SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

FACULTY OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTING

18CSS202J COMPUTER COMMUNICATIONS

LAB MANUAL

Course Code	18CSS202J	Course Name	COMPUTER COMMUNICATIONS	Course Category	S	*Engineering Sciences*	L	T	P	C
							2	0	2	3

Pre-requisite Courses	*Nil*	Co-requisite Courses	*Nil*	Progressive Courses	*Nil*
Course Offering Department	*Computer Science and Engineering*	Data Book / Codes/Standards	*Nil*		

Course Learning Rationale (CLR):	*The purpose of learning this course is to:*	Learning		
		1	2	3
CLR-1 :	*Understand the basic services and concepts related to Internetwork*	Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLR-2 :	*Understand the layered network architecture*			
CLR-3 :	*Acquire knowledge in IP addressing*			
CLR-4 :	*Exploring the services and techniques in the physical layer*			
CLR-5 :	*Understand the functions the of Data Link layer*			
CLR-6 :	*Implement and analyze the different Routing Protocols*			

Course Learning Outcomes (CLO):	*At the end of this course, learners will be able to:*	Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	*Apply the knowledge of communication*	*2*	*80*	*70*
CLO-2 :	*Identify and design the network topologies*	*3*	*85*	*75*
CLO-3 :	*Design the network using addressing schemes*	*3*	*75*	*70*
CLO-4 :	*Identify and correct the errors in transmission*	*1*	*85*	*80*
CLO-5 :	*Identify the guided and unguided transmission media*	*1*	*85*	*75*
CLO-6 :	*Design and implement the various Routing Protocols*	*3*	*80*	*70*

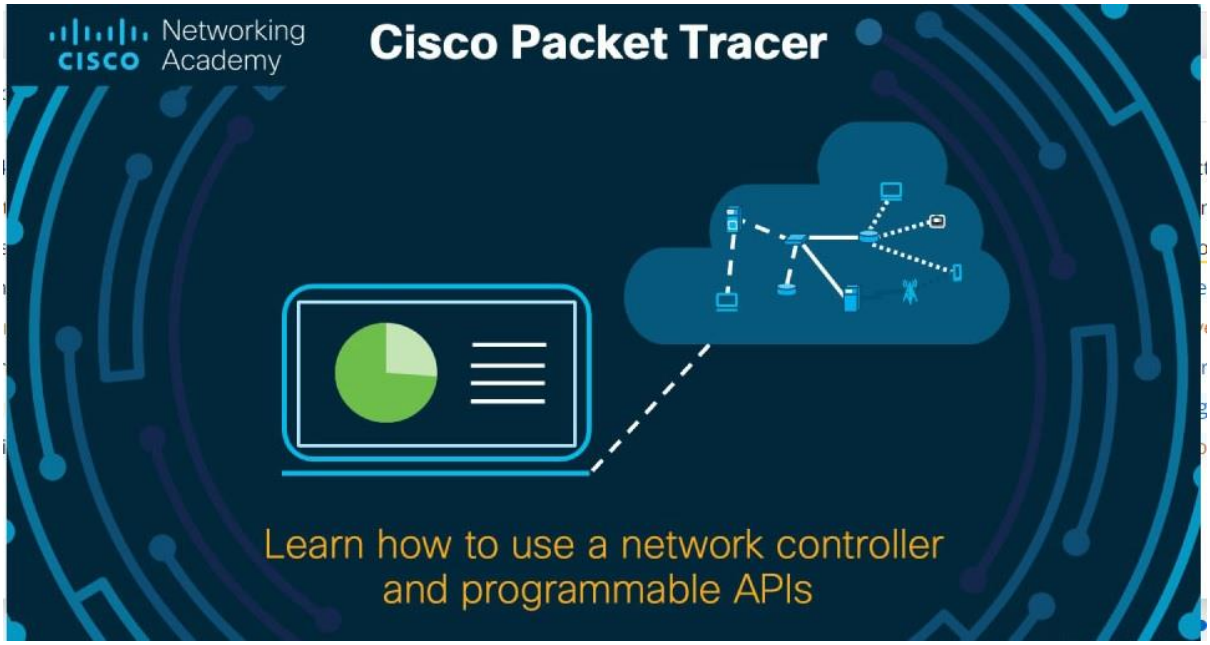
Program Learning Outcomes (PLO)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life-Long Learning	PSO - 1	PSO - 2	PSO – 3
CLO-1 :	*H*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-2 :	*H*	-	*H*	-	-	-	-	-	-	-	-	-	*M*	-	-
CLO-3 :	*H*	*H*	-	-	-	-	-	-	-	-	-	-	*M*	-	*M*
CLO-4 :	*H*	*H*	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-5 :	*H*	-	-	*H*	-	-	-	-	-	-	-	-	-	-	-
CLO-6 :	*H*	*H*	*H*	*H*	*H*	-	-	-	-	-	-	-	*M*	-	*M*

Session 2 Periods	Exercise	CLO	Page No
Lab 1	1.a - Introduction to Packet Tracer		
	1.b - Networking Commands (Windows/ Unix)		
Lab 2	Cabling the Devices		
	2. a - Demonstration of cross over cable with P-P network		
	2 .b - Demonstration of straight-through cable with local area network		
Lab 3	Configuration of IP Address in Router		
Lab 4	Subnetting in WAN Configuration (DTE and DCE)		
Lab 5	5. a - VLAN Switch Configuration		
	5. b - Router Configuration through a Console cable		
Lab 6	6. a Demonstration of Static Routing		
	6. b Demonstration of Default Routing		
Lab 7	7. a Demonstration of RIP v1		
	7. b Demonstration of RIP v2		
Lab 8	EIGRP Configuration, Bandwidth, and Adjacencies		
Lab 9	EIGRP Authentication and Timers		
Lab 10	Single-Area OSPF Link Costs and Interface		
Lab 11	Multi-Area OSPF with Stub Areas and Authentication		
Lab 12	Examining Network Address Translation (NAT)		
Lab 13	BGP Configuration		
Lab 14	Mini - Project Review		
Lab 15	Mini – Project Review		
Model Practical Examination			
End Semester Practical Examination			

SESSION 1

1.1 INTRODUCTION TO PACKET TRACER

Cisco Packet Tracer is a free application that enables you to practice network configuration and troubleshooting on your desktop or laptop computer. It enables you to mimic networks without having physical access to the underlying hardware. Along with networking, you may improve your Internet of Things (IoT) and cybersecurity skills through education and practice. You have the option of creating a network from scratch, using a pre-built sample network, or completing lab projects. While Packet Tracer is not a substitute for practising on physical routers, switches, firewalls, and servers, it does offer a number of advantages.

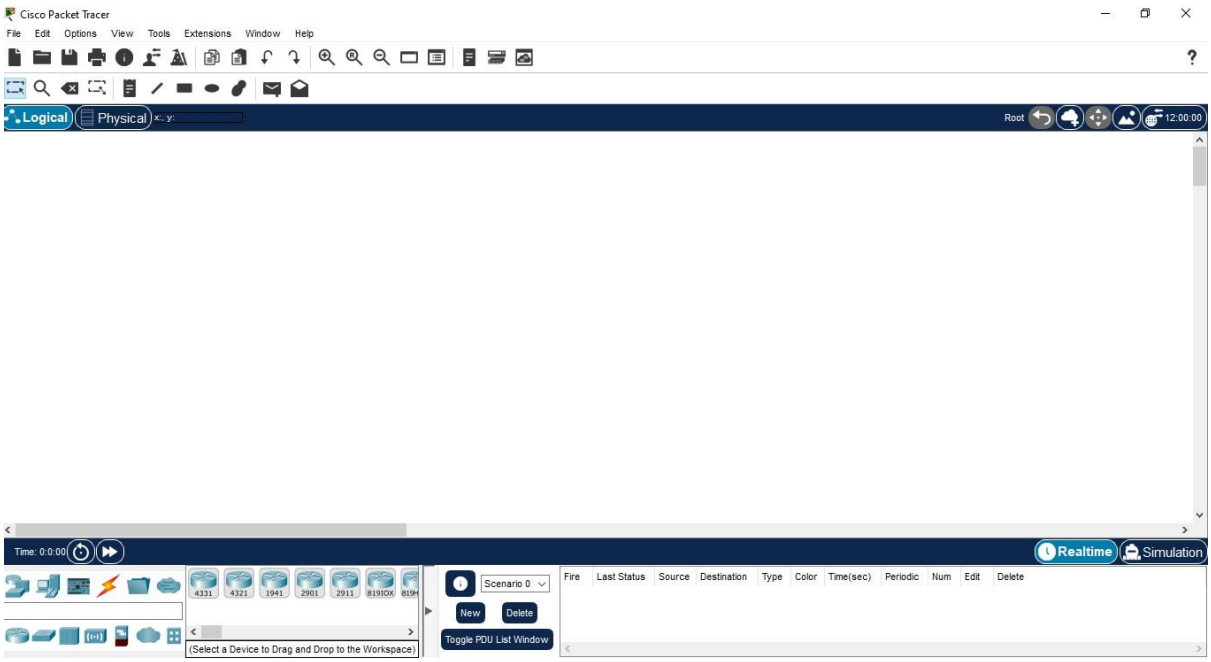


1.a What are the Benefits of Using Packet Tracer?

Imagine being able to peer inside a small business network or the internet. Have you ever wished to create an Internet of Things system that would notify you through the phone if there was an issue in your home environment? Welcome to Cisco Packet Tracer, the simulation environment that may assist you in doing all of these tasks and more. It is intended to familiarize you with the Cisco Packet Tracer network simulation and visualization tool.

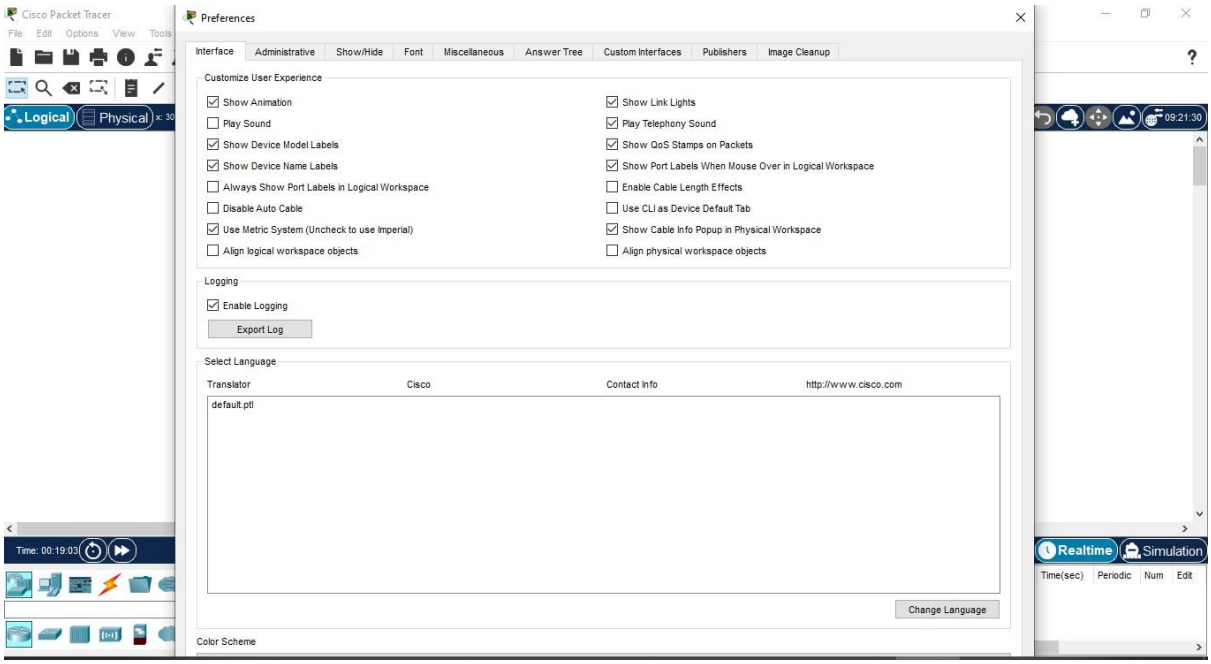
In Packet Tracer, you will design your own network (PT). Additionally, you will learn about the many sorts of PT files.

1.b Packet Tracer UI:



Packet Tracer is a tool that allows you to simulate real networks. It provides three main menus that you can use for the following:

- Add devices and connect them via cables or wireless.
- Select, delete, inspect, label, and group components within your network.
- Manage your network.



The network management menu lets you do the following:

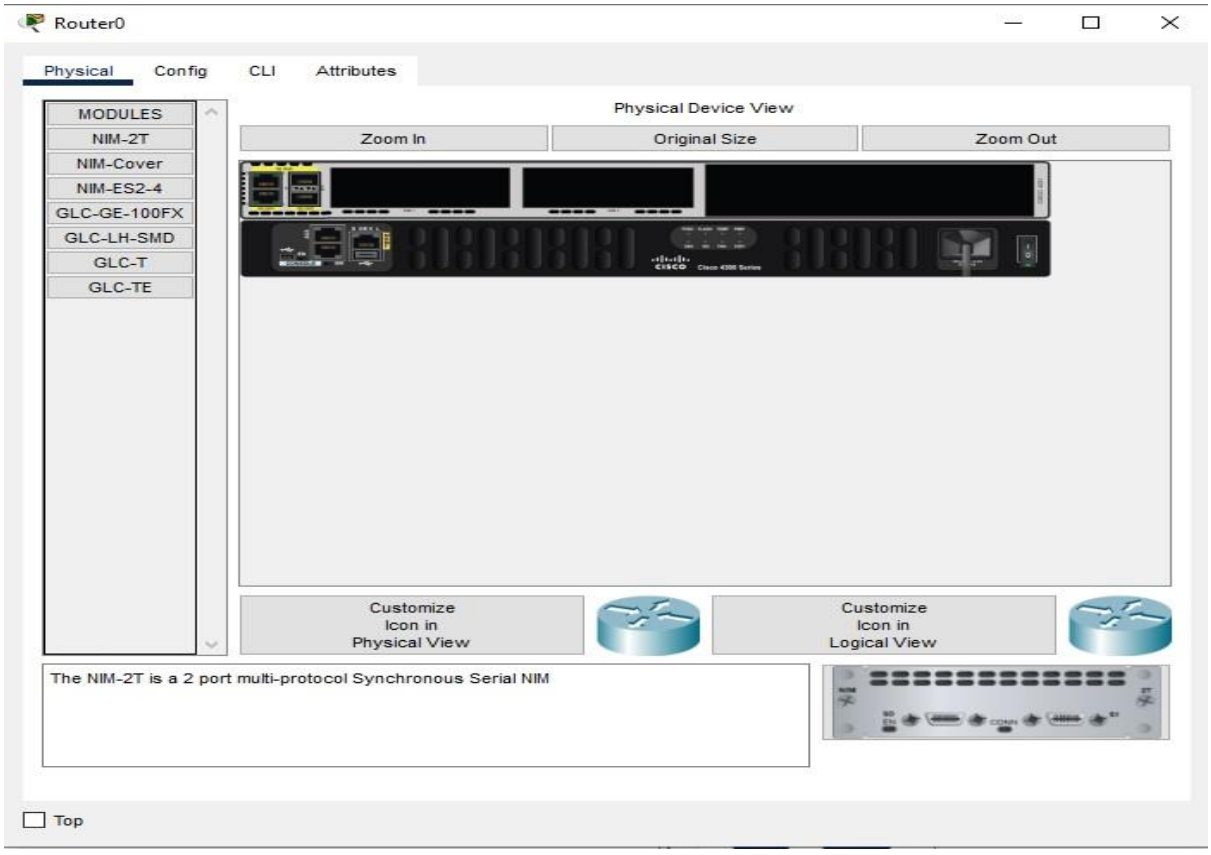
- Open an existing/sample network.
- Save your current network.
- Modify your user profile or your preferences.

Packet Tracer also provides a variety of tabs for device configuration including the following:

- Physical
- Config
- CLI
- Desktop
- Services

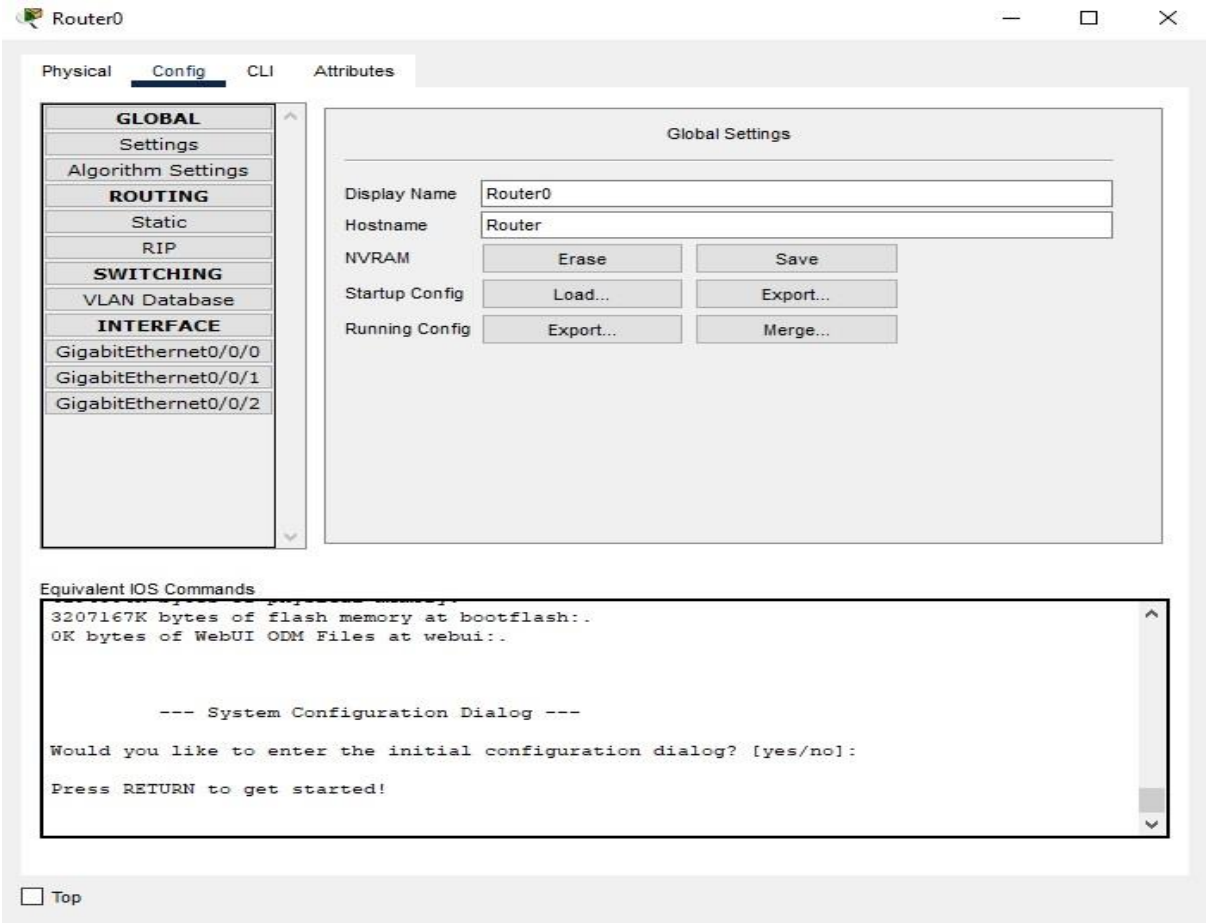
The tabs that are shown depend on the device you are currently configuring.

Physical Tab



The Physical tab provides an interface for interacting with the device including powering it on or off or installing different modules, such as a wireless network interface card (NIC).

Config Tab

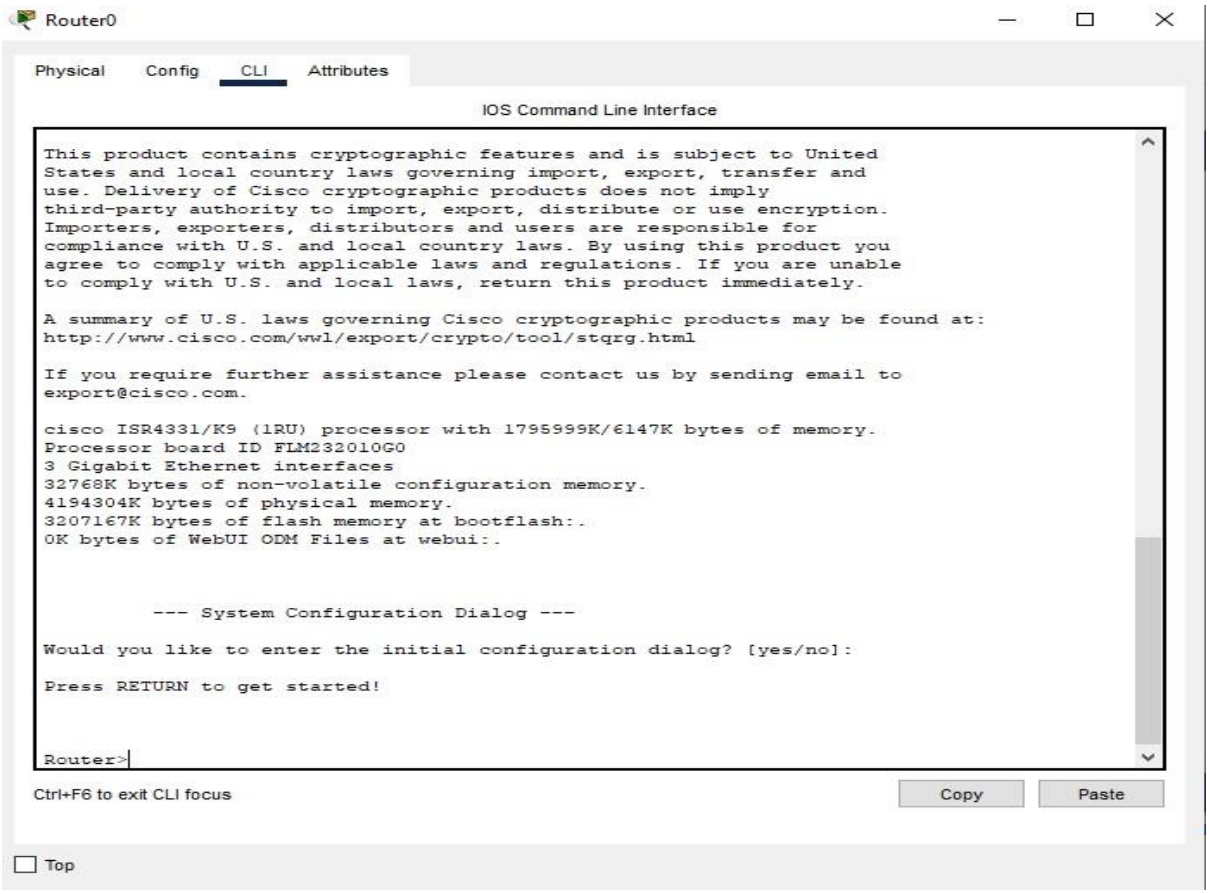


For intermediate devices such as routers and switches, there are two ways to access device configurations. Configurations can be accessed via a Config tab, which is a Graphical User Interface (GUI). Configurations can also be accessed using a command line interface (CLI).

The Config tab does not simulate the functionality of a device. This tab is unique to Packet Tracer. If you don't know how to use the command line interface, this tab provides a way to use a Packet Tracer-only GUI to configure basic settings. As settings are changed in the GUI, the equivalent CLI commands appear in the Equivalent IOS Commands window. This helps you to learn the CLI commands and the Cisco Internetwork Operating System (IOS) while you are using the Config tab.

For example, in the figure, the user has configured MyRouter as the name of the device. The Equivalent IOS Commands window shows the IOS command that achieves the same results in the CLI. In addition, device configuration files can be saved, loaded, erased, and exported here.

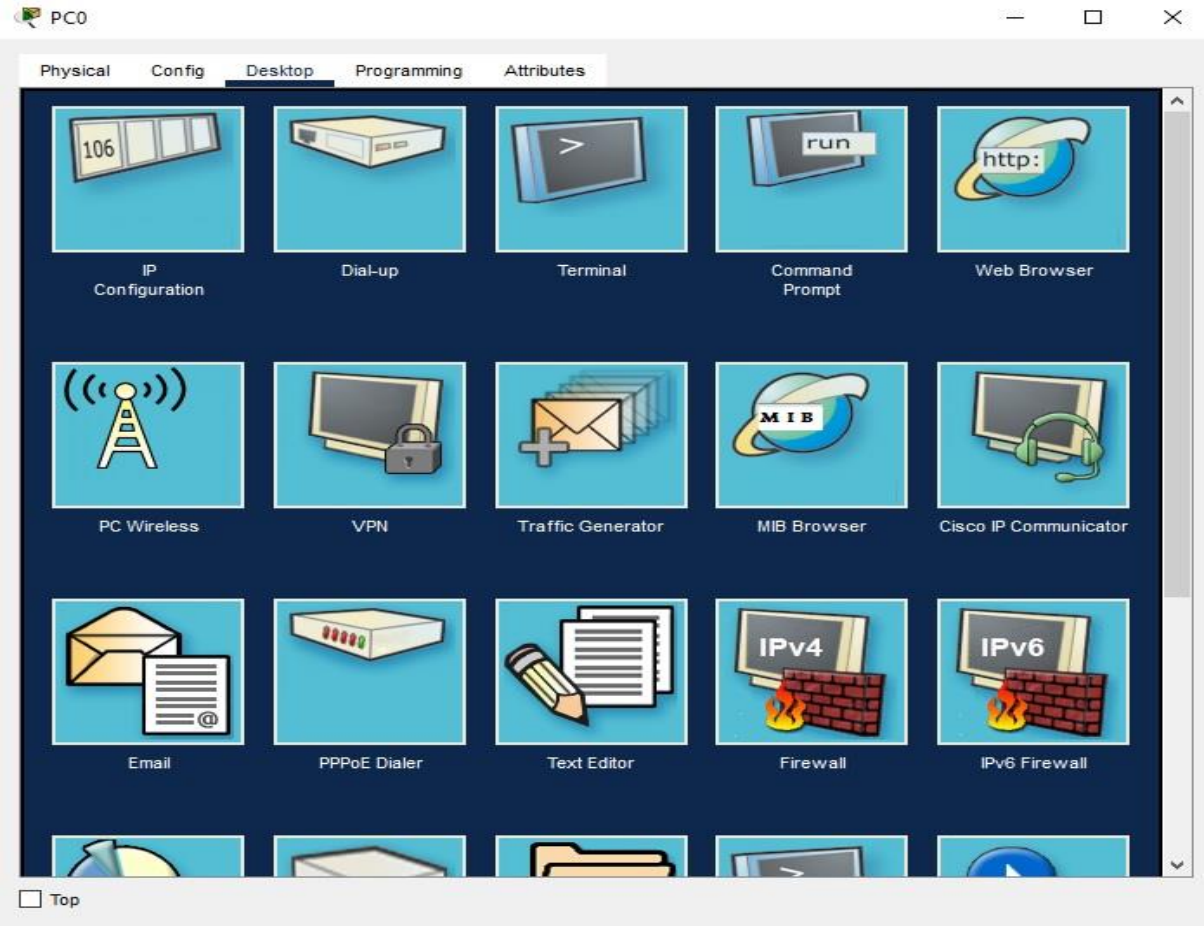
CLI Tab



The CLI tab provides access to the command line interface of a Cisco device. Using the CLI tab requires knowledge of device configuration with IOS. Here, you can practice configuring Cisco devices at the command line. CLI configuration is a necessary skill for more advanced networking implementations.

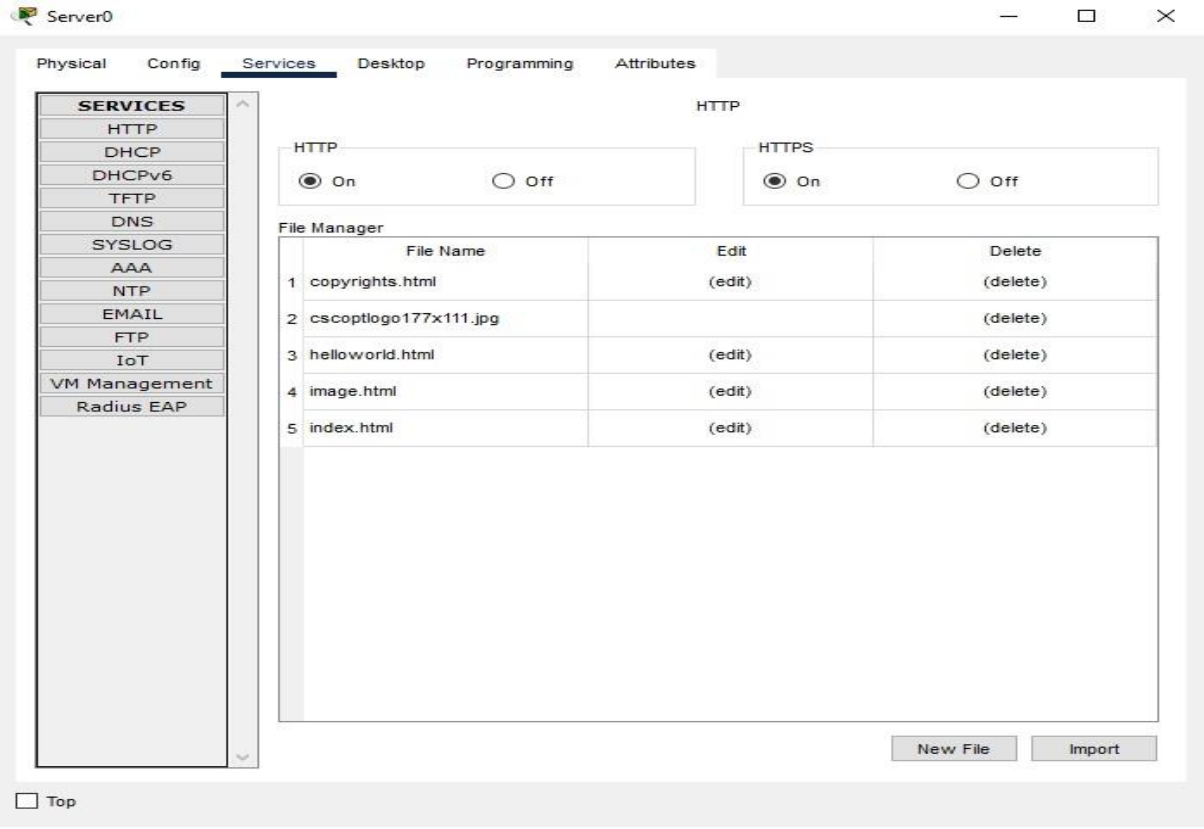
Note: Any commands that were entered from the Config tab are also shown in the CLI tab.

Desktop Tab



For some end devices, such as PCs and laptops, Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a web browser, and other applications.

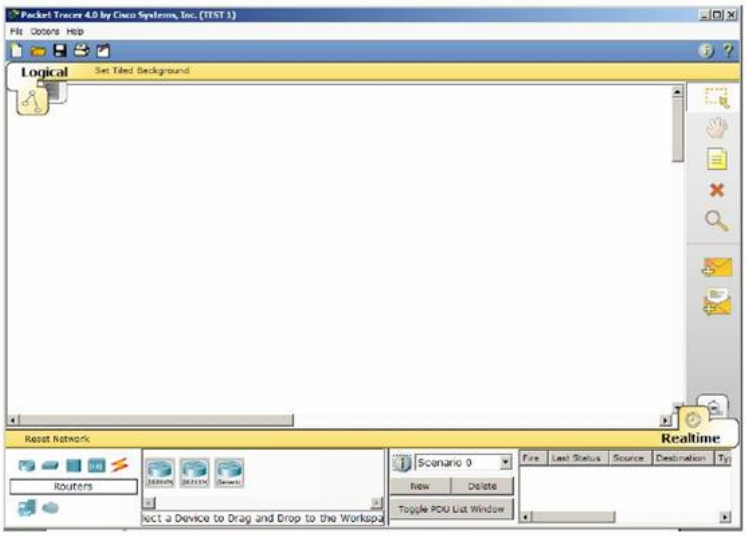
Services Tab



A server has all of the functions of a host with the addition of one more tab, the Services tab. This tab allows a server to be configured with common server processes such as HTTP, DHCP, DNS, or other services, as shown in the figure.

1.3 Demonstration of Packet Tracer Interface using a Hub Topology

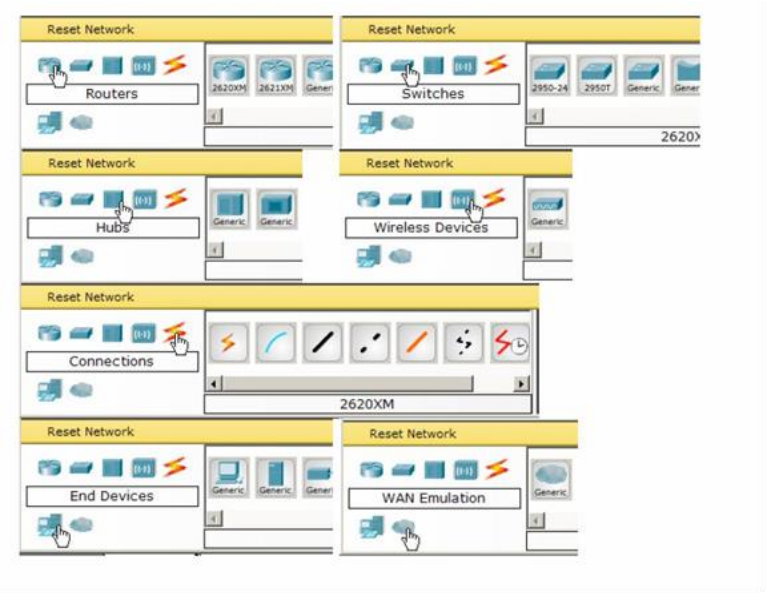
Step 1: Start Packet Tracer and Enter Simulation Mode



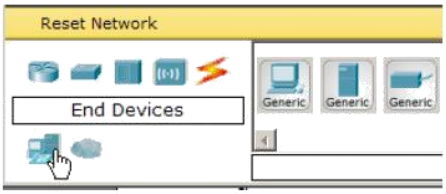
Step 2: Choosing Devices and Connections

We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, Hubs, and Connections.

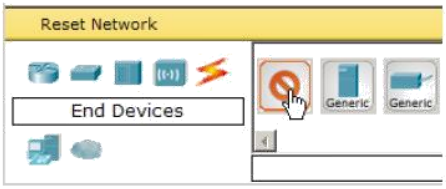
A single click on each group of devices and connections to display the various choices.



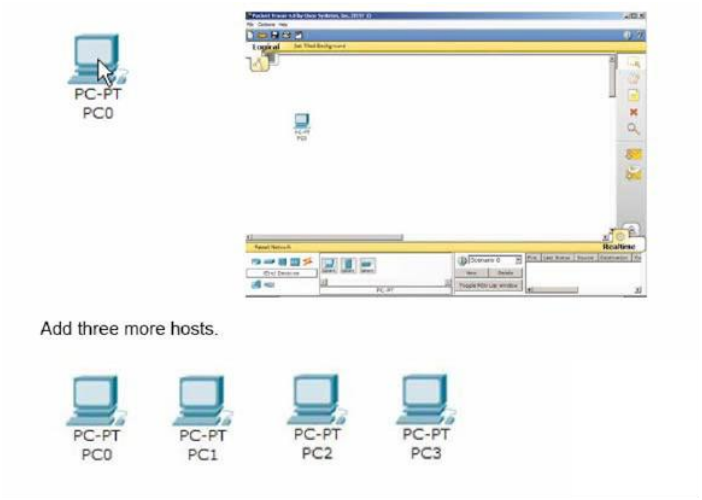
Step 3: Building the Topology – Adding Hosts Single click on the End Devices.



Single click on the **Generic** host.

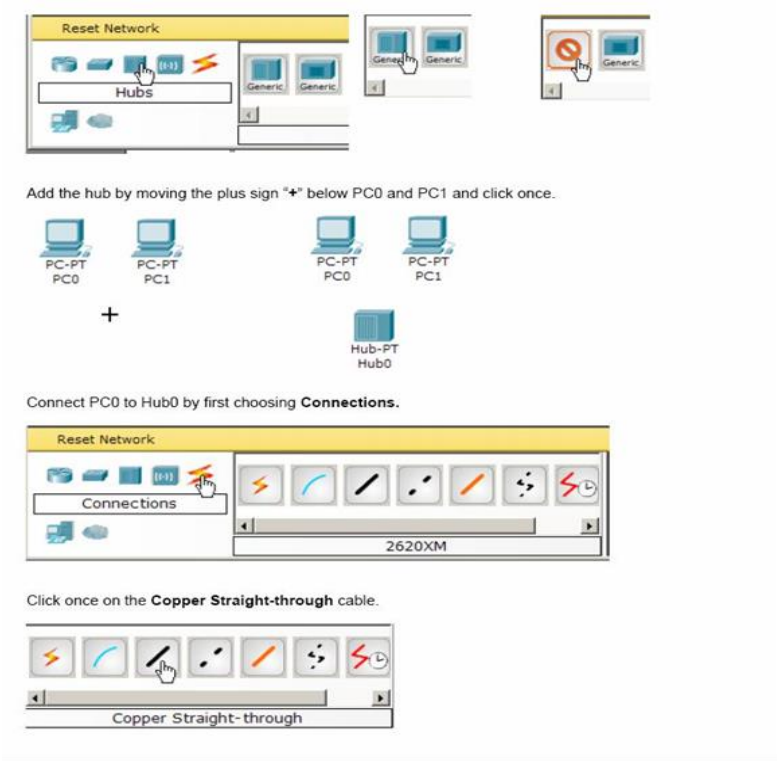


Move the cursor into the topology area. You will notice it turns into a plus "+" sign. Single-click in the topology area and it copies the device.



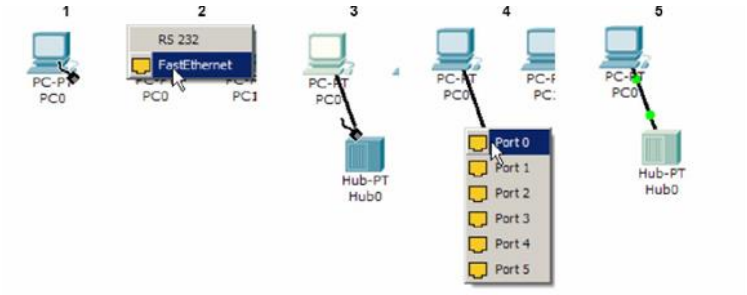
Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

Adding a Hub - Select a hub, by clicking once on Hubs and once on a Generic hub.

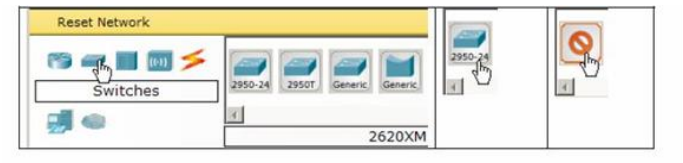


Perform the following steps to connect PC0 to Hub0:

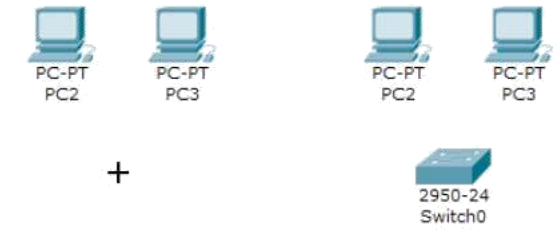
1. Click once on PC0
2. Choose FastEthernet
3. Drag the cursor to Hub0
4. Click once on Hub0 and choose Port 0
5. Notice the green link lights on both the PC0 Ethernet NIC and the Hub0 Port 0 showing that the link is active.



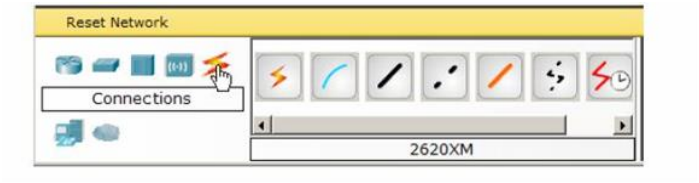
Adding a Switch - Select a switch, by clicking once on Switches and once on a 2950-24 switch.



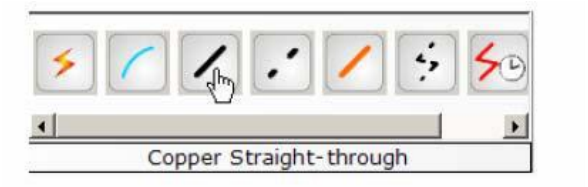
Add the switch by moving the plus sign "+" below PC2 and PC3 and click once.



Connect PC2 to Hub0 by first choosing Connections.

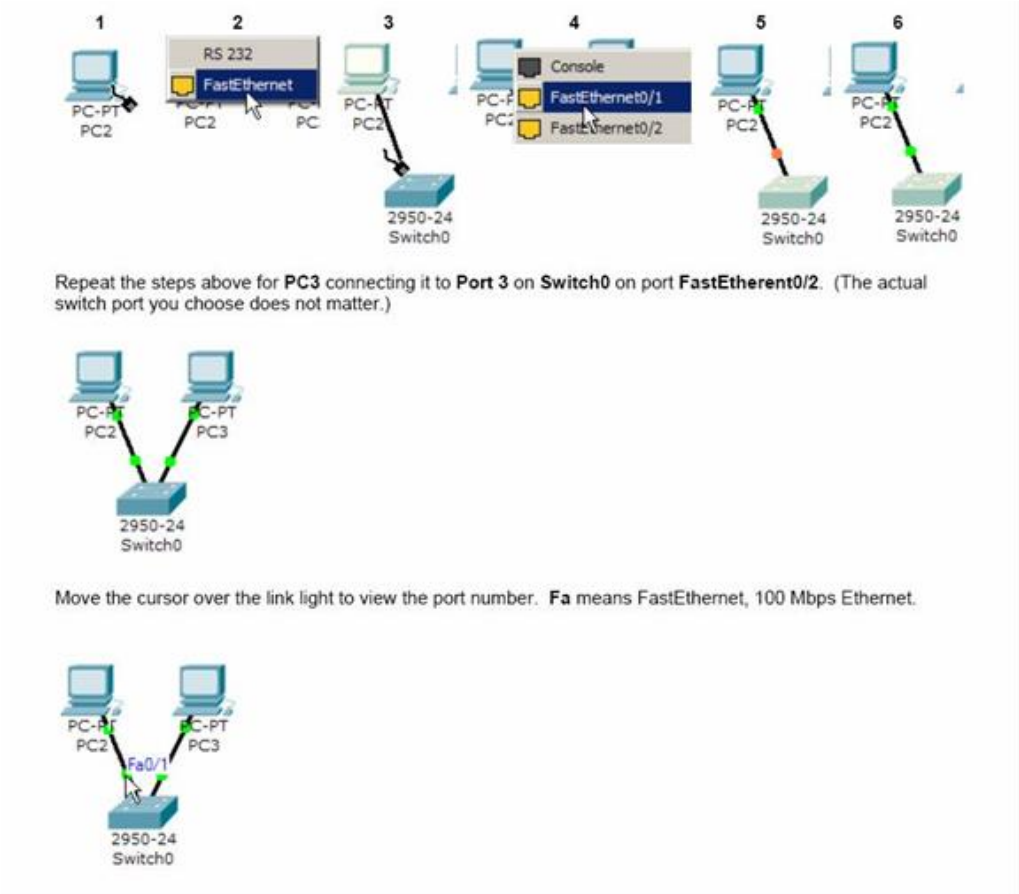


Click once on the Copper Straight-through cable.



Perform the following steps to connect PC2 to Switch0:

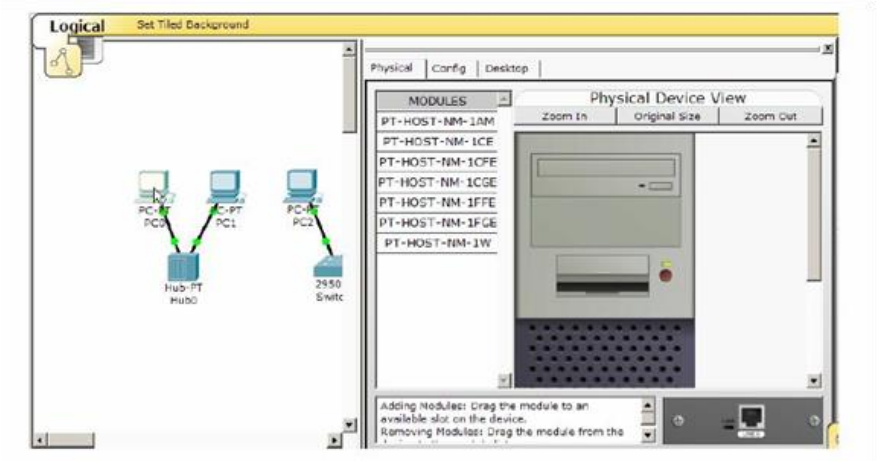
1. Click once on PC2
2. Choose FastEthernet
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0 FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP) process.
6. After a about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now forwarded out the switch port.



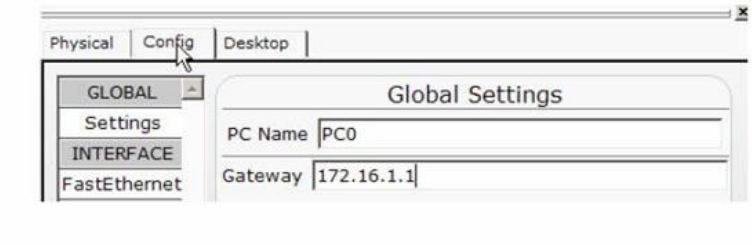
Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

Before we can communicate between the hosts we need to configure IP Addresses and Subnet Masks on the devices.

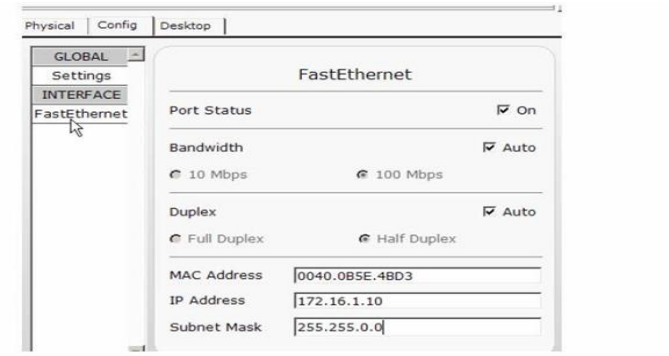
Click once on PC0.



Choose the Config tab. It is here that you can change the name of PC0. It is also here where you would enter a Gateway IP Address, also known as the default gateway. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the IP Address 172.16.1.1, although it will not be used in this lab.



Click on FastEthernet. Although we have not yet discussed IP Addresses, add the IP Address to 172.16.1.10. Click once in the Subnet Mask field to enter the default Subnet Mask. You can leave this at 255.255.0.0. We will discuss this later.



Also, notice this is where you can change the Bandwidth (speed) and Duplex of the Ethernet NIC (Network Interface Card). The default is Auto (autonegotiation), which means the NIC will negotiate with the hub or switch. The bandwidth and/or duplex can be manually set by removing the check from the Auto box and choosing the specific option.

Bandwidth - Auto

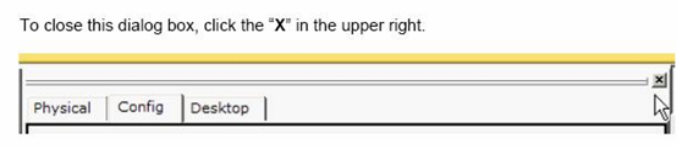
If the host is connected to a hub or switch port which can do 100 Mbps, then the Ethernet NIC on the host will choose 100 Mbps (Fast Ethernet). Otherwise, if the hub or switch port can only do 10 Mbps, then the Ethernet NIC on the host will choose 10 Mbps (Ethernet).

Duplex - Auto

Hub: If the host is connected to a hub, then the Ethernet NIC on the host will choose Half Duplex.

Switch: If the host is connected to a switch, and the switch port is configured as Full Duplex (or Autonegotiation), then the Ethernet NIC on the host will choose Full Duplex. If the switch port is configured as Half Duplex, then the Ethernet NIC on the host will choose Half Duplex. (Full Duplex is a much more efficient option.)

The information is automatically saved when entered.

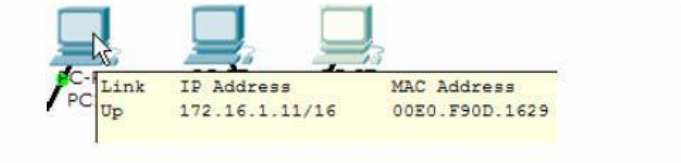


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

Host	IP Address	Subnet Mask
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

Verify the information

To verify the information that you entered, move the Select tool (arrow) over each host.

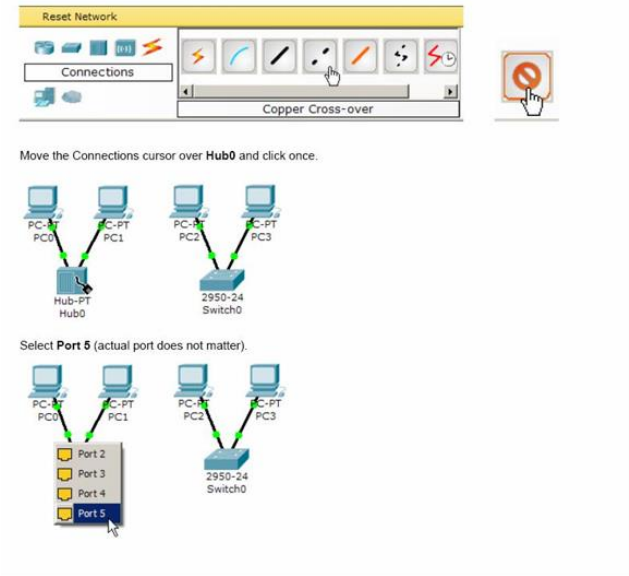


Deleting a Device or Link

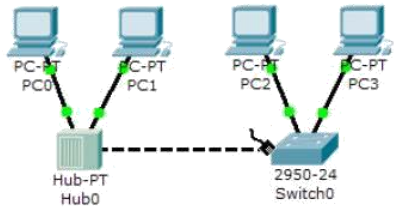
To delete a device or link, choose the Delete tool and click on the item you wish to delete.

Step 6: Connecting Hub0 to Switch0

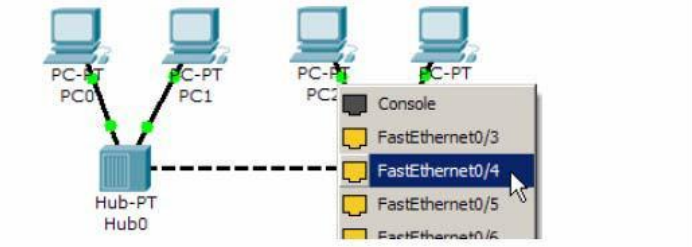
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.



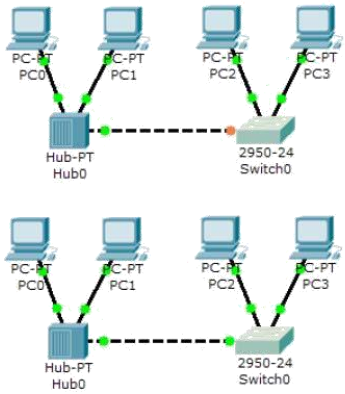
Move the Connections cursor to Switch0.



Click once on Switch0 and choose FastEthernet0/4 (actual port does not matter).



The link light for switch port FastEthernet0/4 will begin as amber and eventually change to green as the Spanning Tree Protocol transitions the port to forwarding.



1.2 NETWORKING COMMANDS

VNStat

It is one of the most complete network commands. It works on all Linux and BSD systems, and allows us to monitor network traffic from the console.

- Installation is simple and fairly quick, allowing monitoring of all network interfaces.
- With VNStat we can collect all traffic needed from any configured interface.
- One of the big differences between VNStat and other tools is that VNStat collects kernel data instead of the interface itself, which means a lighter execution for the system.
- It will not require administrator permissions to run.
- It has the ability to store gathered information so your information never goes missing, even if the system crashes or reboots itself.
- You can set Vnstat to listen to traffic, daily or by billing period, as well as many other options.
- It stands out for its flexibility when configuring the reading of traffic.
- Finally, it is possible to set Vnstat output to generate console graphics and even customize them with colours.

Ping (Unix/Windows)

Ping dates from the 70s and is known for being one of the most basic network commands. However, it is not as simple as we believe and has many more uses than those we already know. It is based on the ICMP protocol and is used to determine:

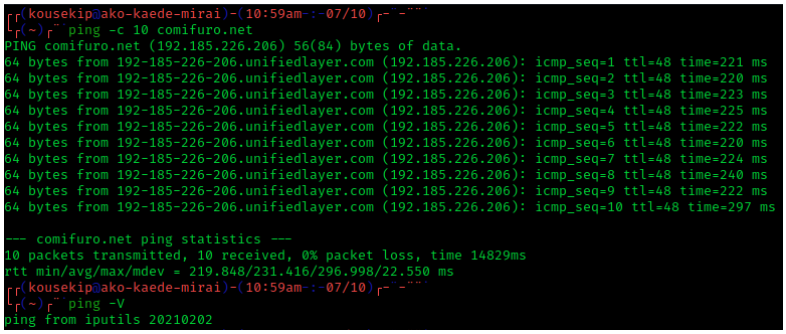
- If there is connectivity between your machine and another machine on the network.
- It’s used to measure the “speed” or latency time.

It is a command that exists on all operating systems that support TCP/IP, and it is a basic command that you should know.

Ping is known for having dozens of parameters and the one that we find more useful is the one responsible for monitoring “the number of packages to send.” There are networks that undo the first package, so it is essential to send at least three so we can check that at least one has arrived without being discarded. For this, we use the -c parameter.

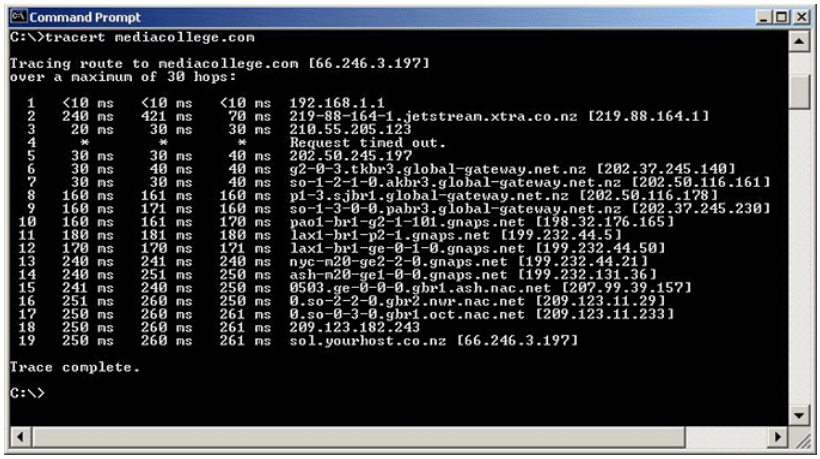
The same technique can be used to determine the loss percentage of packages in our network, sending ten packages and seeing if any gets lost. The number of packages that usually get lost in the network will surprise you. (This tool is included in Pandora FMS)

Execution: Ping name/System IP



Traceroute (Unix/Windows)

The main objective of this tool is to know the traveling path of a package through our network. This network command will tell us where the package is going through (machines, switches, routers) and check that our network is working properly. If you encounter any problems, it will allow us to have a rough idea about where the fault lies.



Execution:

traceroute –n (on Unix / Linux)

tracert –d (on Windows)

Arp (Unix/Windows)

This network command is used to change and view the ARP table, which contains the mappings between the IP address and the MAC address. It only sees the connections in our local area network segment (LAN), so it could be called “low level”. However, it’s used to discover what machines are directly connected to our host or what machines we are connected to. It is a diagnostic tool, and sometimes it can be interesting to monitor it in order to discard ARP Poisoning attacks, which are one of the most common forms of phishing attacks in local networks.

Execution: arp –a

Curl and wget (Unix/ Windows)

These are essential commands to do HTTP, HTTPS or FTP requests to remote servers. It allows you to download files or whole web pages, even recursively (it literally allows us to make a “copy” of a website, including images). It supports cookies and allows you to send POST requests, in addition to “simulate a” user agent, use a http proxy or even a SOCKS4/5 proxy.

One of the most common utilities in integration with Pandora FMS, is to verify the contents of a specific web page. Because wget / curl allows us to download the entire contents of a web, it is easy to compare the MD5 of that content with a value previously verified. If it changes, it means that the Web has been altered.

Netstat (Unix/Windows)

Network command identifies all TCP connections and UDP open on a machine. Besides this, it allows us to know the following information:

- Routing tables to meet our network interfaces and its outputs.
- Ethernet statistics that show sent and received packages and possible errors.
- To know the id of the process that is being used by the connection.
- Netstat is another basic command as Ping that meets many elementary functions.

Whois (Unix/ Windows)

This network command is used to query data domains: to find out who owns the domain, when that domain expires, to view the configured logs, contact details, etc. Its use is

highly recommended to contact the administrators of the domains or when incidents of migration of services such as mail and web happen.

To use 'whois' on Windows you need to download the software from this url: https://technet.microsoft.com/en-us/sysinternals/whois.aspx

SSH (Unix/Linux/Windows)

Command to run terminals on remote machines safely. SSH allows any user to run a console just by registering and entering his credentials. So you can run the commands you want as if you were in local.

More details you need to know about SSH:

Putty is recommended when using SSH in Windows. You can find it here: http://www.putty.org/

- To enable a remote computer to connect to our server via SSH, an SSH server must be installed and set up as FreeSSHd.
- SSH also allows to obtain an interactive remote Shell, execute remote commands and copy files in both directions.
- SSH is the natural replacement of classic tools like Telnet or FTP, and has become a basic tool in the administration of systems over the years. It is extremely powerful despite its complex combinations of symmetric encryption and authentication schemes, and verification, and it is the target of continuous attacks.

TCPDump (Unix/Linux/Windows)

It is one of the "basic" tools of network commands, and when used right, goes on to become a great ally for network administrators, system administrators or programmers.

TCPDump is an advanced command used to inspect traffic from different interfaces of a machine so you can get the exchanged packages. You can dump output to file so then you can analyse it with more powerful sniffers and graphical interfaces such as Wireshark. For Windows, you must use WinDump.

Ngrep (Unix/Linux/Windows)

- The grep command power is taken to the network.

- It is a TCPDump with a substring text filter in real time.
- It has a very powerful filtering system for regular expressions and it is typically used to process files generated by tcpdump, wireshark, etc.
- It is a communication package filter over HTTP, SMTP, FTP, DNS and other protocols.

NMAP (Unix/Windows)

NMAP is considered the father of the general network scanners. Although today there are more reliable tools for some tasks (like Fping), NMAP is a very versatile tool for scanning networks. It is used to determine which hosts are alive in a network and to do different ways of scanning.

Netcat (Windows/Unix)

NetCat, or NC, is the network command most versatile that exists nowadays and one of the lightest. However, its use requires some imagination. Only if you've played with scripting, you will understand the subtlety of its name: NetCat. It is a tool designed to be used as a destination of a redirect (one pipe or |). It is used to send or receive information about a connection. For example, a WEB request to service would be something as simple as:

echo -e "GET http://pandorafms.com HTTP/1.0\n\n" | nc pandorafms.com 80

Lsof (Unix/Windows)

The 'lsof' command is not only used as a network tool, but also is used to identify which files have an open process. In Unix environments, a file can be a network connection, so that is used to know which ports have an open particular running process, something extremely useful in specific cases.

IPtraf (Linux)

Special command to obtain traffic statistics. It has a ncurses interface (text) to analyze real-time traffic passing through an interface. It allows you to work at low-level and to see what pairs of connections are established on each machine, and to see in detail the traffic connection of every pair, all in real-time.

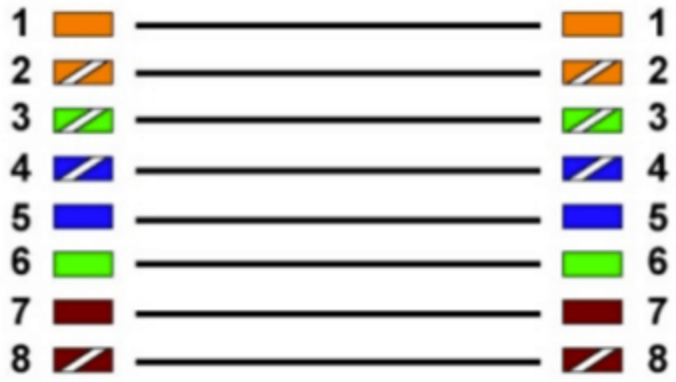
Exercise 2: Cabling – Straight Through and Cross-over Cabling

Ethernet cable:

An Ethernet cable is a network cable used for high-speed wired network connections between two devices. This network cable is made of four-pair cable, which is consists of twisted pair conductors. It is used for data transmission at both ends of the cable, which is called RJ45 connector.

The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps.

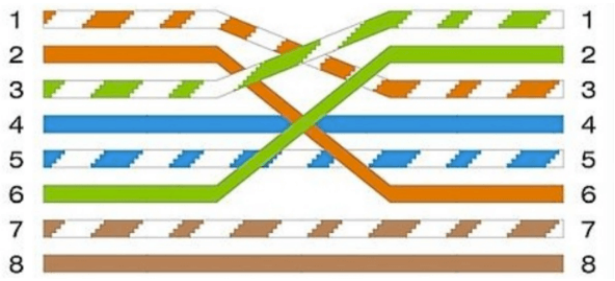
Straight Through Cable:



Straight Through Cable

Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

Crossover Cable:



Crossover Cable

A Crossover cable is a type of CAT 5 where one end isT568A configuration and the other end as T568BConfiguration. In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.

Crossover cable is used to connect two or more computing devices. The internal wiring of crossover cables reverses the transmission and receive signals. It is widely used to connect two devices of the same type: e.g., two computers or two switches to each other.

In regard to physical appearance, Crossover Ethernet cables are very much similar to regular Ethernet cables. Still, they are different with regard to the order with which the wires are arranged. This type of Ethernet cable is made to connect to network devices of the same kind over Ethernet directly. Crossover cables are mostly used to connect two hosts directly.

Devices Connectivity:

DEVICES	HUB	SWITCH	ROUTER	PC
HUB	**CO**	**CO**	**ST**	**ST**
SWITCH	**CO**	**CO**	**ST**	**ST**
ROUTER	**ST**	**ST**	**CO**	**CO**
PC	**ST**	**ST**	**CO**	**CO**

Exercise 2.a

Objective: To demonstrate the Copper Cross-over cabling by designing a Peer to Peer Network

Components:

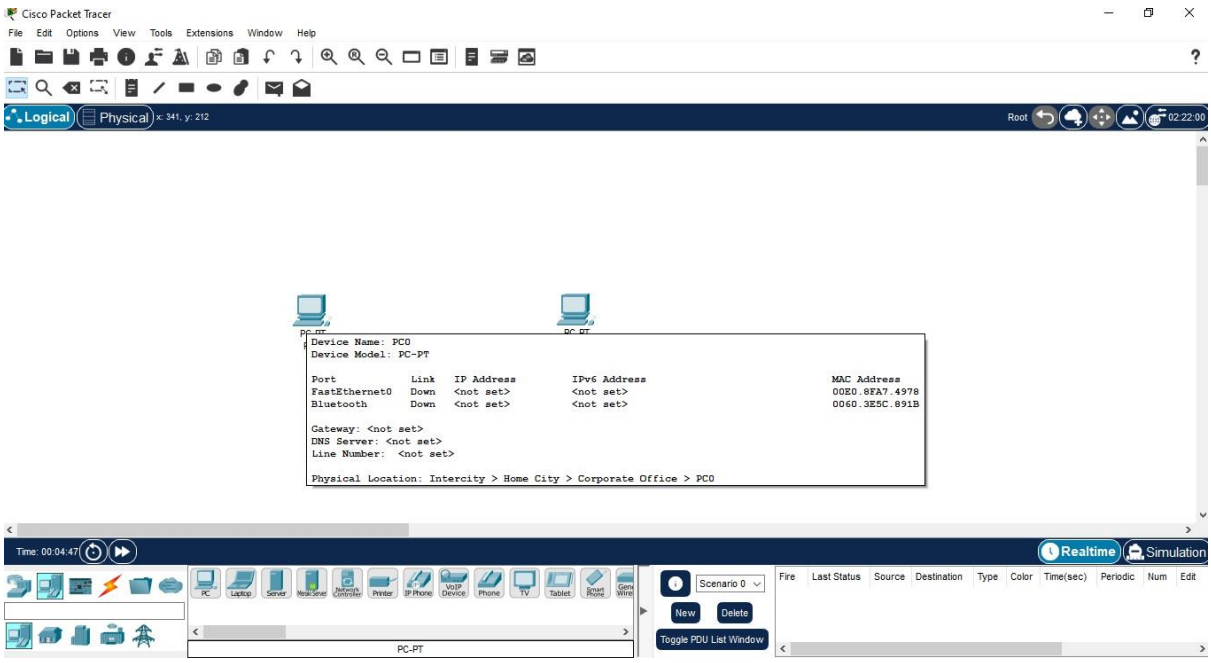
Devices	Required Nos
PCs	2
Copper Cross – Over Cable	1

Addressing Table:

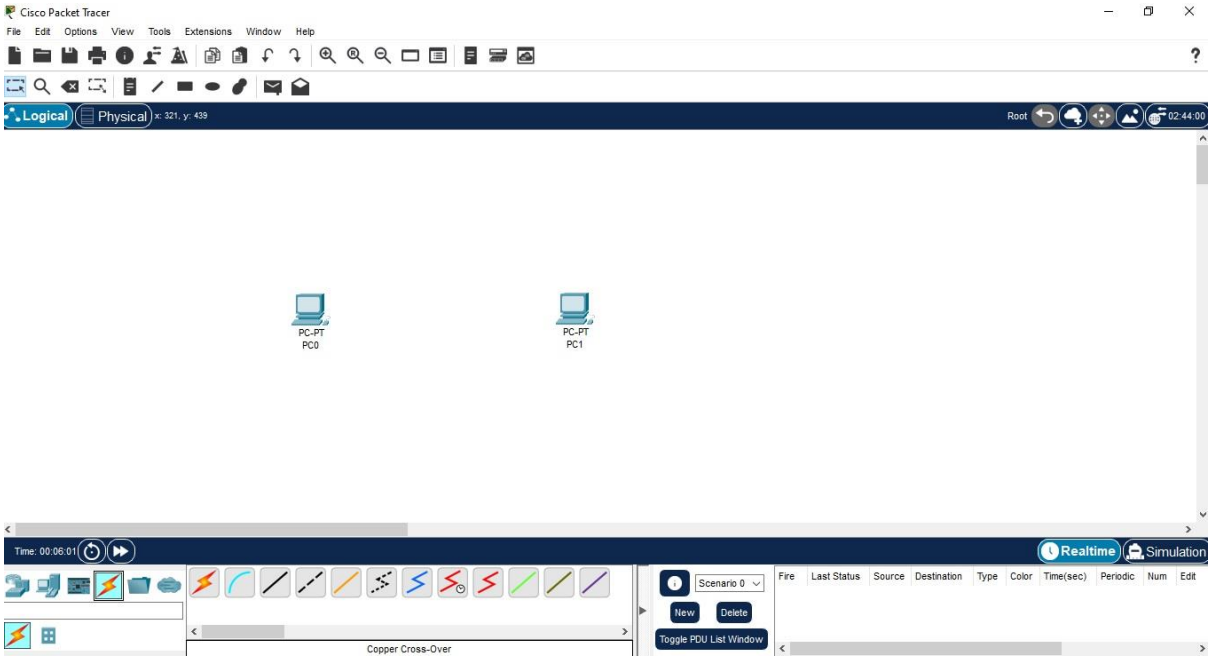
Device	Interface	IP Address	Subnet Mask
PC0	Fa0/0	192.168.10.1	255.255.255.0
PC1	Fa0/0	192.168.10.2	255.255.255.0

Procedure:

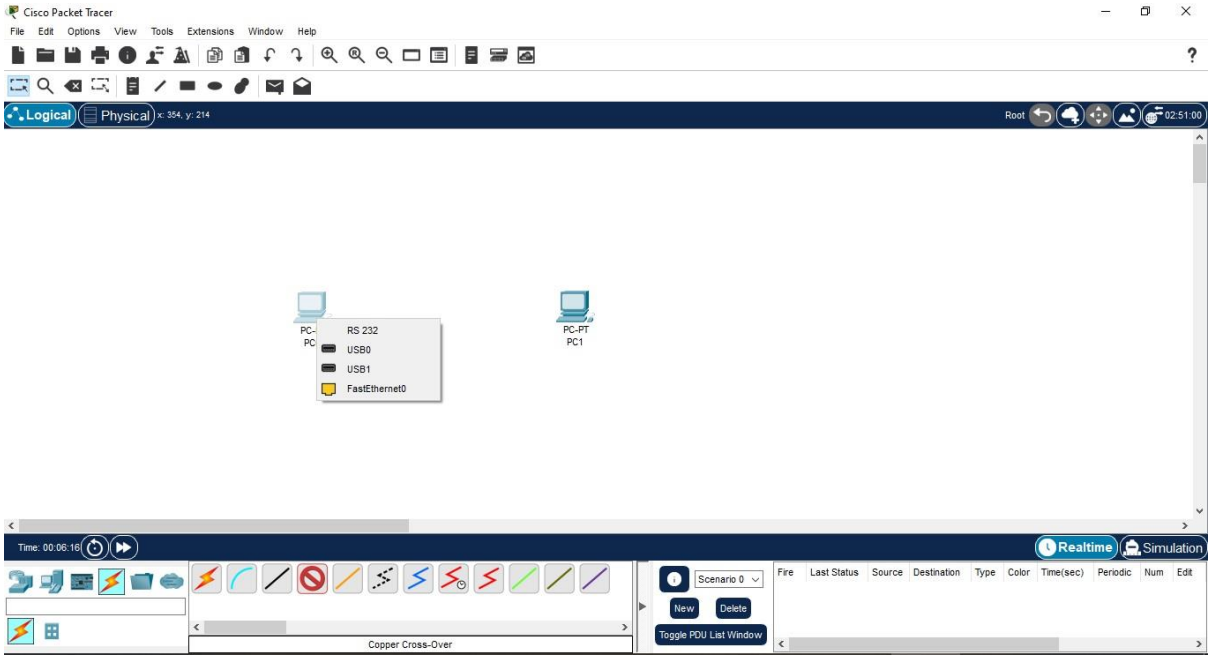
Step 1: Drag 2 PCs in the console area. Each PC will have interfaces as shown in the figure.



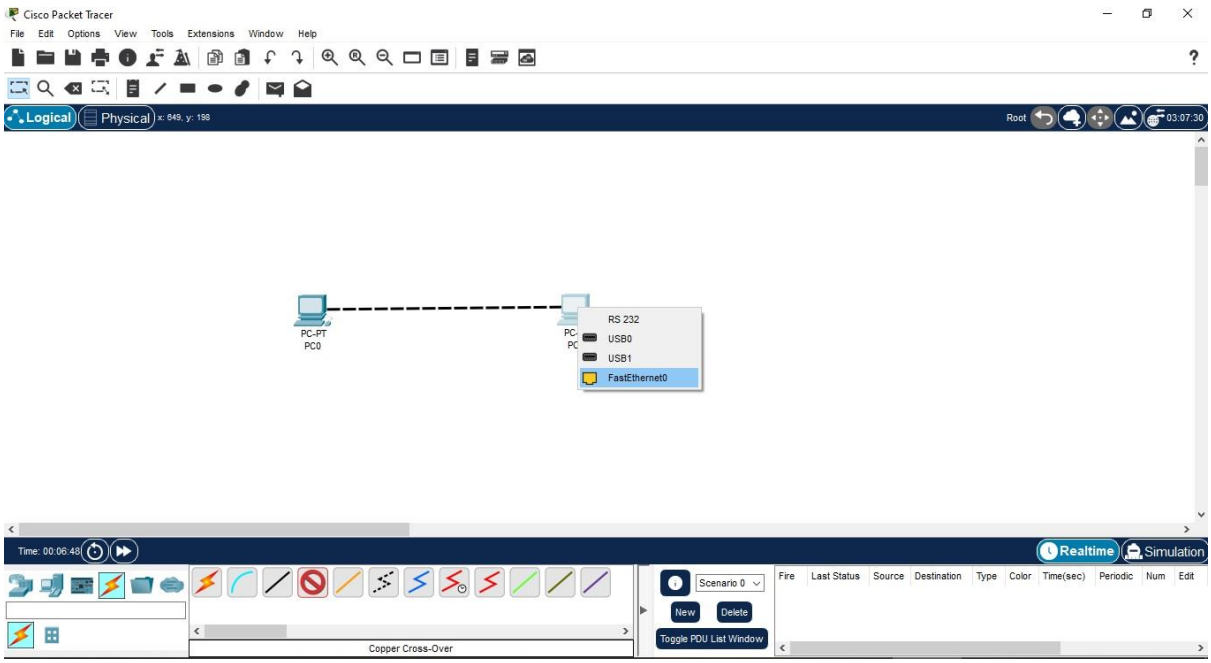
Step 2: Select Connectivity & Copper cross-over cable.



Step 3: Click on PC0 to get the interface options. Select Fa0/0

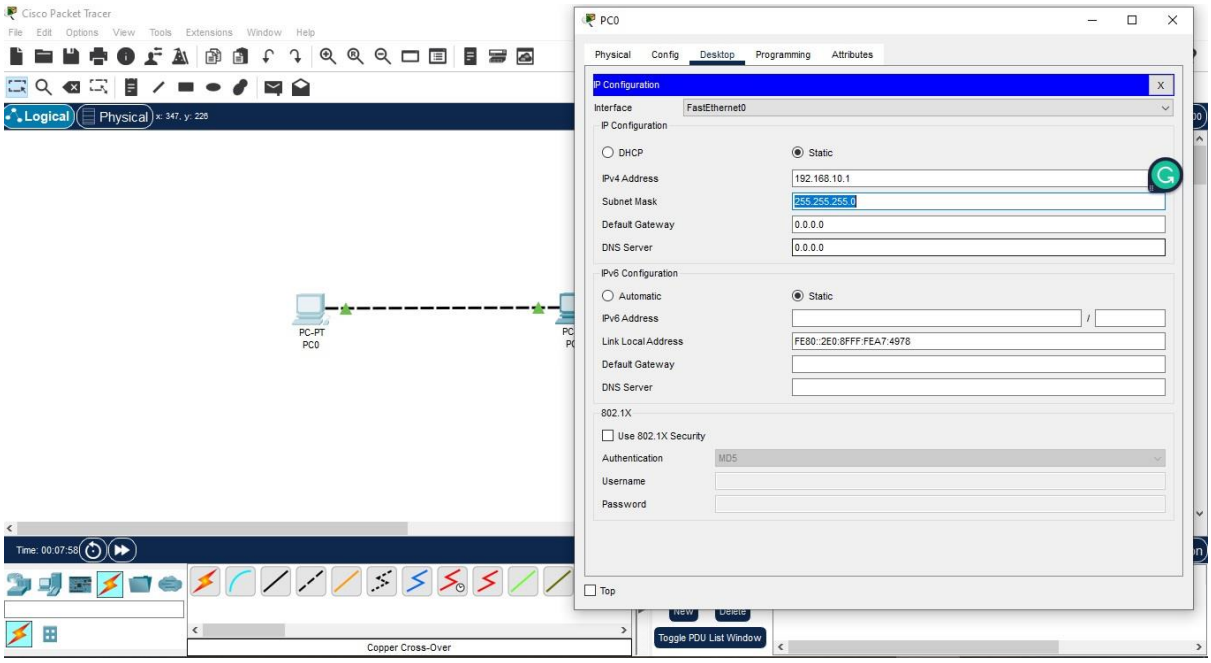


Step 4: Click on PC1 to get the interface options and select Fa0/0.

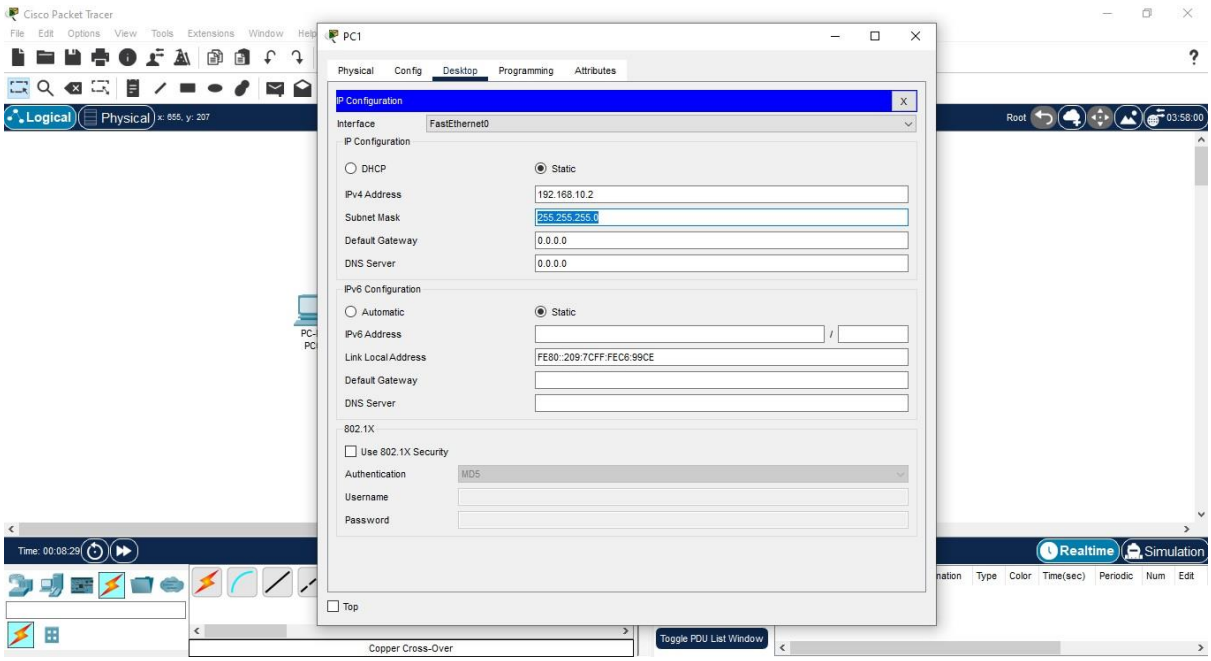


Step 5: Now the PCs are physically connected. To establish logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on IP Configuration icon.
- Configure as in the following figure

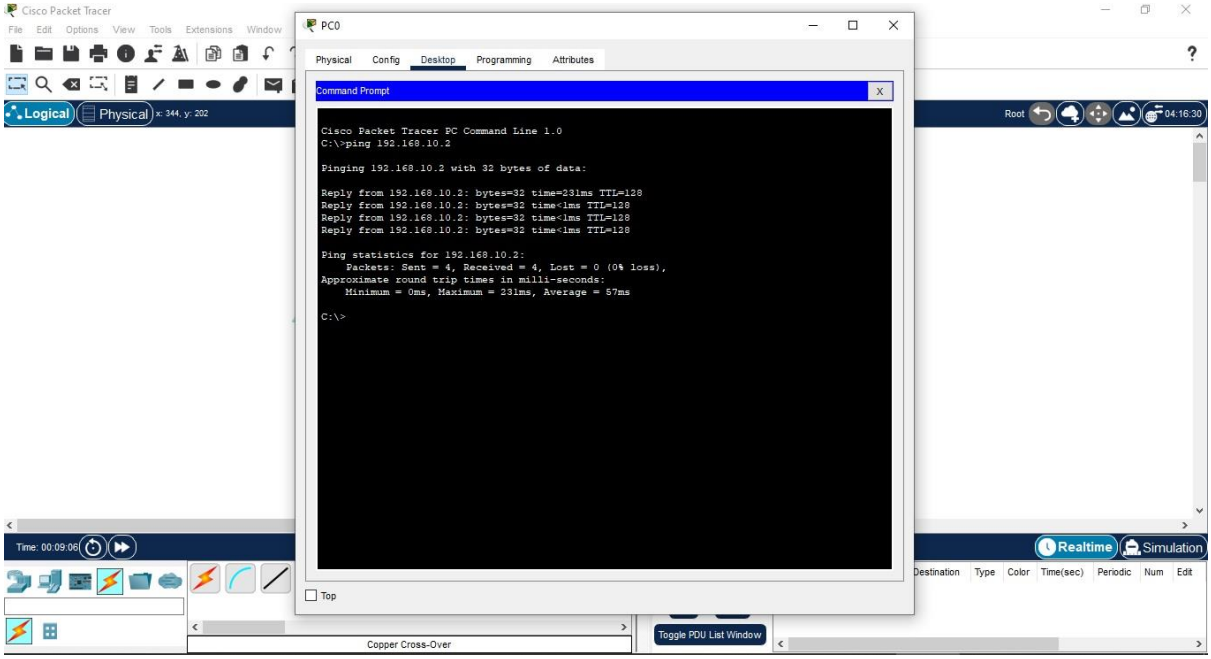


Step 6: Configure IP address for PC1 with the same procedure.



Step 7: Now both the PCs are physically and logically connected. To check the logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on Command Prompt icon.
- Type ping 192.168.10.2 to fetch the output as follows



Exercise 2.b

Objective: To demonstrate the straight through cabling by designing a Local Area Network

Components:

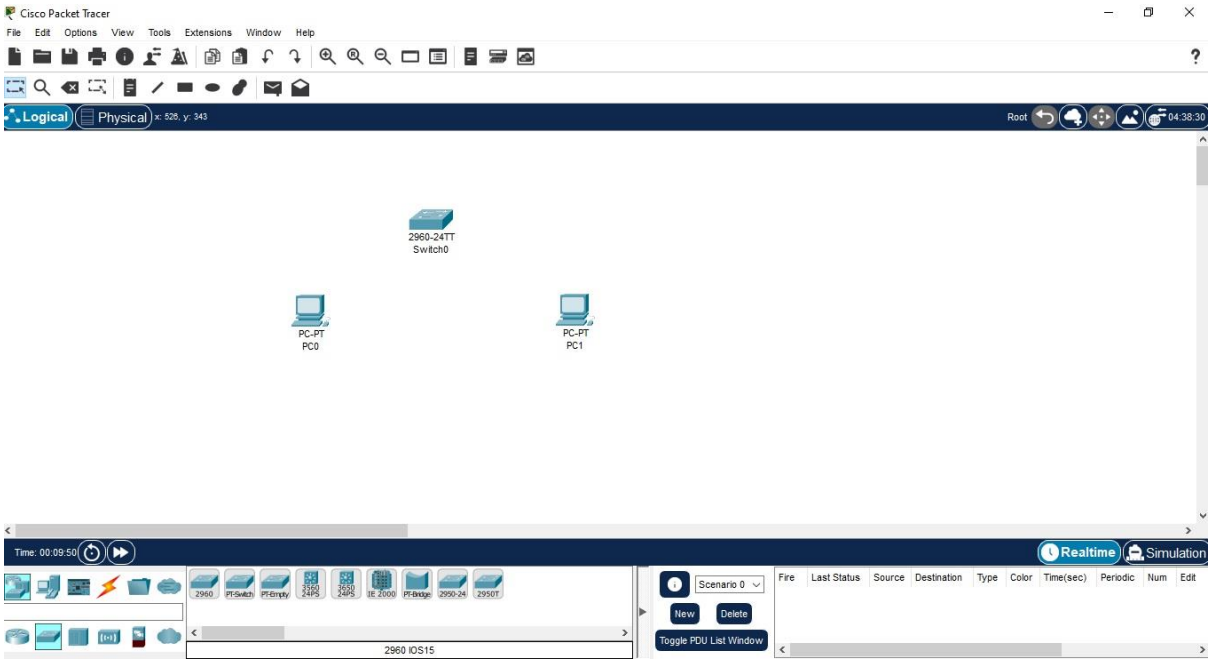
Devices	Required Nos
PCs	2
Copper Straight – Through Cables	2
Switch	1

Addressing Table:

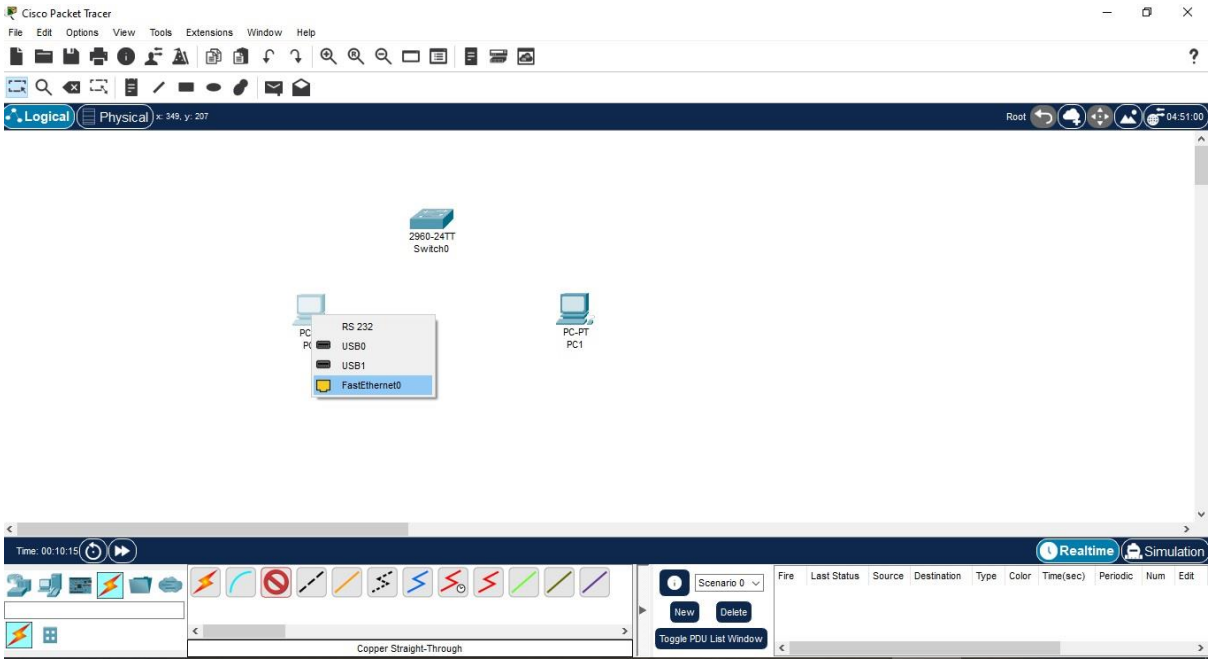
Device	Interface	IP Address	Subnet Mask
PC0	Fa0/0	192.168.10.1	255.255.255.0
PC1	Fa0/0	192.168.10.2	255.255.255.0

Procedure:

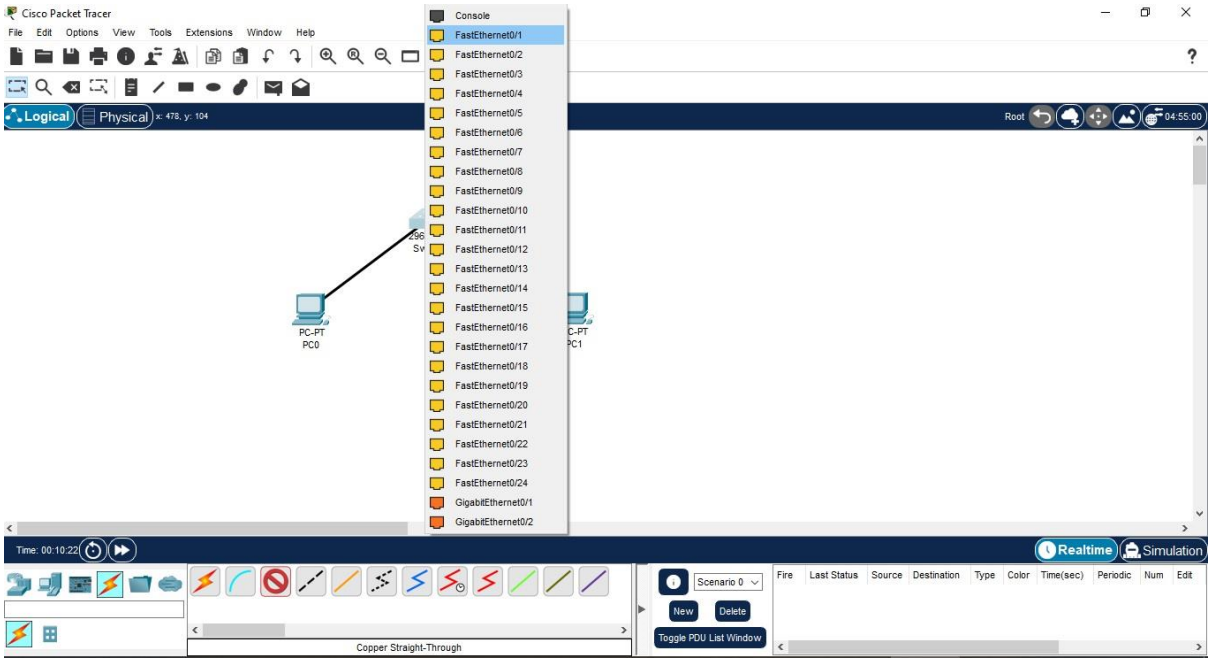
Step 1: Drag 2 PCs and a switch in the console area. Each PC will have interfaces as shown in the figure.



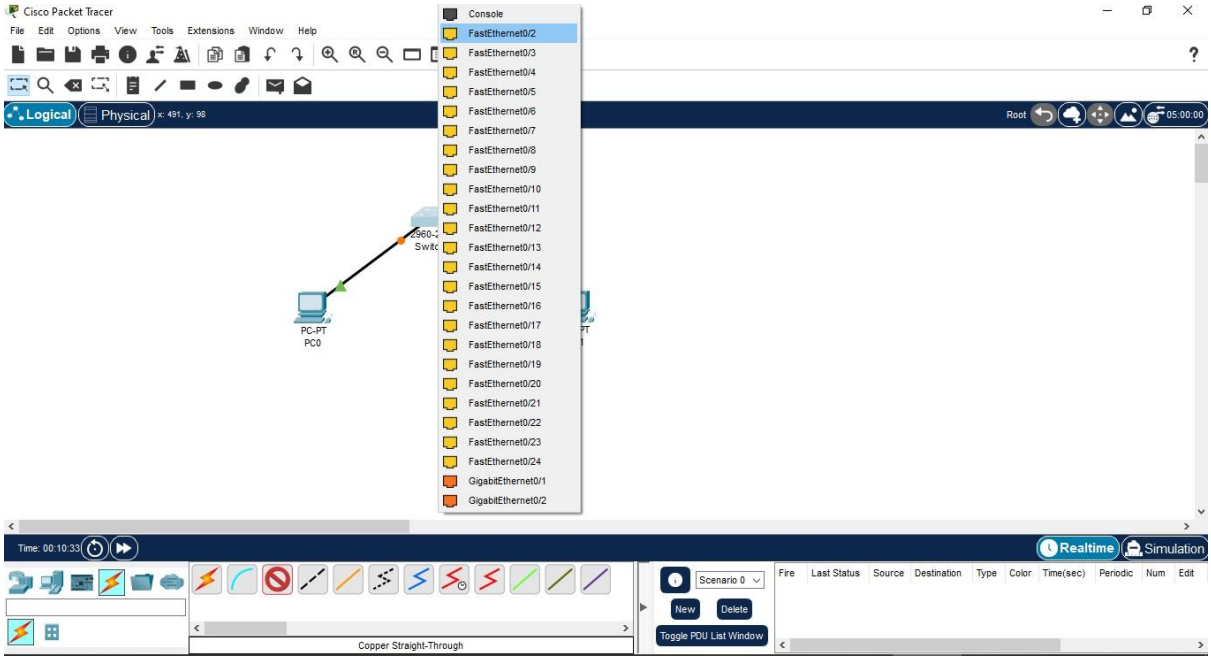
Step 2: Select Connectivity & Copper Straight-Through cable. Click on PC0 to get the interface options. Select Fa0/0



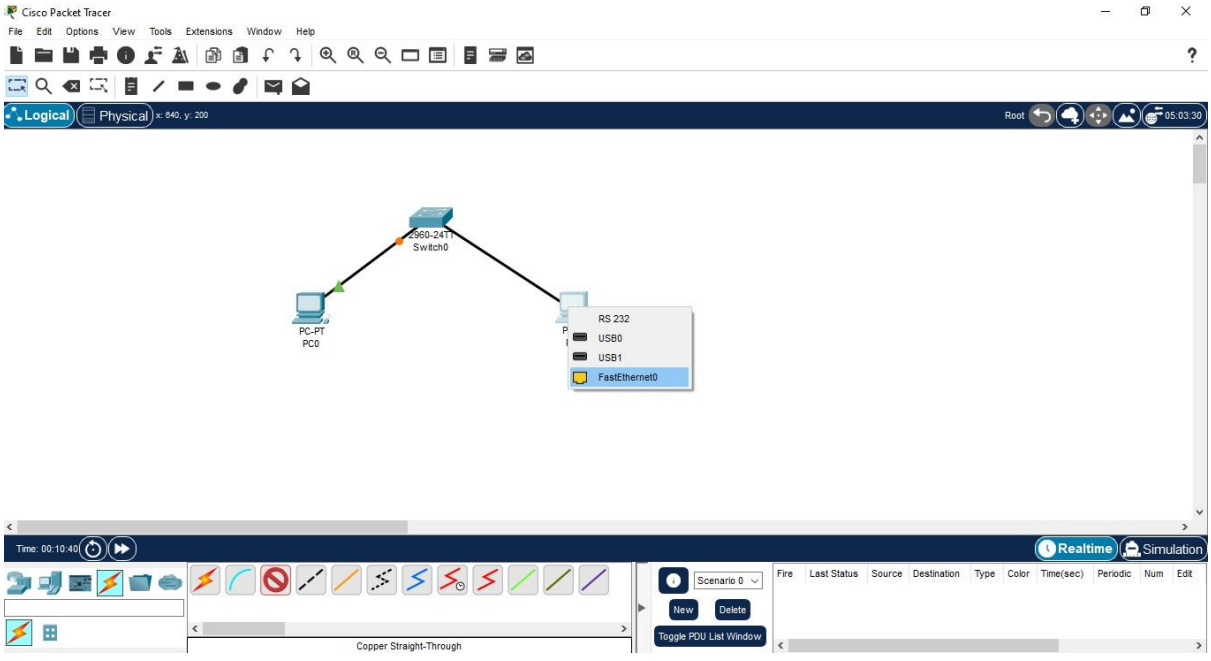
Step 3: Click on Switch to get the interface options and select Fa0/0.



Step 4: Now PC0 and Switch are physically connected. Again select copper straight-through cable and again click on Switch to get the interface options and select Fa0/1.



Step 5: Click on PC1 to get the interface options and select Fa0/0.

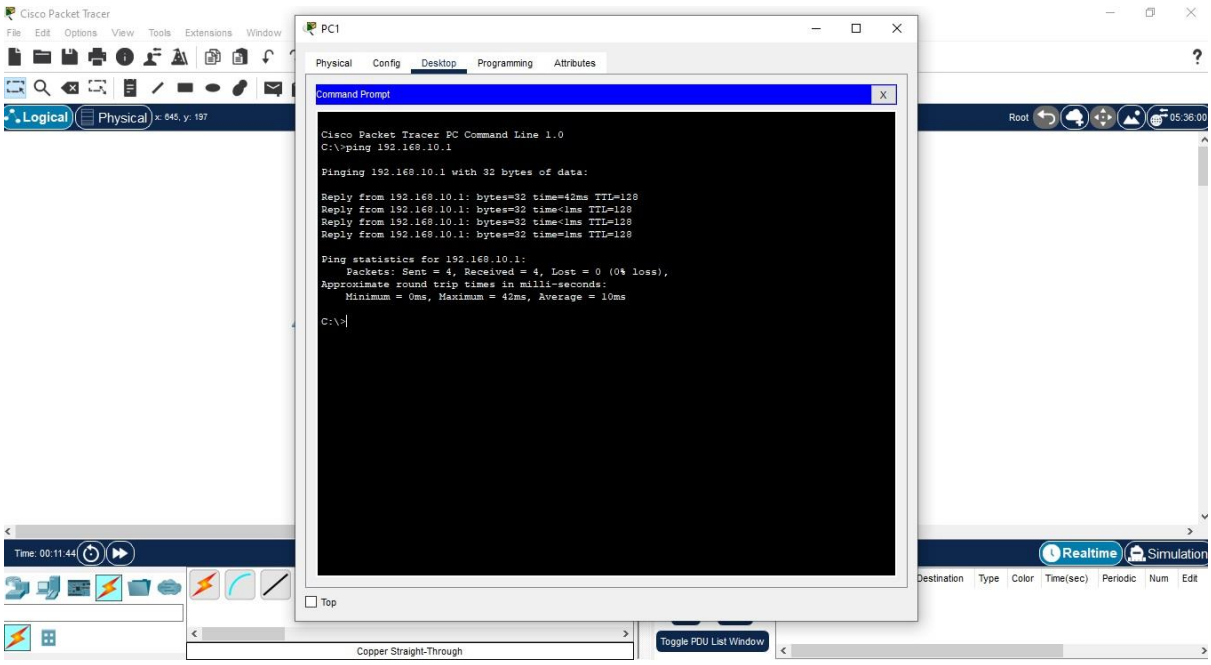


Step 6: Now the PCs are physically connected through switch. To establish logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on IP Configuration icon.
- Configure the ip address 192.168.10.1 and subnet mask 255.255.255.0
- Repeat the same procedure for PC1 and configure with the ip address 192.168.10.2 and subnet mask 255.255.255.0

Step 7: Now both the PCs are physically and logically connected. To check the logical connectivity,

- Click on PC1.
- Select Desktop tab.
- Click on Command Prompt icon.
- Type ping 192.168.10.1 to fetch the output as follows



Exercise 3: Configuration of IP Address in Router

Objective: To demonstrate the configuration of IP Address in router

Pre-requisite: IP Address, Range of IP Address and Classes of IP Address

Components:

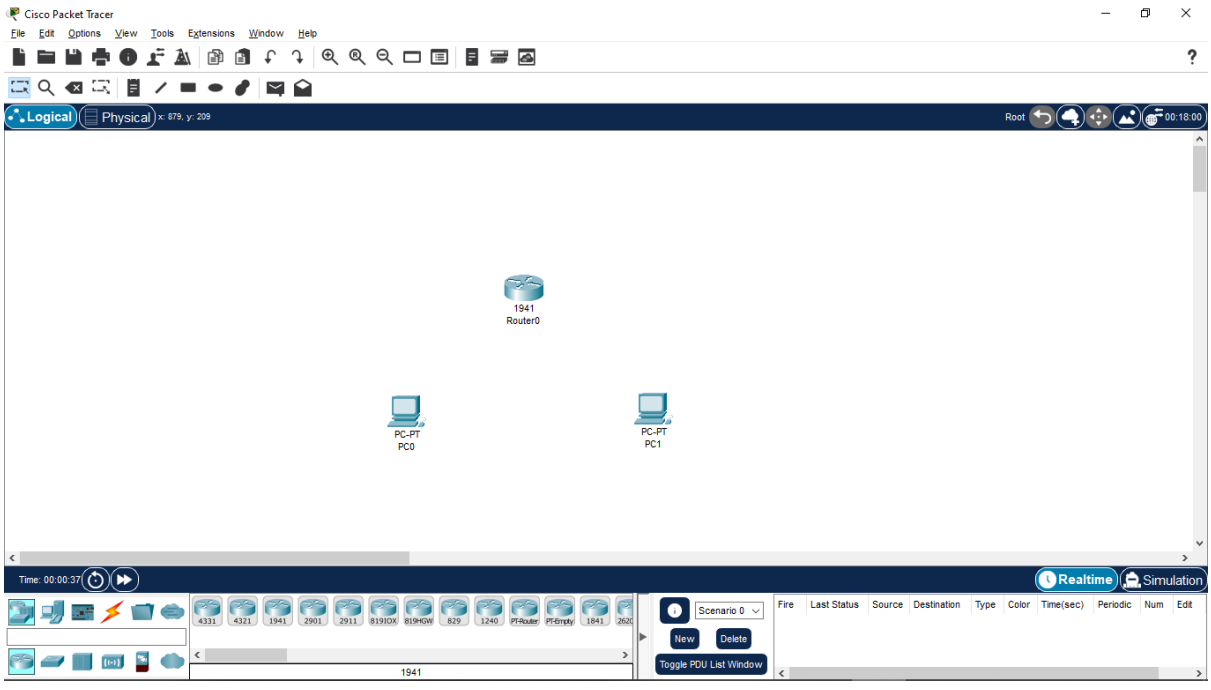
Devices	Required Nos
PCs	2
Copper cross-over Cables	2
Router	1

Addressing Table:

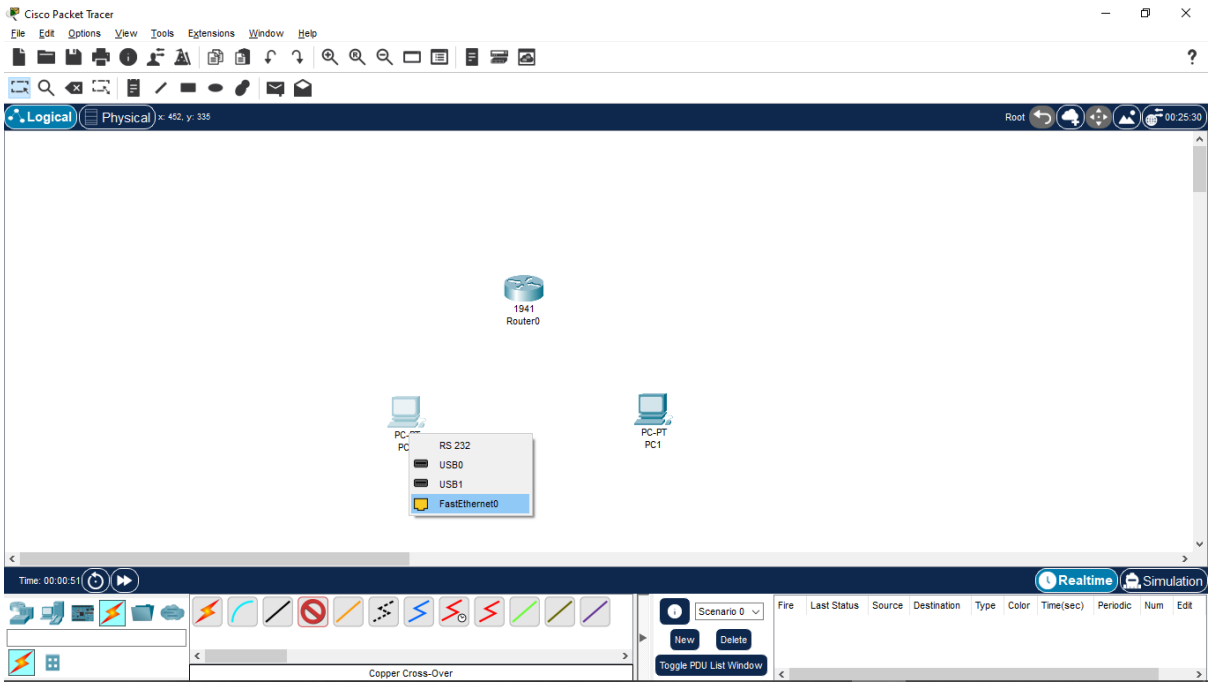
Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	Fa0/0	192.168.11.2	255.255.255.0	192.168.11.1
Router0	Gigabit 0/0	192.168.10.1	255.255.255.0	-
Router0	Gigabit 0/1	192.168.11.1	255.255.255.0	-

Procedure:

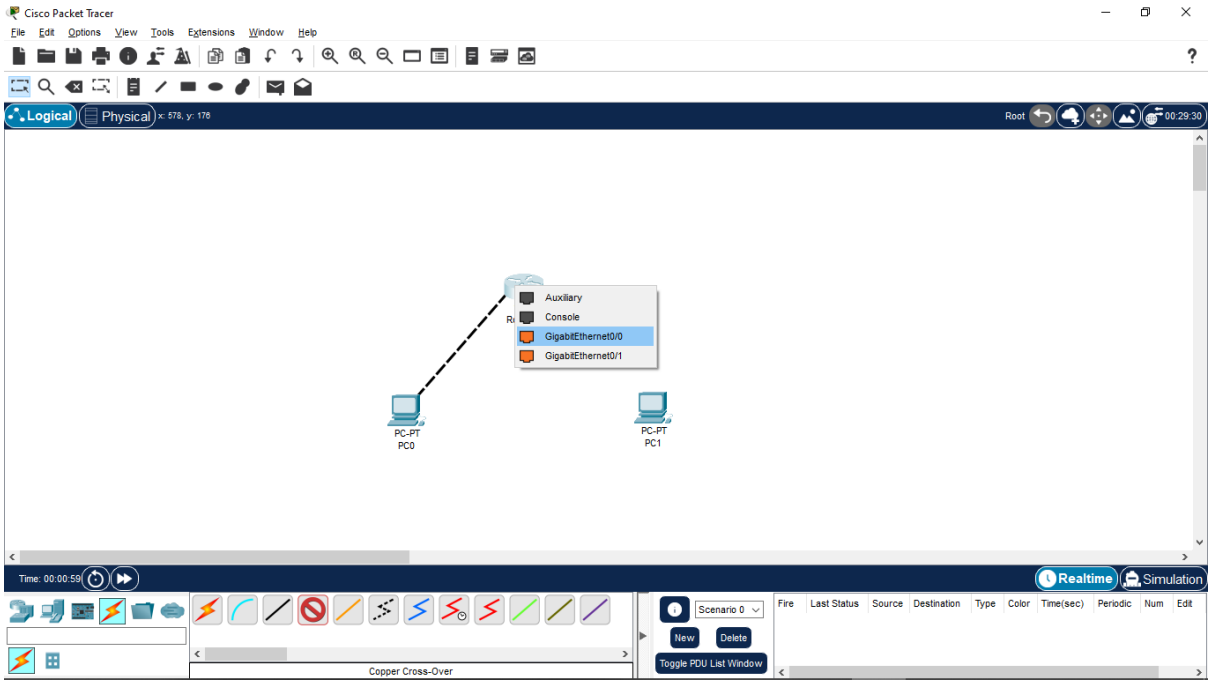
Step 1: Drag 2 PCs and a router in the console area.



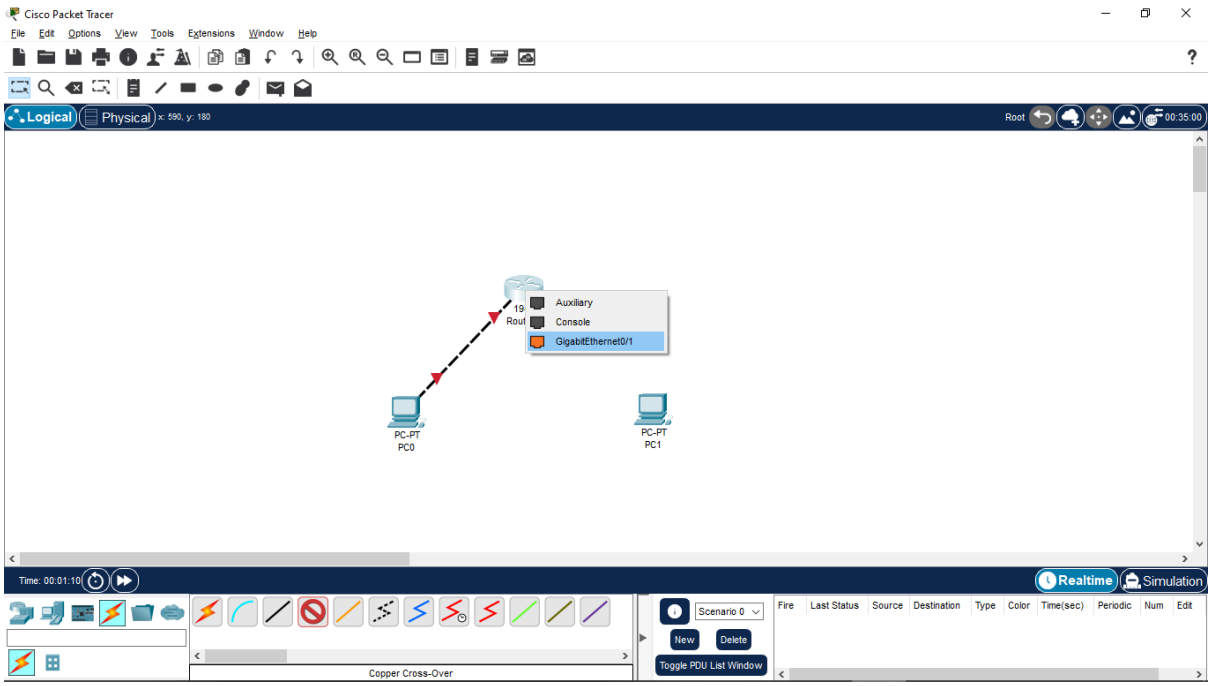
Step 2: Select Connectivity & Copper cross-over cable. Click on PC0 to get the interface options. Select Fa0/0



Step 3: Click on router0 to get the interface options and select GigabitEthernet0/0.



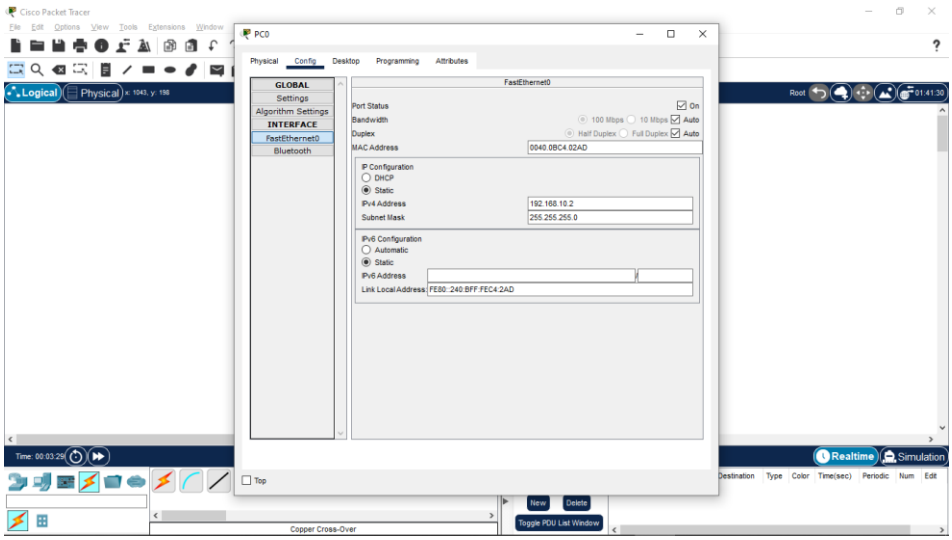
Step 4: Now PC0 and Router0 are physically connected. Again select copper cross-over cable and again click on Router0 to get the interface options and select GigabitEthernet0/1.



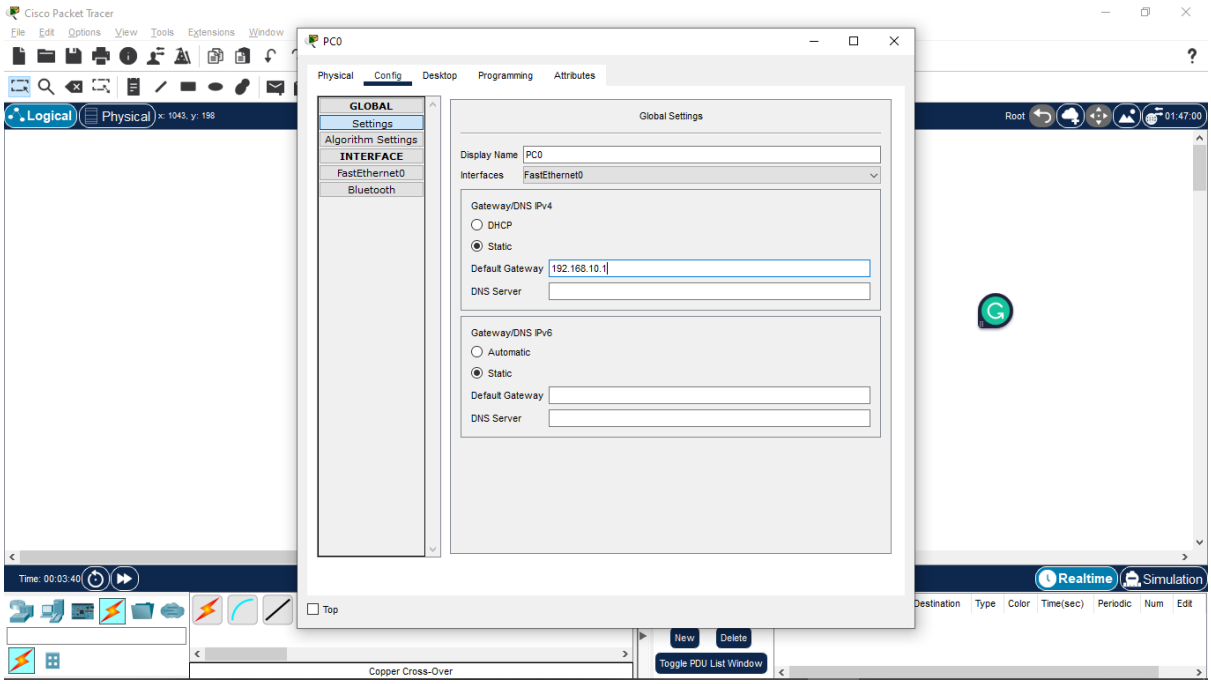
Step 5: Click on PC1 to get the interface options and select Fa0/0.

Step 6: Now the PCs are physically connected through Router. To establish logical connectivity,

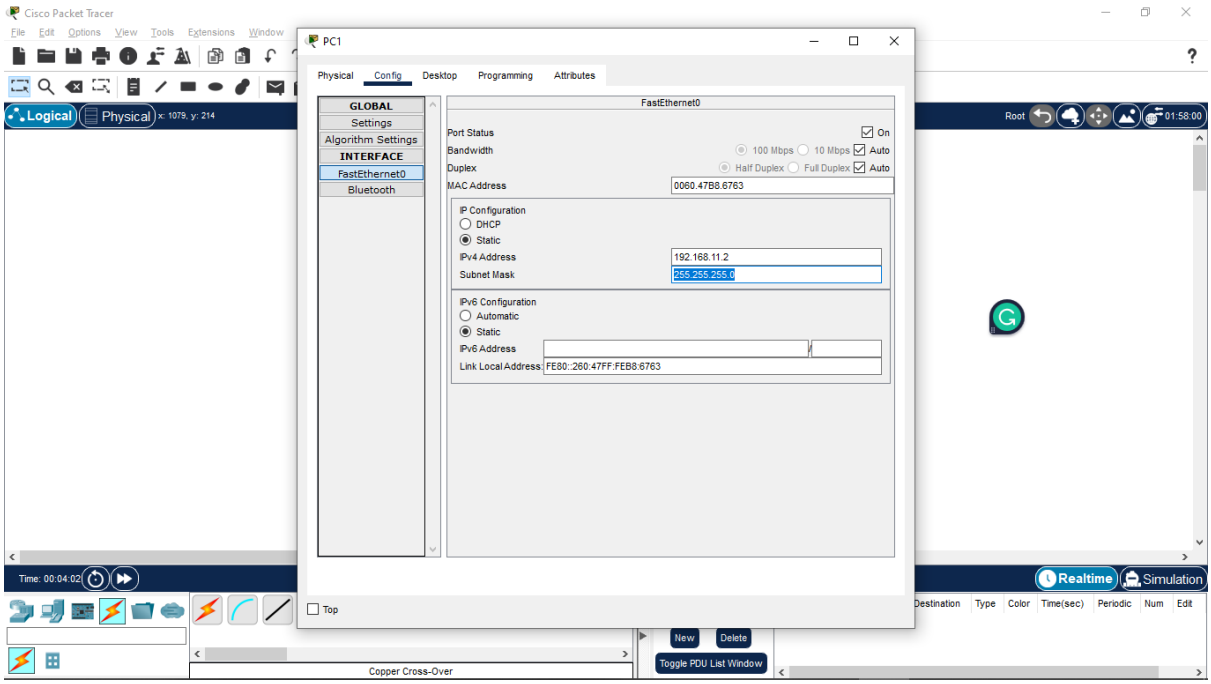
- Click on PC0.
- Select Config tab.
- Click on FastEhternet0/0 in the left pane.
- Configure the ip address 192.168.10.2 and subnet mask 255.255.255.0



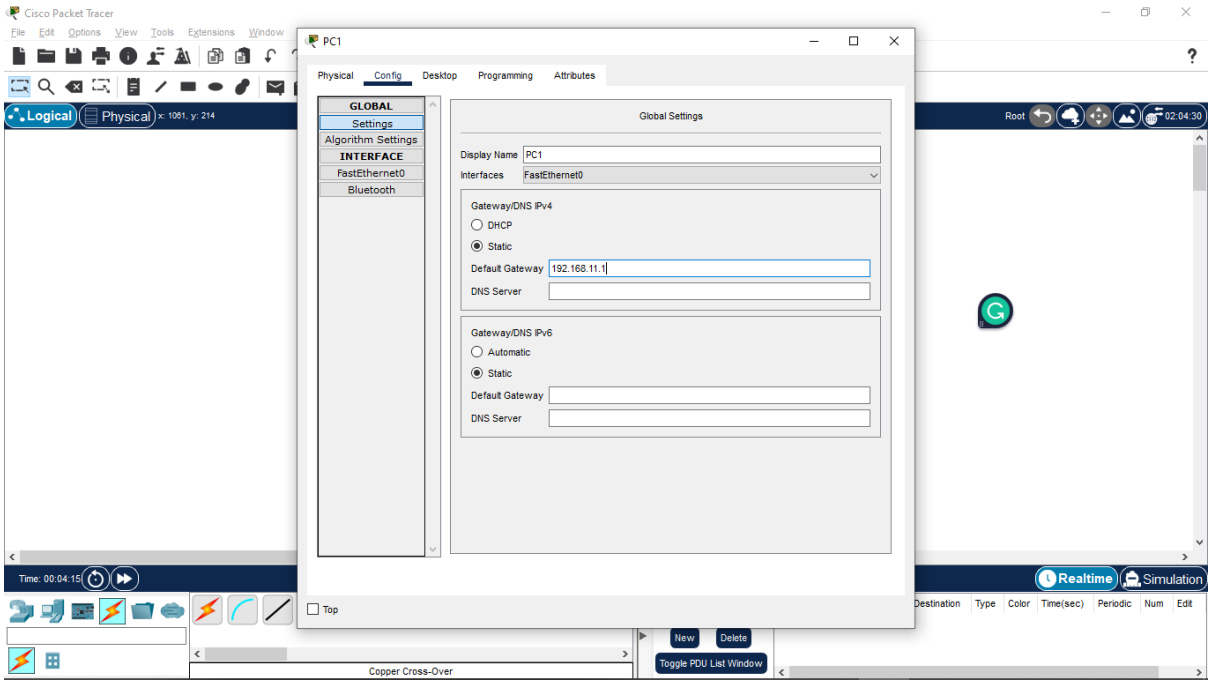
Step 7: Now click on settings and configure the gateway as 192.168.10.1



Step 8: Repeat the same procedure for PC1 and Configure the ip address 192.168.11.2 and subnet mask 255.255.255.0

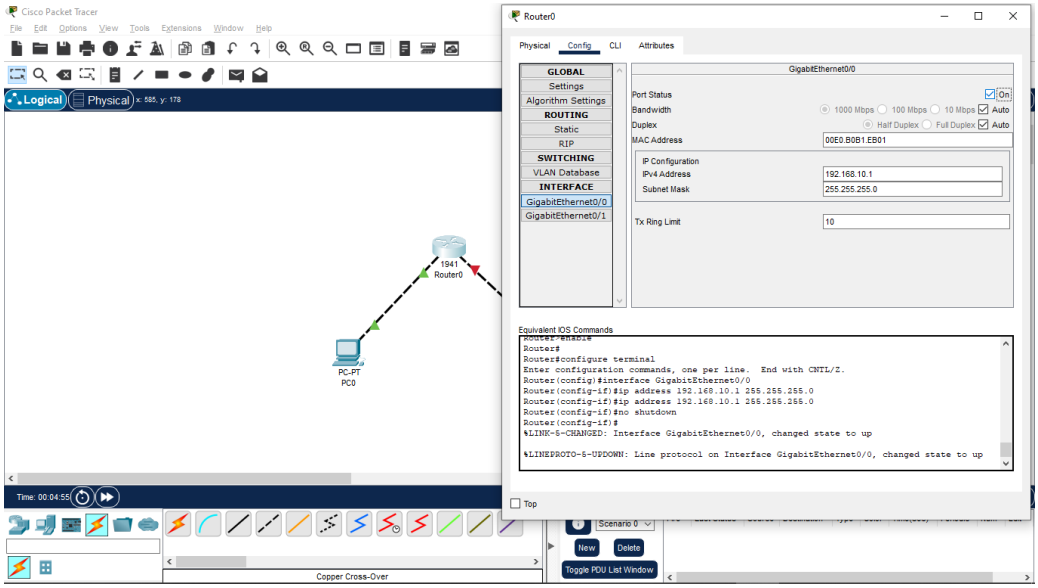


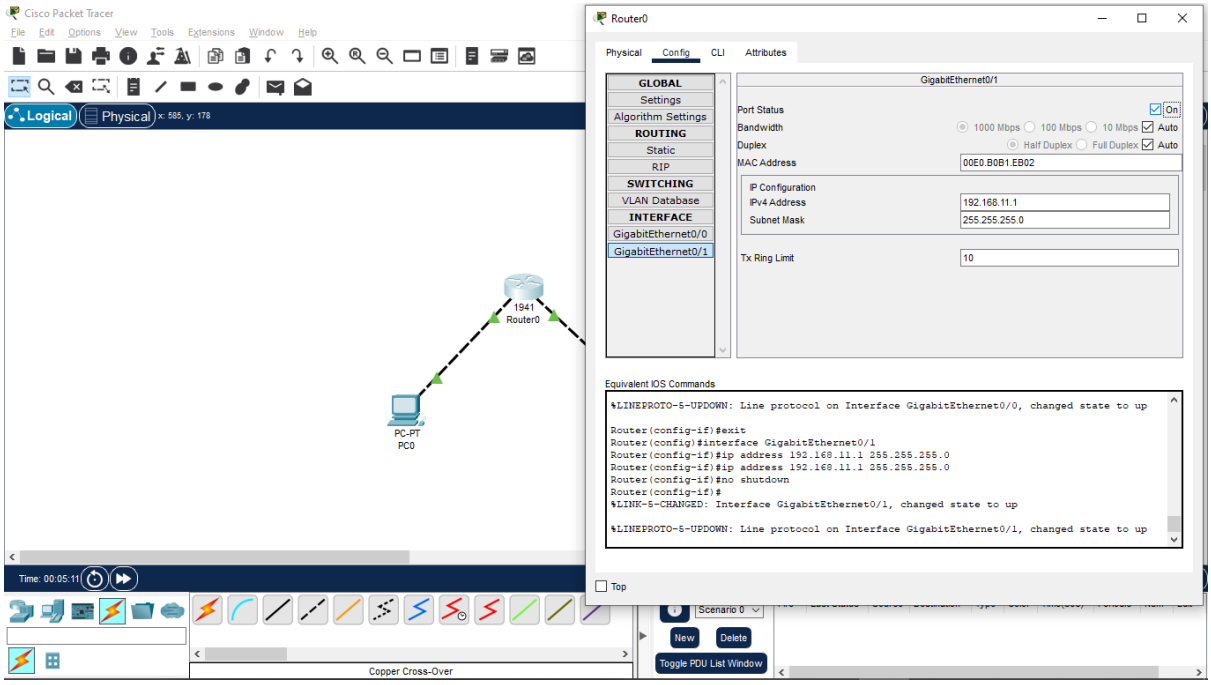
Step 9: Now click on settings and configure the gateway as 192.168.11.1



Step 10: Router configuration

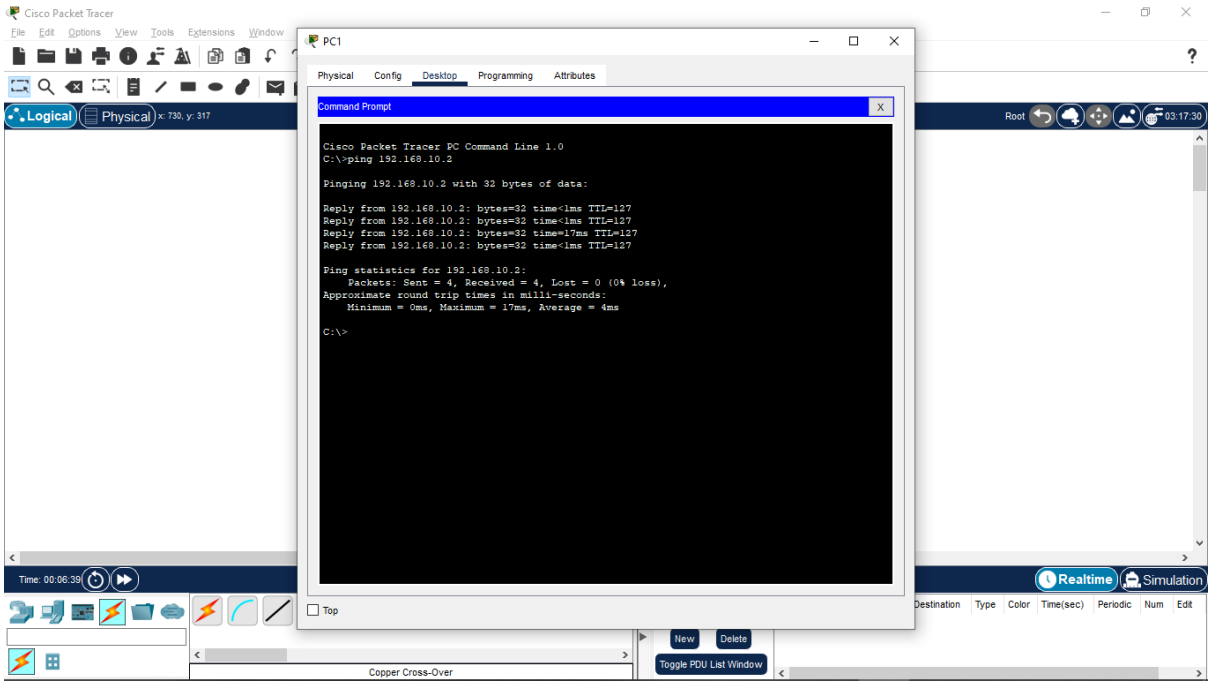
- Click on Router0 and select Config tab.
- Click on GigabitEthernet0/0 in the left pane and configure the ip address 192.168.10.1 and subnet mask 255.255.255.0
- Click on GigabitEthernet0/1 in the left pane and configure the ip address 192.168.11.1 and subnet mask 255.255.255.0





Step 11: Now both the PCs are physically and logically connected. To check the logical connectivity,

- Click on PC1.
- Select Desktop tab.
- Click on Command Prompt icon.
- Type ping 192.168.10.2 to fetch the output as follows



Exercise 4: Subnetting in WAN Configuration (DTE and DCE)

Objective: To demonstrate the configuration of IP Addressing with Subnetting in WAN Configuration

Pre-requisite: IP Address, Range of IP Address, Classes of IP Address, Subnetting

Components:

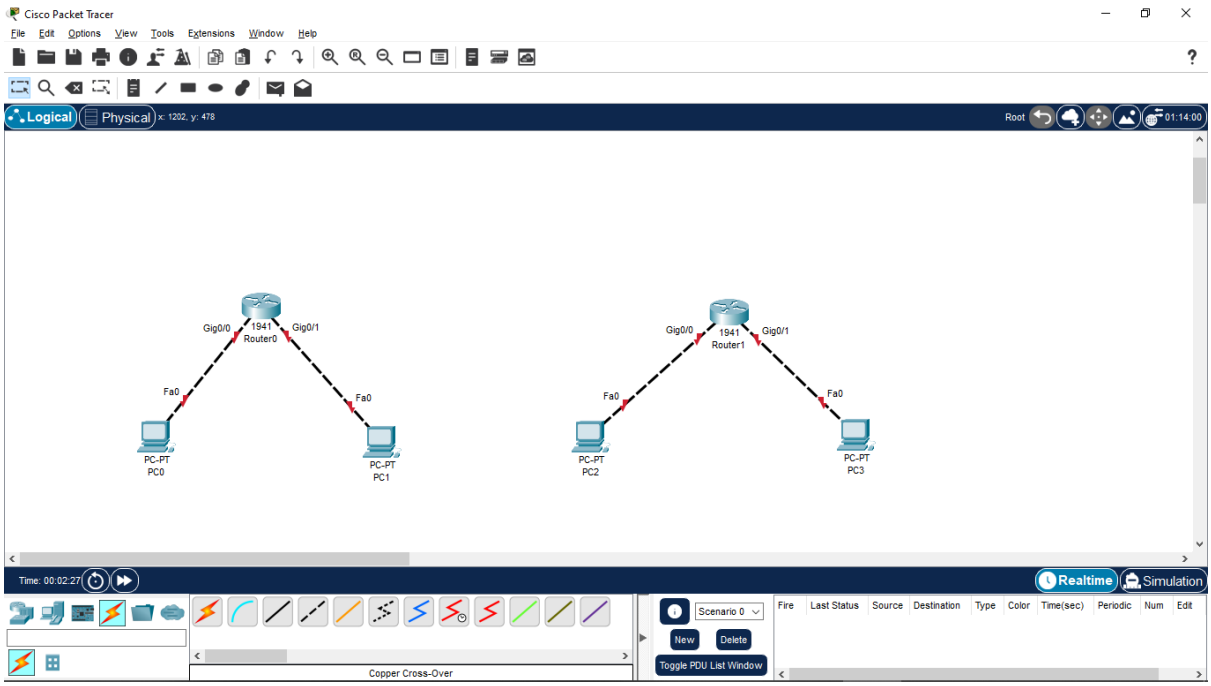
Devices	Required Nos
PCs	4
Copper cross-over Cables	4
Routers	2
Serial DCE	1

Addressing Table:

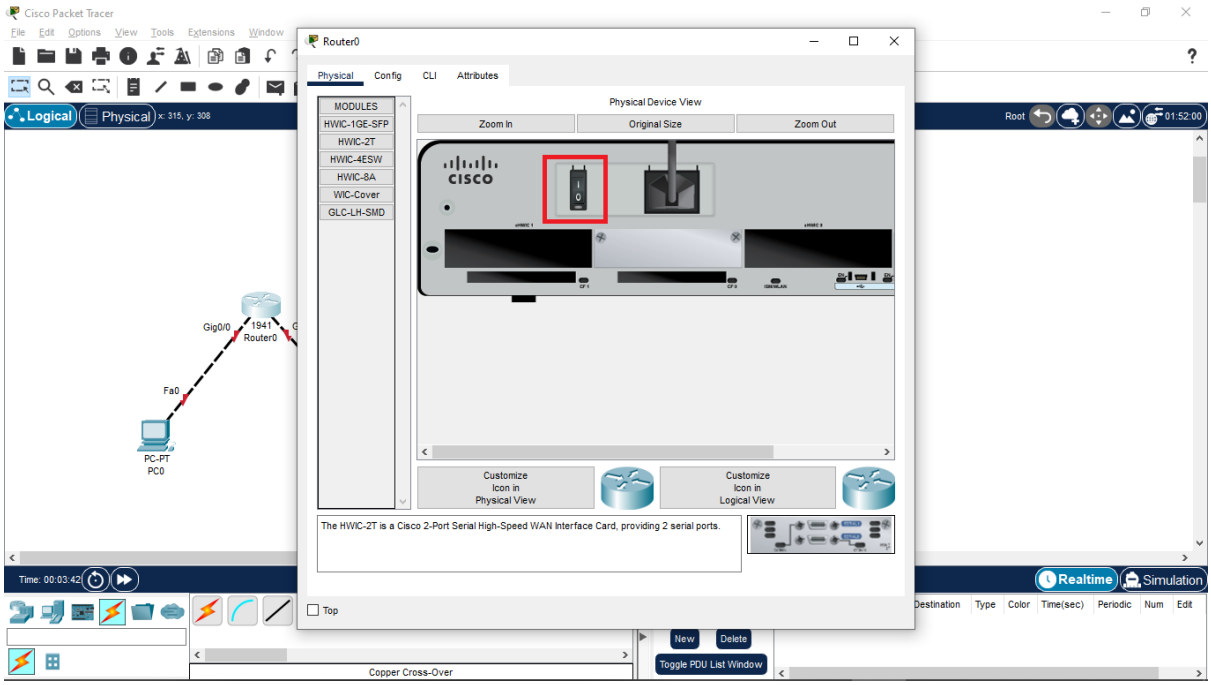
Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit 0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit 0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit 0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit 0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-

Procedure:

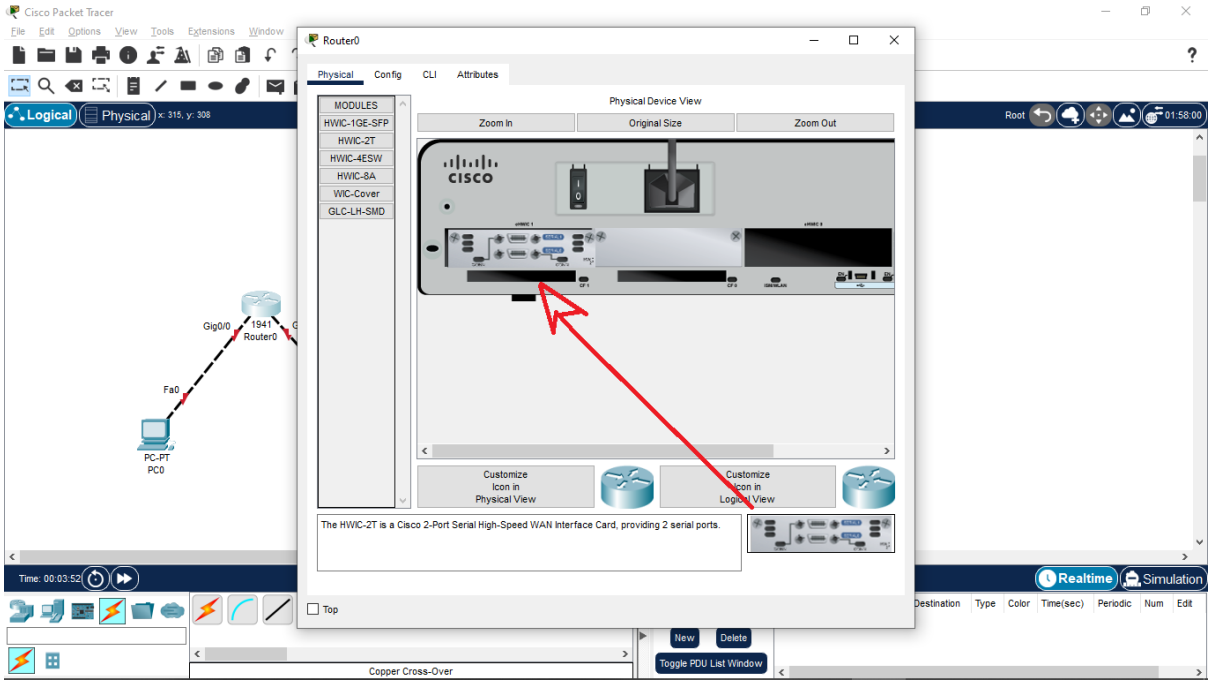
Step 1: Drag 4 PCs and 2 routers in the console area as shown in figure



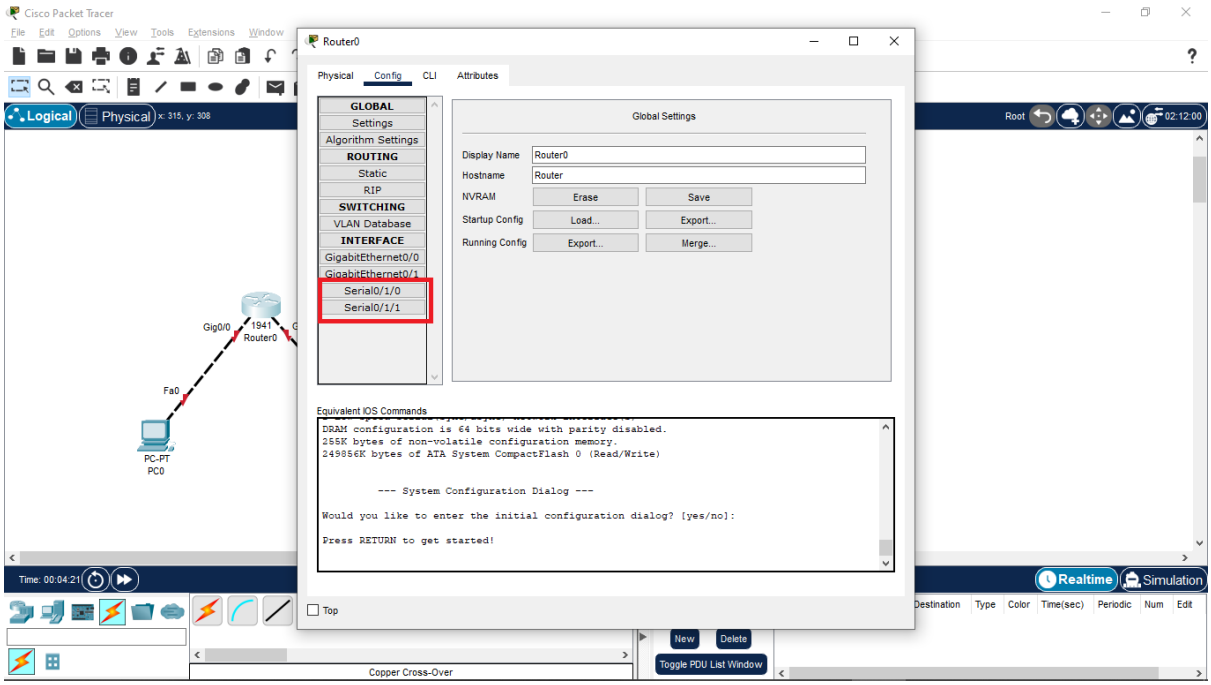
Step 2: Click on Router0 and go to Physical tab. Click HWIC2T in the left pane and Click on zoom in. Switch off the Hardware



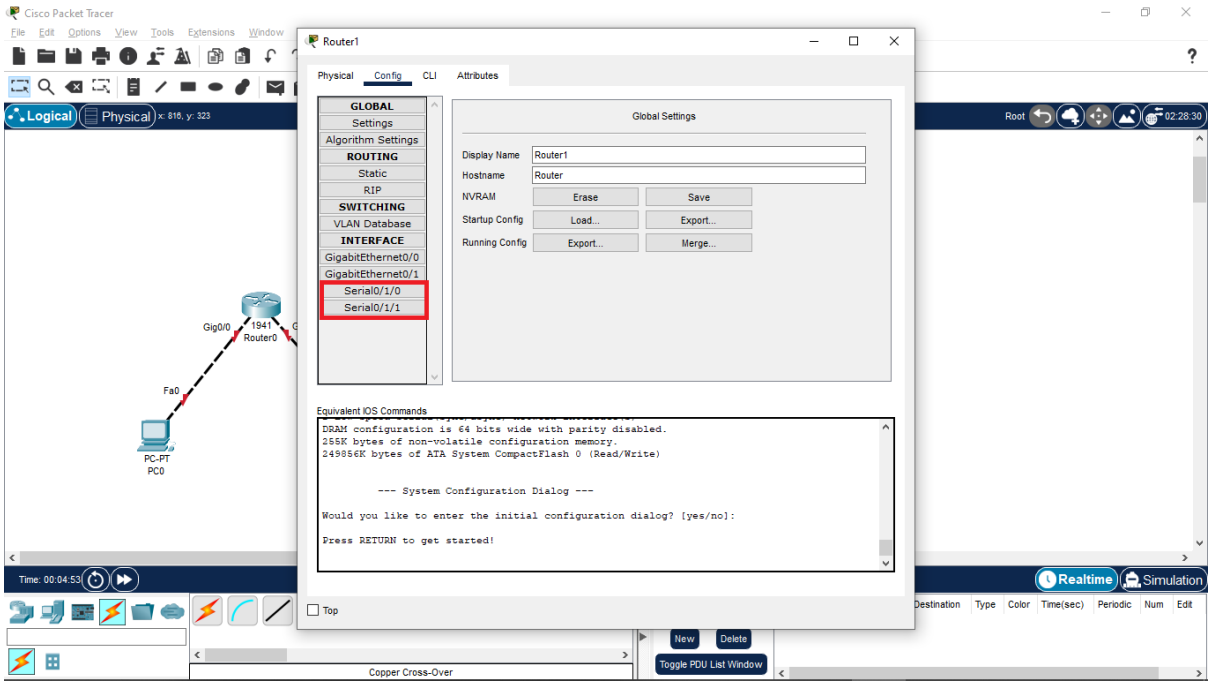
Step 3: Find the console from lower right corner. Drag and drop the console in the empty area as shown in the figure.



Step 4: Now again switch on the hardware and check in config tab for 2 serial ports added.

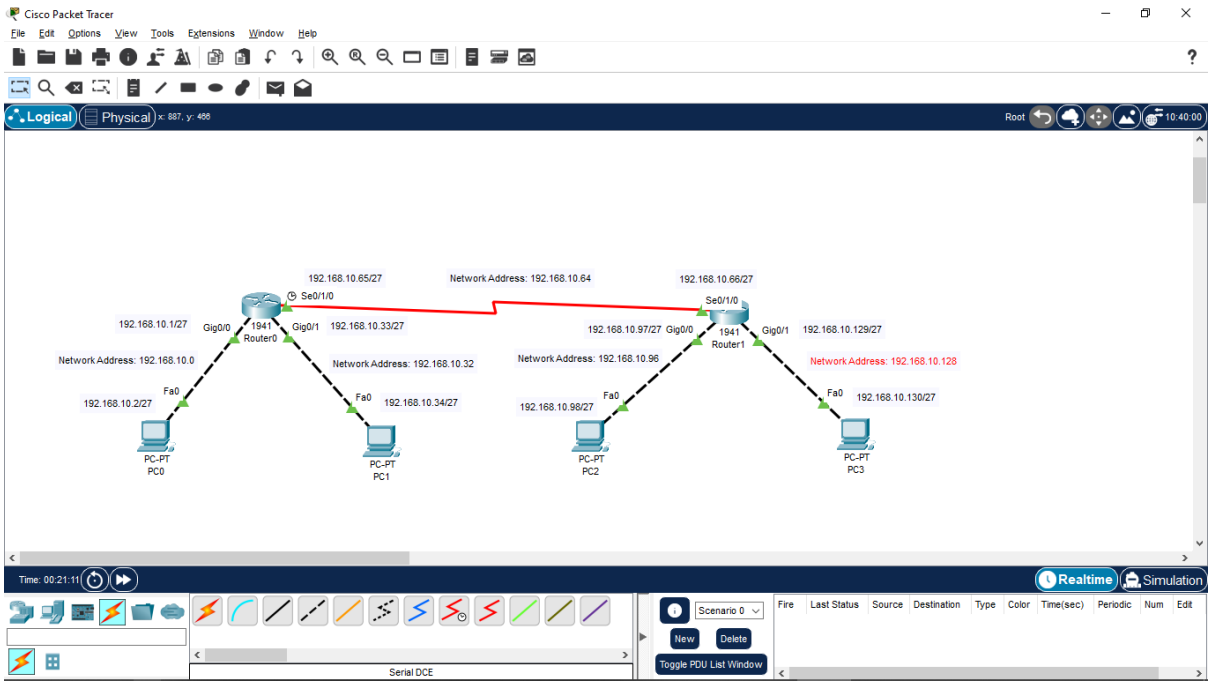


Step 5: Repeat the same procedure (Step 3 and Step 4) for Router1



Step 6: Now the PCs are physically connected through Router. To establish logical connectivity, assign IP addresses for 4 PCs (each 1 interface and corresponding router interface as gateway) and 2 Routers (each 3 ip addresses for 3 interfaces) as shown in the following table.

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit 0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit 0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit 0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit 0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-



Scenario with Network Address for each link

Step 7:

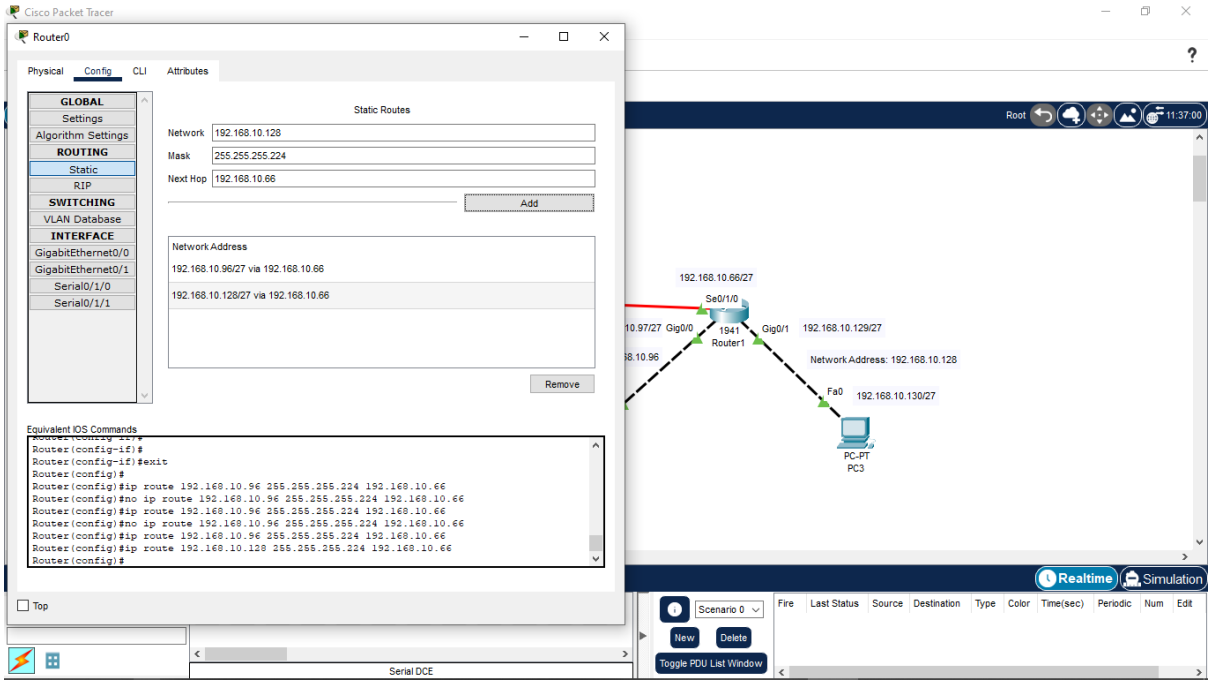
- **To enable packet transmission among the devices in the scenario, Static Routing has to be configured.**
- **To configure static routing, unknown networks and next-hop IP address to reach the unknown network for Router0 and Router1 has to be determined.**
- **Note: While specifying devices we should use IP-Address and while specifying network we should use Network Address.**
- **Unknown networks for the routers are derived in the following table**

Device	Known Networks	Subnet Mask	Unknown Networks	Subnet Mask	Next-hop Address
Router0	192.168.10.0	255.255.255.224	192.168.10.96	255.255.255.224	192.168.10.66
Router0	192.168.10.32	255.255.255.224	192.168.10.128	255.255.255.224	192.168.10.66
Router0	192.168.10.64	255.255.255.224	-	-	-
Router1	192.168.10.96	255.255.255.224	192.168.10.0	255.255.255.224	192.168.10.65
Router1	192.168.10.128	255.255.255.224	192.168.10.32	255.255.255.224	192.168.10.65
Router1	192.168.10.64	255.255.255.224	-	-	-

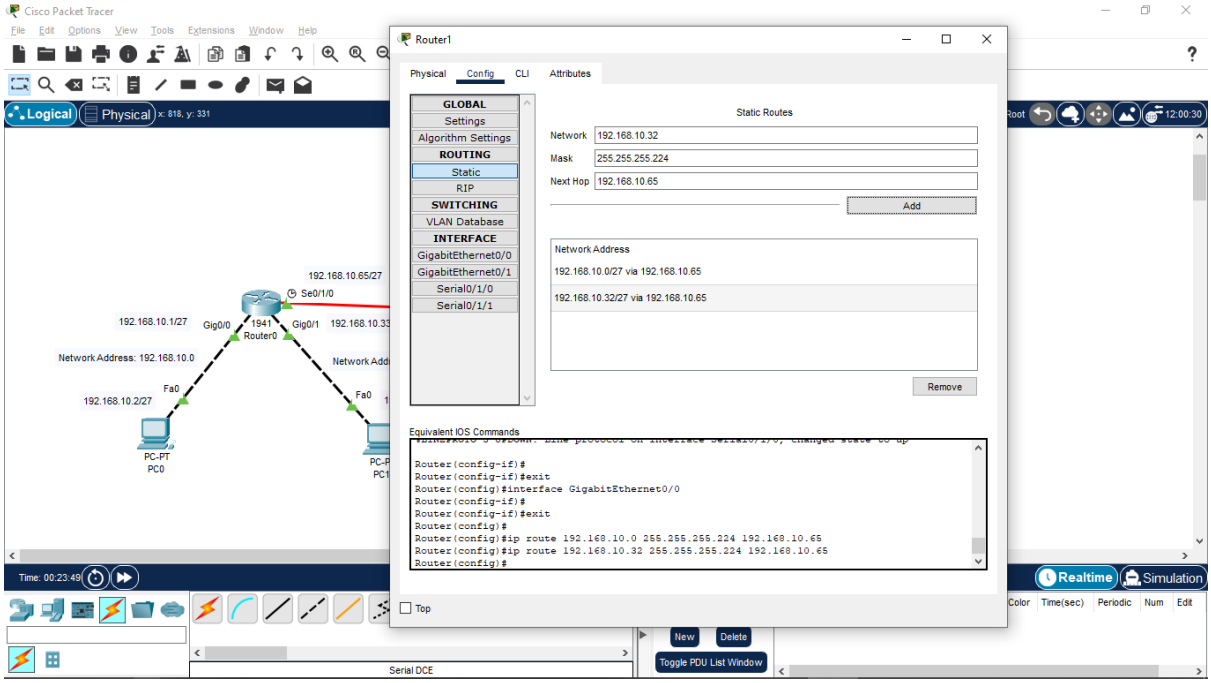
Only unknown networks should be configured for static routing

Step 8:

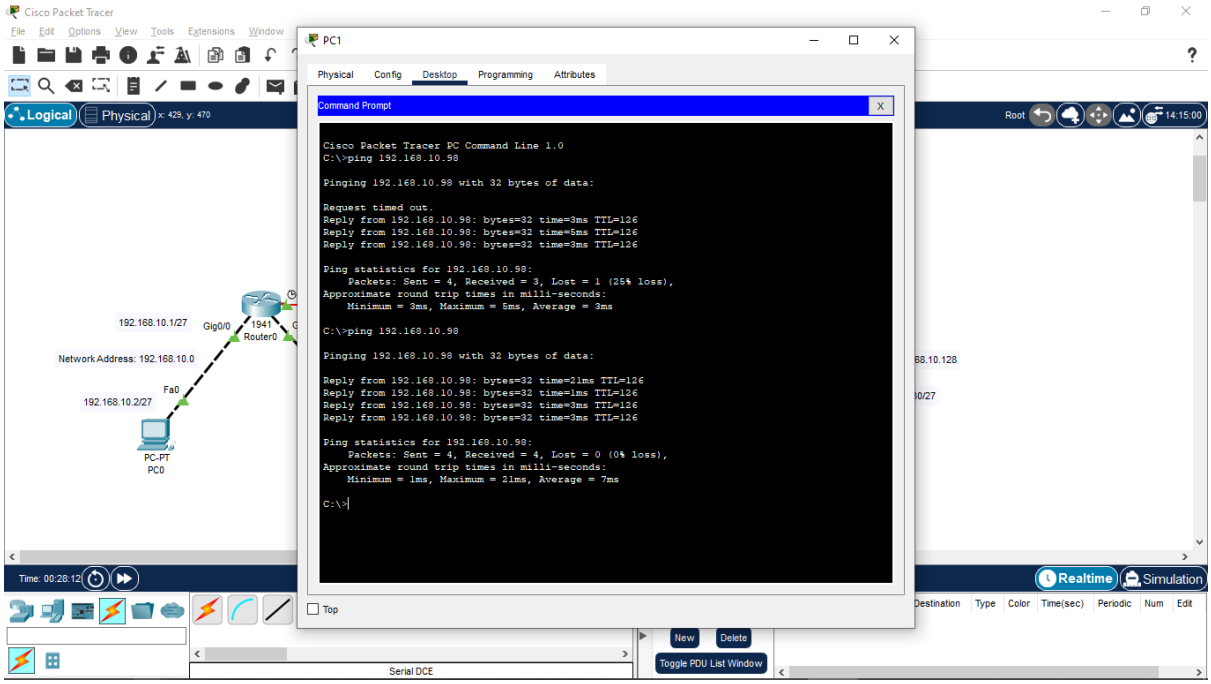
- To configure static routing, click on
    - Router0 => Config tab => Static =>Enter network address (refer unknown network for router0) => Subnet Mask for network address => Next-hop address => Add network
- Repeat the same to add the next network.
- Two networks should be added for the given scenario



Step 9: Repeat the same procedure to configure for Router1



Step 10: After configuration of Static routing in both Routers, Check the connectivity among any two devices using Ping Command



Step 11:

- To check routing table, go to CLI tab in Router and press enter to get the router prompt.
    - Router>
- Now type enable or en and press enter
    - Router>en
    - Router#

Follow the command “show ip route” to get the routing table of a router

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

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.10.0/27 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
C 192.168.10.32/27 is directly connected, GigabitEthernet0/1
L 192.168.10.33/32 is directly connected, GigabitEthernet0/1
C 192.168.10.64/27 is directly connected, Serial0/1/0
L 192.168.10.65/32 is directly connected, Serial0/1/0
S 192.168.10.96/27 [1/0] via 192.168.10.66
S 192.168.10.128/27 [1/0] via 192.168.10.66
```

Exercise 5. a: VLAN Switch Configuration

Objective: To demonstrate the configuration of VLAN switch with authentication

Pre-requisite: IP Address, Range of IP Address, Classes of IP Address, Subnetting

Components:

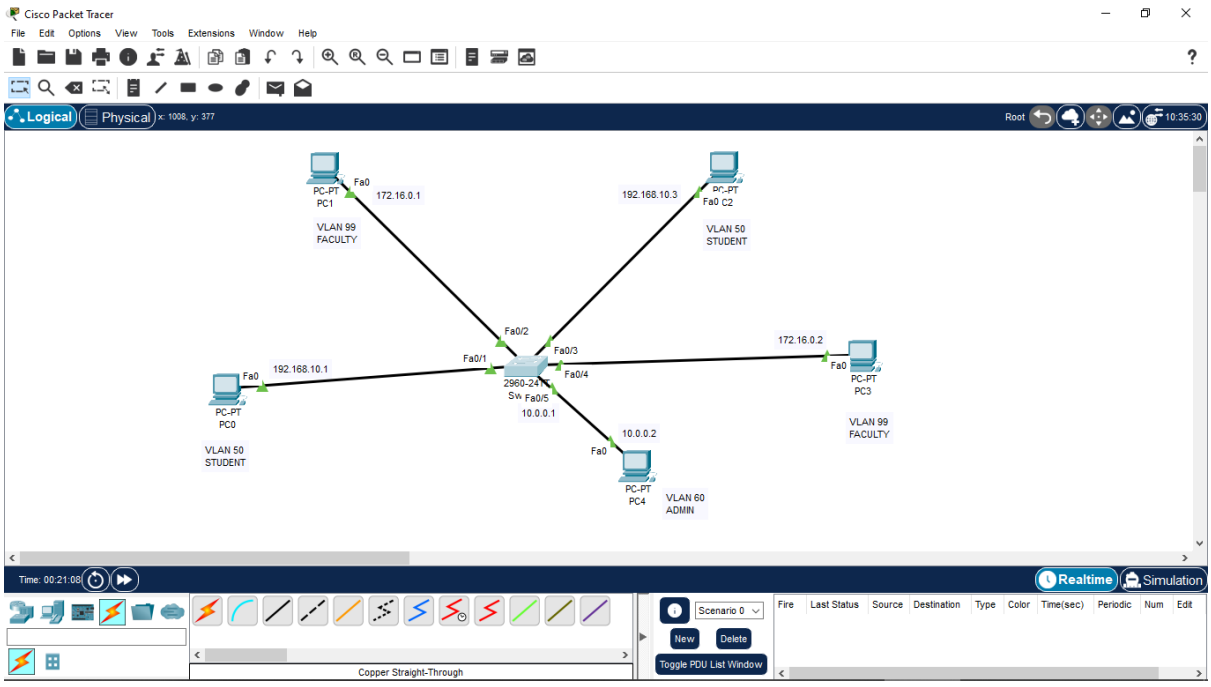
Devices	Required Nos
PCs	5
Copper straight-through Cables	5
Switch 2940	1

Addressing Table:

VLAN	Device	Interface	IP Address	Subnet Mask	Gateway
VLAN 50	PC0	Fa0/0	192.168.10.1	255.255.255.0	-
VLAN 99	PC1	Fa0/0	172.16.0.1	255.255.0.0	-
VLAN 50	PC2	Fa0/0	192.168.10.2	255.255.255.0	-
VLAN 99	PC3	Fa0/0	172.16.0.2	255.255.0.0	-
VLAN 60	PC3	Fa0/0	10.0.0.2	255.0.0.0	-
	Switch0	Fa0/5	10.0.0.1	255.0.0.0	-

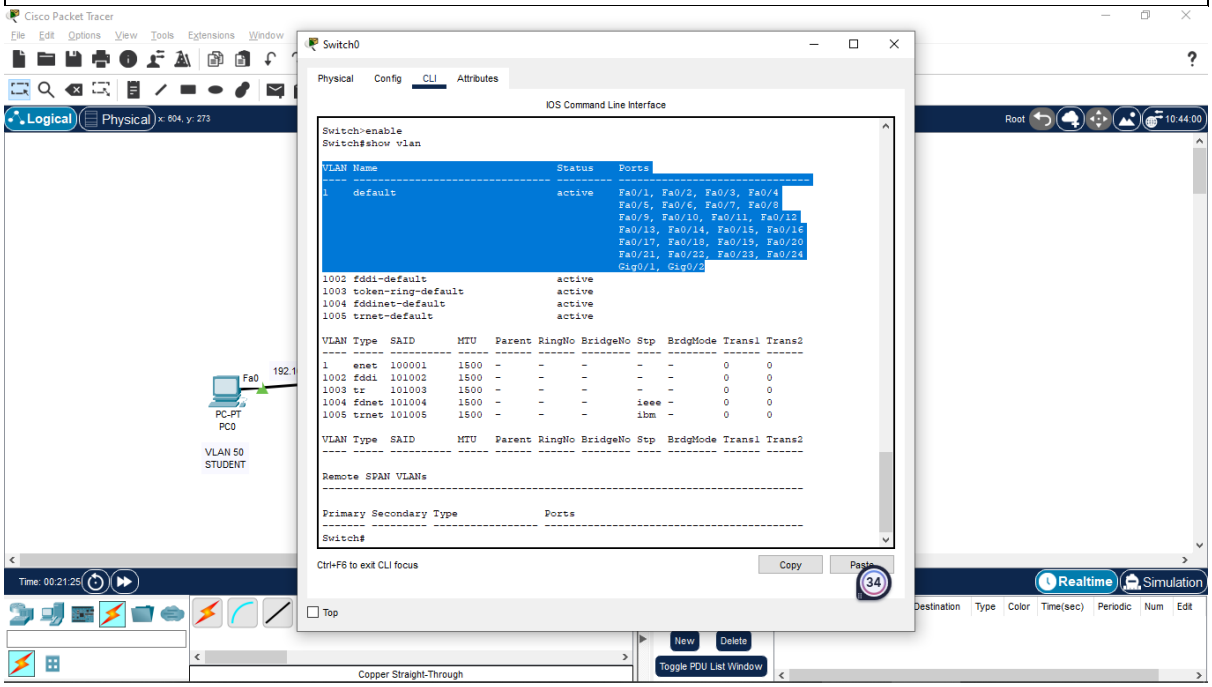
Procedure:

Step 1: Drag 5 PCs and 1 number of 2940 Switch in the console area and configure the IP address for all the PCs as shown in figure [Do not try to configure IP address for switch in this step]



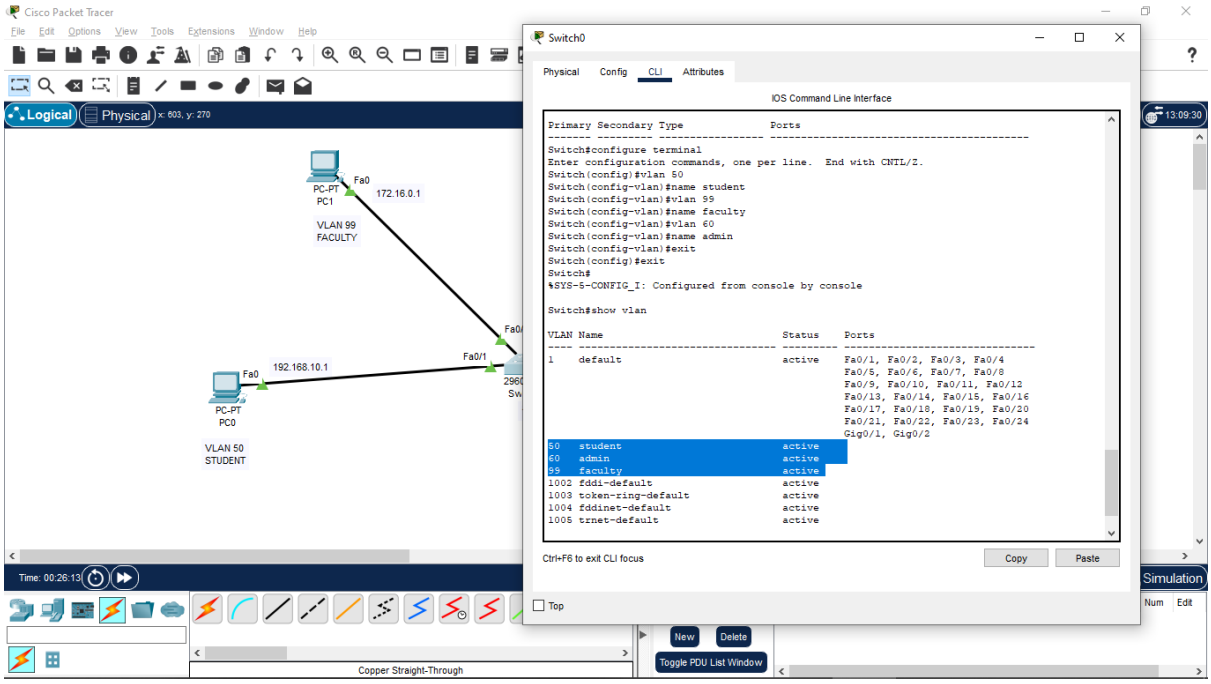
Step 2: To check the default VLAN, Click on Switch and go to the CLI tab and type the following in the prompt to check the default VLANs referred to as 1,1002,1003,1004,1005 with their names, status and ports assigned for the VLANs. Note that VLAN1 is the default VLAN where all ports are assigned to. You cannot delete these default VLANs but assign the ports to different VLANs

```
Switch>enable
Switch#show vlan
```



Step 3: To create new VLANs, type the following commands in the CLI

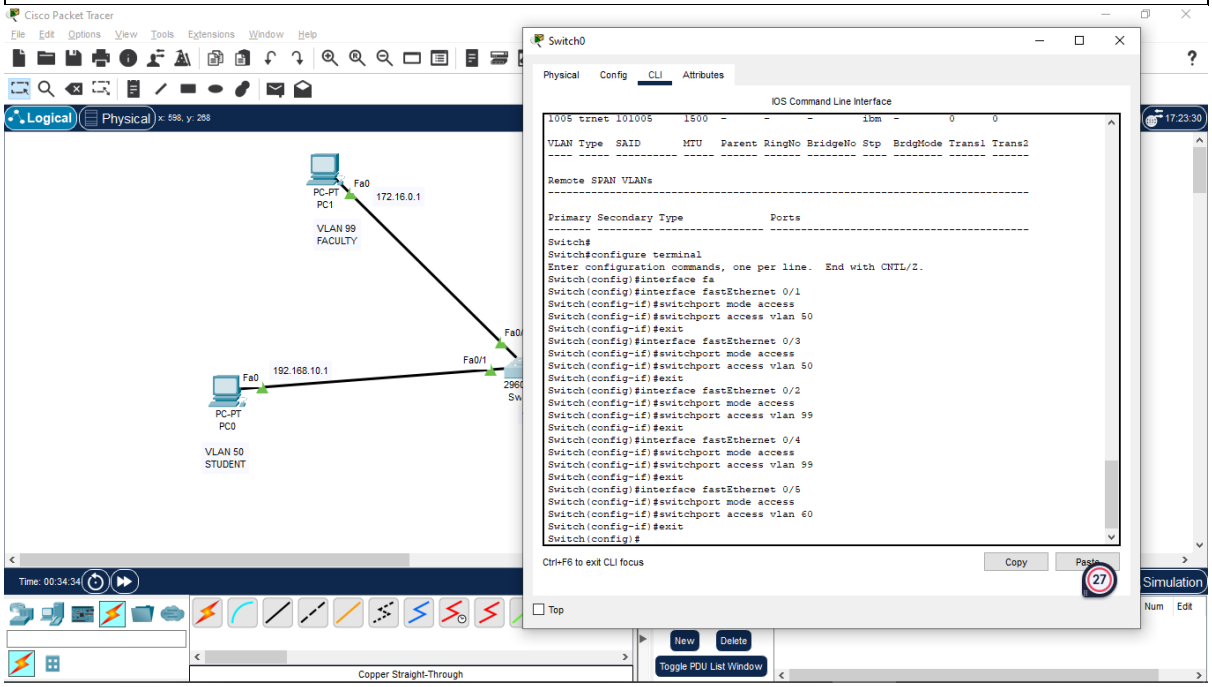
```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name student
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name faculty
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name admin
Switch(config-vlan)#exit
Switch(config)#exit
Switch#show vlan
```



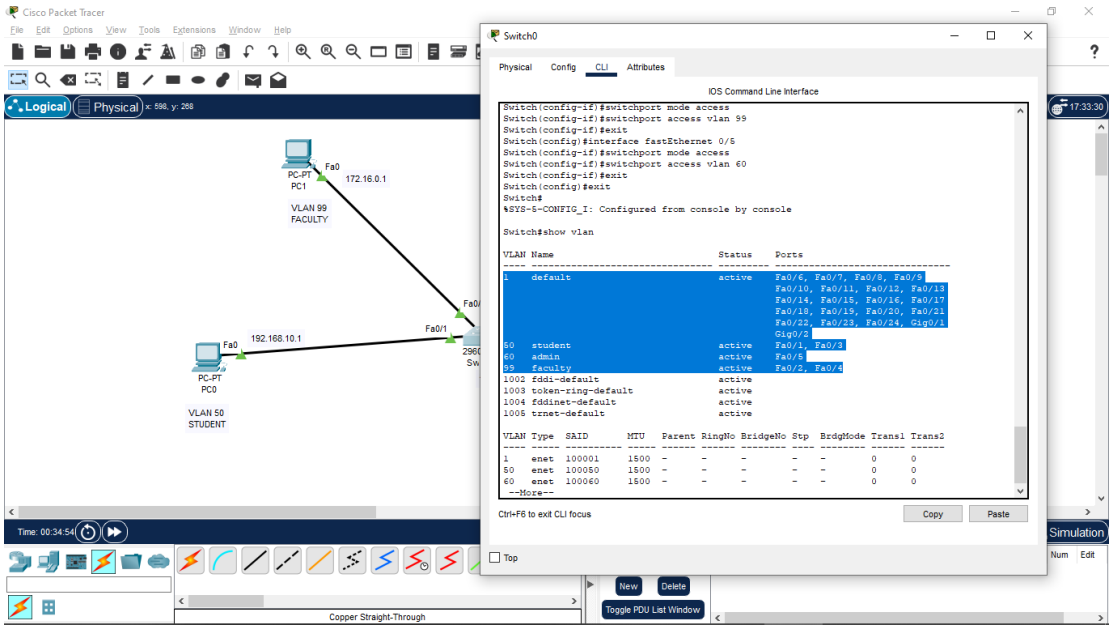
Step 4: Now the VLANs are created and are active. To assign the ports to the corresponding VLAN, type the following commands.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/4
```

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
Switch(config)#
```

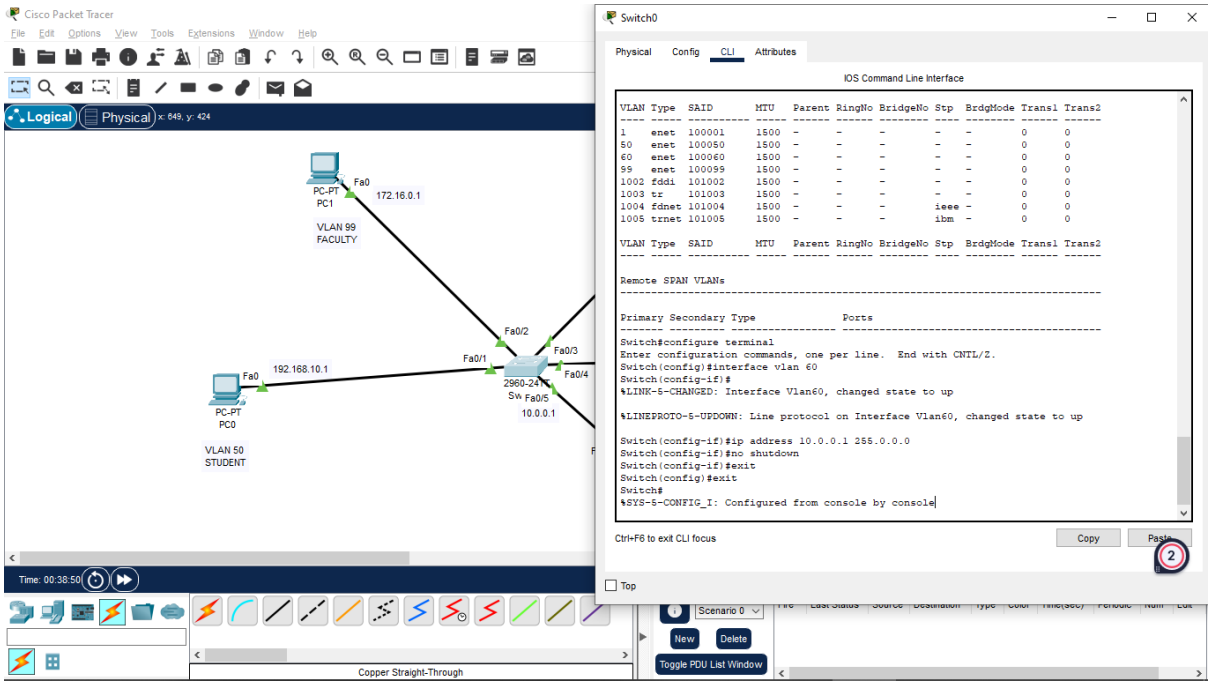


Step 5: Again check with the command "show vlan" in switch# prompt to check

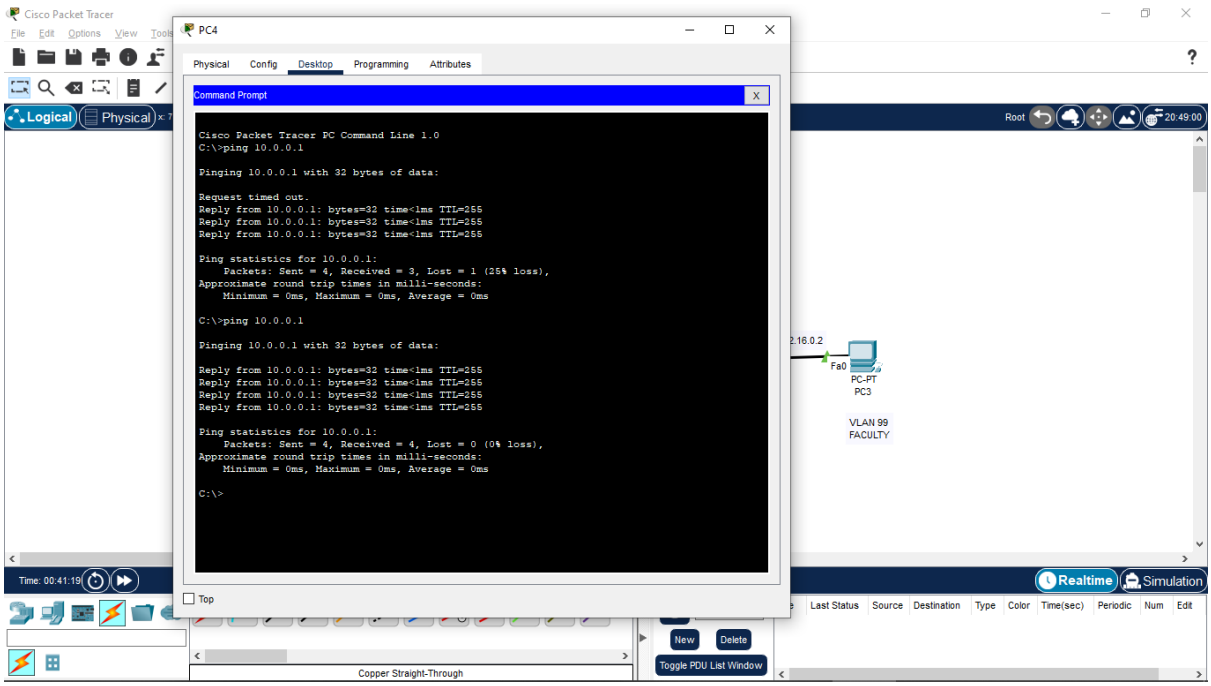


Step 6: The admin VLAN 60 needs to be enabled with a remote access privilege. To do so, the VLAN 60 has to be assigned with an IP address. Type the following commands to assign IP address for VLAN 60.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 60
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to up

Switch(config-if)#ip address 10.0.0.1 255.0.0.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
```

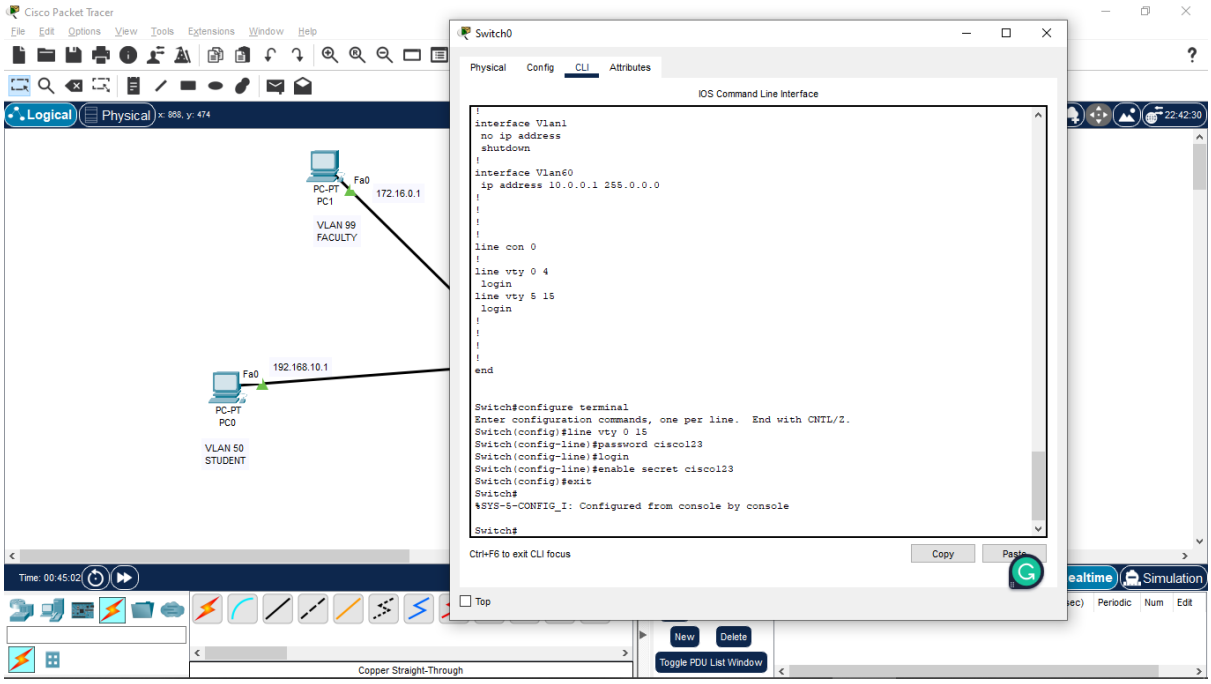


Step 7: To check the connectivity of the VLAN 60 IP address, click on PC5 (IP address – 10.0.0.2) and go to Desktop => Command Prompt => ping 10.0.0.1



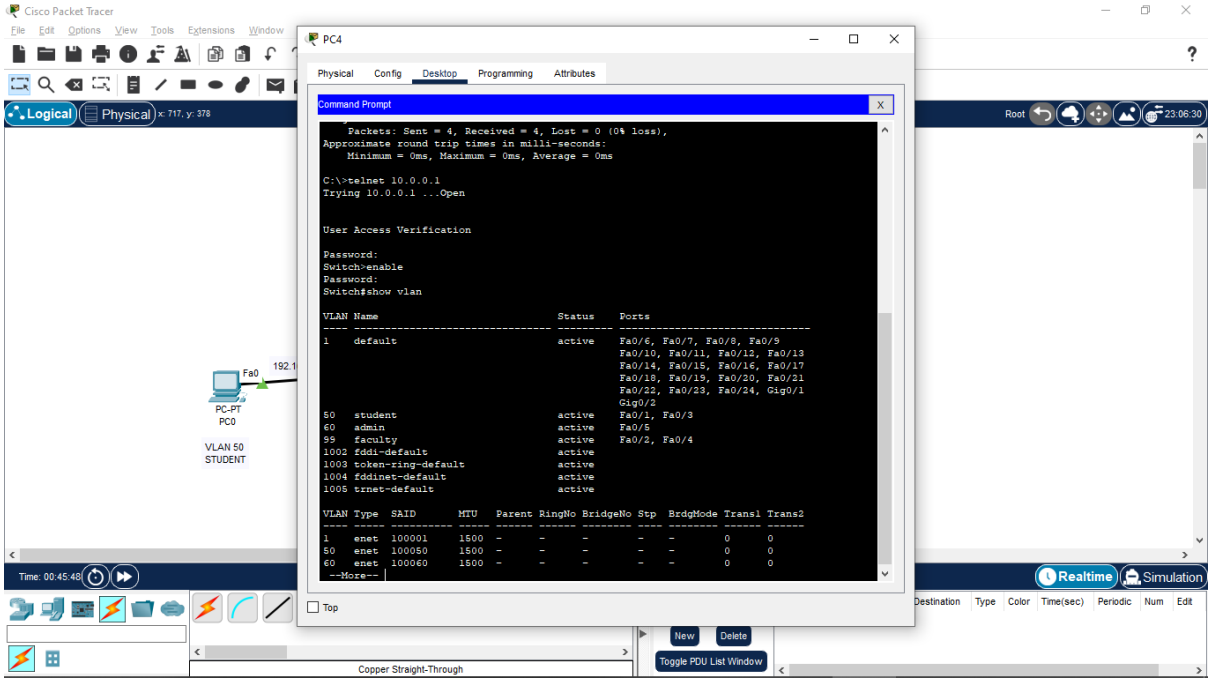
Step 8: To provide remote access privilege with authentication, type the following, in the CLI tab of switch.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 15
Switch(config-line)#password cisco123
Switch(config-line)#login
Switch(config-line)#enable secret cisco123
Switch(config)#exit
Switch#
```



Step 8:

- To check for the remote access and authentication, click on PC5 and go to command prompt and type “telnet 10.0.0.1”
- Enter the password “cisco123” whenever asked
- Once authenticated to “Switch>” prompt, type “enable” and try the command “show vlan” to find out all the VLANs assigned in the switch from the PC5.



Exercise 5. b: Router Configuration through a Console

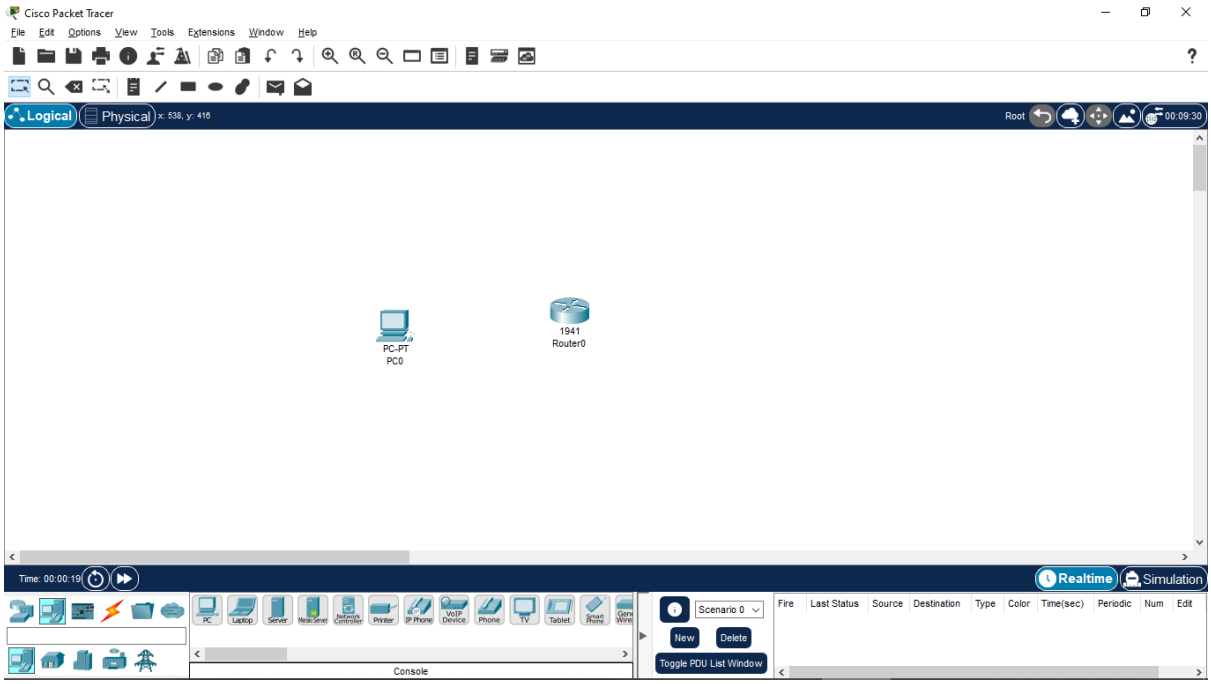
Objective: To demonstrate the configuration of Router with authentication through a console

Components:

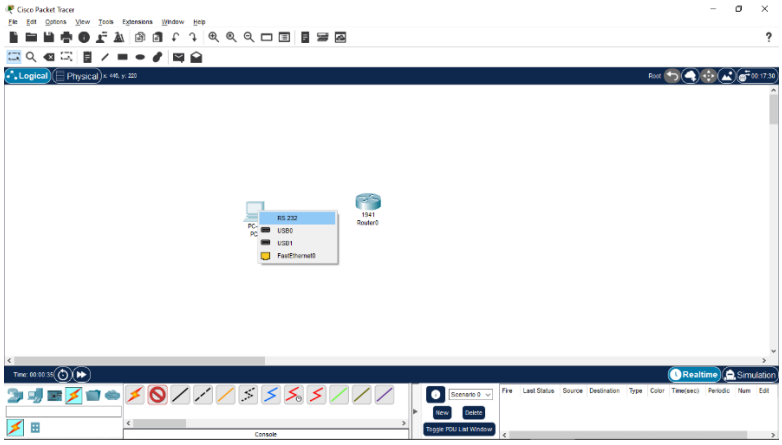
Devices	Required Nos
PCs	1
Console Cables	1
Router 1941	1

Procedure:

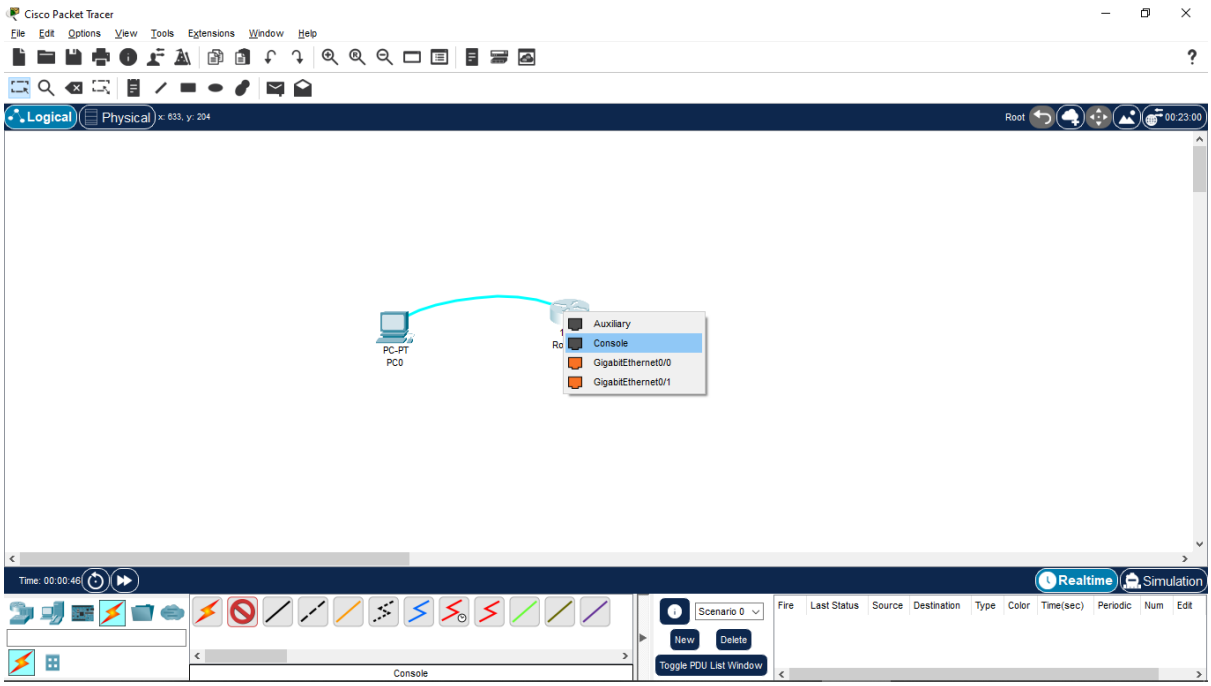
Step 1: Drag 1 PC and 1 number of 1941 Router in the console area



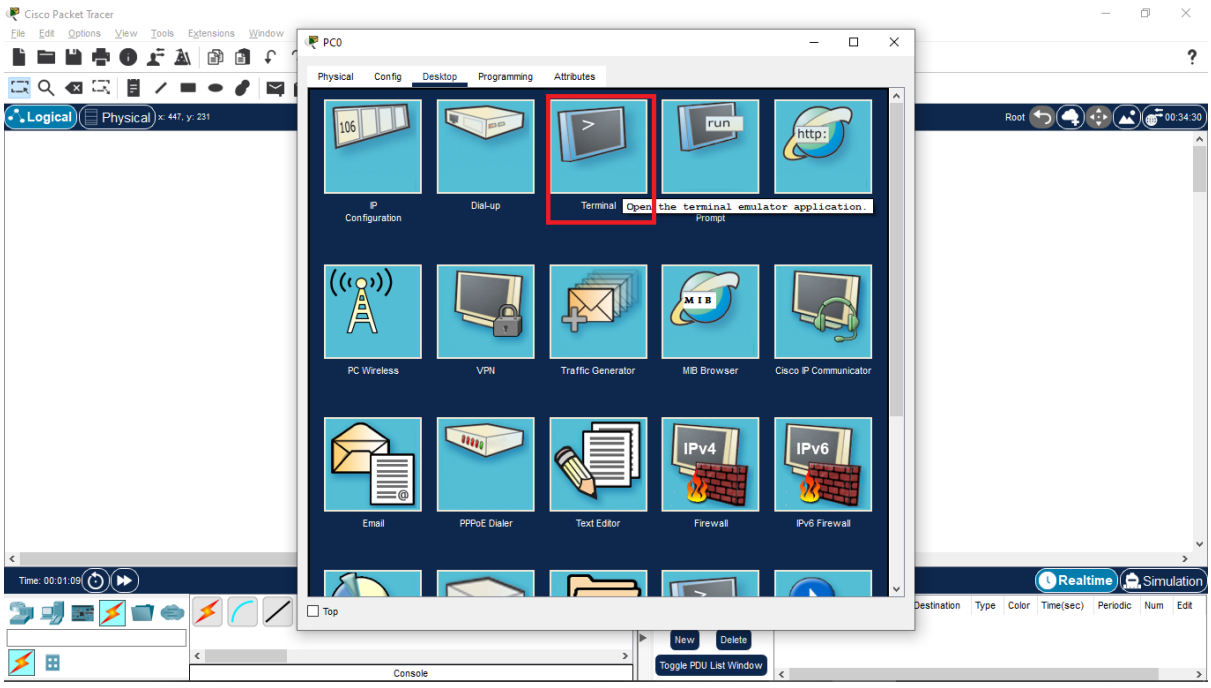
Step 2: Click on Connectivity and select Console cable. Click on PC and select RS232 interface.



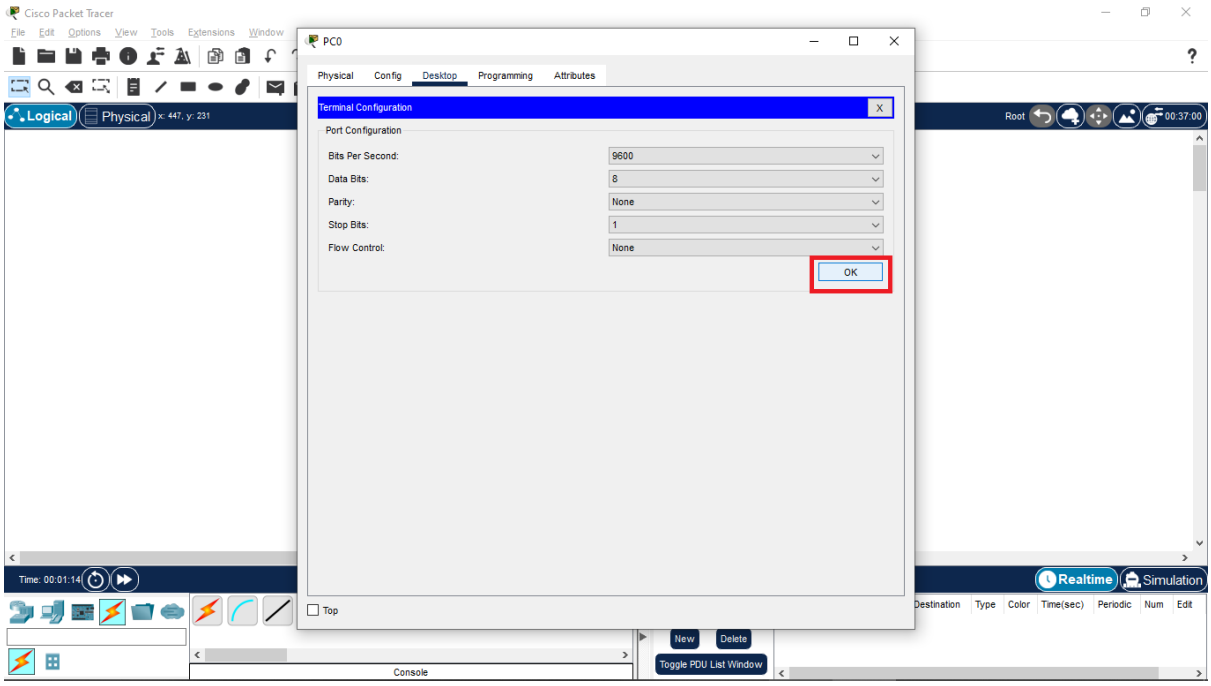
Step 3: Now click on Router and select Console interface to connect PC and Router with Console cable



Step 4: Now click on PC0 and go to Desktop => Terminal



Step 5: Click on OK for default Terminal parameters.



Step 6:

- Enter “no” when prompted, and type the following to configure “line console password” as “cisco” and privilege mode password as “cisco123”
- The “copy run start” command copies the running configuration parameters to start-up configuration parameters such that when you reload or reboot the router the configured parameters will not be erased from the Router memory RAM.

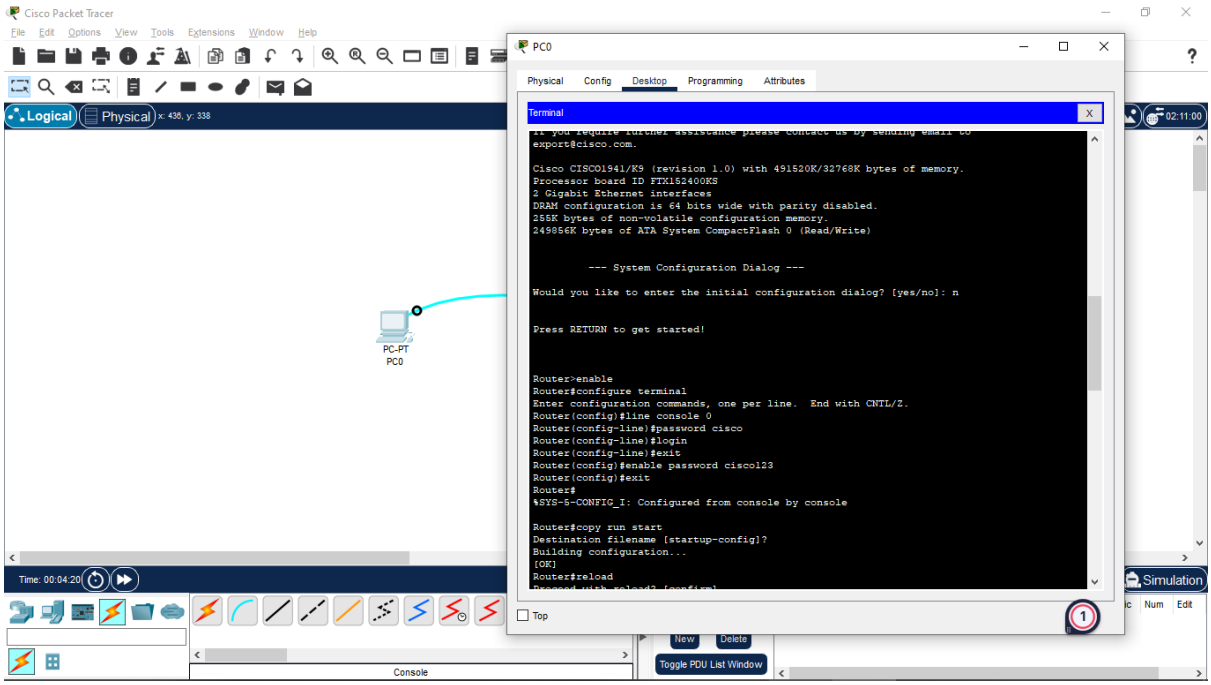
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password cisco123
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy run start
Destination filename [startup-config]?
```

Building configuration...

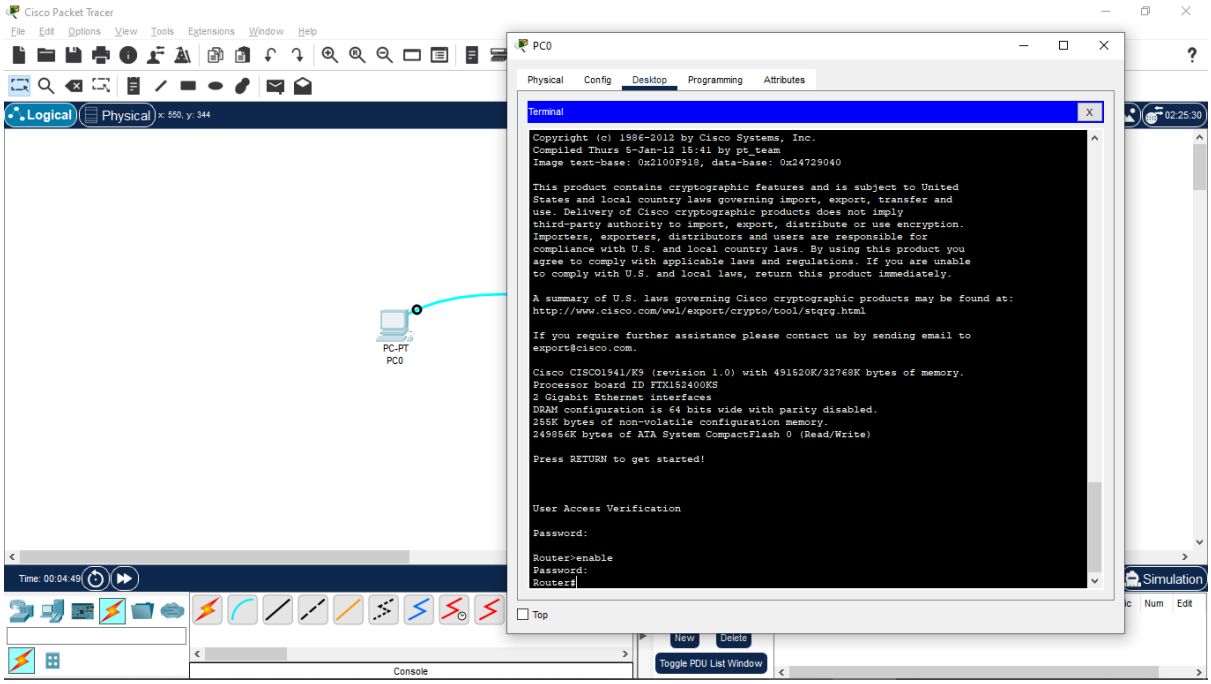
[OK]

Router#reload

Proceed with reload? [confirm]



Step 7: After reloading enter “cisco” as the password, when prompted to remote access and the password “cisco123” when you type “enable” to use Privilege mode access of Router from PC.



Exercise 6: Demonstration of Static and Default Routing

[Note: Static Routing procedure is same as Exercise 4 and for Default Routing Step 8 and Step 9 must be replaced with Step 12 and Step 13]

Exercise 6. a: Demonstration of Static Routing

Objective: To demonstrate the configuration of IP Addressing with Subnetting in WAN Configuration

Pre-requisite: IP Address, Range of IP Address, Classes of IP Address, Subnetting

Components:

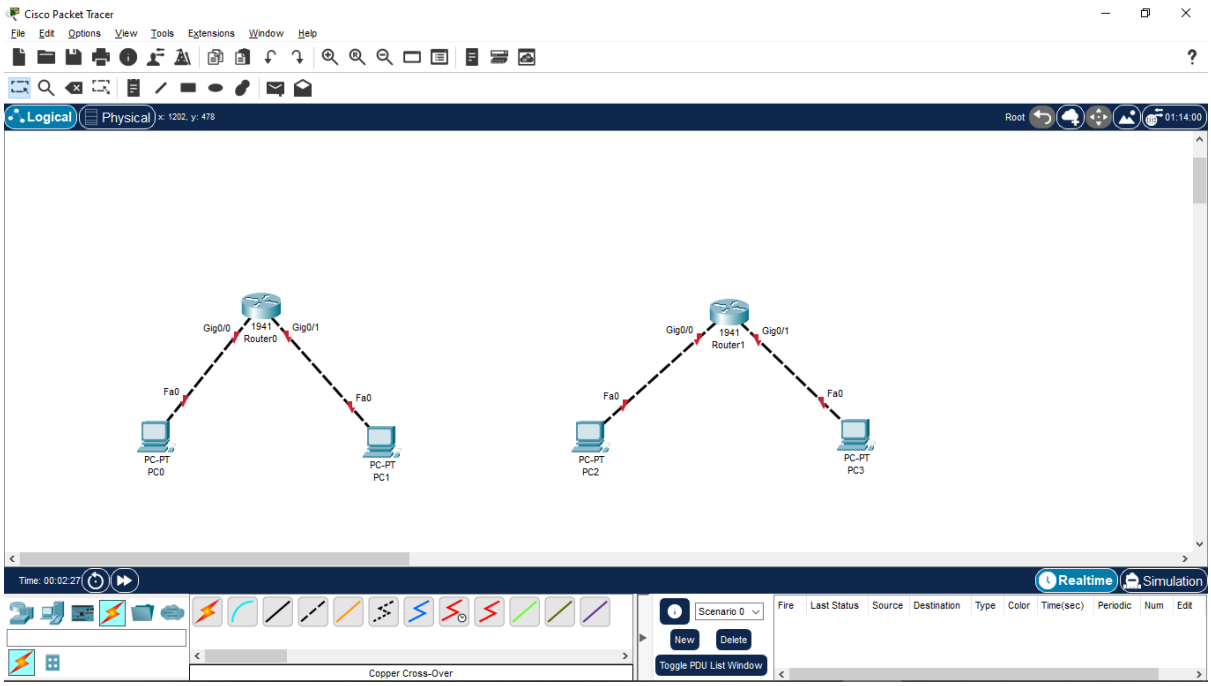
Devices	Required Nos
PCs	4
Copper cross-over Cables	4
Routers	2
Serial DCE	1

Addressing Table:

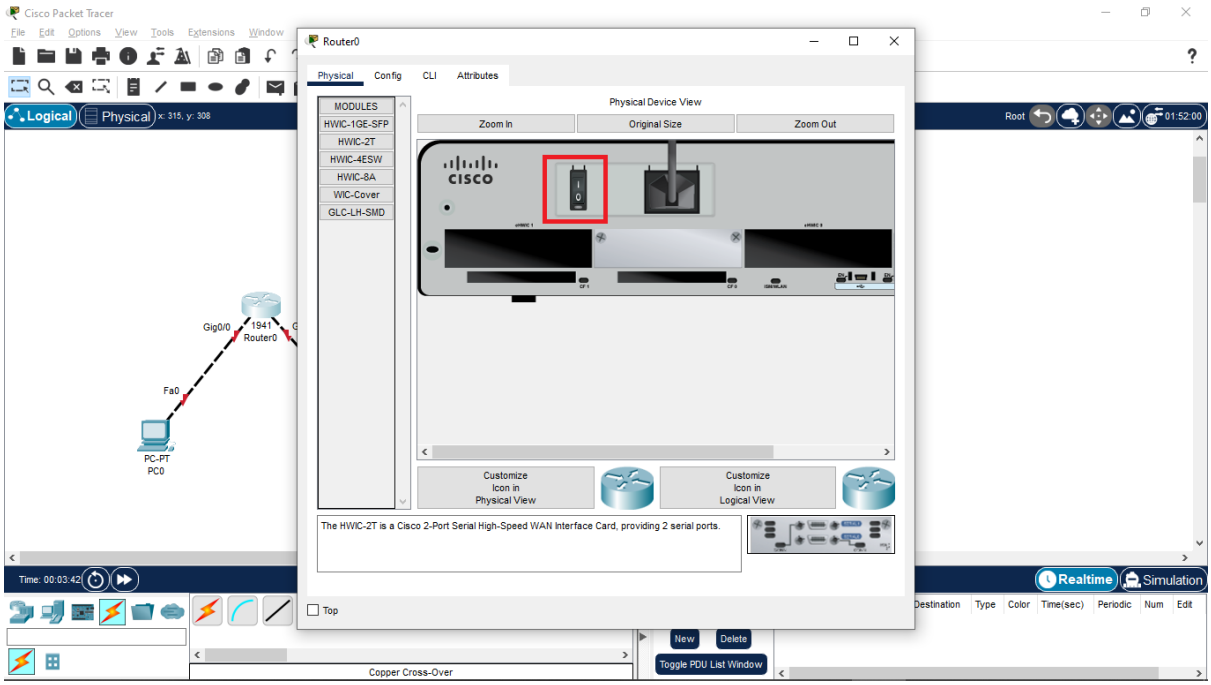
Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit 0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit 0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit 0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit 0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-

Procedure:

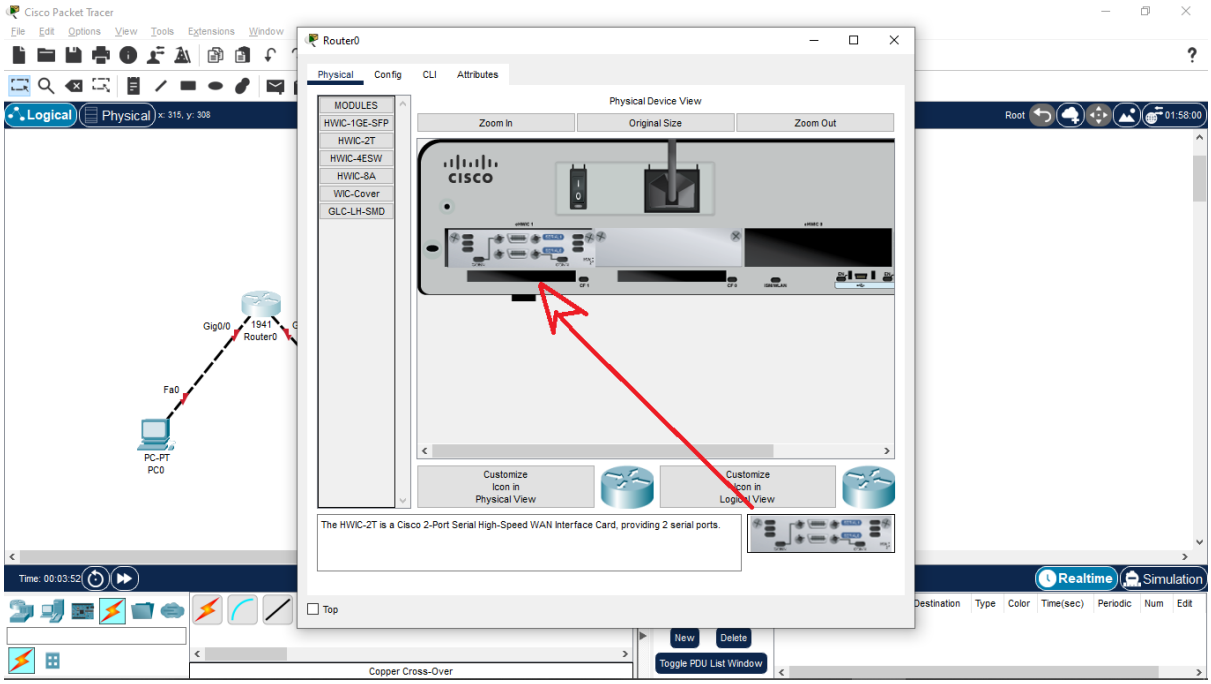
Step 1: Drag 4 PCs and 2 routers in the console area as shown in figure



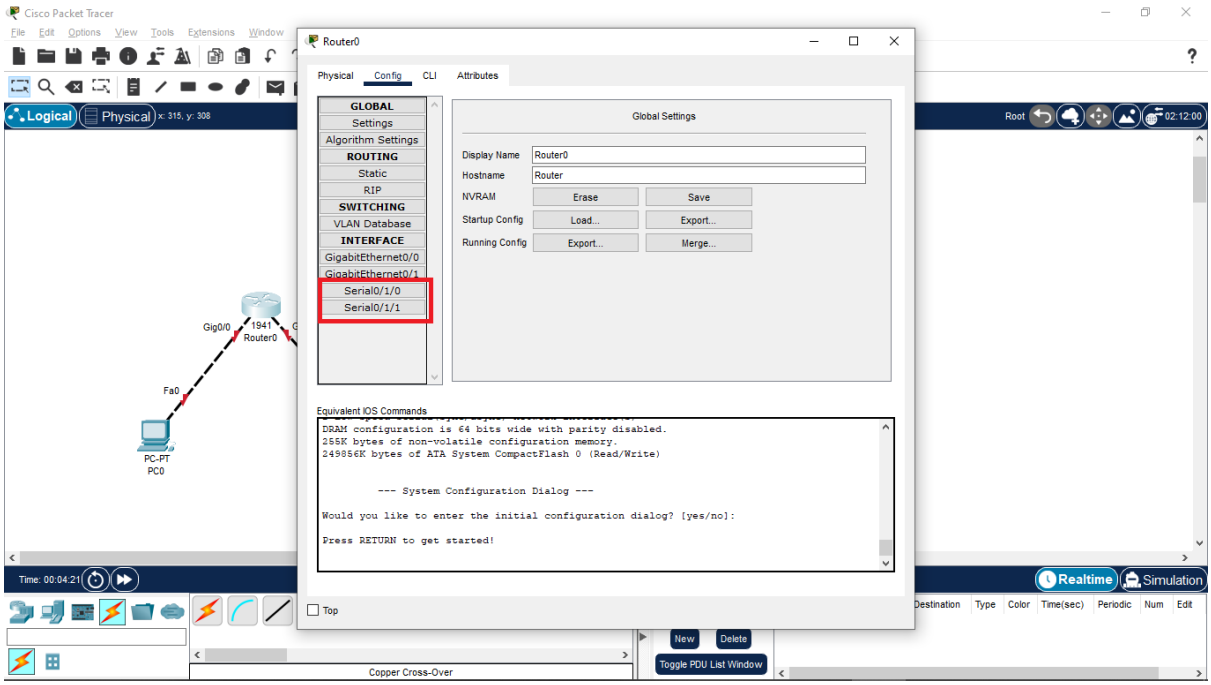
Step 2: Click on Router0 and go to Physical tab. Click HWIC2T in the left pane and Click on zoom in. Switch off the Hardware



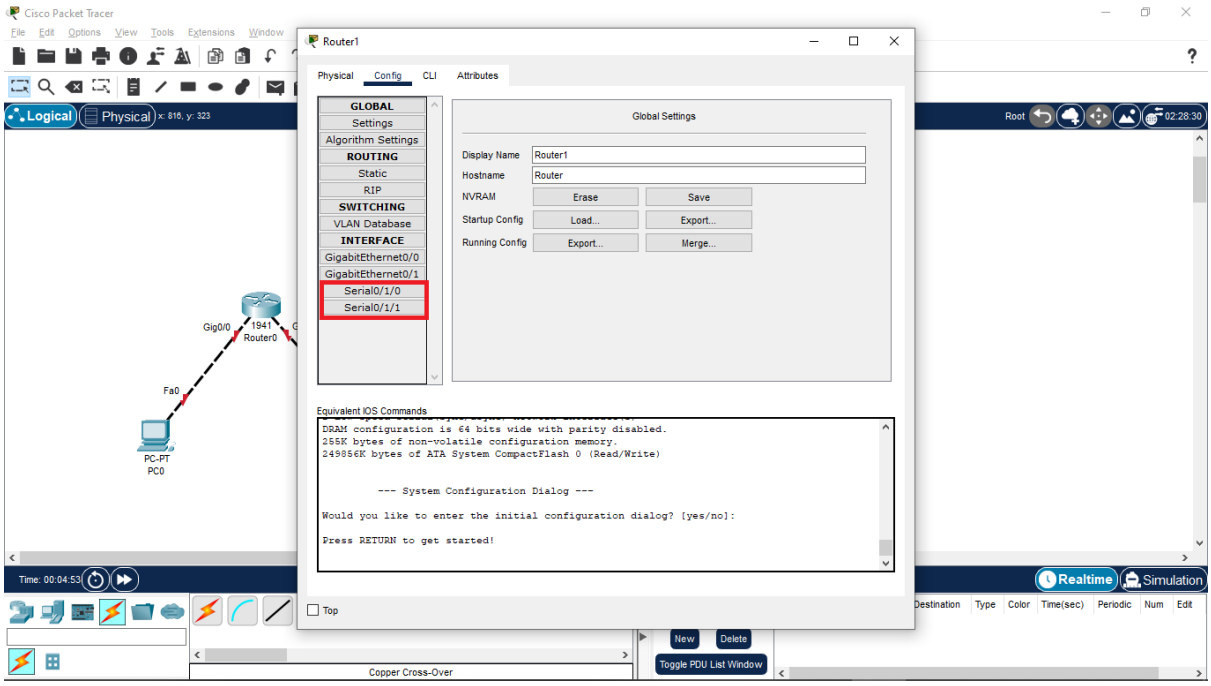
Step 3: Find the console from lower right corner. Drag and drop the console in the empty area as shown in the figure.



Step 4: Now again switch on the hardware and check in config tab for 2 serial ports added.

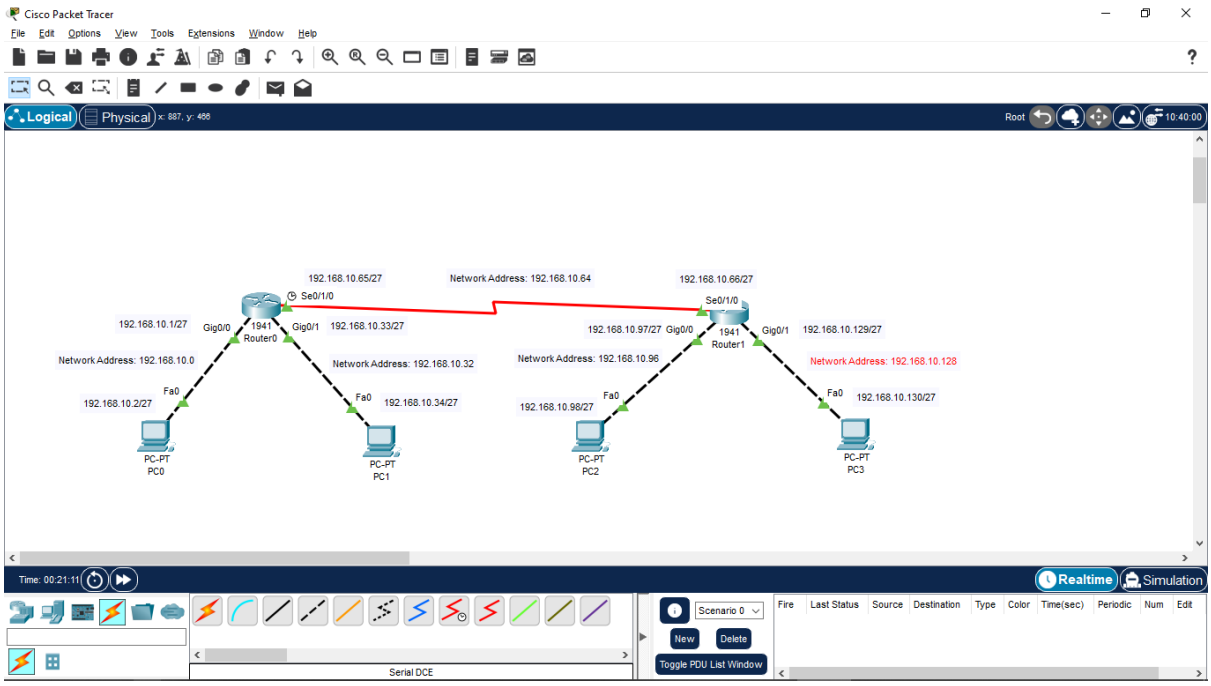


Step 5: Repeat the same procedure (Step 3 and Step 4) for Router1



Step 6: Now the PCs are physically connected through Router. To establish logical connectivity, assign IP addresses for 4 PCs (each 1 interface and corresponding router interface as gateway) and 2 Routers (each 3 ip addresses for 3 interfaces) as shown in the following table.

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit 0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit 0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit 0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit 0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-



Scenario with Network Address for each link

Step 7:

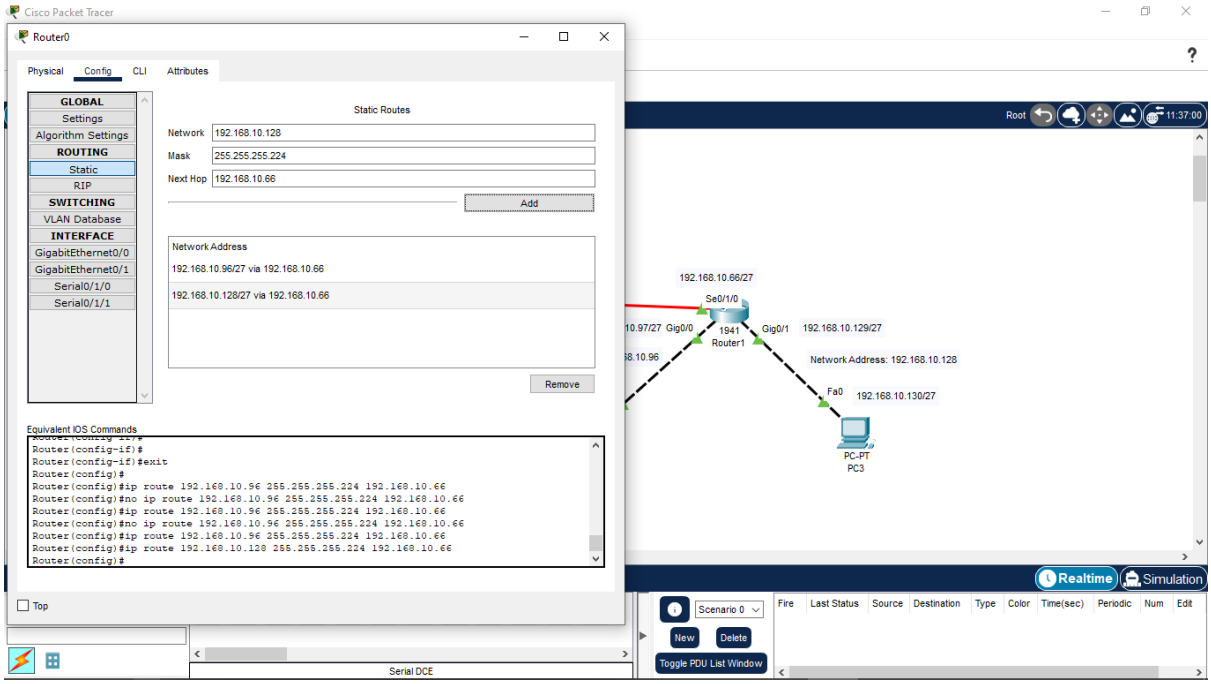
- **To enable packet transmission among the devices in the scenario, Static Routing has to be configured.**
- **To configure static routing, unknown networks and next-hop IP address to reach the unknown network for Router0 and Router1 has to be determined.**
- **Note: While specifying devices we should use IP-Address and while specifying network we should use Network Address.**
- **Unknown networks for the routers are derived in the following table**

Device	Known Networks	Subnet Mask	Unknown Networks	Subnet Mask	Next-hop Address
Router0	192.168.10.0	255.255.255.224	192.168.10.96	255.255.255.224	192.168.10.66
Router0	192.168.10.32	255.255.255.224	192.168.10.128	255.255.255.224	192.168.10.66
Router0	192.168.10.64	255.255.255.224	-	-	-
Router1	192.168.10.96	255.255.255.224	192.168.10.0	255.255.255.224	192.168.10.65
Router1	192.168.10.128	255.255.255.224	192.168.10.32	255.255.255.224	192.168.10.65
Router1	192.168.10.64	255.255.255.224	-	-	-

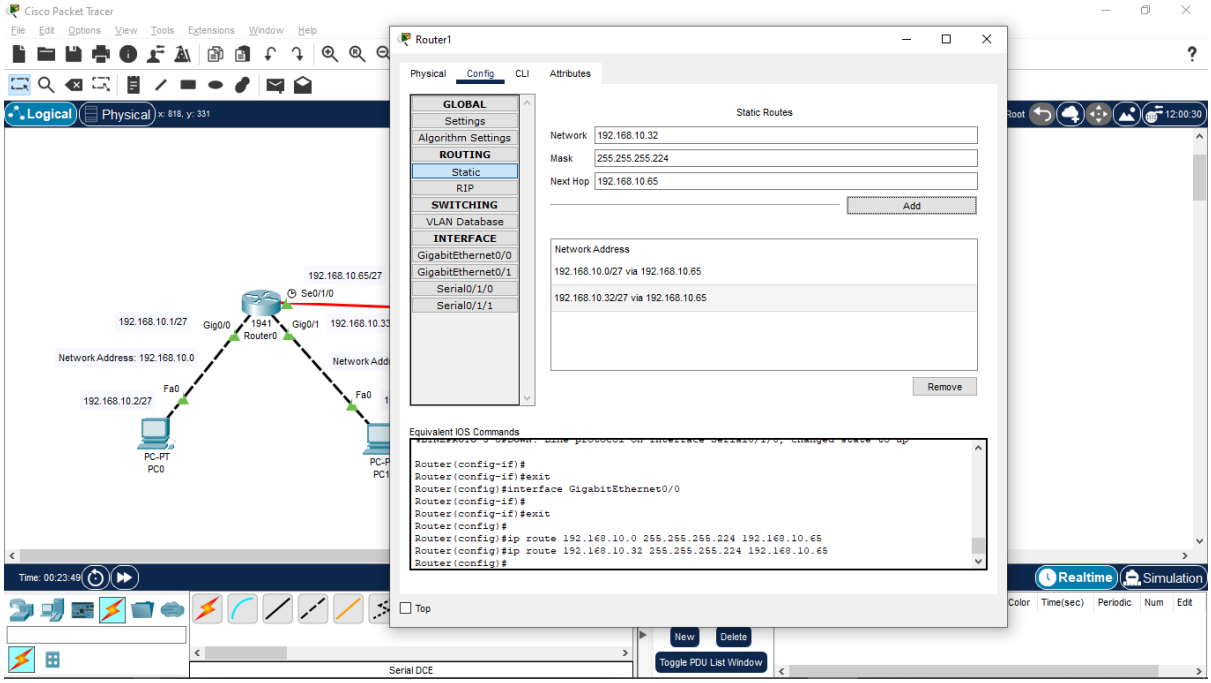
Only unknown networks should be configured for static routing

Step 8:

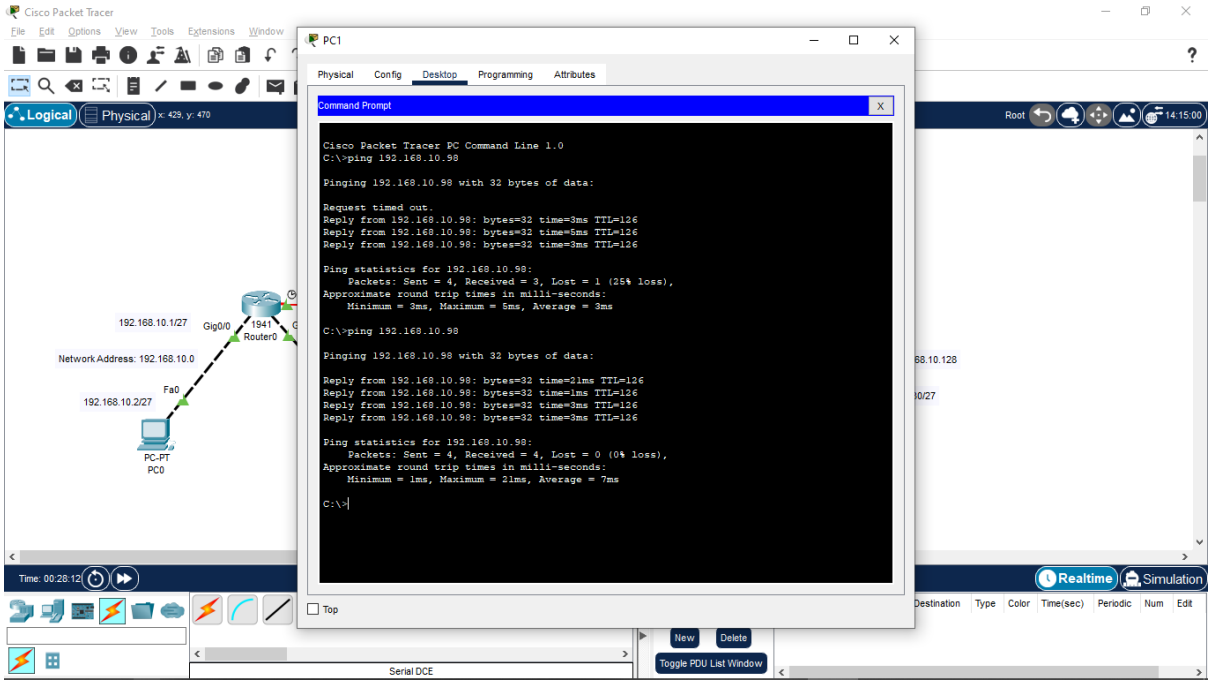
- To configure static routing, click on
    - Router0 => Config tab => Static =>Enter network address (refer unknown network for router0) => Subnet Mask for network address => Next-hop address => Add network
- Repeat the same to add the next network.
- Two networks should be added for the given scenario



Step 9: Repeat the same procedure to configure for Router1



Step 10: After configuration of Static routing in both Routers, Check the connectivity among any two devices using Ping Command



Step 11:

- To check routing table, go to CLI tab in Router and press enter to get the router prompt.
    - Router>
- Now type enable or en and press enter
    - Router>en
    - Router#

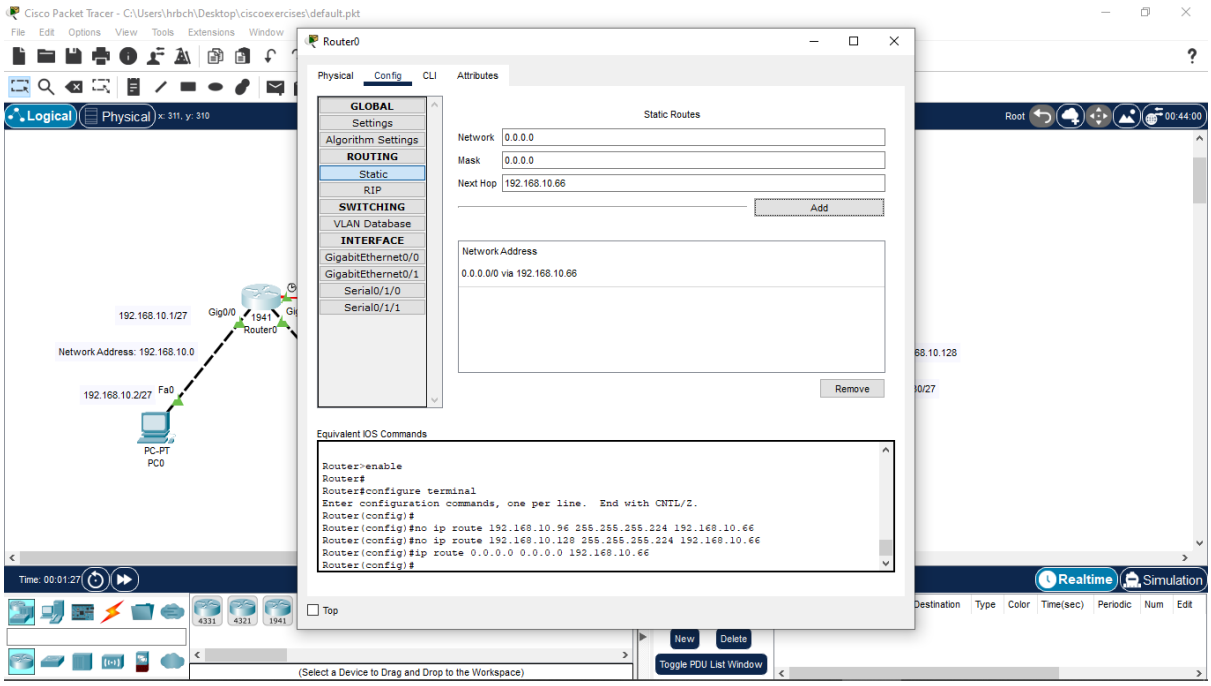
Follow the command “show ip route” to get the routing table of a router

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

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.10.0/27 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
C 192.168.10.32/27 is directly connected, GigabitEthernet0/1
L 192.168.10.33/32 is directly connected, GigabitEthernet0/1
C 192.168.10.64/27 is directly connected, Serial0/1/0
L 192.168.10.65/32 is directly connected, Serial0/1/0
S 192.168.10.96/27 [1/0] via 192.168.10.66
S 192.168.10.128/27 [1/0] via 192.168.10.66
```

6. **b: For Default Routing replace Step 8 and Step 9 with Step 12 and Step 13**

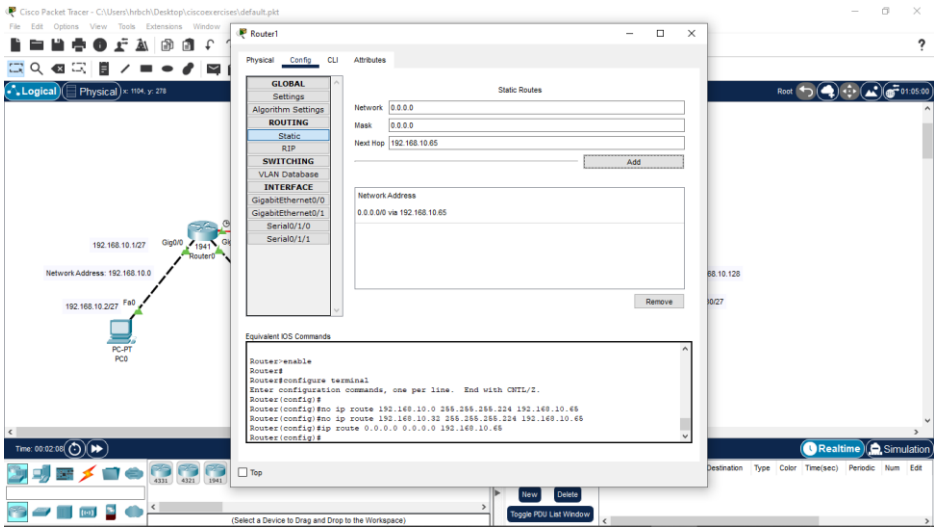
Step 12:

- To configure static routing, click on
    - Router0 => Config tab => Static =>Enter network address (as 0.0.0.0) => Subnet Mask (as 0.0.0.0) => Next-hop address (192.168.10.66) => Add network
- One entry should be added for the given scenario

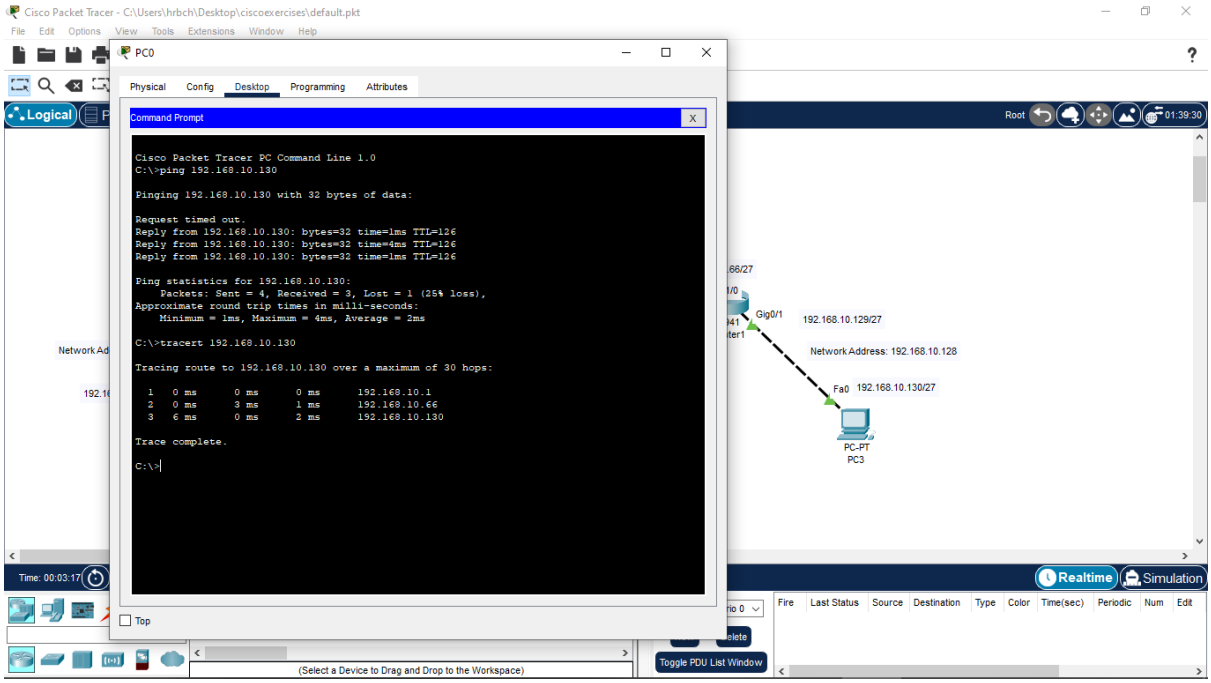


Step 13: Repeat the same procedure to configure for Router1.

Router1 => Config tab => Static =>Enter network address (as 0.0.0.0) => Subnet Mask (as 0.0.0.0) => Next-hop address (192.168.10.65) => Add network



Output for Default Routing: Click on PC0 => Desktop => Command Prompt and check **"tracert 192.168.10.130"** command



Exercise 7. a: Demonstration of RIP v1

[Note: RIP v1 does not support classless addressing mode and RIP v2 must be used in Subnet enabled Scenario]

Objective: To demonstrate the configuration of IP Addressing with Subnetting in WAN Configuration

Pre-requisite: IP Address, Range of IP Address, Classes of IP Address, Subnetting

Components:

Devices	Required Nos
PCs	4
Copper cross-over Cables	4
Routers [1941]	2
Serial DCE	1

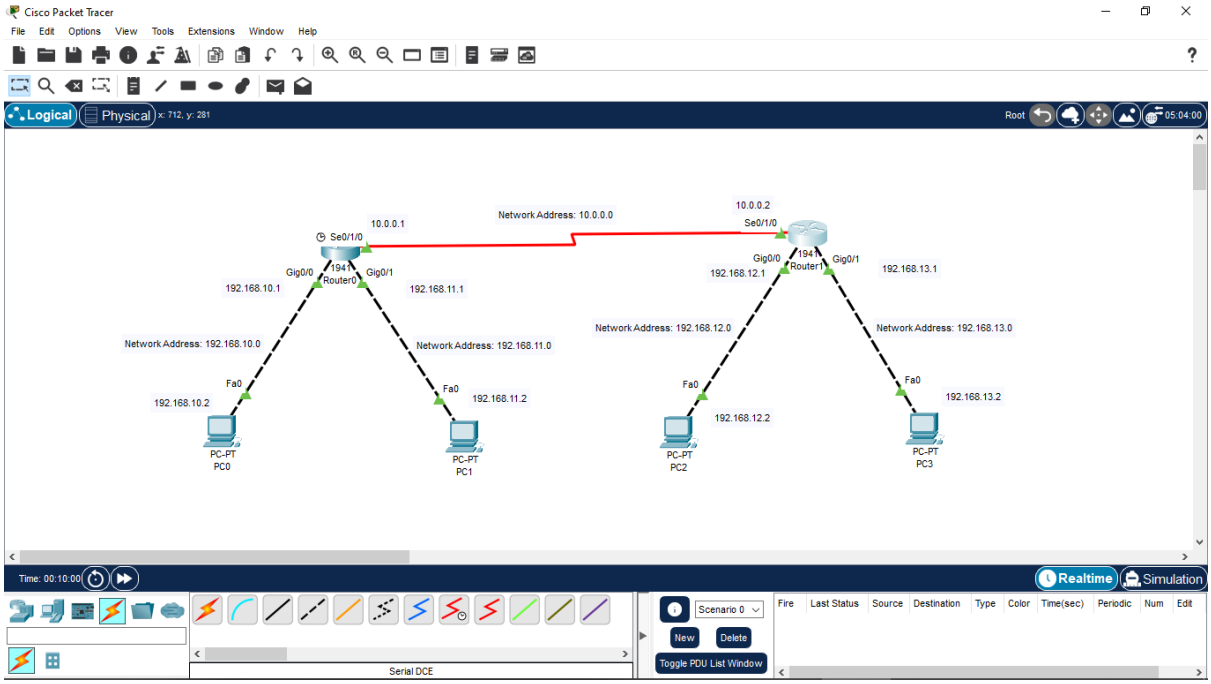
Addressing Table:

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	Fa0/0	192.168.11.2	255.255.255.0	192.168.11.1
PC2	Fa0/0	192.168.12.2	255.255.255.0	192.168.12.1
PC3	Fa0/0	192.168.13.2	255.255.255.0	192.168.13.1
Router0	Gigabit 0/0	192.168.10.1	255.255.255.0	-
Router0	Gigabit 0/1	192.168.11.1	255.255.255.0	-
Router0	Se0/1/0	10.0.0.1	255.0.0.0	-
Router1	Gigabit 0/0	192.168.12.1	255.255.255.0	-
Router1	Gigabit 0/1	192.168.13.1	255.255.255.0	-
Router1	Se0/1/0	10.0.0.2	255.0.0.0	-

Procedure:

Step 1:

- Drag 4 PCs and 2 routers in the console area as shown in the figure.
- Follow the procedure for connecting **Serial DCE cable from Exercise 4.**
- Assign IP addresses for 4 PCs (each 1 interface and corresponding router interface as gateway) and 2 Routers (each 3 ip addresses for 3 interfaces) as shown in the Addressing Table



Step 2:

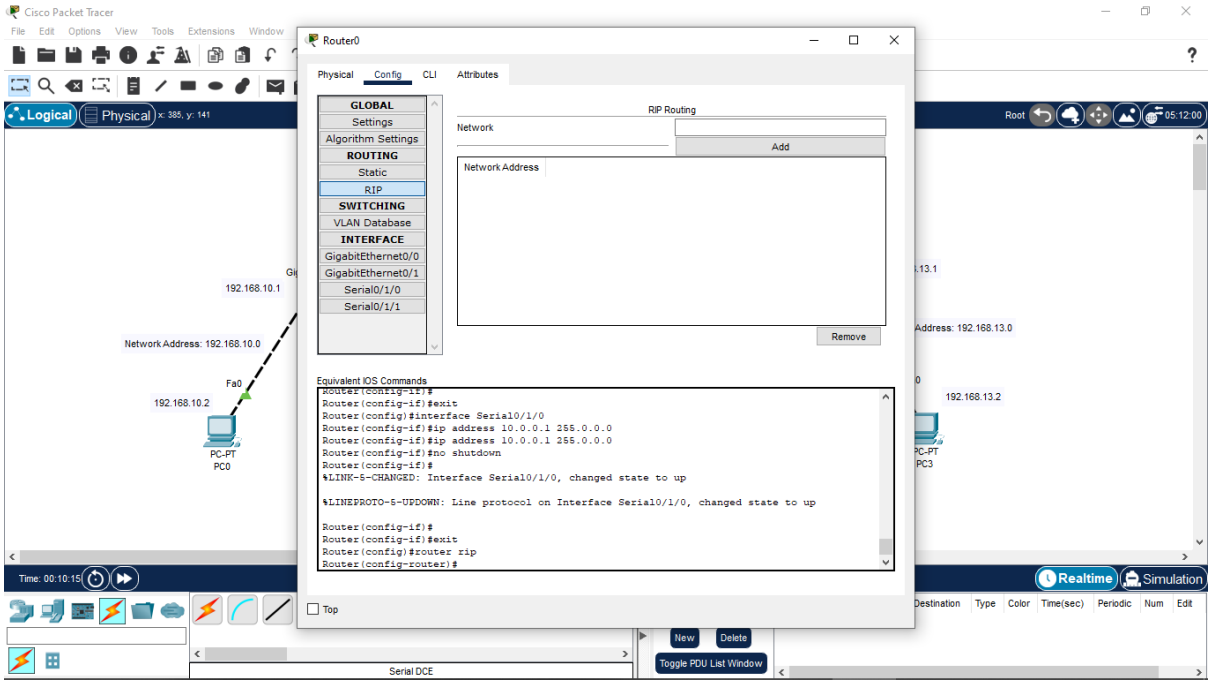
- To enable packet transmission among the devices in the scenario, RIP Routing has to be configured.
- To configure RIP routing, **known networks** for Router0 and Router1 has to be determined.
- Note: While specifying devices we should use IP-Address and while specifying network we should use Network Address.
- The **known networks** for the routers are derived in the following table

Device	Known Networks	Subnet Mask
Router0	192.168.10.0	255.255.255.0
Router0	192.168.11.0	255.255.255.0
Router0	10.0.0.0	255.0.0.0
Router1	192.168.12.0	255.255.255.0
Router1	192.168.13.0	255.255.255.0
Router1	10.0.0.0	255.0.0.0

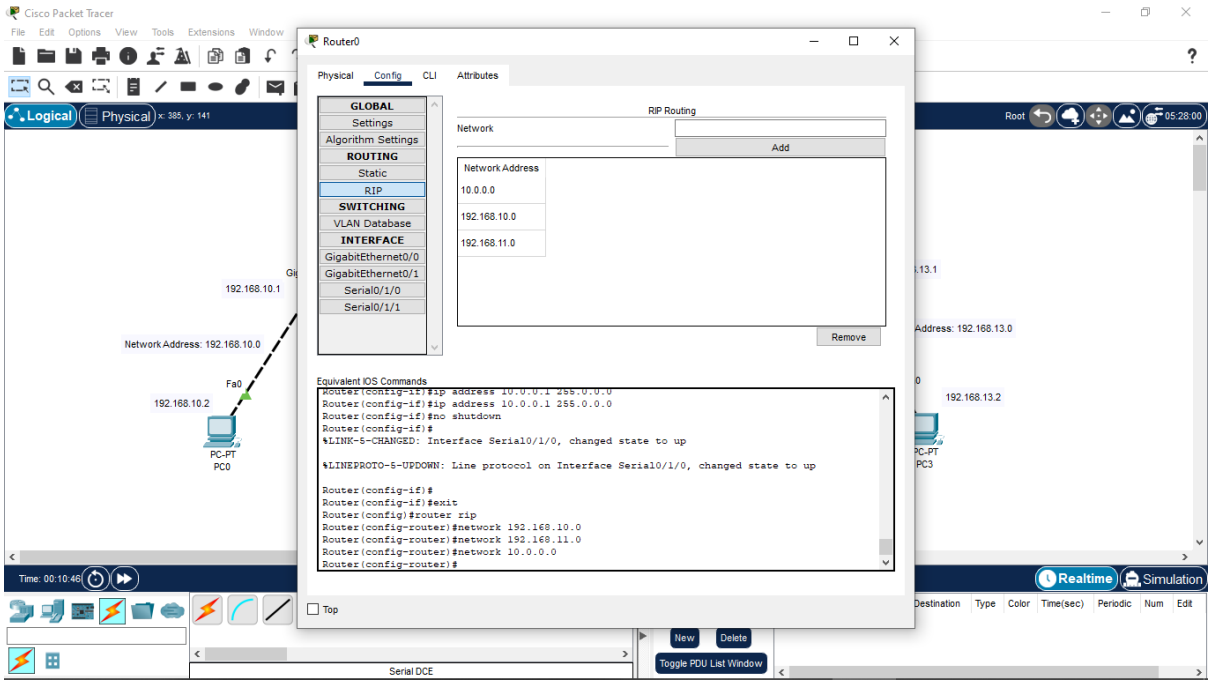
Only known networks should be configured for RIP routing

Step 3:

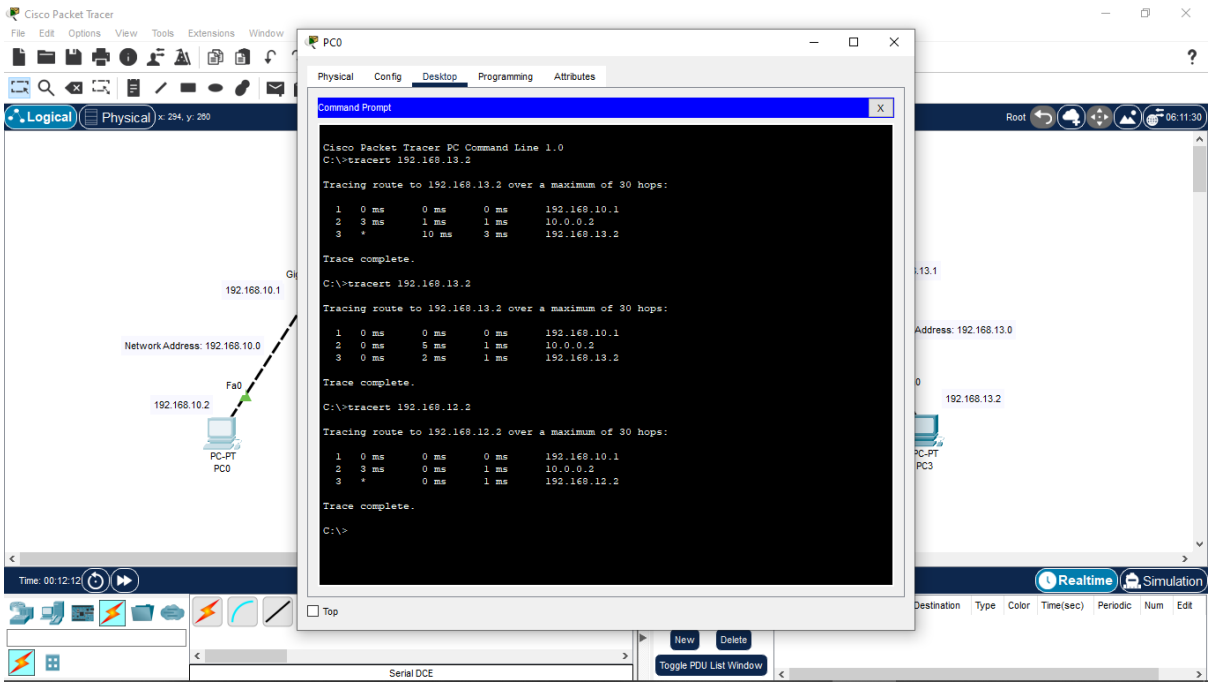
- To configure RIP routing, click on
  - Router0 => Config tab => RIP =>Enter network address (refer table) => Add network
- Repeat the same to add the next network.
- Three networks should be added for the given scenario



Step 4: Repeat the same procedure to configure for Router1

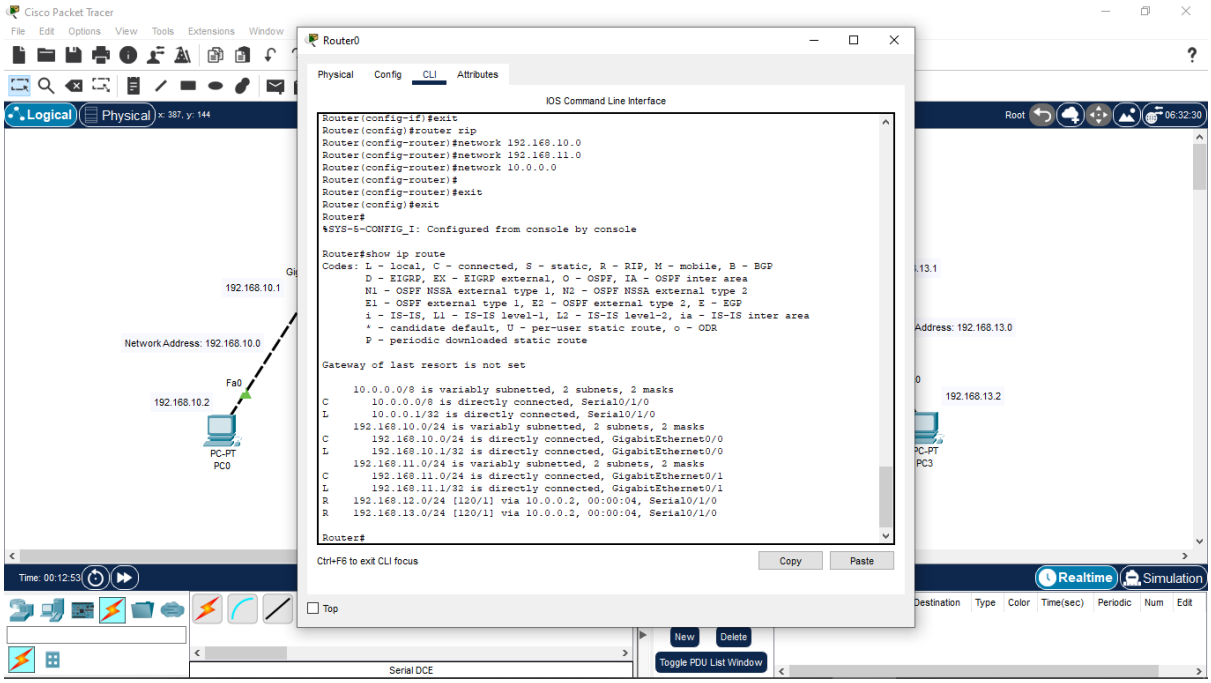


Step 5: After configuration of RIP routing in both Routers, Check the connectivity among any two devices using Ping Command or tracertcommand



Step 6:

- To check routing table, go to CLI tab in Router and press enter to get the router prompt.
    - Router>
- Now type enable or en and press enter
    - Router>en
    - Router# show ip route



Exercise 7. b: Demonstration of RIP v2

Objective: To demonstrate the configuration of RIP v2

Pre-requisite: IP Address, Range of IP Address, Classes of IP Address, Subnetting

Components:

Devices	Required Nos
PCs	4
Copper cross-over Cables	4
Routers	2
Serial DCE	1

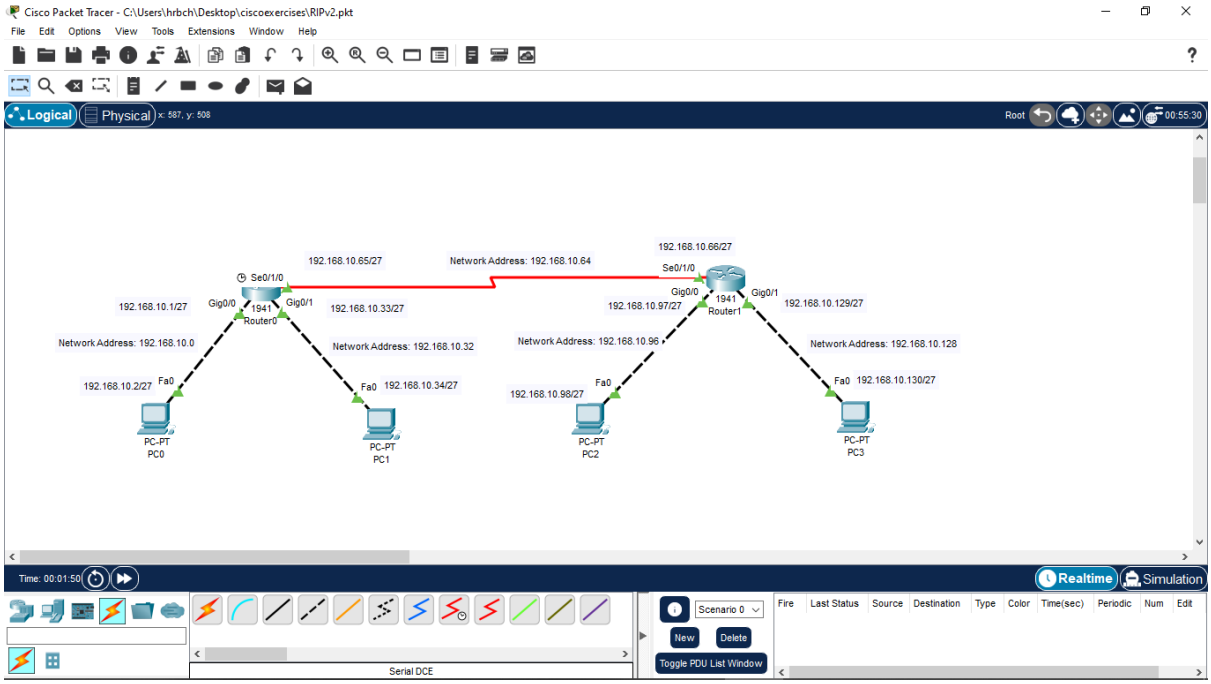
Addressing Table:

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit 0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit 0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit 0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit 0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-

Procedure:

Step 1:

- Drag 4 PCs and 2 routers in the console area as shown in the figure.
- Follow the procedure for connecting **Serial DCE cable from Exercise 4.**
- Assign IP addresses for 4 PCs (each 1 interface and corresponding router interface as gateway) and 2 Routers (each 3 ip addresses for 3 interfaces) as shown in the Addressing Table



Step 2:

- To enable packet transmission among the devices in the scenario, RIP v2 Routing has to be configured.
- To configure RIP v2 routing, **known networks** for Router0 and Router1 has to be determined.
- Note: While specifying devices we should use IP-Address and while specifying network we should use Network Address.
- The **known networks** for the routers are derived in the following table

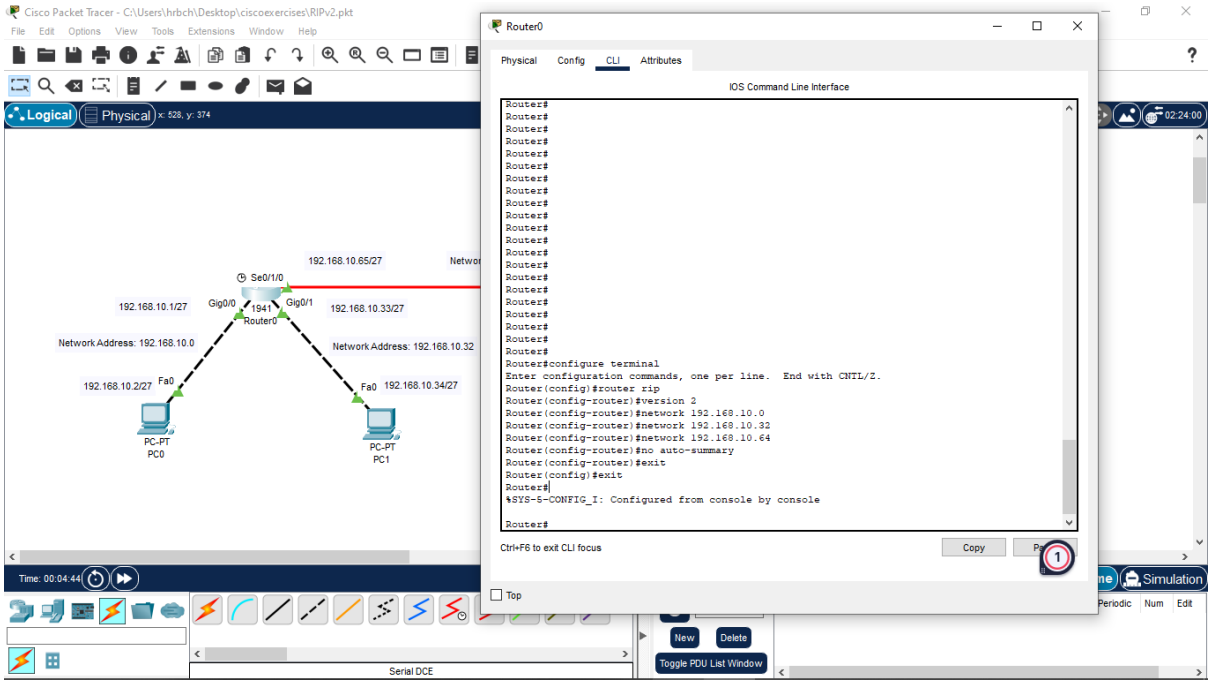
Device	Known Networks	Subnet Mask	Unknown Networks	Subnet Mask	Next-hop Address
Router0	192.168.10.0	255.255.255.224	192.168.10.96	255.255.255.224	192.168.10.66
Router0	192.168.10.32	255.255.255.224	192.168.10.128	255.255.255.224	192.168.10.66
Router0	192.168.10.64	255.255.255.224	-	-	-
Router1	192.168.10.96	255.255.255.224	192.168.10.0	255.255.255.224	192.168.10.65
Router1	192.168.10.128	255.255.255.224	192.168.10.32	255.255.255.224	192.168.10.65
Router1	192.168.10.64	255.255.255.224	-	-	-

Only unknown networks should be configured for static routing

Step 3:

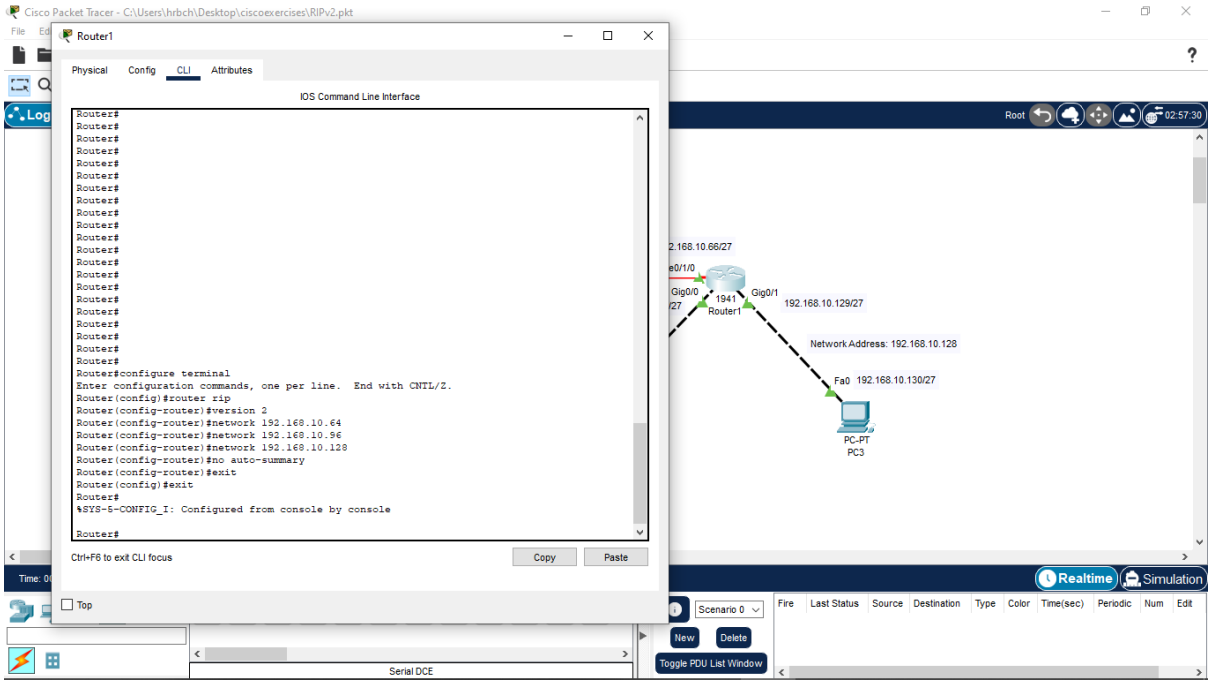
- To configure static routing, click on
  - Router0 => Config tab => CLI
- Type “enable” in “Router>” prompt and type the following commands to configure RIP v2 in Router0

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.10.32
Router(config-router)#network 192.168.10.64
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```



Step 4: Repeat the same procedure to configure for Router1

```
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.64
Router(config-router)#network 192.168.10.96
Router(config-router)#network 192.168.10.128
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console


Router#
```



Step 5: After configuration of RIP v2 routing in both Routers, Check the connectivity among any two devices using Ping Command/ tracert command