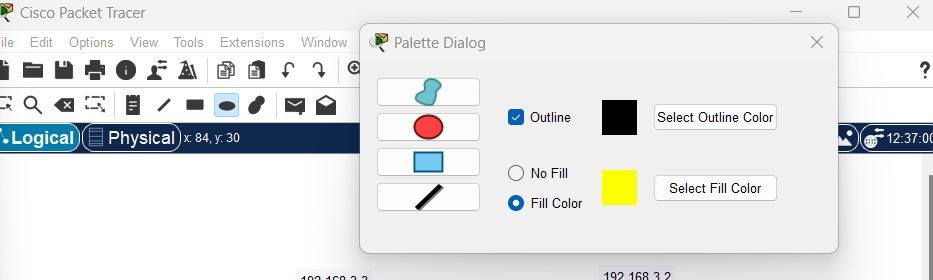
1. Now, to transfer the message from router 0 to router 1 you need to setup the path of delivery, in this case we’re gonna use OSFP. For this we need to define an area. Select Pallet Dialog to create a visual area.

**Class:** **SYIT**

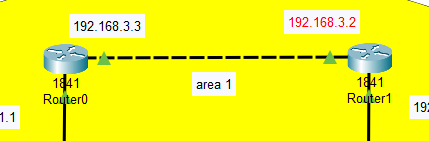
Sem: III Roll No.: SYIT33 Date : 20-08-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **08**



1. Next, use the note feature to name the area as ‘area 1’.



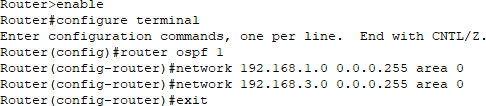
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-08-2024

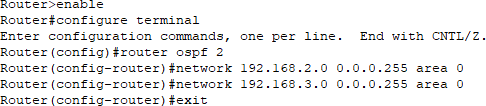
**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **08**

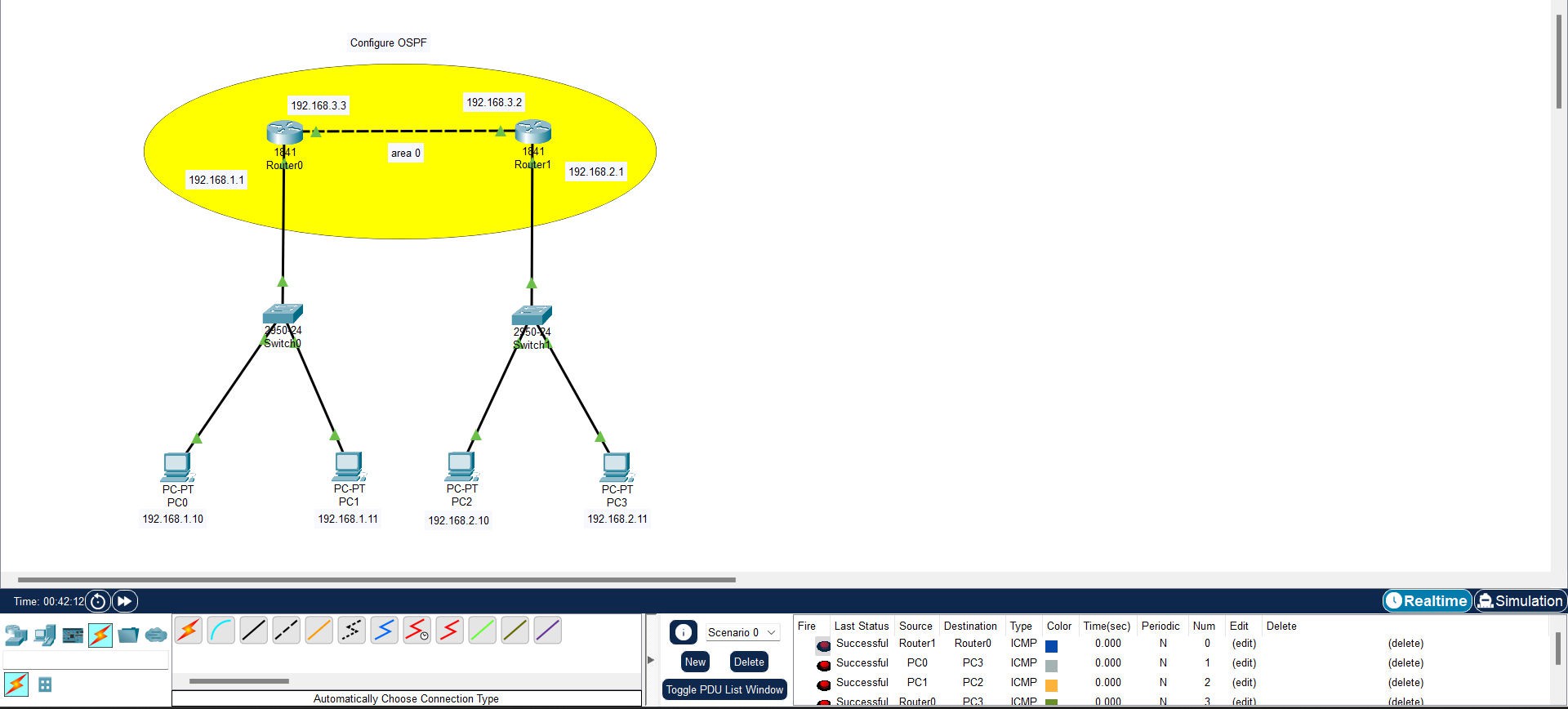
1. Now configure the pathway of router 0 using CLI.



Now configure the pathway of router 1 using CLI.



1. The two routers are now connected. You can use the PDU to test your connection, the result will be successful if the packet is delivered.



**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-09-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **09**

Q. Using Cisco Packet Tracer configure DHCP Server and Client.

What is DHCP?

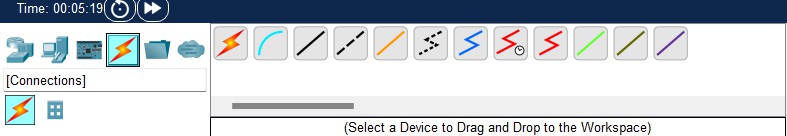
DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. This allows devices like computers, phones, or printers to communicate on a network without needing manual IP configuration.

**Steps:**

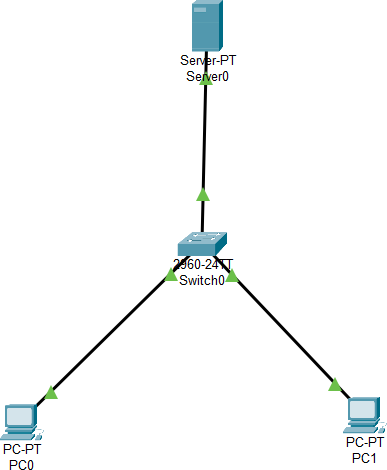
1. Open Cisco Packet Tracer and from Network Devices select one server, one switch, 2 PC’s and place them in the empty canvas.



1. Click on the Connections icon and select either ‘Copper straight-through’ or ‘Automatically choose connection type’ and using them connect the switches, routers and the end nodes.



1. Your schema should look something like this:



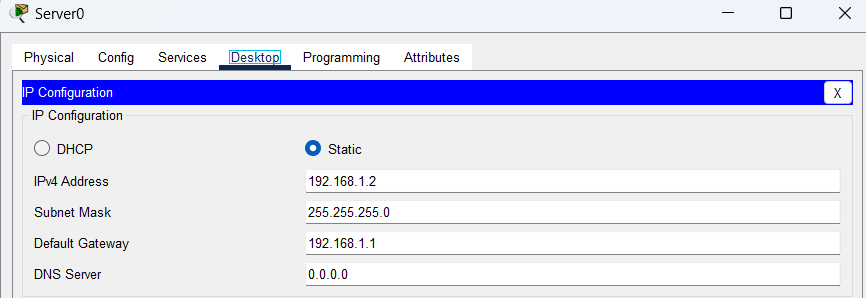
**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-09-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **09**

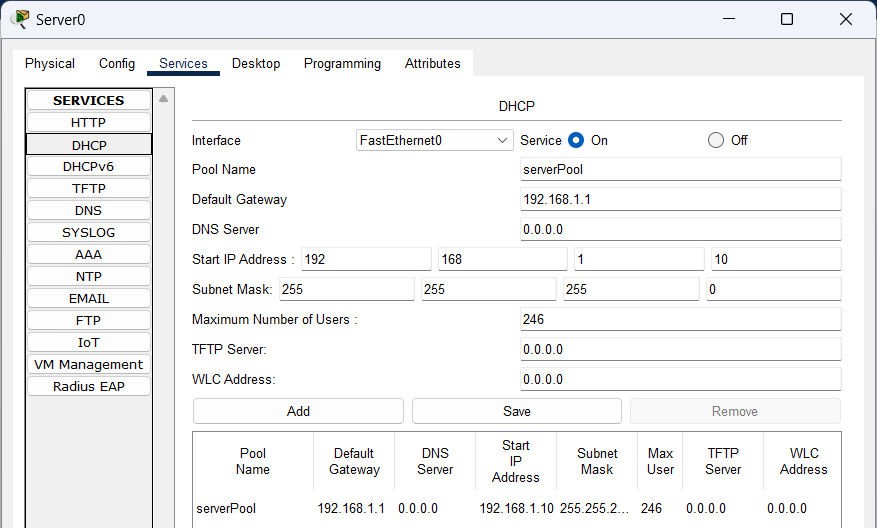
1. Assign IP Addresses to Devices. The server will act as the DHCP server, and the two PCs will receive dynamic IP addresses from it. First configure the IP address of the server.



1. Configure the Server to Act as a DHCP Server. Select the Server 0 in your Packet Tracer simulation. Go to the Services tab. Click on DHCP. Turn on the DHCP Service. Configure a DHCP Pool:

Set the Start IP Address (e.g., 192.168.1.10). Set the Subnet Mask (e.g., 255.255.255.0). Set the Default Gateway (e.g., 192.168.1.1). Add DNS Server if needed (optional).

And click on save.



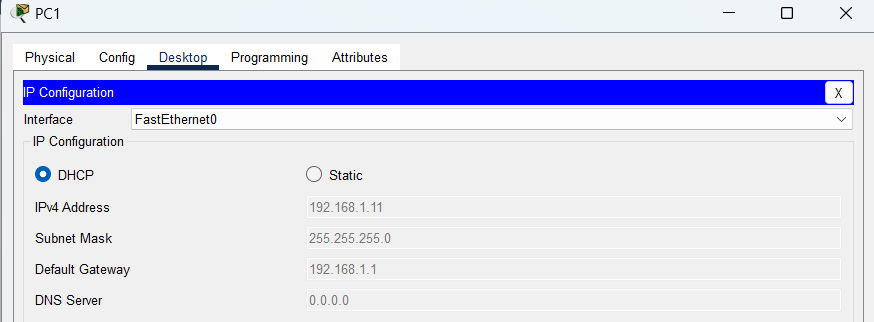
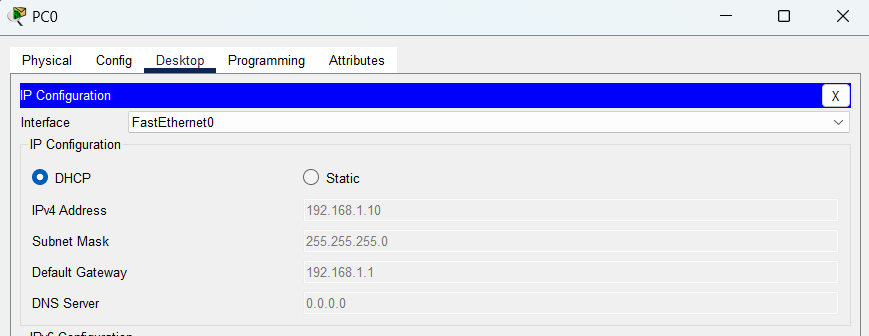
1. Configure the PCs to Obtain IP Addresses Dynamically. Click on PC0 and then go to the Desktop tab. Select IP Configuration and choose DHCP. Repeat this for PC1. The PCs should now receive IP addresses from the server.

**Class:** **SYIT**

Sem: III Roll No.: SYIT33 Date : 20-09-2024

**Course** **Name:** **Computer** **Network** **Page no:**

**Practical** **Number:-** **09**



1. After configuring everything, you can use the PDU to verify if the PCs are receiving IP addresses from the DHCP server and the message is being transferred.

