

**Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidyapeetham
2024-2025 Odd Semester
B. Tech CSE – (2022-2026 Batch) Semester: 5**

LAB NAME: 19CSE 301 COMPUTER NETWORKS

Expt. 1: Basic Networking Commands

Note: Execute these commands in Windows Operating System

1) hostname: A hostname is the name assigned to a device on a network. Using this command, we can find out the host name of the computer.

Example: `c:\>hostname`

Questions

1. What is a network?
 2. What is the hostname of your device?
-

2) ipconfig: This command is used to find out the ipaddress of the computer.

Examples:

a) c:\>ipconfig (default gateway: In computer networking, a gateway is a node (a router) on a TCP/IP network that serves as an access point to another network)

b) c:\>ipconfig/? : displays all available options with this command

c) c:\>ipconfig/all :displays additional information such as DNS and WINS

Questions

- 1.What do you mean by IP address?
 - 2.What is IPV4 and IPv6 address?
 3. What is the IPV4 address you got on executing above commands?
-

3) ping: it is used to test the ability of the source computer to reach a specified destination computer. That is to test a computer can communicate over the network with another computer or network device.

How it operates:

It sends ICMP (it is a protocol that gives or reports the status of the network: errors in the underlying communications of network applications, availability of remote hosts and network congestion) Echo request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

Syntax: **ping** [-t] [-a] [-n *count*] [-l *size*] [-f] [-i *TTL*] [-v *TOS*] [-r *count*] [-s *count*] [-w *timeout*] [-R] [-S *srcaddr*] [-4] [-6] *target* [/?]

Examples:

a) **c:\>ping www.google.com**

b) **c:\>ping 192.168.2.32**

c) **c:\>ping -t 192.168.2.32** : it pings the target until we force it to stop using ctrl-c

d) **c:\>ping -a 192.168.2.32**: it will give you the host name of the target if possible

d) **c:\>ping -n count 192.168.2.32**: it sets how many number of request messages to be sent. By default 4 request messages will be sent

e) **c:\>ping -l size 192.168.2.32**: it sets the size of the request message in bytes. By default 32 bytes is the size.

f) **c:\>ping -w timeout**: by using this, we can adjust the amount of time in milliseconds that ping waits for each reply. By default for every reply, ping waits for 4000 ms

g) **c:\>ping /?**: displays all available options with this command

h) **c:\>ping 127.0.0.1**: 127.0.0.1 is localhost ip address or loopback ip address. It is for testing the window's network features are working properly or not.

Questions

1. What is the use of ping command?
2. What is the expansion of ICMP?
3. How much time does it take to receive the reply?
4. What is a packet?
5. How much packets are sent, received and lost?

6. What is roundtrip time and what is the roundtrip time you observed?

4) tracert: it is used to show several details about the path that a packet takes from the computer or device you are on to whatever destination 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 takes

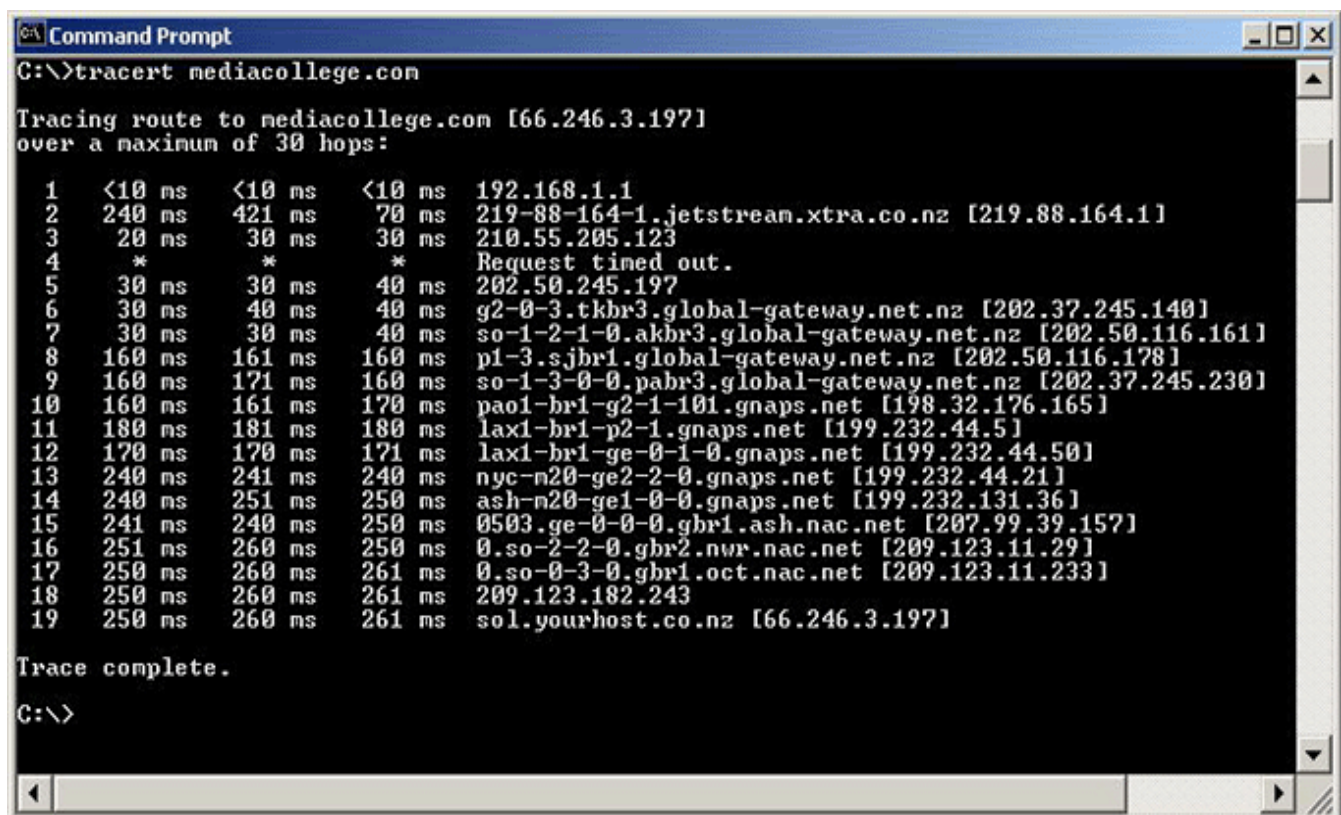
Syntax: **tracert** [-d] [-h *MaxHops*] [-w *TimeOut*] [-4] [-6] *target* [/?]

Examples:

a) tracert www.google.com : To trace the route to a website like www.google.com

b) tracert 8.8.8.8 : If you want to trace the route to a specific IP address, use the IP instead of the domain name

c:>tracert -h 5 8.8.8.8 : This tracert option specifies the maximum number of hops in the search for the target. If you do not specify MaxHops, and target has not been found by 30 hops, tracert will stop looking



```
Command Prompt
C:\>tracert mediacollege.com

Tracing route to mediacollege.com [66.246.3.197]
over a maximum of 30 hops:

  0  <10 ms  <10 ms  <10 ms  192.168.1.1
  1  240 ms  421 ms  70 ms  219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
  2  20 ms  30 ms  30 ms  210.55.205.123
  3  *      *      *      Request timed out.
  4  30 ms  30 ms  40 ms  202.50.245.197
  5  30 ms  40 ms  40 ms  g2-0-3.tkbr3.global-gateway.net.nz [202.37.245.140]
  6  30 ms  30 ms  40 ms  so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
  7  160 ms  161 ms  160 ms  pl-3.sjbr1.global-gateway.net.nz [202.50.116.178]
  8  160 ms  171 ms  160 ms  so-1-3-0-0.pabr3.global-gateway.net.nz [202.37.245.230]
  9  160 ms  161 ms  170 ms  pa01-br1-g2-1-101.gnaps.net [198.32.176.165]
 10  180 ms  181 ms  180 ms  lax1-br1-p2-1.gnaps.net [199.232.44.5]
 11  170 ms  170 ms  171 ms  lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
 12  240 ms  241 ms  240 ms  nyc-n20-ge2-2-0.gnaps.net [199.232.44.21]
 13  240 ms  251 ms  250 ms  ash-n20-ge1-0-0.gnaps.net [199.232.131.36]
 14  241 ms  240 ms  250 ms  0503.ge-0-0-0.gbr1.ash.nac.net [207.99.39.157]
 15  251 ms  260 ms  250 ms  0.so-2-2-0.gbr2.nwr.nac.net [209.123.11.29]
 16  250 ms  260 ms  261 ms  0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
 17  250 ms  260 ms  261 ms  209.123.182.243
 18  250 ms  260 ms  261 ms  sol.yourhost.co.nz [66.246.3.197]
 19

Trace complete.
C:\>
```

Questions:

- 1.What is a router?.
 2. What do you mean by a hop?
 3. What does tracert do?
 - 4.What is the difference between Ping and Tracert?
-

5) pathping: The PathPing tool is a route tracing tool that combines features of Ping and Tracert with additional information that neither of those tools provides. PathPing sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Since PathPing shows the degree of packet loss at any given router or link, you can pinpoint which routers or links might be causing network problems.

Example 1: Basic Usage

To trace the route and analyze network performance to `www.google.com`:

```
pathping www.google.com
```

This command sends packets to each router along the path to `www.google.com` and provides detailed statistics about each hop.

Example 2: Specifying the Number of Queries per Hop

You can specify the number of queries to each router along the path using the `-q` option. For example, to send 10 queries per hop:

```
pathping -q 10 www.google.com
```

Example 3: Specifying the Maximum Number of Hops

The `-h` option allows you to set the maximum number of hops. For example, to limit the trace to 20 hops:

```
pathping -h 20 www.google.com
```

Example 4: Specifying Wait Time

You can specify the wait time (in milliseconds) for each reply using the `-w` option. For example, to set the wait time to 500 milliseconds:

```
pathping -w 500 www.google.com
```

Questions:

- 1.What additional features does pathping provide compared to tracert and ping?
- 2.Why would you use pathping over tracert in a network diagnostic scenario?

Expt. 2: Basic Networking Commands-cont

6) netstat: is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

- a Displays all connections and listening ports.
- b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
- e Displays Ethernet statistics. This may be combined with the -s option.
- f Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
- n Displays addresses and port numbers in numerical form.
- o Displays the owning process ID associated with each connection.
- p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s

option to display per-protocol statistics, proto may be any of:

IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

- q Displays all connections, listening ports, and bound nonlistening TCP ports. Bound nonlistening ports may or may not be associated with an active connection.
 - r Displays the routing table.
 - s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
 - t Displays the current connection offload state.
 - x Displays NetworkDirect connections, listeners, and shared endpoints.
 - y Displays the TCP connection template for all connections.
Cannot be combined with the other options.
- interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

Answer the below questions. Make a file (named as your register number (example cse22078)) with answers to below questions.Drive to upload file will be given by your faculty

Questions

1. What is TCP?
2. What is OSI model?
3. What are the 7 layers of OSI model?
4. What is the purpose of netstat command
5. What is a port?
6. What is a routing table?
7. What is a network interface?
8. Explore what is TCP and UDP?
9. What is a router?
- 10.What is a routing table?
- 11.What is meant by Local and Foreign address?
- 12.What are the different states that will be displayed when command is executed?
- 13.What is a process?
- 14.What is DNS?
- 15.What is FQDN?
- 16.Explore all the options of netstat given above and observe the output of the commands

Expt. 3: Packet Tracer Introduction

PACKET TRACER 8.1.1

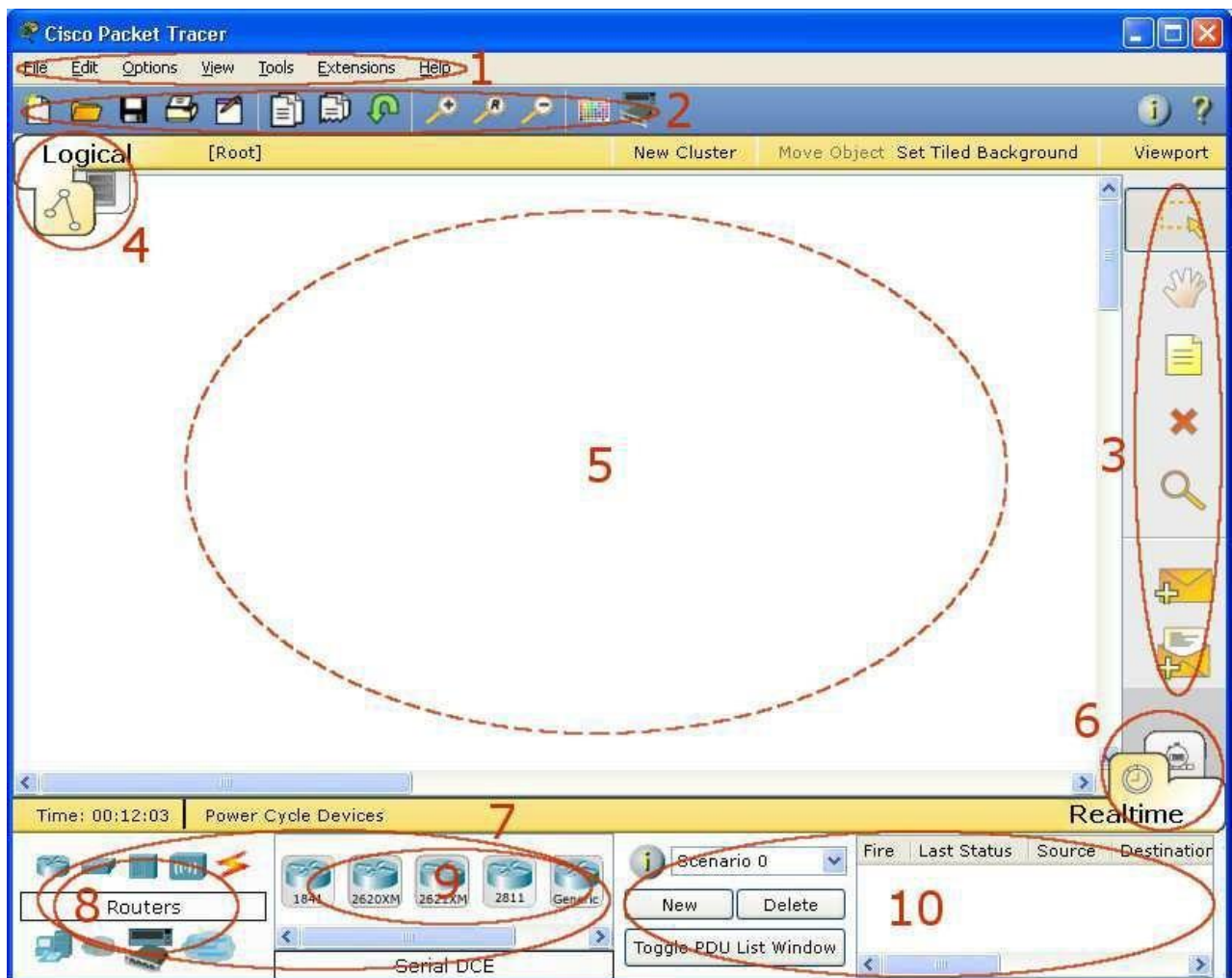
Installation

<https://www.youtube.com/watch?v=QyAfx8iuVUQ>

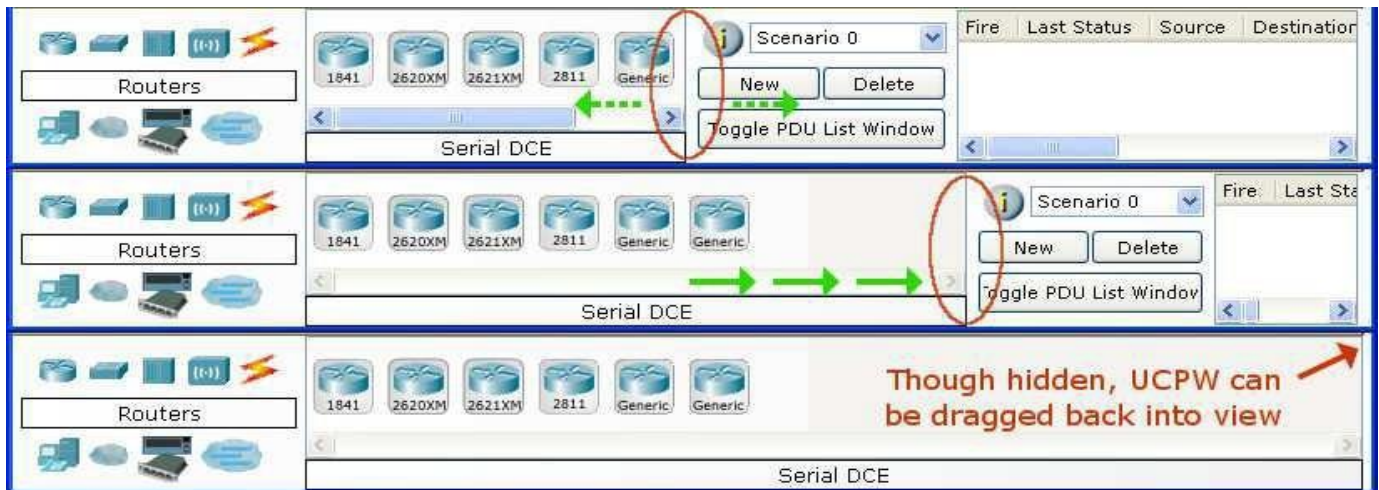
<https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html>

<https://www.netacad.com/>

Cisco Packet Tracer Overview

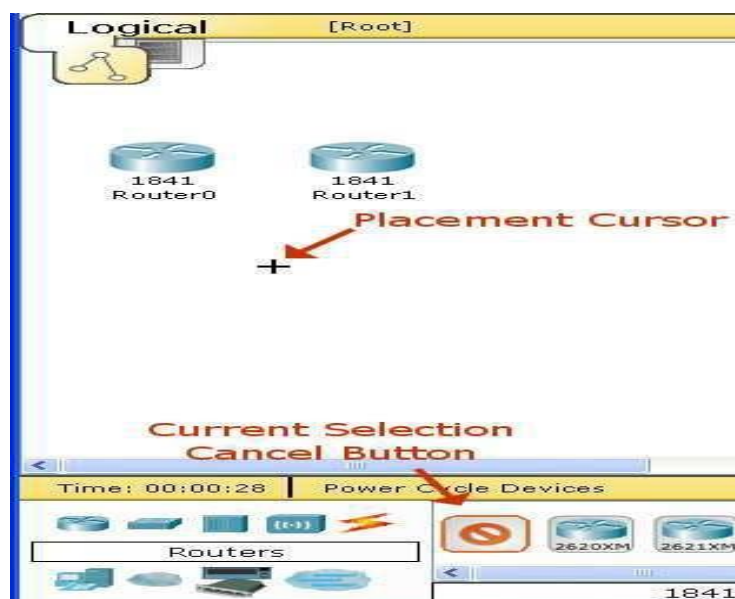


1	Menu Bar	This bar provides the File, Edit, Options, View, Tools, Extensions, and Help menus. You will find basic commands such as Open, Save, Print, and Preferences in these menus. You will also be able to access the Activity Wizard from the Extensions menu.
2	Main Tool Bar	This bar provides shortcut icons to the File and Edit menu commands. This bar also provides buttons for Zoom , the drawing Palette , and the Device Template Manager . On the right, you will also find the Network Information button, which you can use to enter a description for the current network (or any text you wish to include).
3	Common Tools Bar	This bar provides access to these commonly used workspace tools: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU, and Add Complex PDU . See "Workspace Basics" for more information.
4	Logical/Physical Workspace and Navigation Bar	You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar. In Logical Workspace, this bar also allows you to navigate through levels of a cluster, create a new New Cluster, Move Object, Set Tiled Background, and Viewport . In Physical Workspace, this bar allows you to navigate through physical locations, create a New City , create a New Building , create a New Closet, Move Object , apply Grid to the background, Set Background , and go to the Working Closet .
5	Workspace	This area is where you will create your network, watch simulations, and view many kinds of information and statistics .
6	Realtime/Simulation Bar	You can toggle between Realtime Mode and Simulation Mode with the tabs on this bar. This bar also provides buttons to Power Cycle Devices as well as the Play Control buttons and the Event List toggle button in Simulation Mode. Also, it contains a clock that displays the relative Time in Realtime Mode and Simulation mode.
7	Network Component Box	This box is where you choose devices and connections to put into the workspace. It contains the Device-Type Selection Box and the Device-Specific Selection Box.
8	Device-Type Selection	This box contains the type of devices and connections available in Packet Tracer 5.1. The Device-Specific Selection Box will change depending on which type of device you choose.
9	BoxDevice-Specific Selection Box	This box is where you choose specifically which devices you want to put in your network and which connections to make.
10	User Created Packet Window*	This window manages the packets you put in the network during simulation scenarios. See the "Simulation Mode" section for more details.



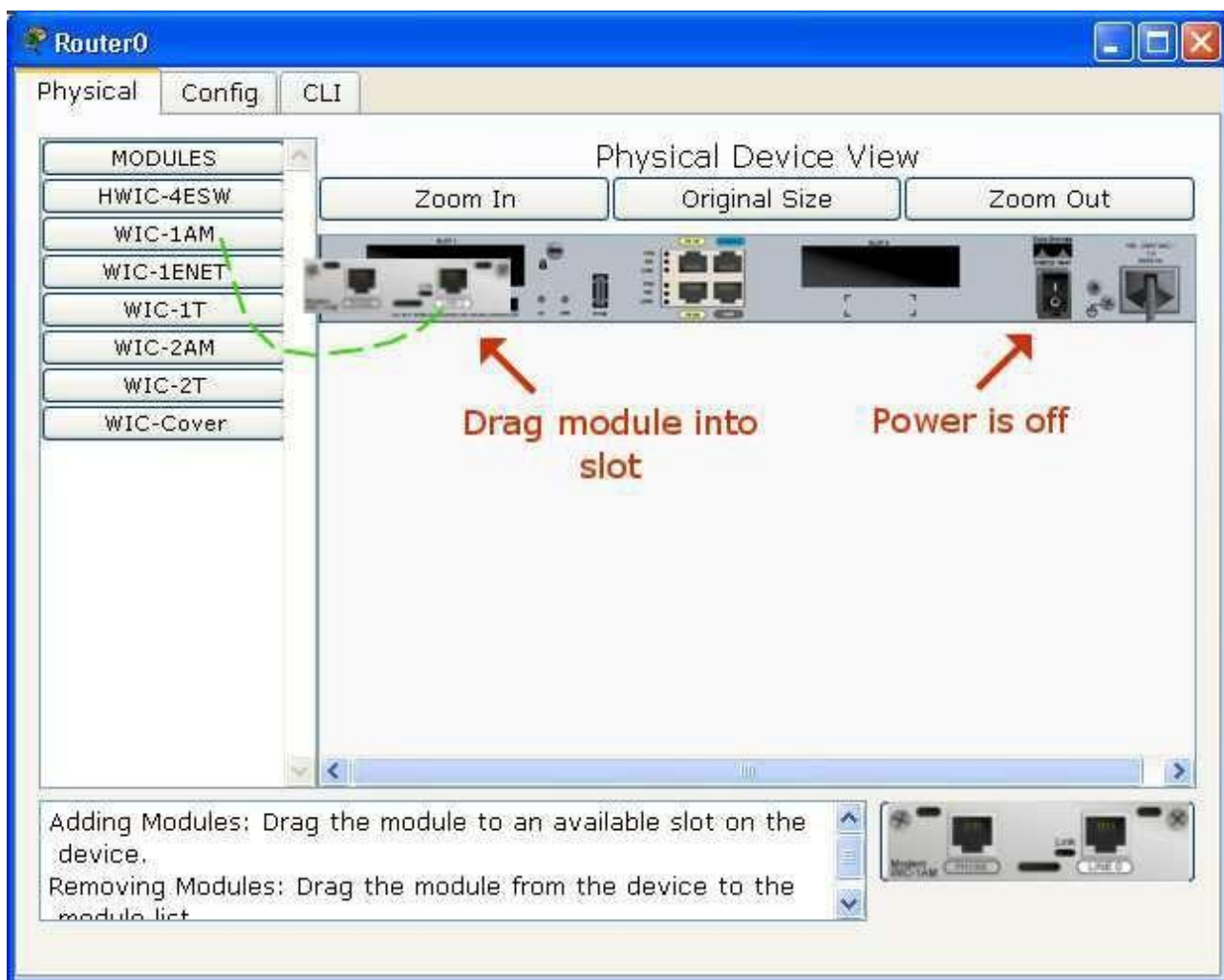
1. Creating Devices

- Choose a device type from the **Device-Type Selection** box
- Click on the desired device model from the **Device-Specific Selection** box.
- Click on a location in the workspace to put your device in that location.
- If you want to cancel your selection, press the **Cancel** icon for that device.
- Alternatively, you can click and drag a device from the **Device-Specific Selection** box onto the workspace.
- You can also click and drag a device directly from the **Device-Type Selection** box and a default device model will be chosen.



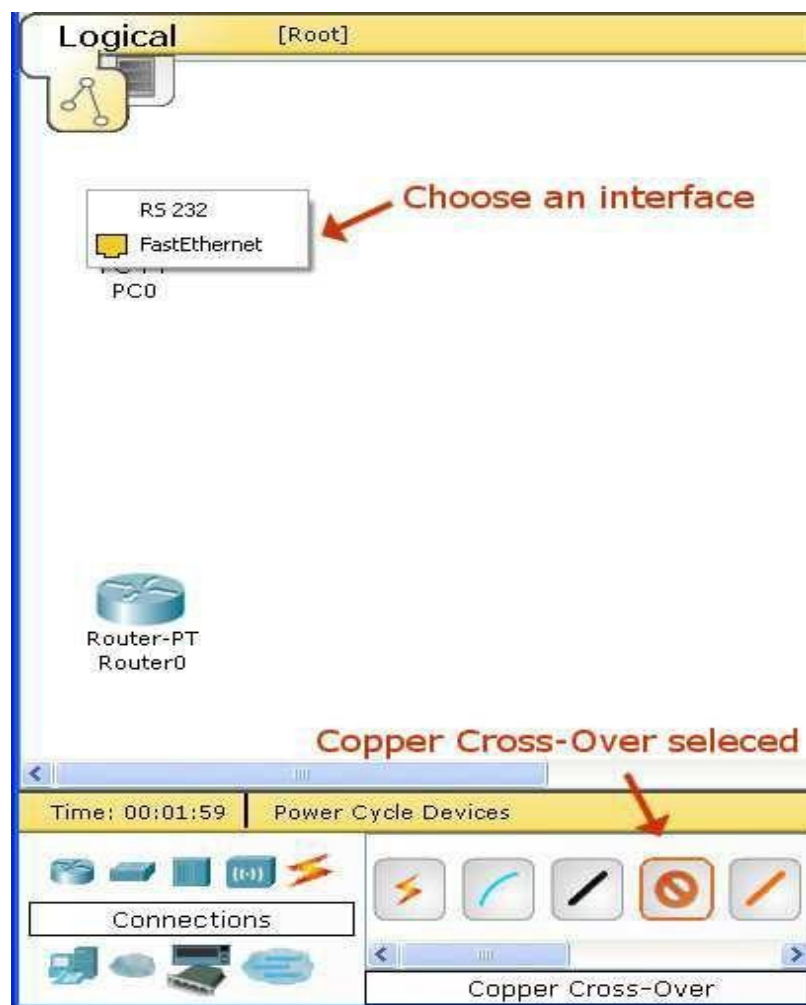
2. Adding Modules

- a. Click on a device to bring up its configuration window.
- b. By default, you will be in the **Physical Device View** subpanel of the device.
- c. You can browse (by clicking) through the list of modules and read their description in the informationbox at the bottom.
- d. When you have found the module you want to add, simply drag it from the list into a compatible bayon the device picture.
- e. You can remove a module by dragging it from the device back into the list.



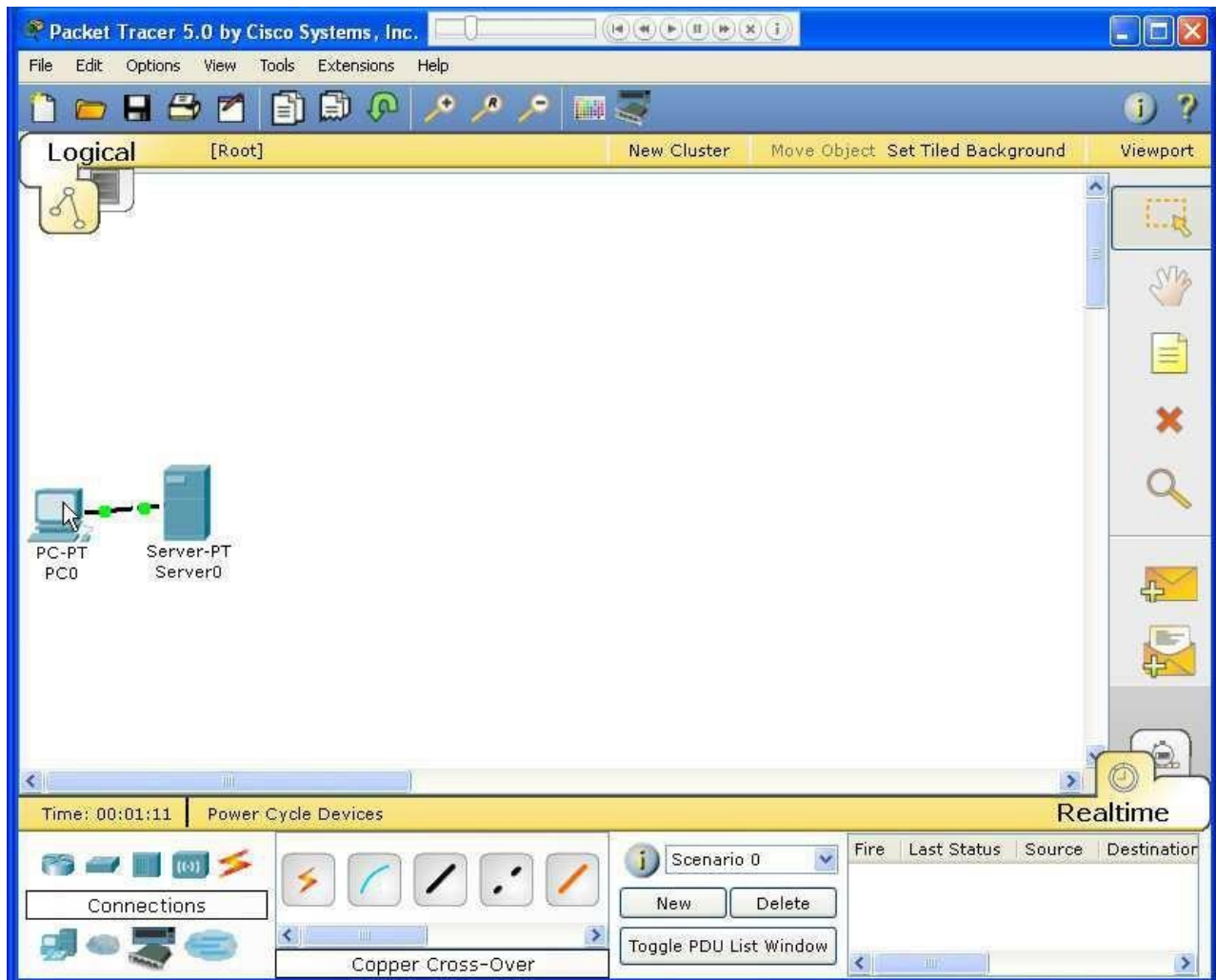
3. Making Connections

- a. To make a connection between two devices, first click the **Connections** icon from the **Device-Type Selection** box to bring up the list of available connections.
- b. Then click the appropriate cable type.
- c. The mouse pointer will change into a "connection" cursor.
- d. Click on the first device and choose an appropriate interface to which to connect.
- e. Then click on the second device and do the same.
- f. A connection cable will appear between the two devices, along with link lights showing the link status on each end (for interfaces that have link lights).



5. Creating Networks

- a. Start creating a network by first selecting the End Devices. Add a Generic PC and a Generic Server to the workspace.
- b. Under Connections, select the Copper Straight-through cable (solid black line) and connect the devices with it. The red lights on the link indicate that the connection is not working. Now, use the Delete tool to remove the Copper Straight-through cable, and use a Copper Cross-over cable (dashed line) instead. The lights should turn green at this point, and if the mouse pointer is held over either the PC or the Server, the link status will be shown as “Up.” The network should look similar to the picture below.
- c. Click on the PC. While paying attention to the link lights, turn the power on, off, and on again. Follow the same steps for the server. The link lights turn red when the device is off. This means that the link is down or is not working. The link lights turn green when the device is turned back on.
- d. Try all three ways to learn about the devices. **First**, mouse over the devices to see basic configuration information about them. **Second**, click on each device with the Select tool to show the device configuration window, which provides several ways to configure the device. **Third**, use the Inspect tool to view tables the network device will build as it learns about the network around it. In this example, only the ARP tables will appear. Since the devices have not been configured yet, the ARP tables are empty. Always remember to close windows after viewing them or they will clutter the workspace.
- e. Open the PC configuration window and change the settings using the Config tab. Change the display name to Client and set the DNS server to **192.168.0.105**. Under Interface, click FastEthernet and set the IP address as **192.168.0.110**. Packet Tracer automatically calculates other parameters. Make sure that the Port Status box is checked. For future reference, note that other Ethernet interface settings, such as bandwidth, duplex, MAC address, and subnet mask can be modified using this window.
- f. Go to the Desktop Tab and click on IP Configuration. Notice that the IP address, subnet mask and DNS server can be changed here as well.
- g. Open the Server configuration window and go to the Config tab. Change the display name to Web Server. Click FastEthernet and set the IP address as 192.168.0.105. Make sure that the Port Status is also on. Click DNS and set the domain name as www.firstlab.com. Set the IP address as 192.168.0.105 and click **Add**. Finally, check to make sure that the service for DNS is on.
- h. Reposition the network devices by dragging them to a new location. Add a network description by using the “i” button on the upper right corner. Then add some text labels within the Logical Workspace by using the Place Note tool.
- i. Load a background grid using the Set Tiled Background button.
- j. Save your work using the File > Save As option and create a meaningful filename.

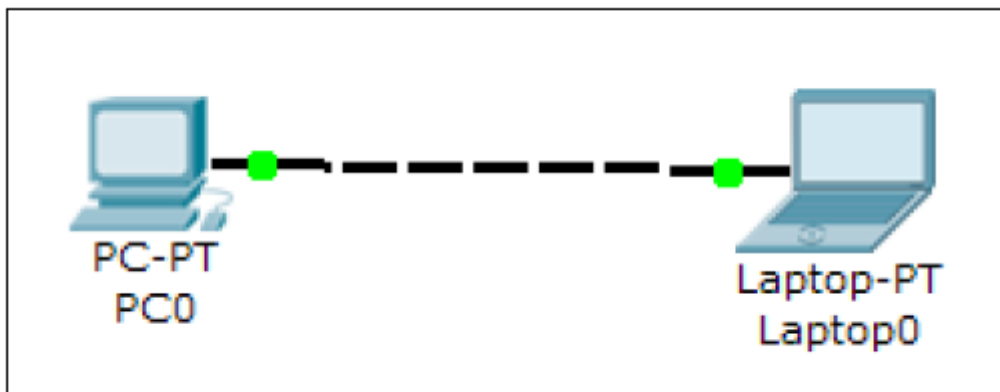


Expt. 4: Packet Tracer -Exercises

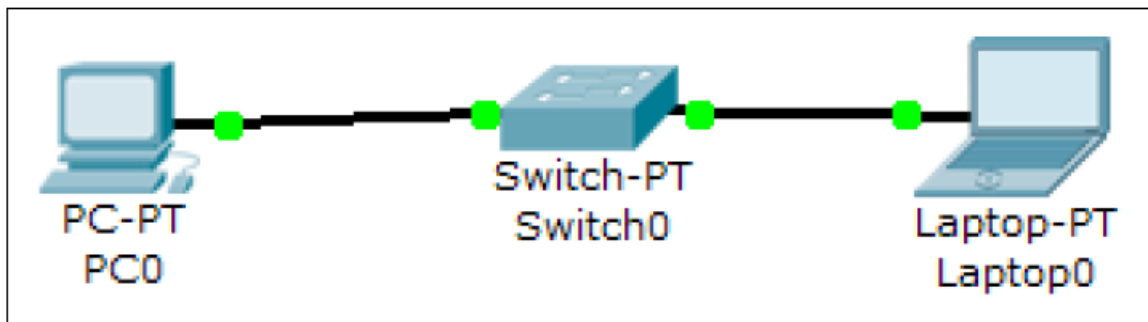
Packet Tracer Experiments

1. Configuration of simple network and network topology using packet tracer.
2. Configuration of LAN using packet tracer

1. Creating a simple topology



2. A network topology with Ethernet switch to connect more than two end devices



3. LAN using the HUB

Cisco Packet Tracer - C:\Users\DHEERAJ\Cisco Packet Tracer 8.1.1\saves\LAN_Hub_nesco.plt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 408, y: 81

Root 01:34:30

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.003	PC3
	0.004	Hub0
	0.004	Hub0
	0.004	Hub0

Reset Simulation Constant Delay Captured to: 1784.549 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Time: 00:30:33.180 PLAY CONTROLS

Scenario 0

New Deletes Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)

Type here to search

ENG 10:11 02-05-2022

Cisco Packet Tracer - C:\Users\DHEERAJ\Cisco Packet Tracer 8.1.1\saves\LAN_Hub_nesco.plt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 288, y: 211

Root 01:29:30

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.003	PC3
	0.004	Hub0
	0.004	Hub0
	0.004	Hub0

Reset Simulation Constant Delay Captured to: 1599.148 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Time: 00:27:27.779 PLAY CONTROLS

Scenario 0

New Deletes Toggle PDU List Window

Destination	Type	Color	Time(sec)	Periodic	Num	Edit
PC3	ICMP		0.000	N	0	(edit)

Type here to search

ENG 10:11 02-05-2022

PC0 Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 10.0.0.1

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::20B:BEFF:FEDE:163B

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MDS

Username

Password

IP address to be allocated for each device eg 10.0.0.1, 10.0.0.2 and so on.

Connect all the devices to the HUB.

HUB delivers to all devices. Only the specific one accepts it. Others

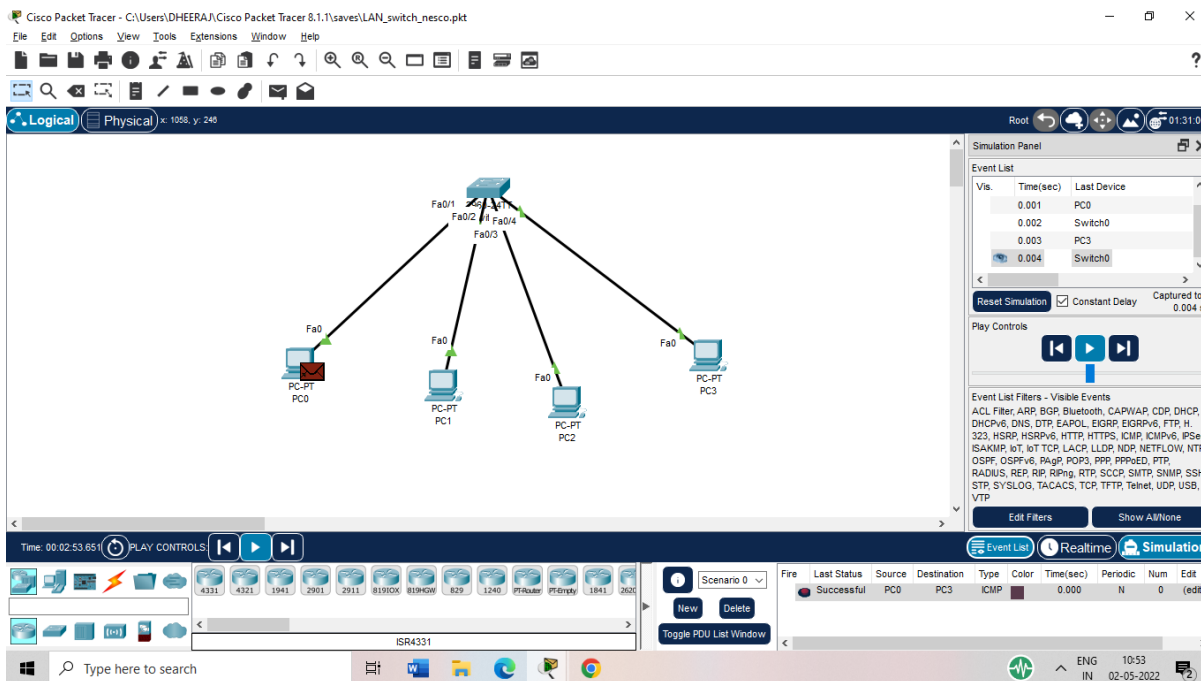
Ping in Real time

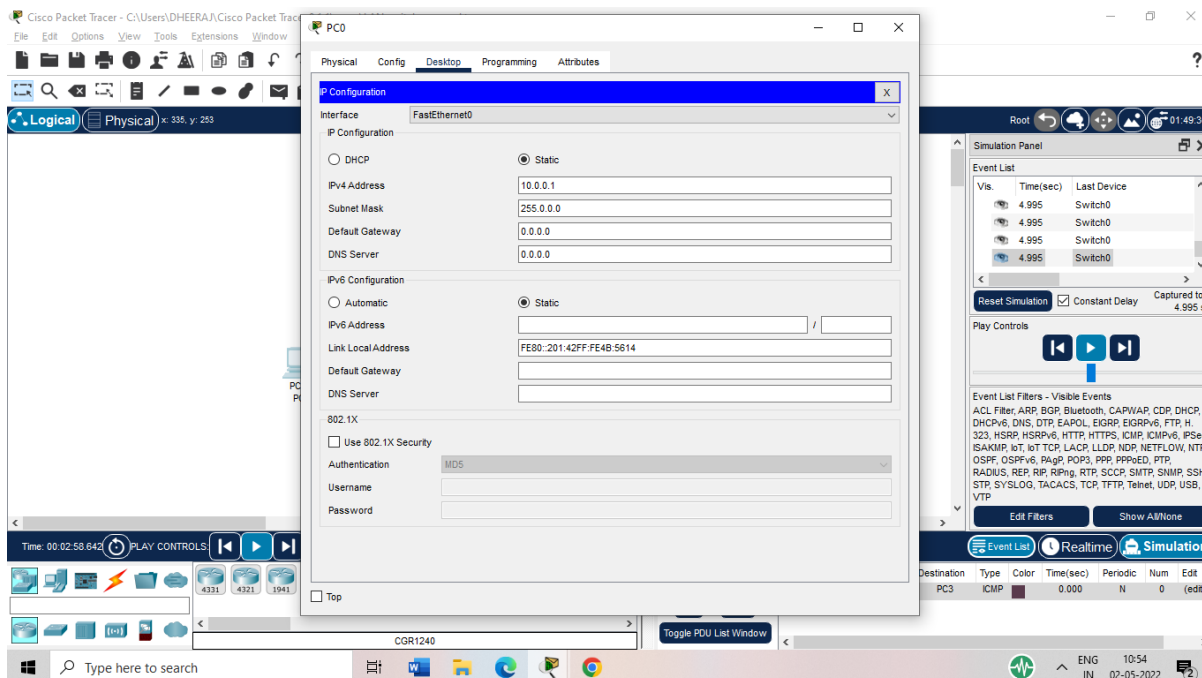
Check the simulation to see the movement of packets.

Resource : <https://www.youtube.com/watch?v=FZ8hRDakHvI> LAN using a HUB

Conceptual Knowledge on HUB: POWERCERT videos

4. LAN using Switch





IP address to be allocated for each device eg 10.0.0.1, 10.0.0.2 and so on.

Connect all the devices to the SWITCH

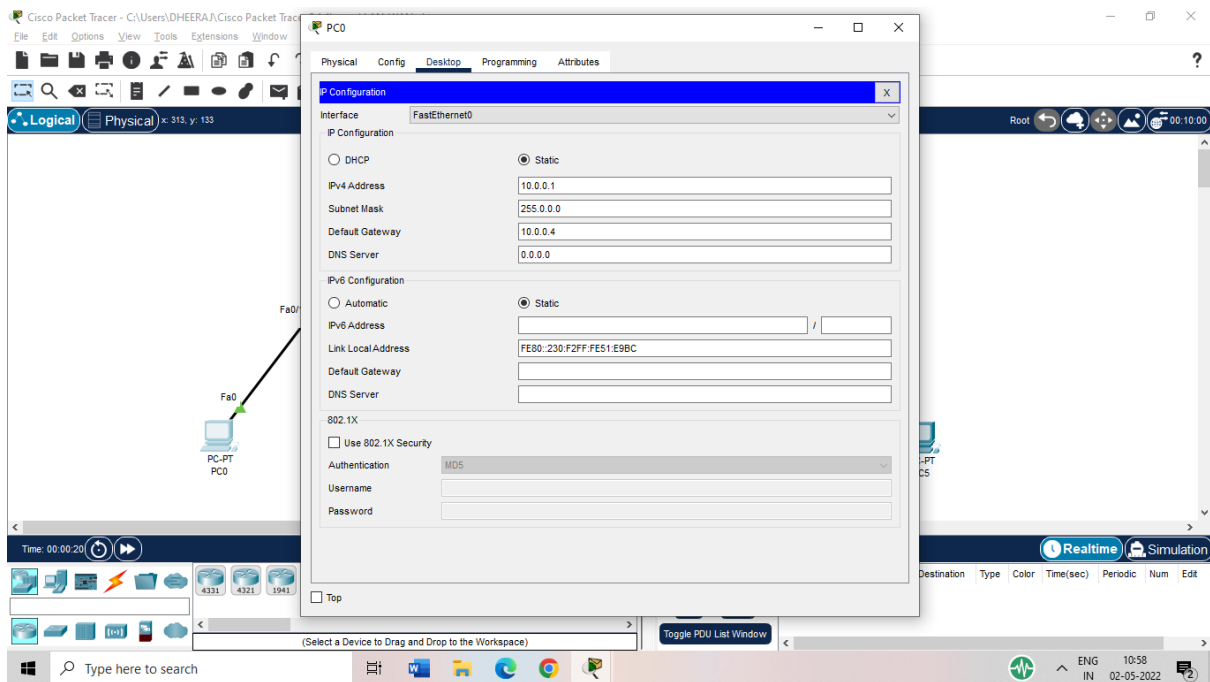
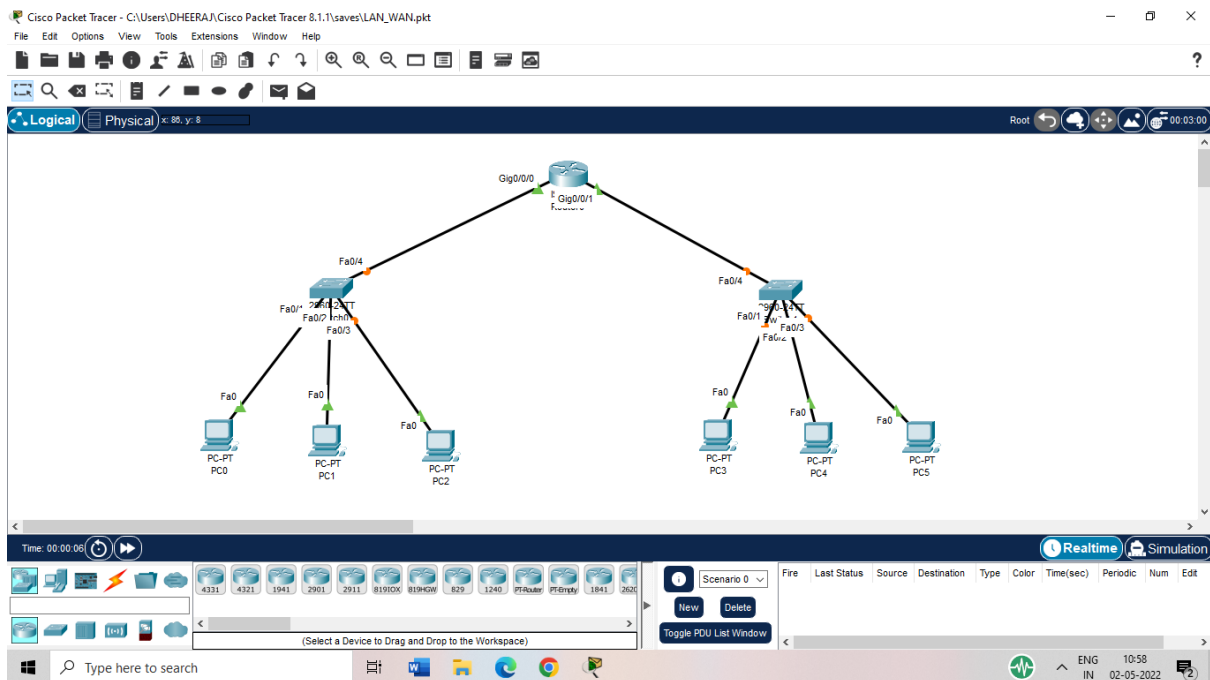
SWITCH delivers to specific devices. Only the specific one accepts it. Others

Ping in Real time

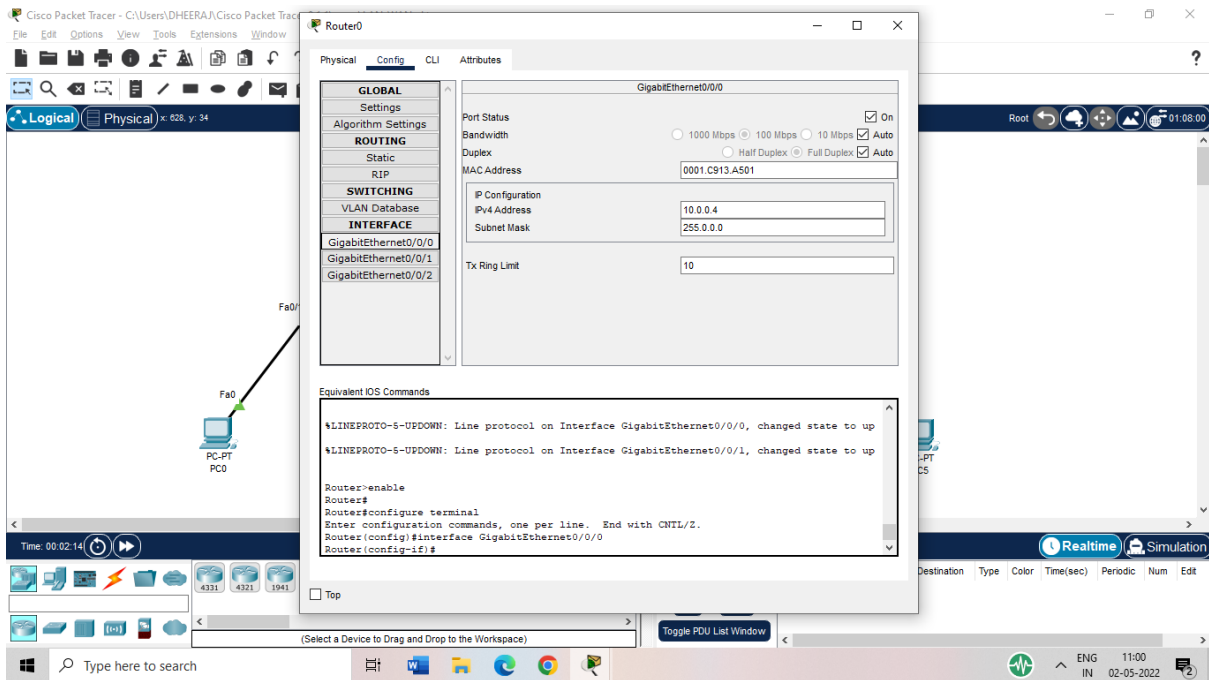
Check the simulation to see the movement of packets.

Resource: <https://www.youtube.com/watch?v=eFY6mi3lmRQ> LAN using a switch

5.TWO LANS Communication using a Router

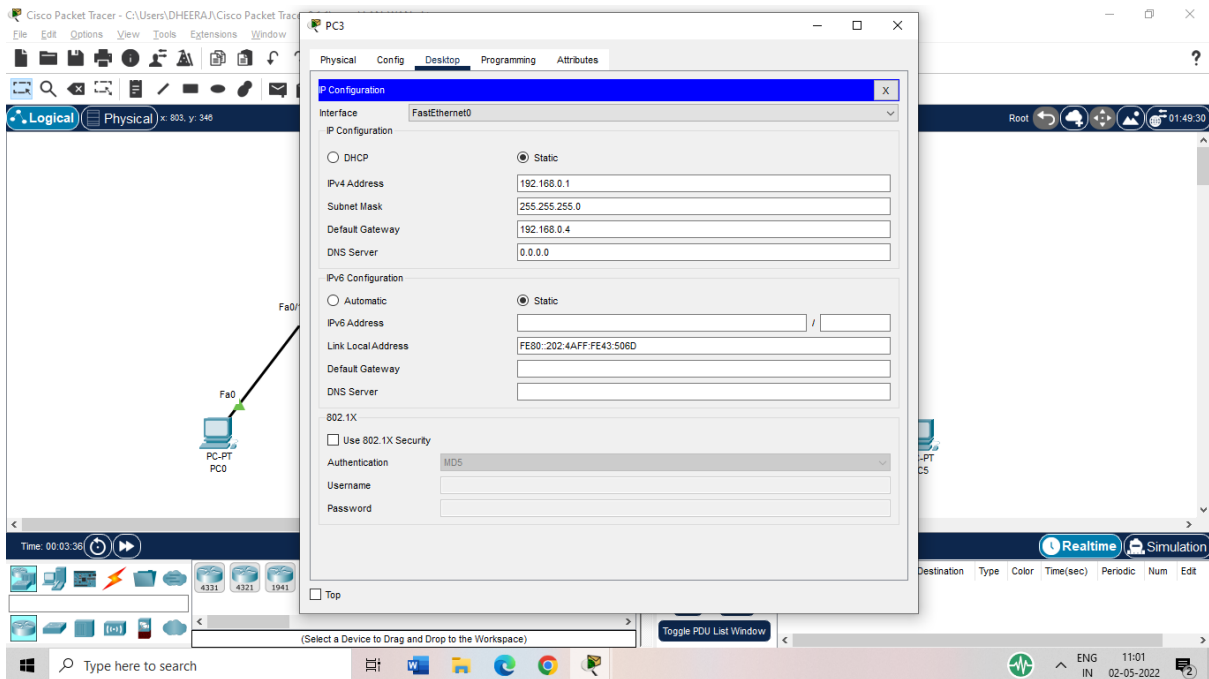


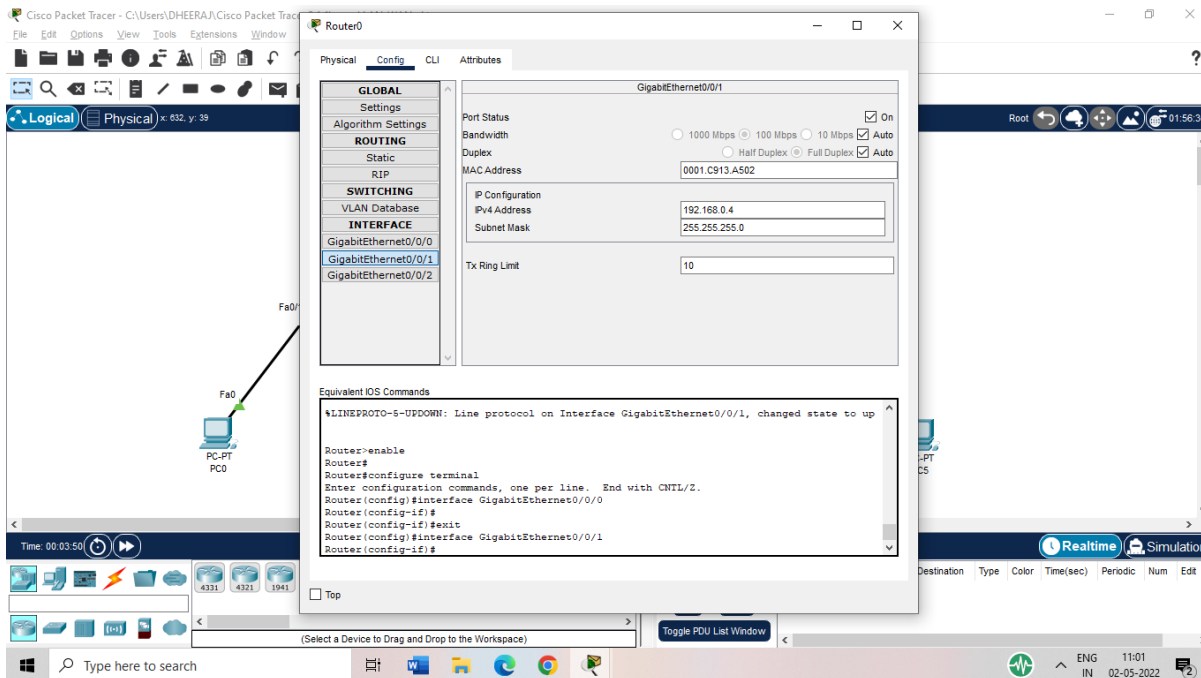
Every PC in this network of 10.0.0.1 and subnet mask 255.0.0.0. Set the default Gateway to that of the Router Interface IP(Gig0/0/0)



Set the Router ON and set the IP address(10.0.0.4). This is the default gateway of the network on the left hand side of the screenshot.

Similarly for the other network

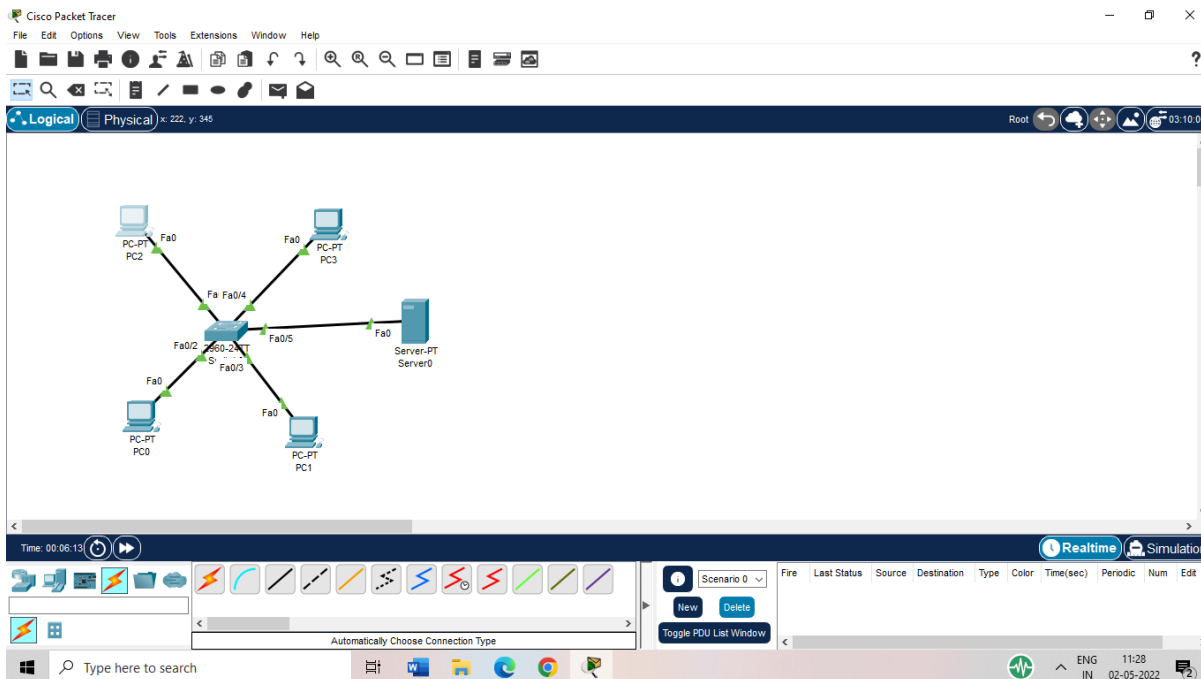


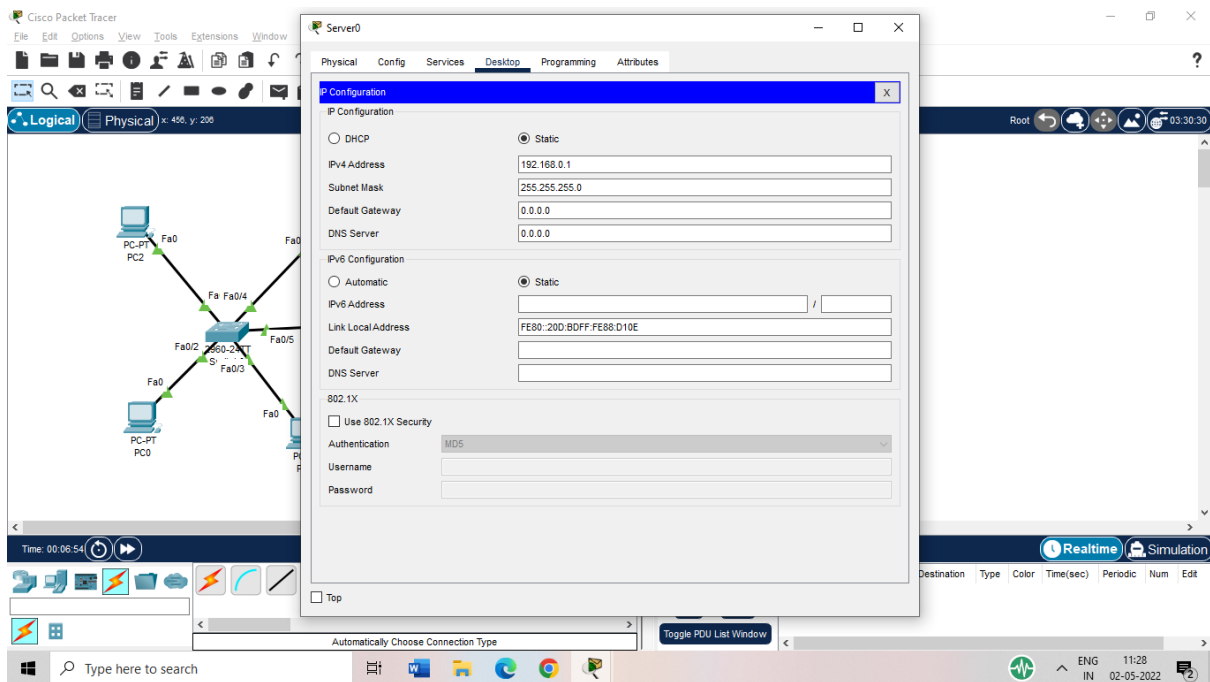
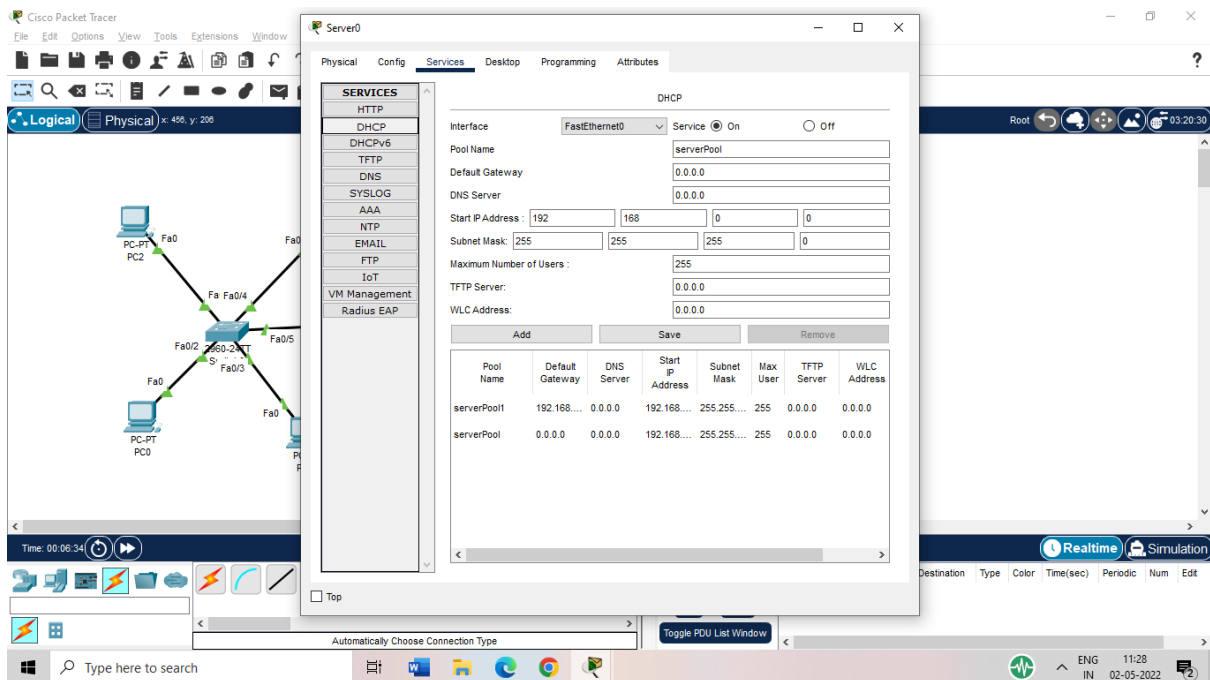


Communication between the Router and LAN is established.

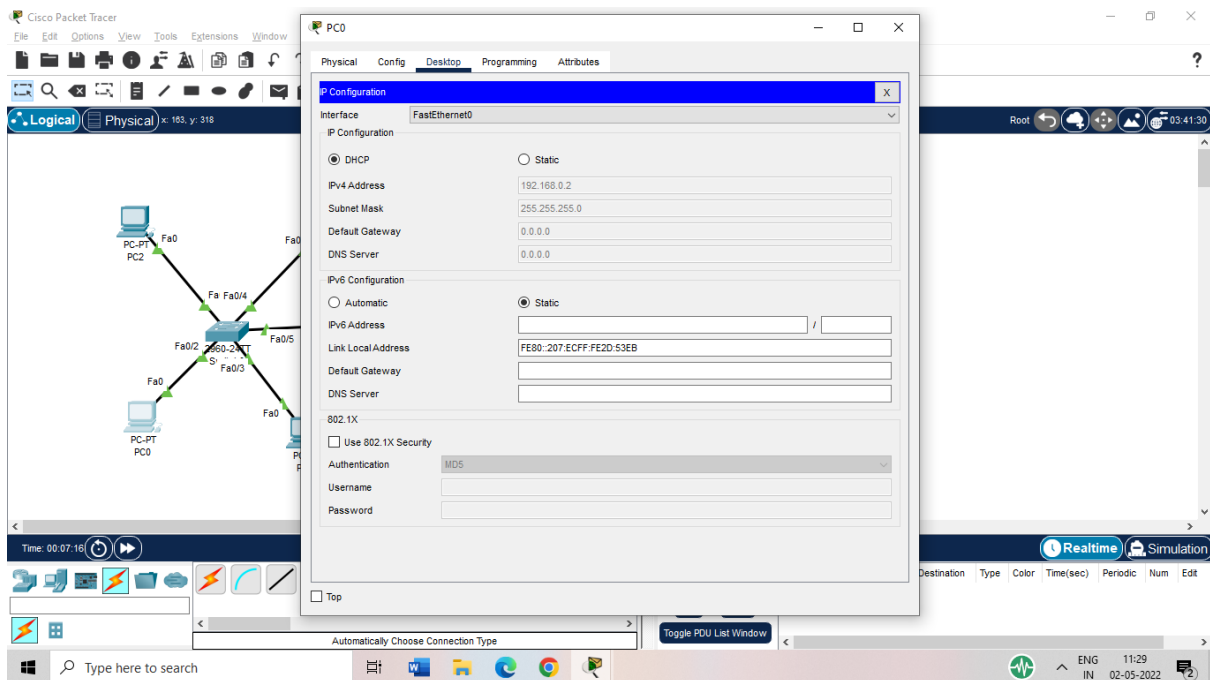
Resource: <https://www.youtube.com/watch?v=FnH1XUQsoD8>

6.DHCP Server

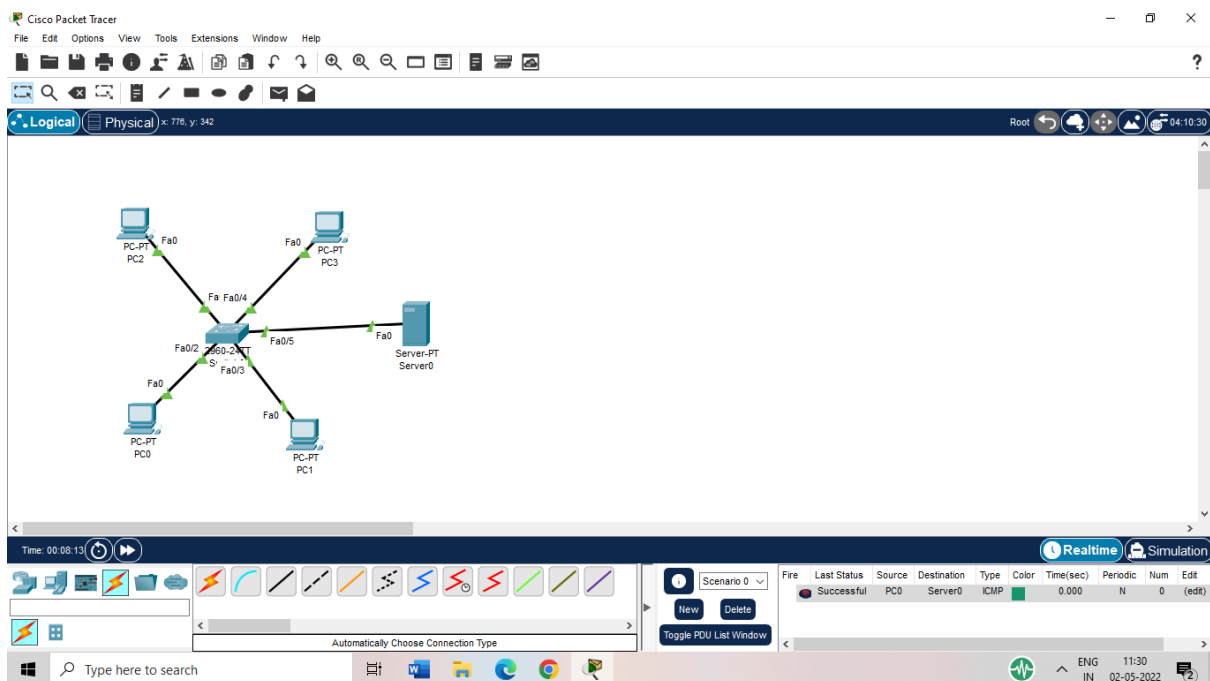




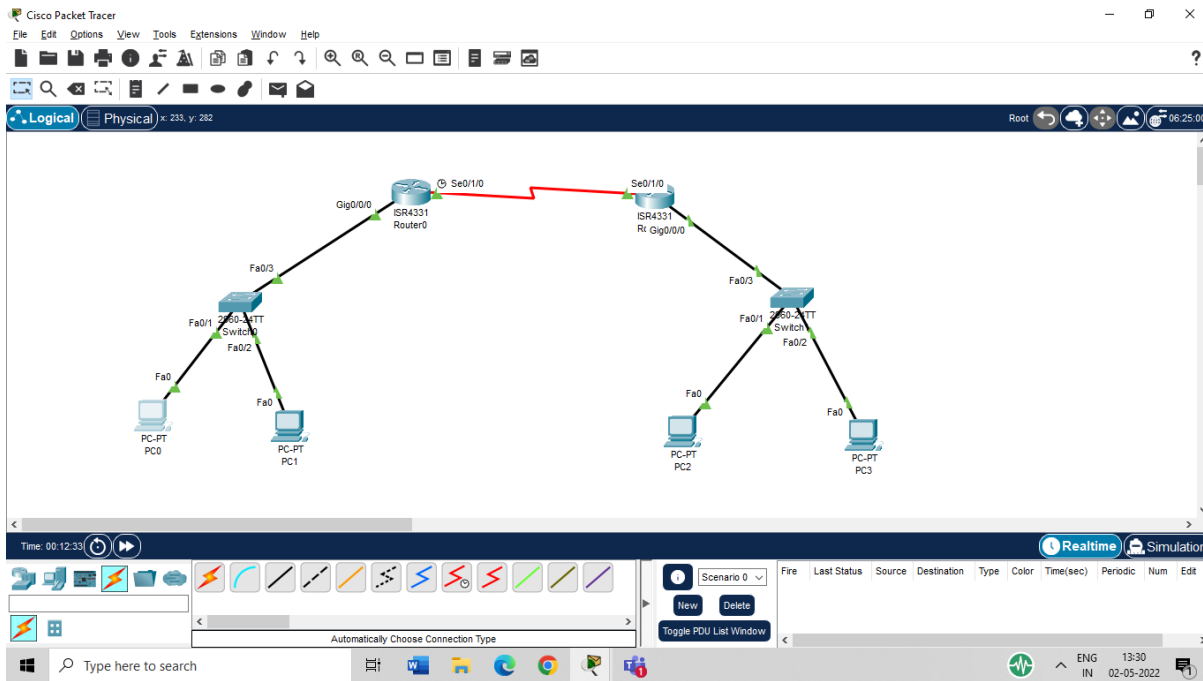
PC given IP address automatically



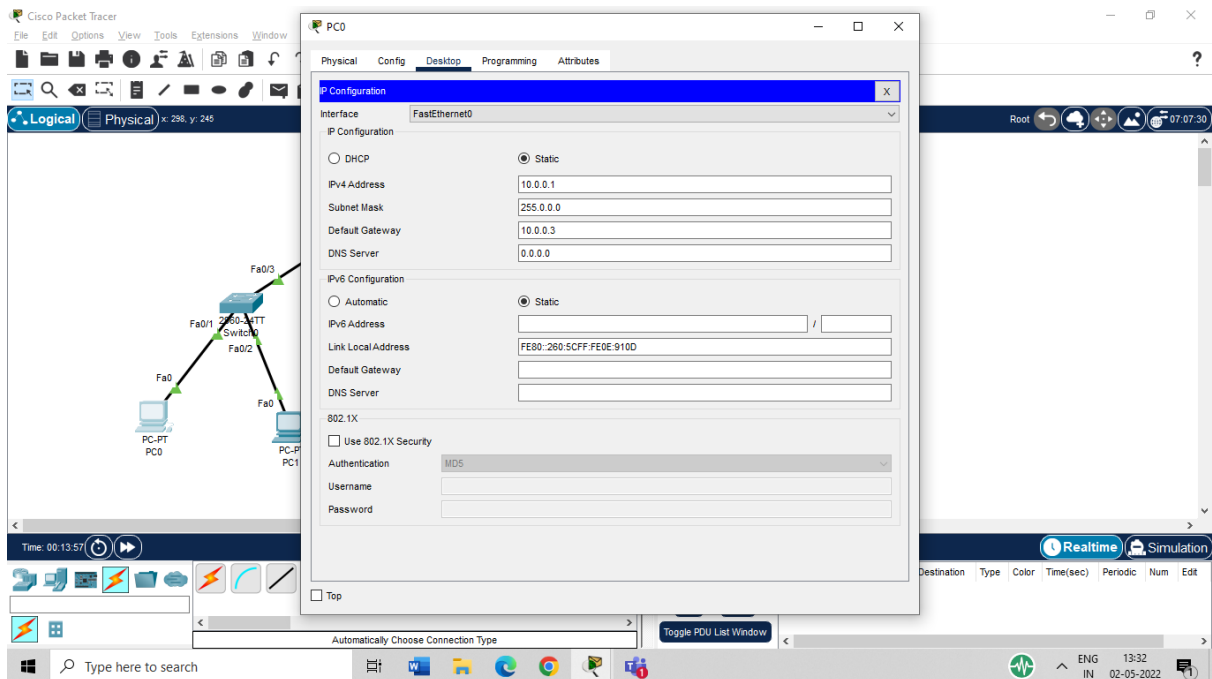
PC0 to Server

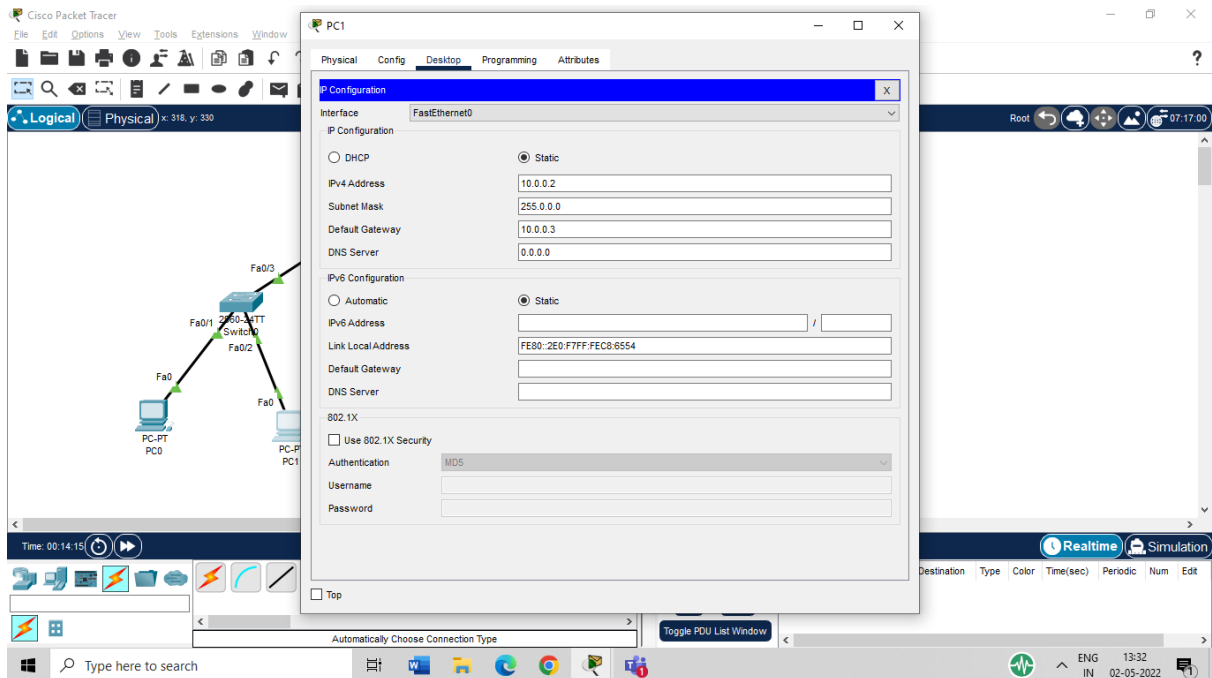


7.Router to Router Communication



1. Assign IP address to PC.
2. They are basically 2 different networks.
3. Let the left hand side network be

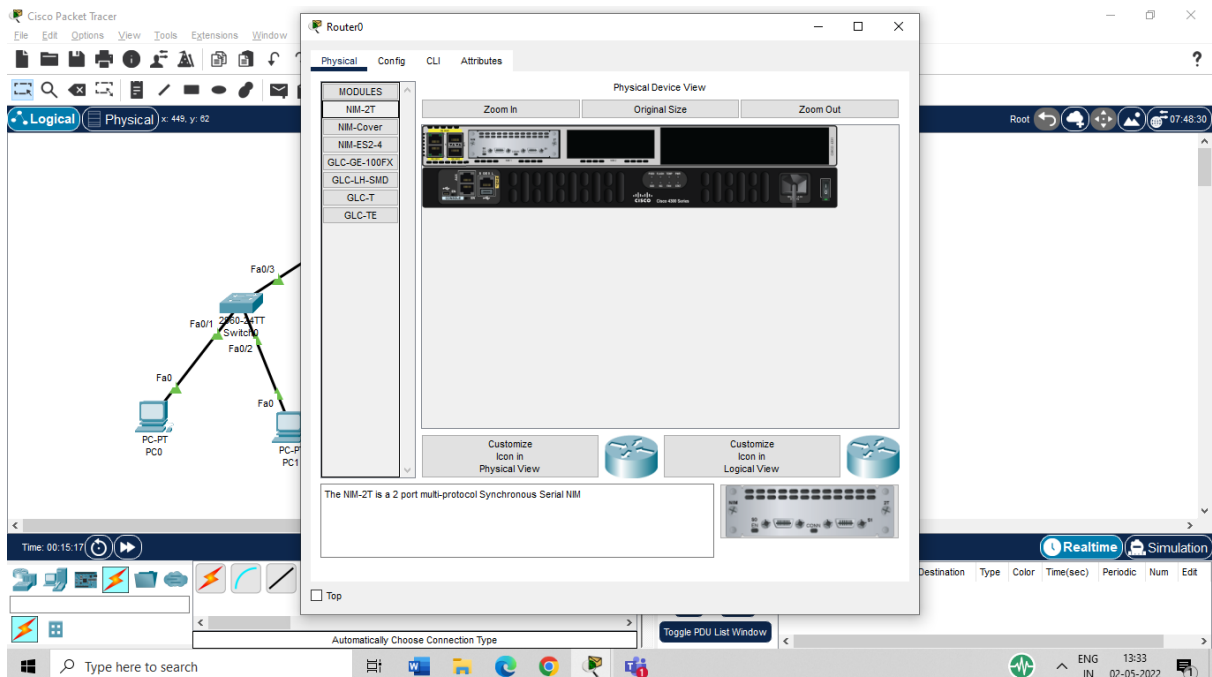


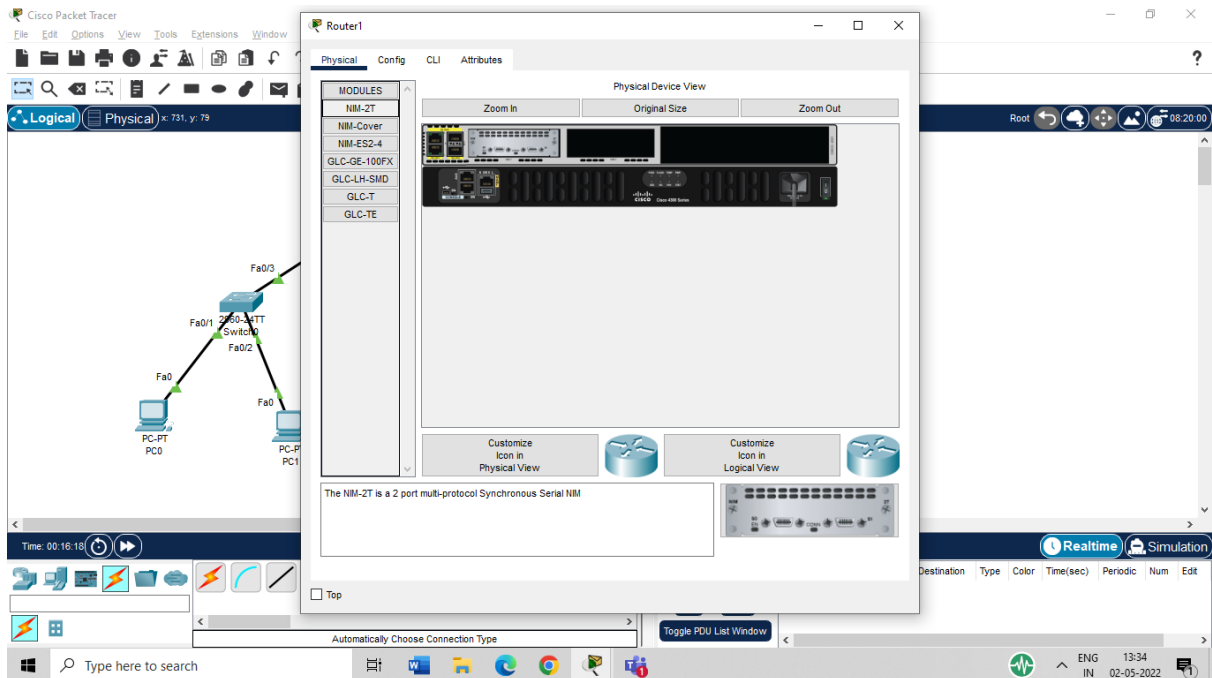


Note Between the Routers do not establish the connection.

Initially select a serial Interface NM-2T and power off the Router and place it as shown

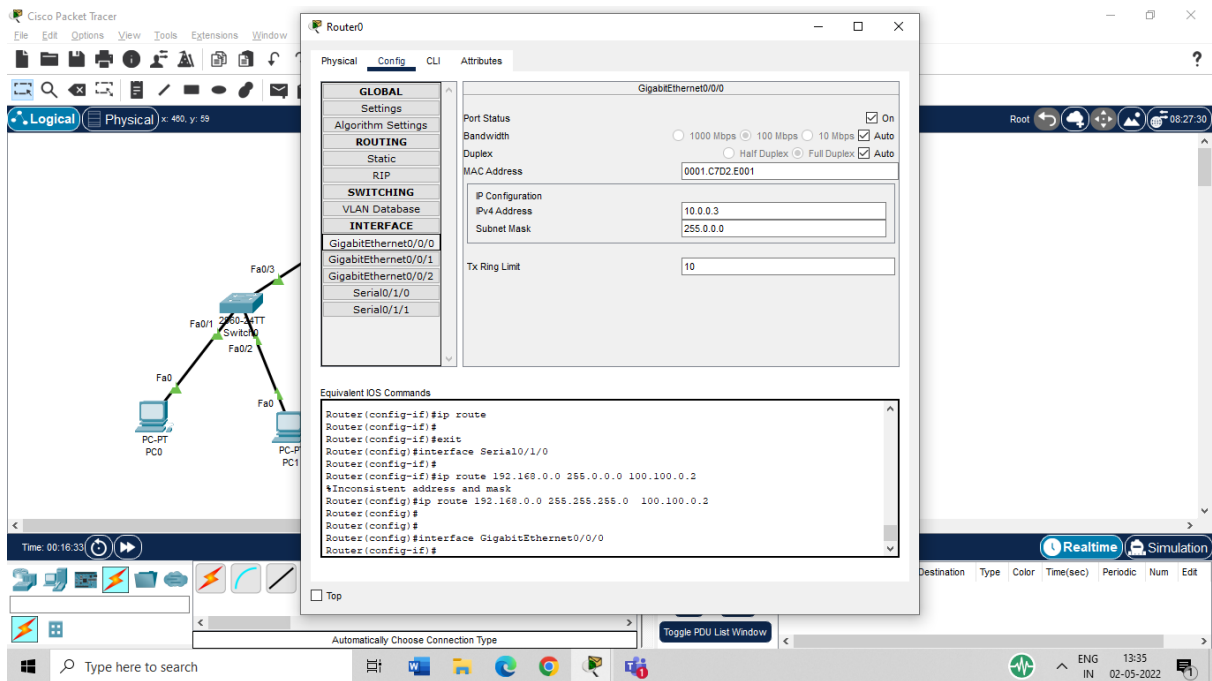
This is done for both the routers.



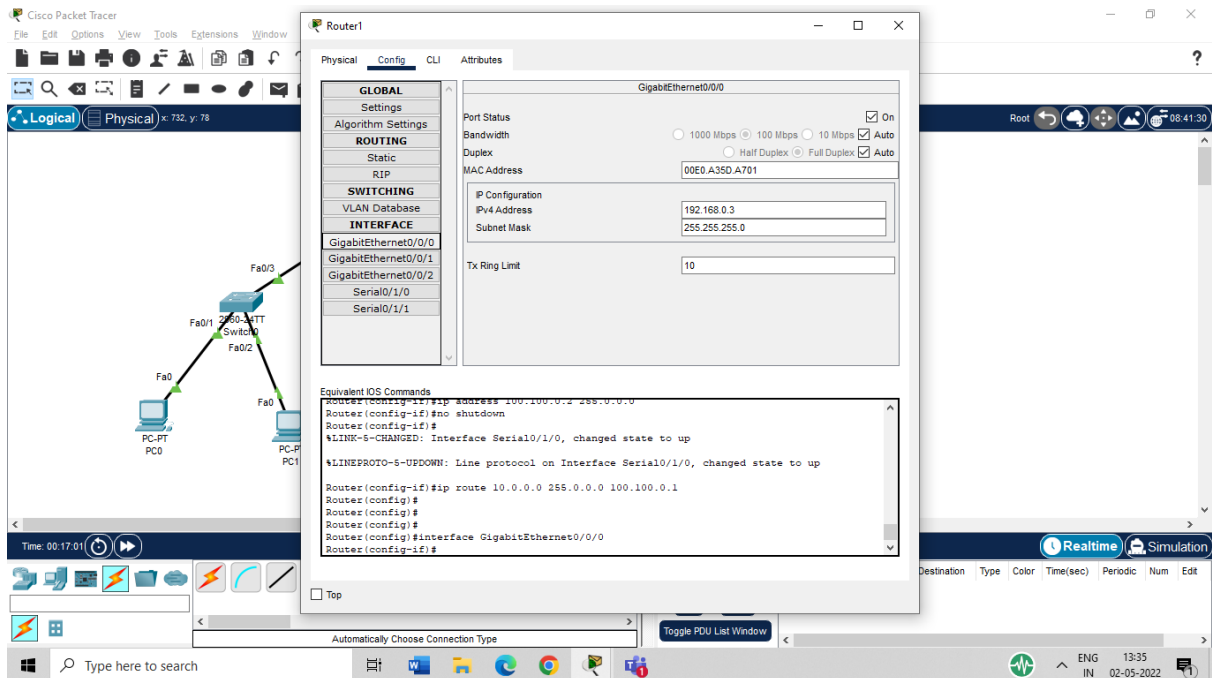


Router 0

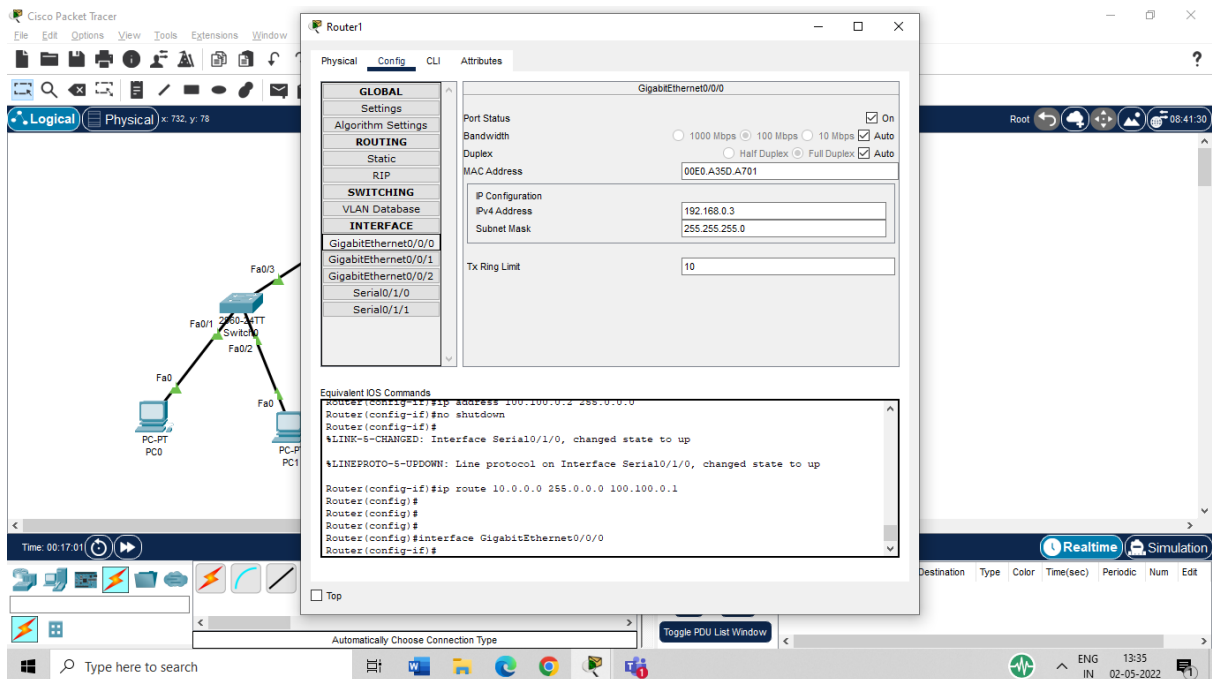
Config



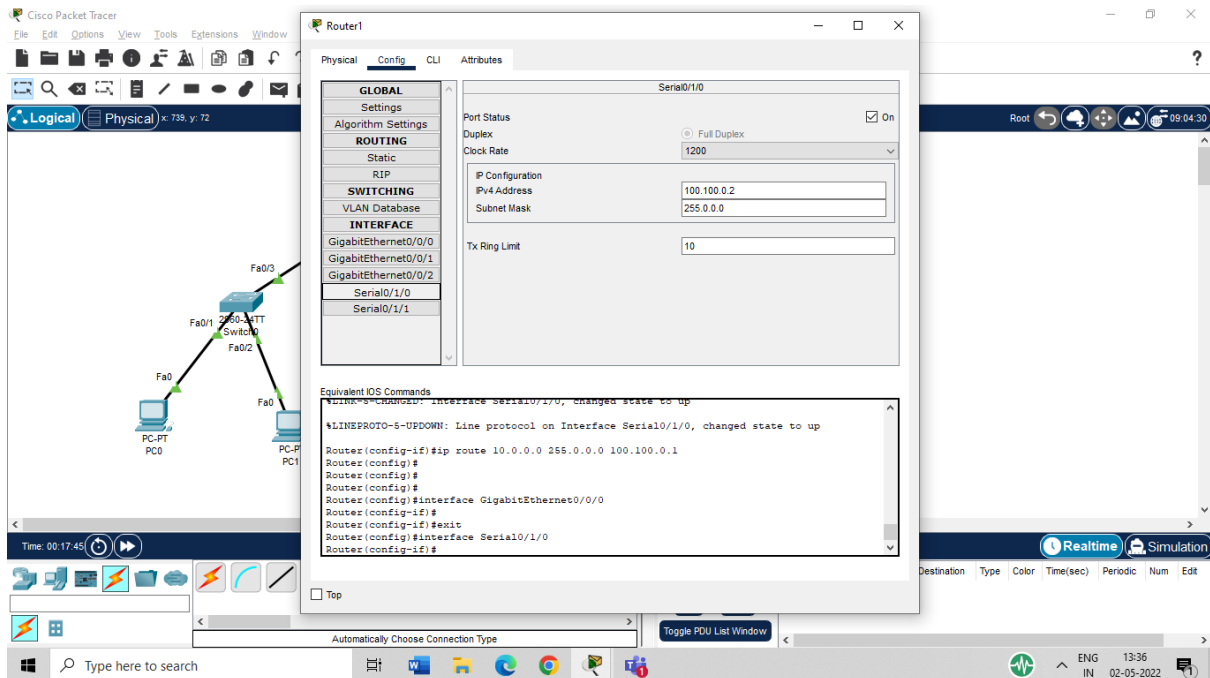
Router 1 Config



Serial Connection between the 2 Routers since they form another network.



Both Routers belong to the same network so give the IP address of similar series

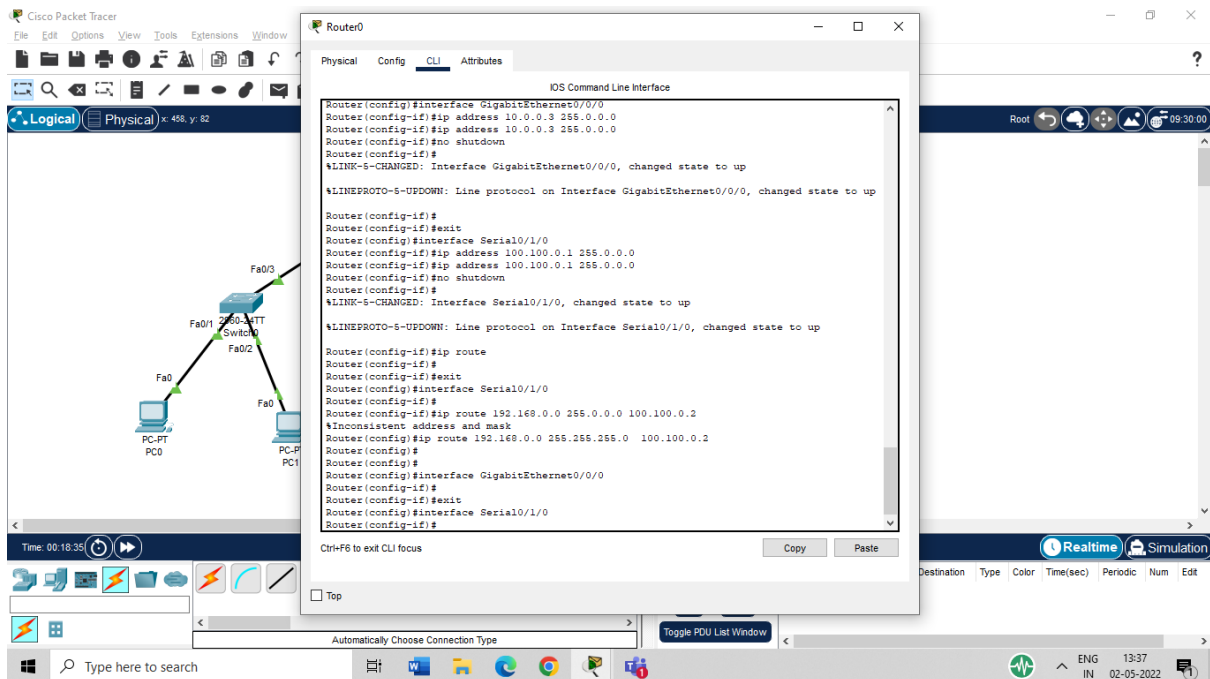


In the CLI window of Router 0 type

Format

Destination Subnet mask of destination next Hop

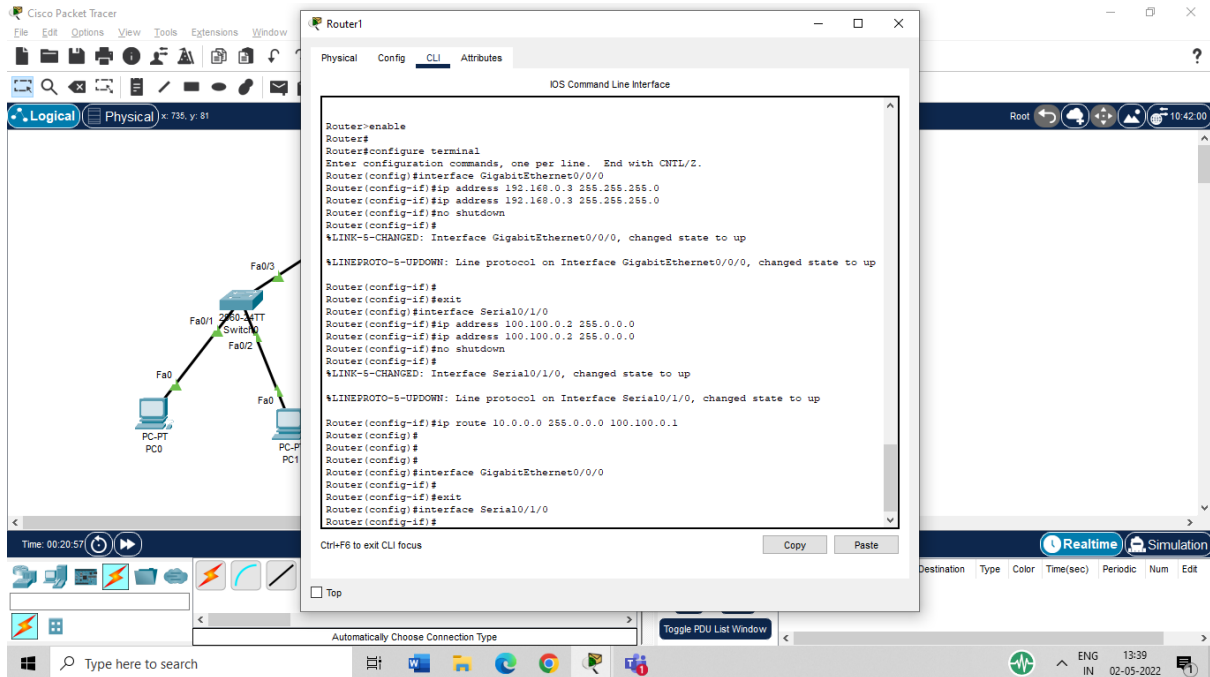
`iproute 192.168.0.0 255.255.255.0 100.100.0.2`



In the CLI window of Router 0l type

Destination	Subnet mask of destination	next Hop
-------------	----------------------------	----------

```
iproute 10.0.0.0 255.0.0.0 100.100.0.1
```



https://www.youtube.com/watch?v=m8_IP74PEm8 --- FTP