DEPARTMENT OF INFORMATION SCIENCE

COMPUTER NETWORK LAB EXPERIMENTS

Module-1

DOS Commands

1.PING Command

How to check internet connection in CMD

To check whether your internet connection works, you can use Command Prompt to test your connection to a certain website or internet location. To do that, you can use the ping network command, followed by a web address or IP address. For instance, you can check the connectivity to GOOGLE without opening a web browser, by typing the command " ping www.google.com." Then press Enter on your keyboard.

Ping is used to check the connectivity with other devices on the network, for example computers, routers, switches etc. Select Start > Programs > Accessories > Command Prompt. This will give you a window like the one below.

Type *C:\>ping x.x.x.x*

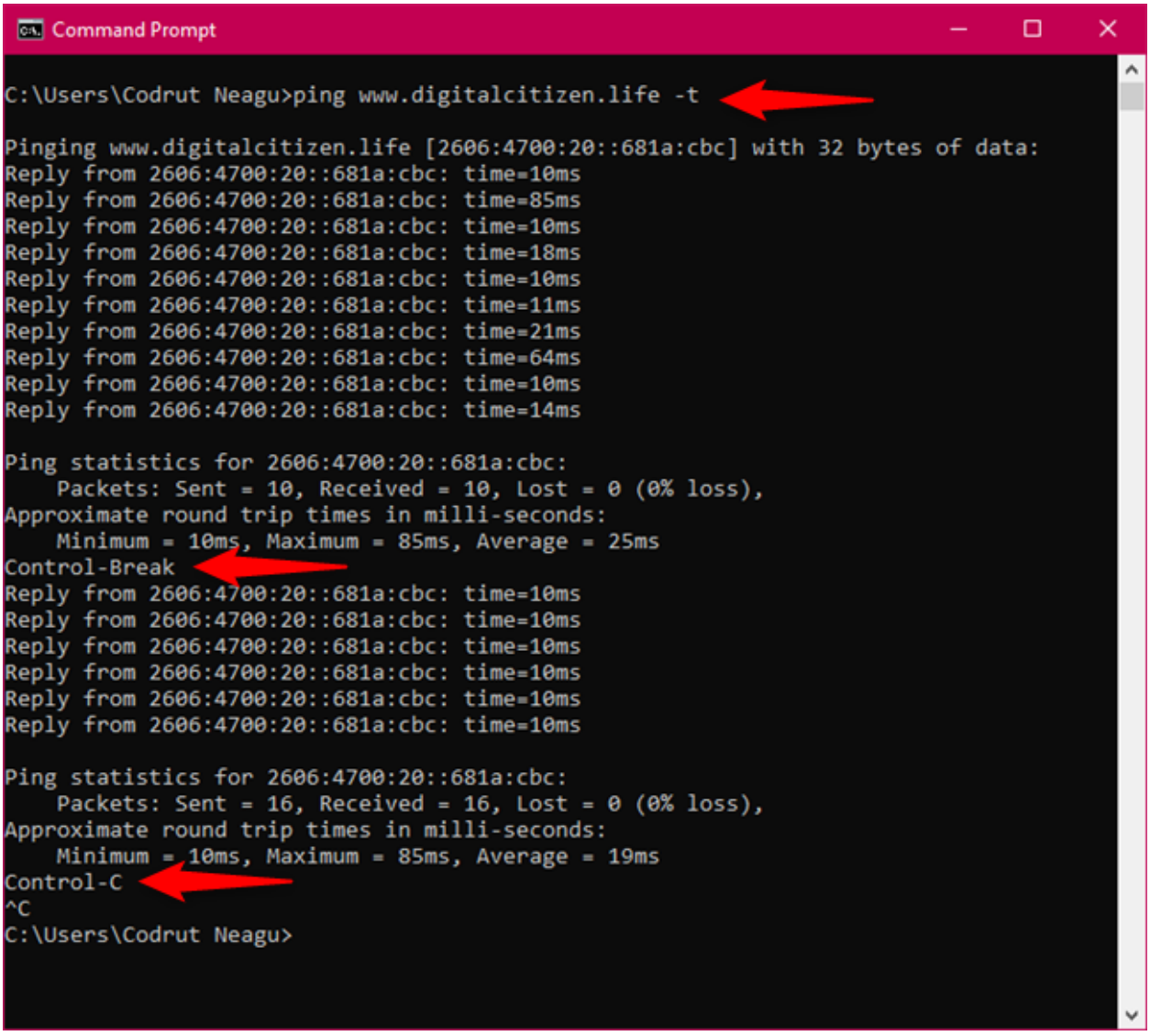
By default, ping sends four ICMP Echo Request packets each of 32 bytes. The response packets are called ICMP Echo Reply Packets.

Fig : The Ping Command

Now Type *C:\>ping x.x.x.x –t*

- The ping command also allows you to use the handy "-t" parameter, which enables you to ping the specified address forever until it's manually stopped. For instance, we typed "ping -t www.digitalcitizen.life." After some time, we wanted to see some connection statistics and we used the keyboard combination "CTRL + Break." This shows the averages of the ping commands run until then.

- "–t" switch will continue to send packets to the destination until user stops this by pressing *Ctrl + C*

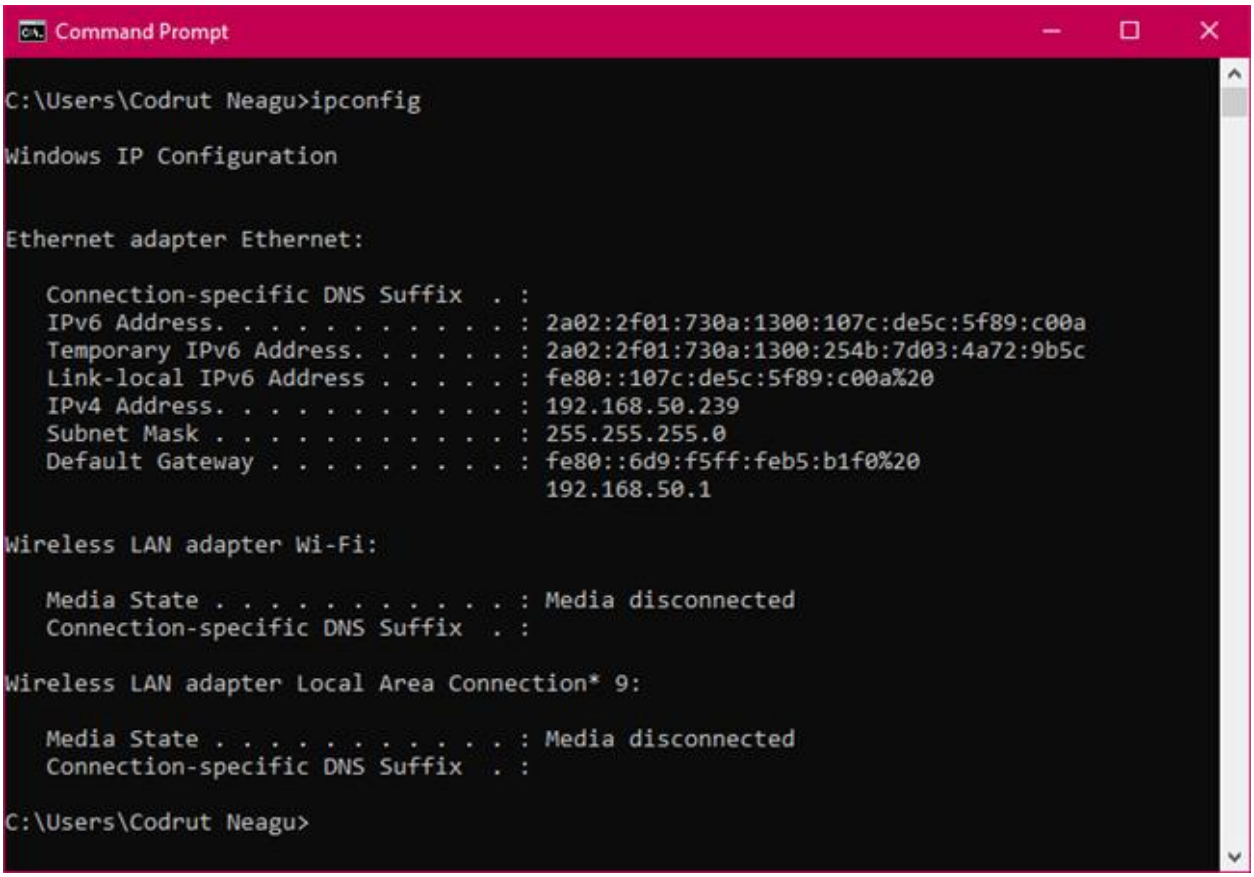


2. IPCONFIG Command

How can I see all the network adapters on my computer using CMD?

To obtain detailed information about your network adapters and connections, use the ipconfig command. Open Command Prompt, type ipconfig, and press Enter. As you can see in the

screenshot below, when you run this command, Windows displays the list of all the active network devices, whether they're connected or disconnected, and their IP addresses. You also get details such as their default gateway IP addresses, subnet masks and the state of each network adapter.



Displays full TCP/IP configuration of all network adapters (Ethernet cards) installed in your system. Type the following command in the command prompt.

C:\ipconfig

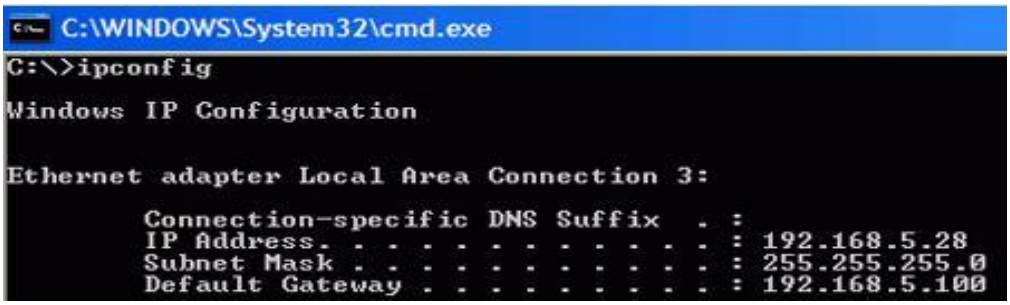
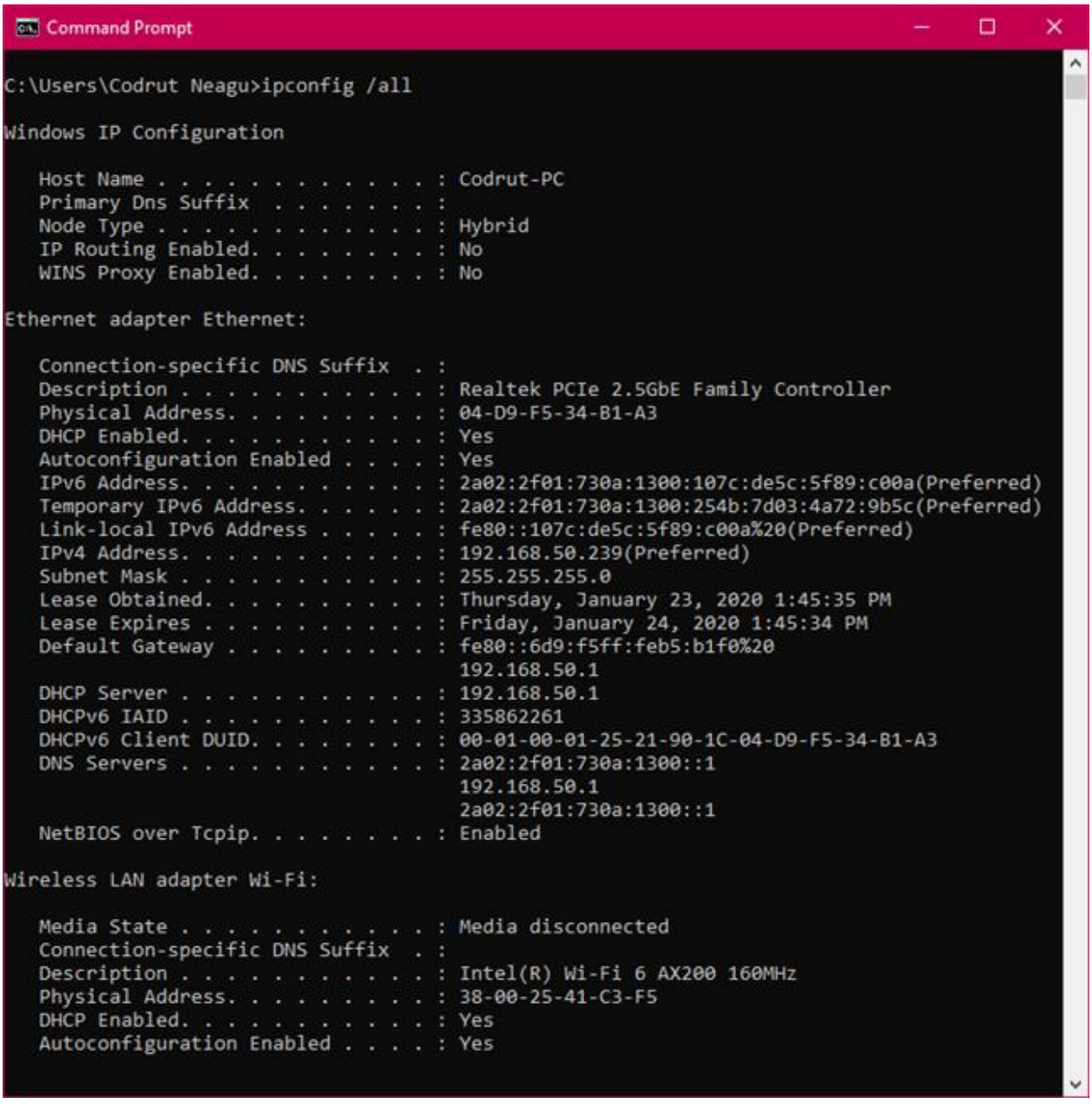


Figure 2: The IPCONFIG Command

Now type *C:\ipconfig /all*

If you add the /all switch to the ipconfig command, you can get to a whole new level of detail: DNS information, the MAC (Media Access Control) (in the Physical Address field), and other information about each network component. Check out the picture below to see a sample of what you get from the "ipconfig /all" command.



Ip config has a number of switches the most common are**:**
ipconfig /all – displays more information about the network setup on your systems including the MAC address.
ipconfig /release – release the current IP address

ipconfig /renew – renew IP address
ipconfig /? -shows help
ipconfig/flushdns – flush the dns cache

How to check your network connection in CMD

If you want to check whether your network connection to the router is operating as it should, you can use a combination of the commands ipconfig and ping. First, get some cmd nic info about your adapter. In other words, open Command Prompt and run ipconfig. In the list of results, identify the network adapter that's used for connecting to the network you want to test. Then, in its details, find the IP address of your router and note it down. For example, if we'd want to check our Ethernet network connection, we'd run ipconfig and see that our router's IP address is 192.168.50.1.

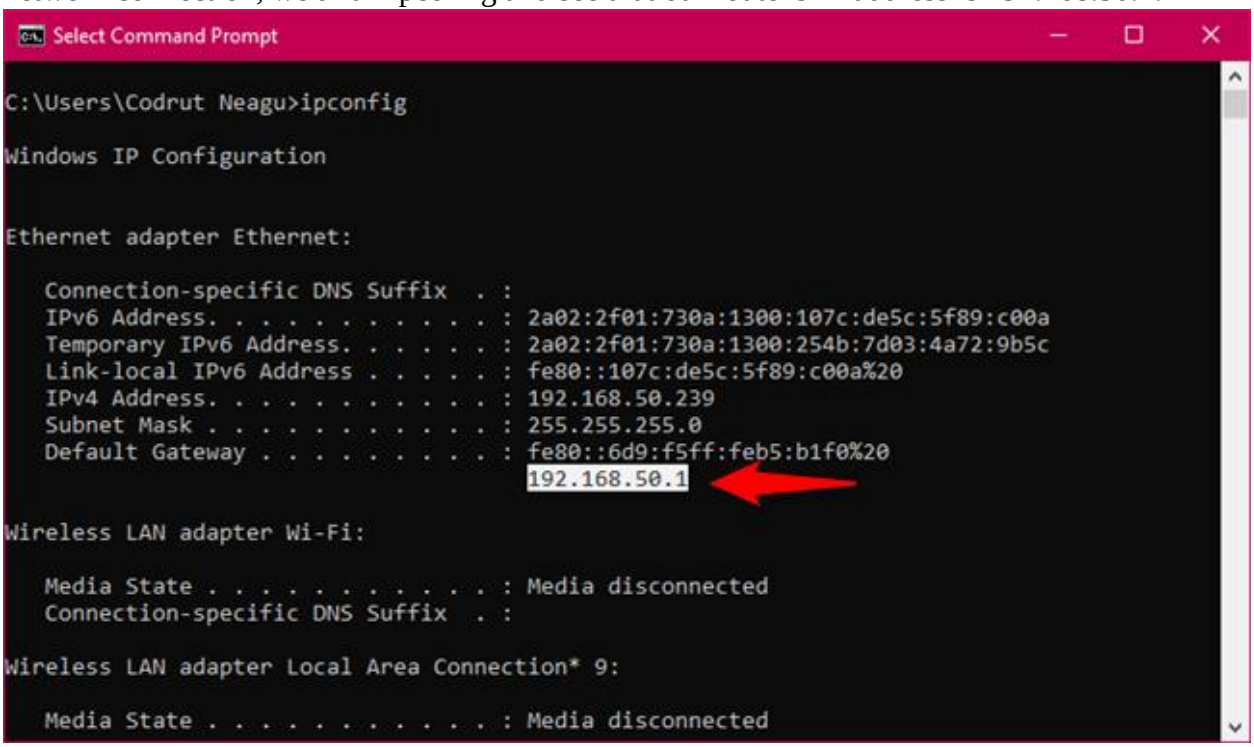


Figure :Running ipconfig to identify the IP address of the router

The next step is to check that the network connection between the router and the computer is OK. To do that, it's enough to run the ping command on the router's IP address. In our example, that would mean that we have to run this command in CMD: ping 192.168.50.1.

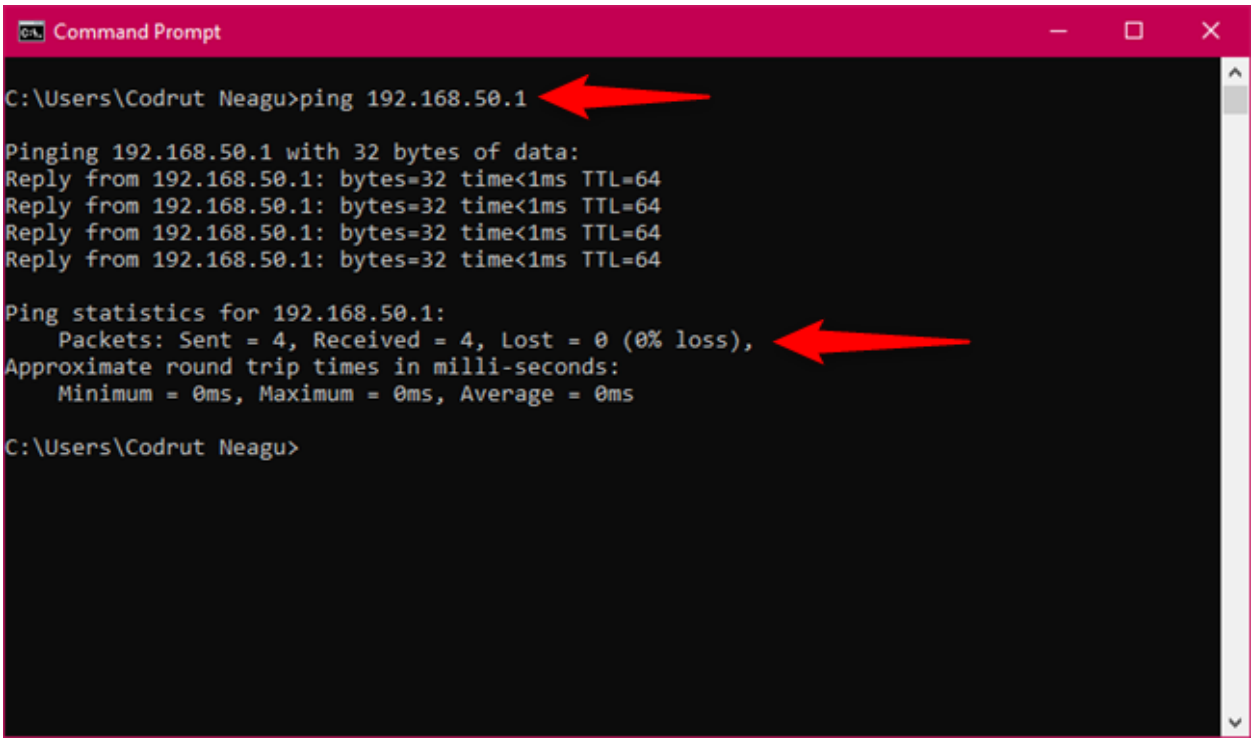


Figure:Pinging the router to check the network connection

If there are no packets lost, then the network connection tested is running well. Otherwise, there's a problem somewhere between your computer and the router, in which case you should check that your PC's network adapter is configured correctly, that the Ethernet cable is OK (if you're using a wired connection), and that the router is configured properly.

How to renew the IP address of your network adapter

When your network connection doesn't work as it should, your network adapter might not have the right IP address assigned. A quick way of trying to solve this issue is to renew its IP address and, fortunately, you can do that quickly, straight from the Command Prompt. Open CMD and run the following commands: ipconfig /release and ipconfig /renew. The first one (ipconfig /release) forces your network adapter to drop its assigned IP address, and the second command (ipconfig /renew) renews the network adapter's IP address.

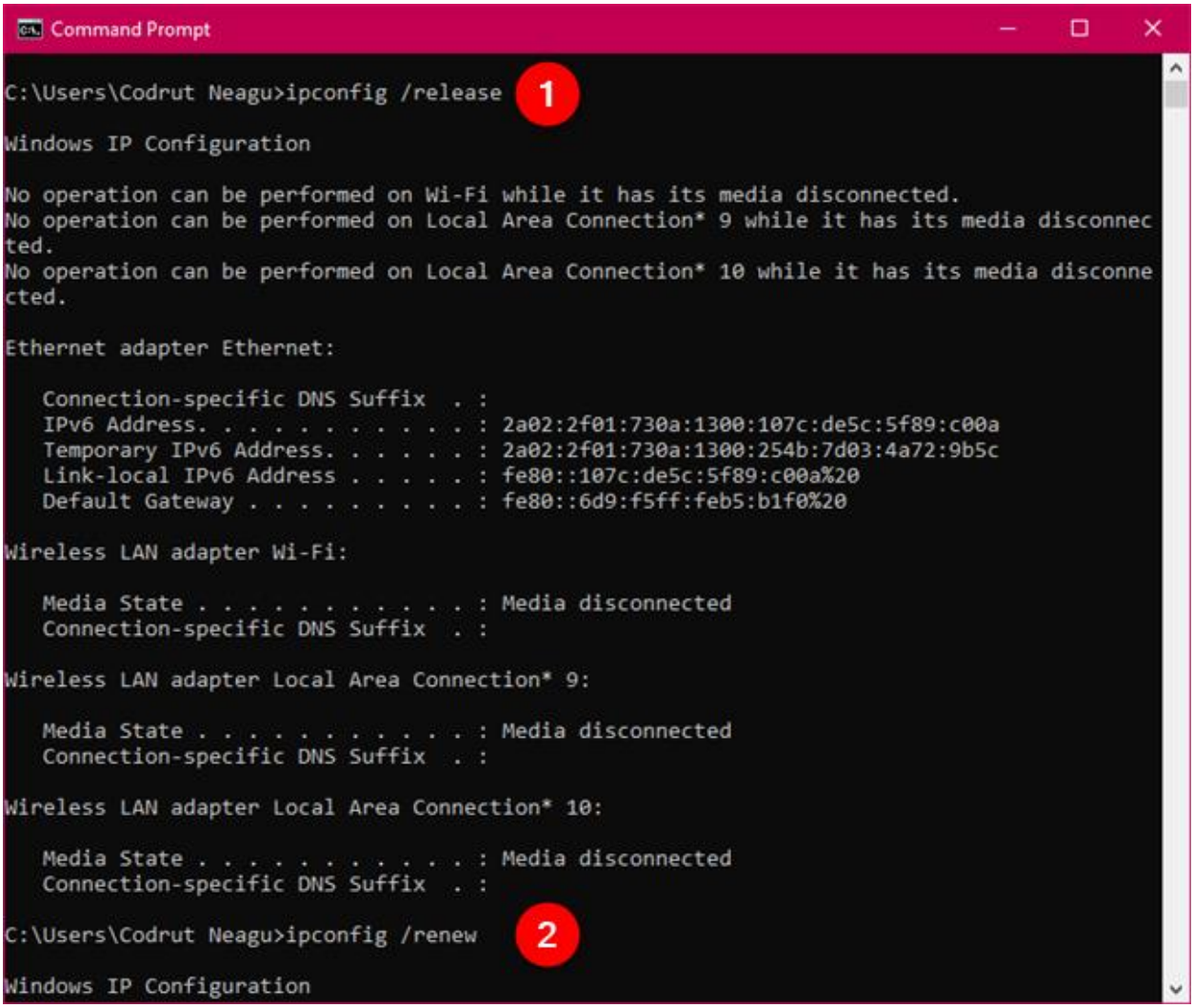
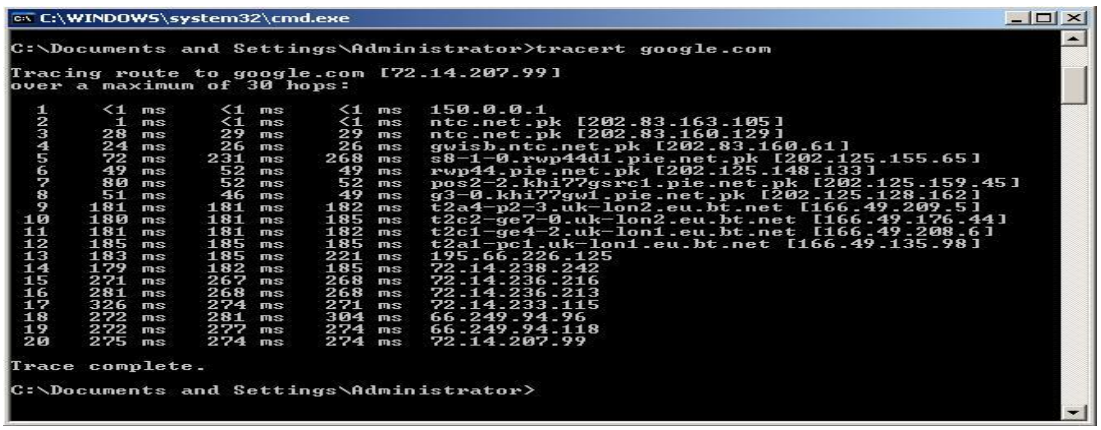


Figure: Running ipconfig /release and ipconfig /renew to reset the IP address

3 TRACERT Command

Tracert command tells you the path a packet takes from your computer to the destination. It will list all the routers from which a packet passes until it reaches its destination.
C:\tracert google.com



4. NSLOOKUP Command

Displays the default DNS server information.

Type the following command

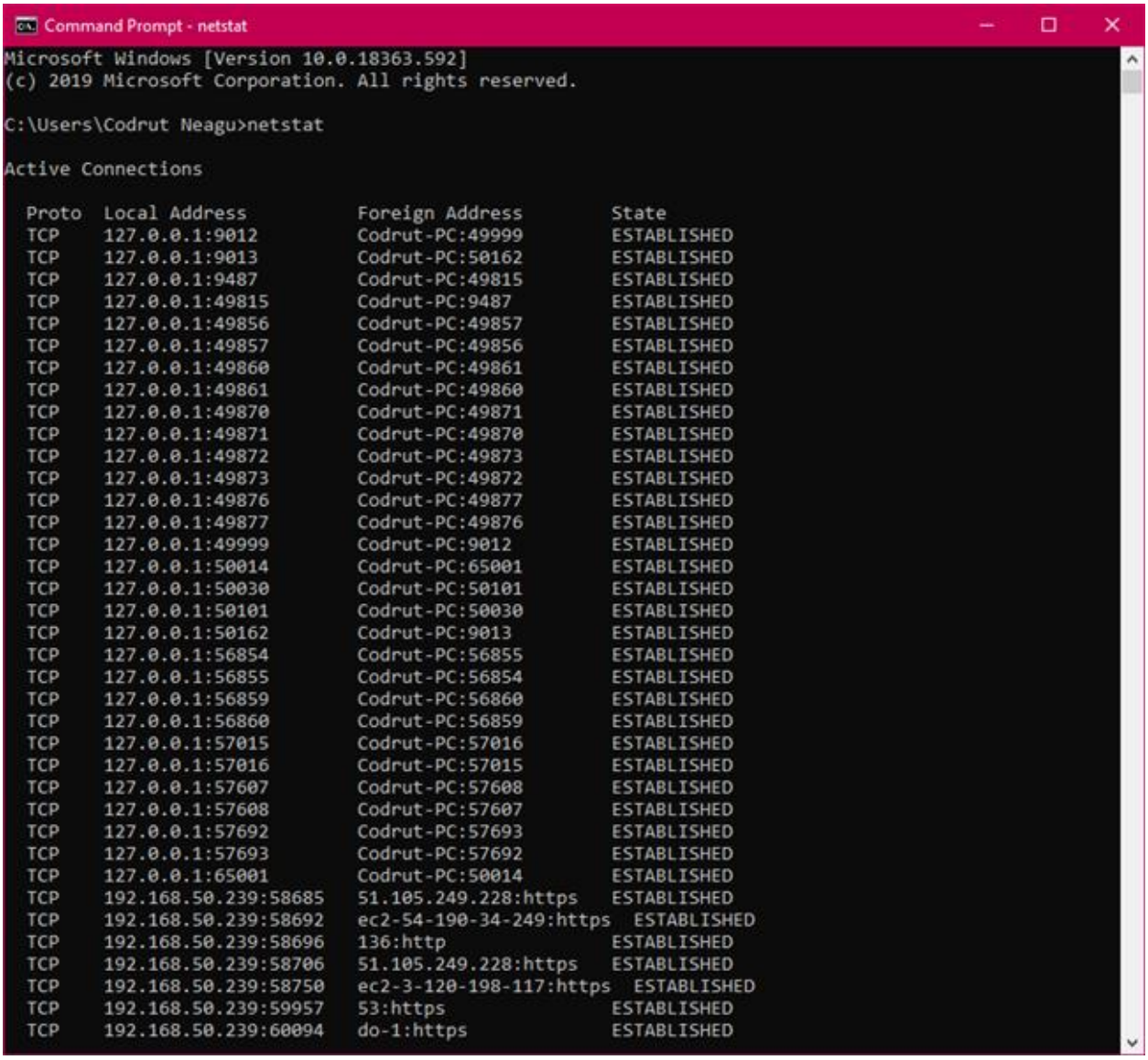
C:\>nslookup

What is your default DNS server's IP address?

5 . NETSTAT Command

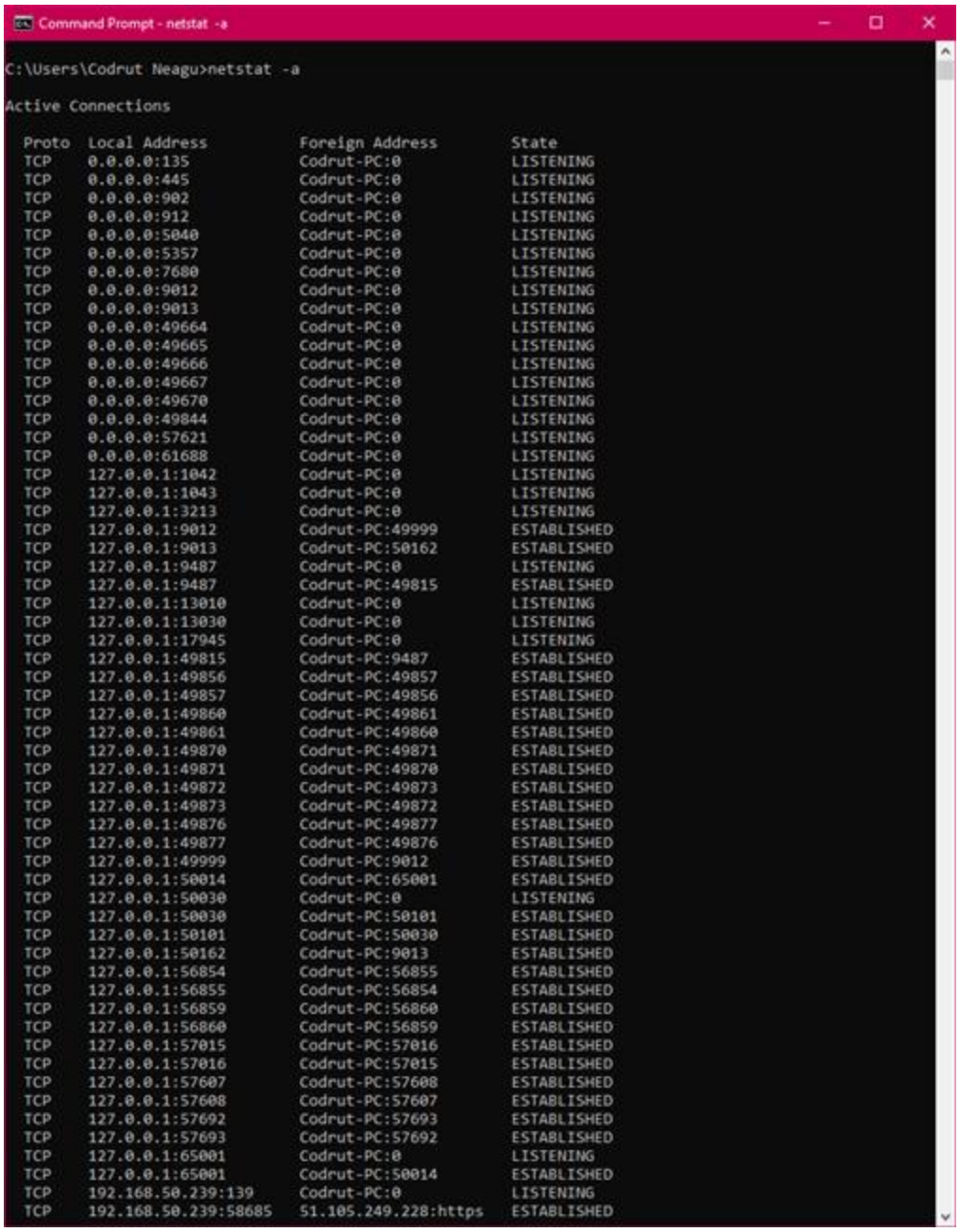
You can get other useful cmd nic info from the netstat command, which lets you see the network connections that are active between your system and any other systems on your network or the internet.

Displays active TCP and UDP connections.
Practice the following commands
C:\>netstat
C:\>netstat -a
C:\>netstat –an



Netstat shows the active network connections and open ports

If you add the -a parameter to the netstat command, you can get a list with all the connections and listening ports, as seen in the image below.



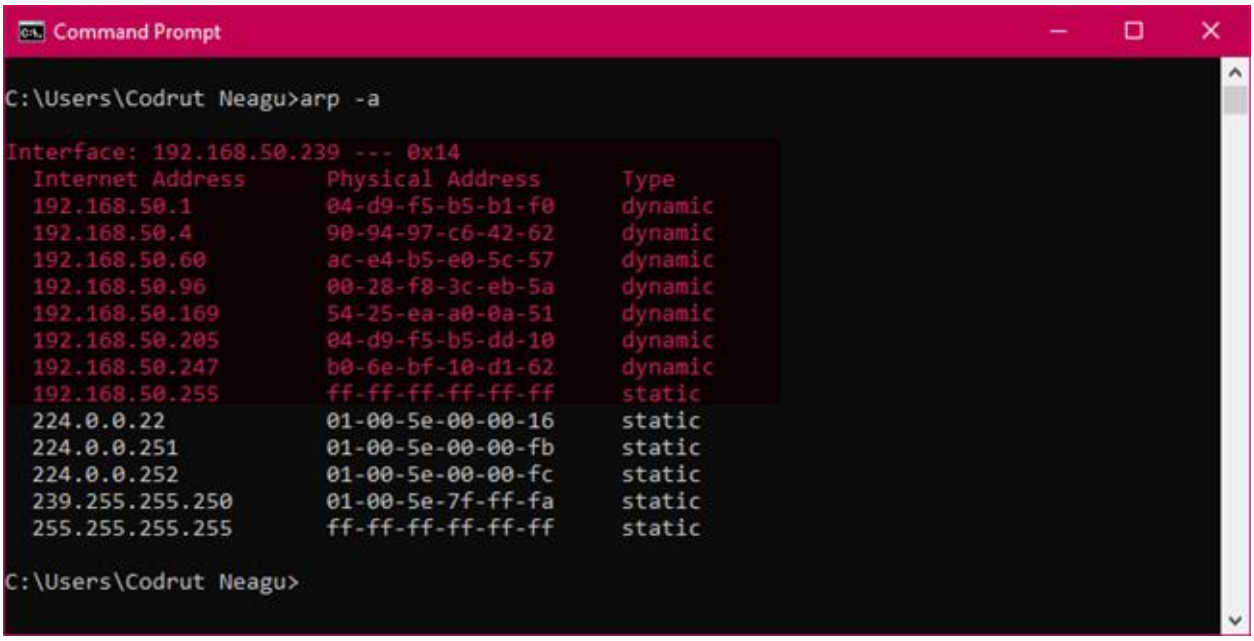
Netstat -a displays the active network connections, open ports and listening ports

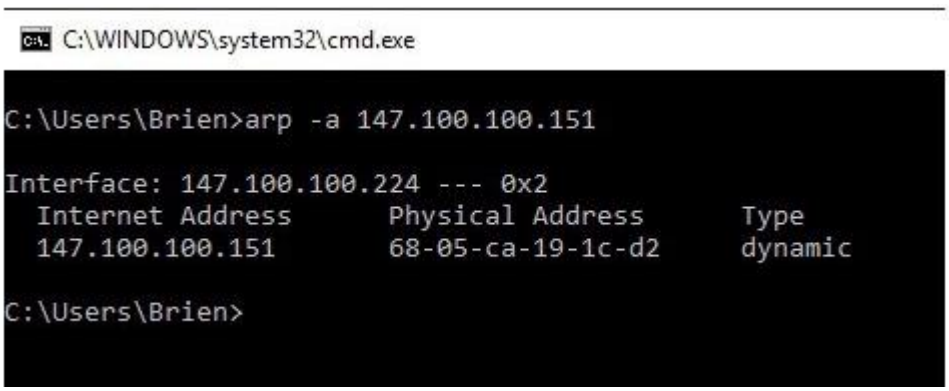
6. ARP Command

ARP command corresponds to the Address Resolution Protocol, it is easy to understand of network communications in terms of IP addressing, packet delivery is ultimately dependent on the Media Access Control (MAC) address of the device's network adapter. This is where the Address Resolution Protocol comes into play. Its job is to map IP addresses to MAC addresses.

Windows devices maintain an ARP cache, which contains the results of recent ARP queries. It shows the contents of this cache by using the ARP -A command. If any problems in communicating with one specific host, you can append the remote host's IP address to the ARP -

A command.



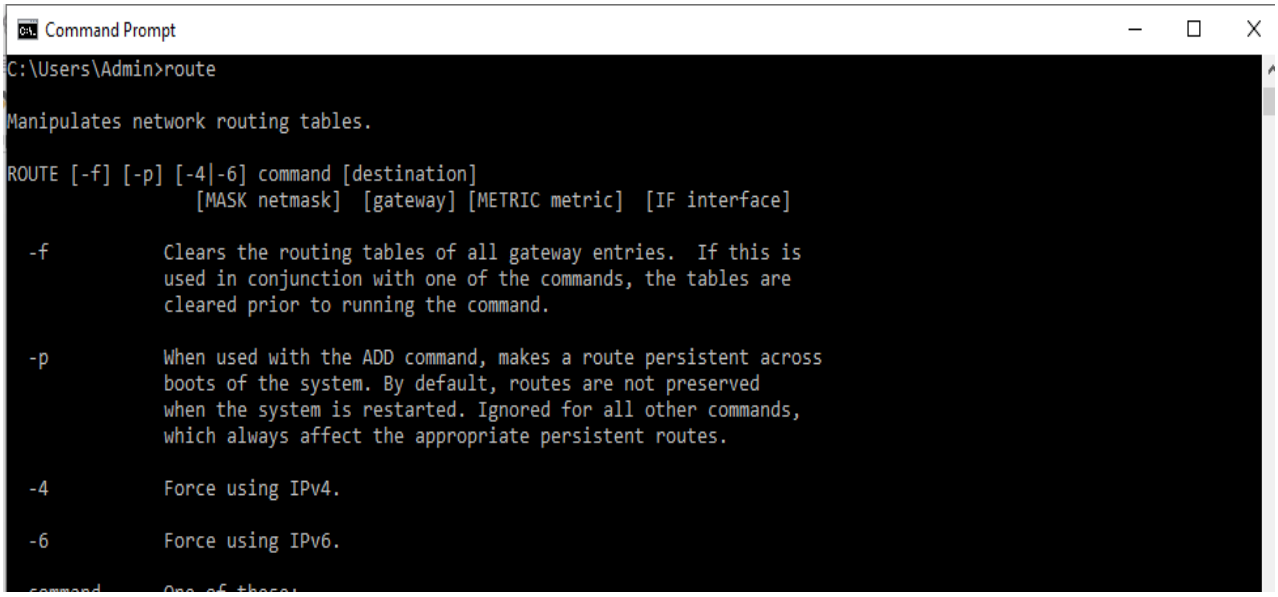


7.NbtStat-n Command

The NbtStat -n command for example, shows the NetBIOS names that are in use by a device. The NbtStat -r command shows how many NetBIOS names the device has been able to resolve recently.

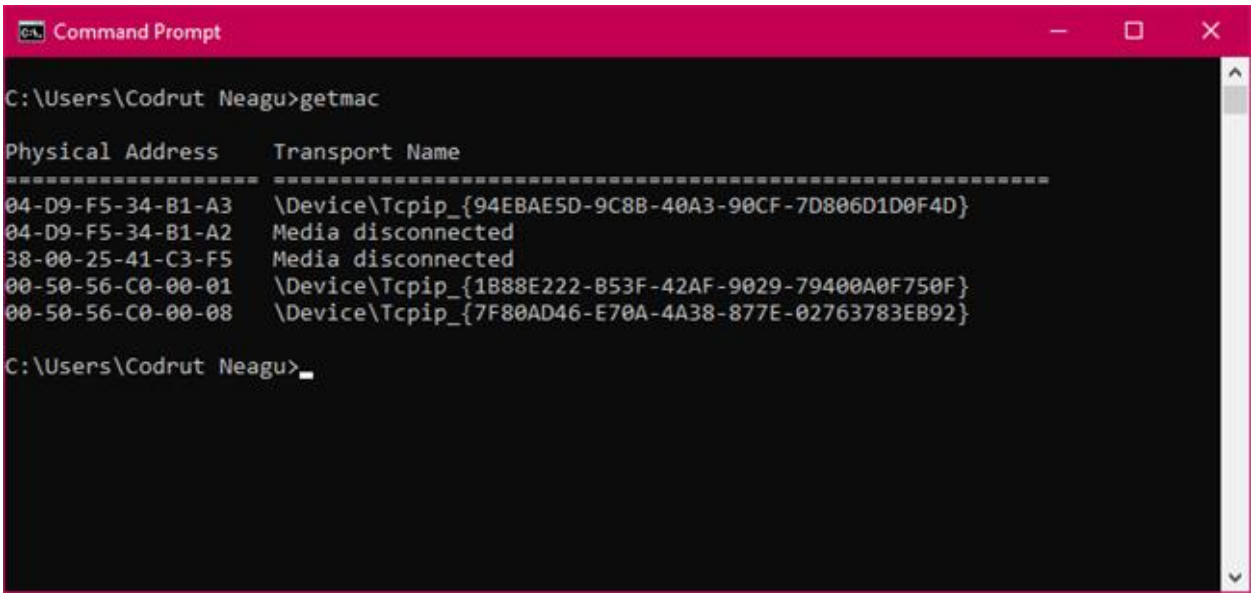
8.Route Command

IP networks use routing tables to direct packets from one subnet to another. The Windows Route utility allows you to view the device's routing tables. The Route command is that it not only shows you the routing table, it lets you make changes. Commands such as Route Add, Route Delete, and Route Change allow you to make routing table modifications on an as needed basis.



9. GETMAC Command

Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer. One of the fastest and easiest ways to obtain the MAC addresses of your network adapters is to use the getmac command. In Command Prompt, type getmac and press Enter, as seen in the image below.



10.SYSTEMINFO Command: System Information

If you need to know what brand of network card you have, processor details, or the exact version of your Windows OS, the SYSTEMINFO command can help.This command polls your system

and pulls the most important information about your system. It lists the information in a clean format that's easy to read.

Module-2

Cisco Packet Tracer tool

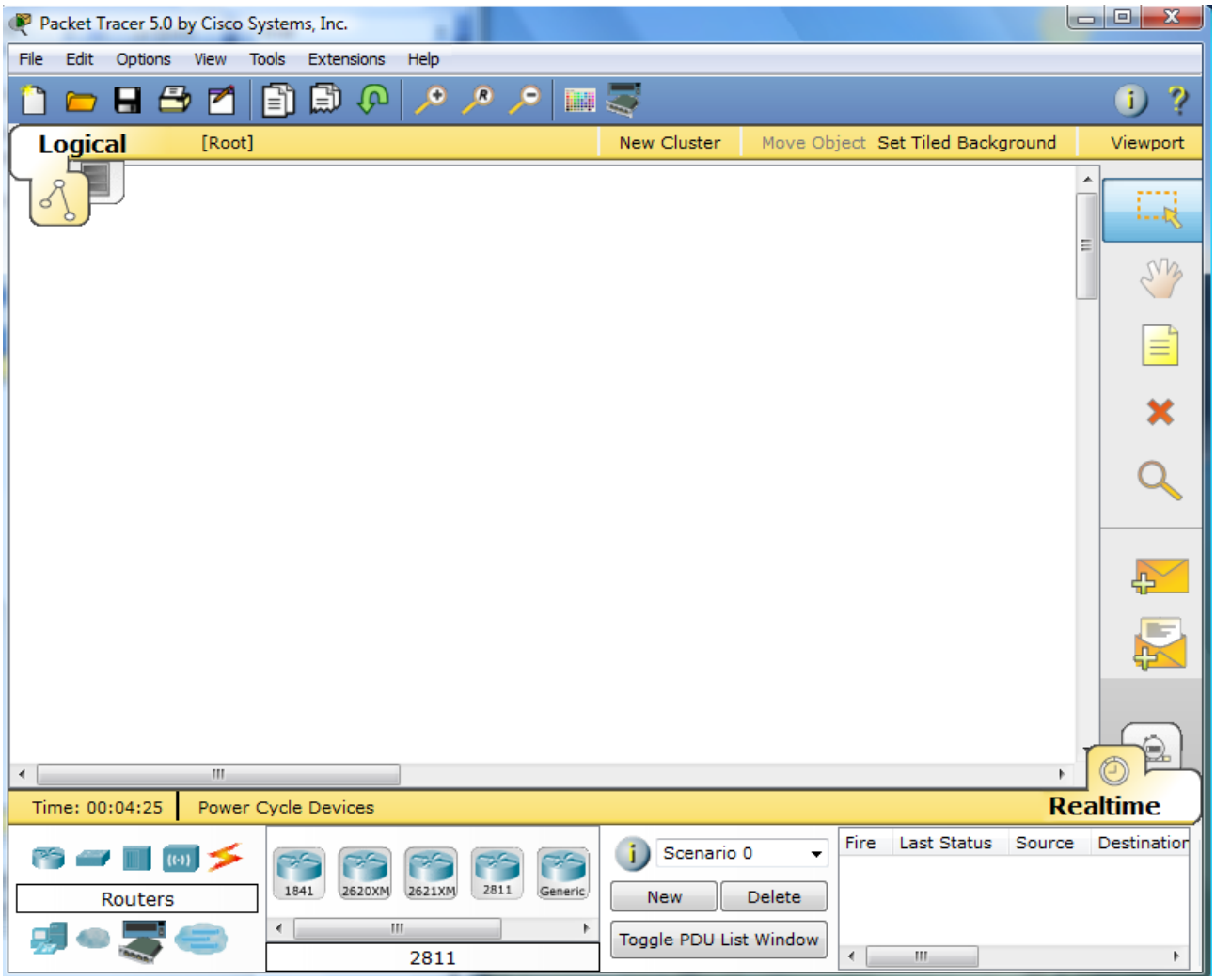
Packet Tracer – Creating a New Topology

What is Packet Tracer? Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

Purpose: The purpose of this lab is to become familiar with building topologies in Packet Tracer.

Version: This lab is based on Packet Tracer 5.0, 7.3.0

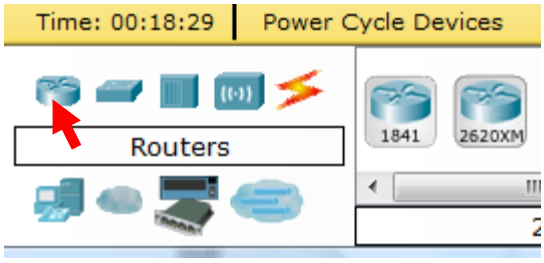
Step 1: Start Packet Tracer

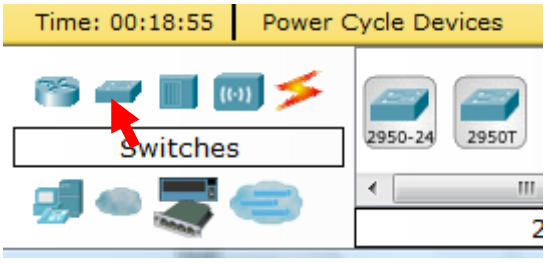


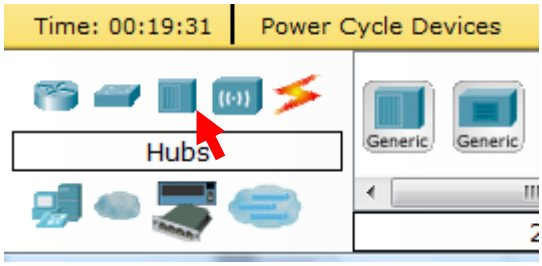
Step 2: Choosing Devices and Connections

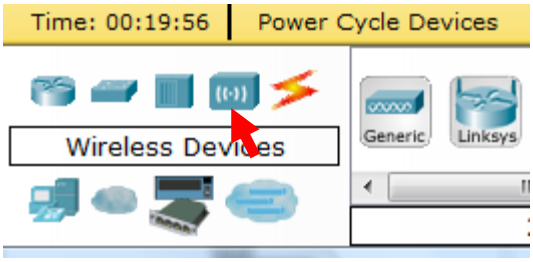
We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using **End Devices**, **Switches**, **Hubs**, and **Connections**.

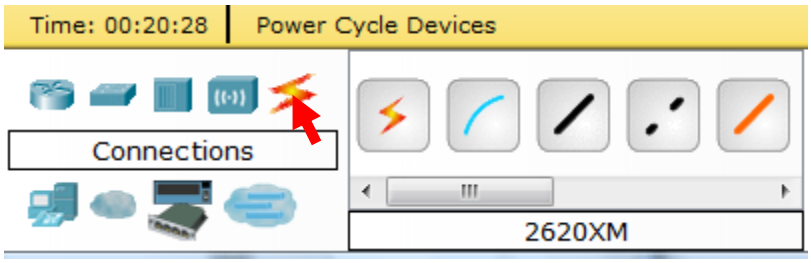
Single click on each group of devices and connections to display the various choices. The devices you see may differ slightly.

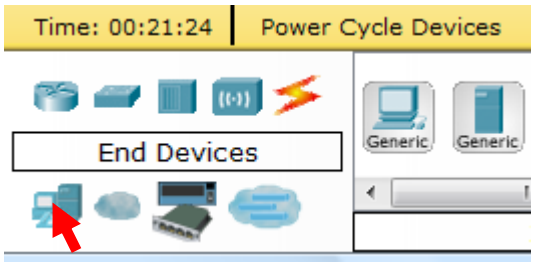

Time: 00:18:29
Power Cycle Devices
Routers
1841
2620XM

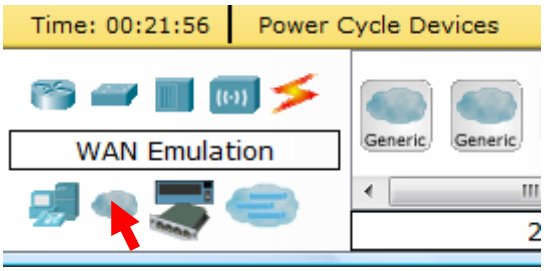

Time: 00:18:55
Power Cycle Devices
Switches
2950-24
2950T

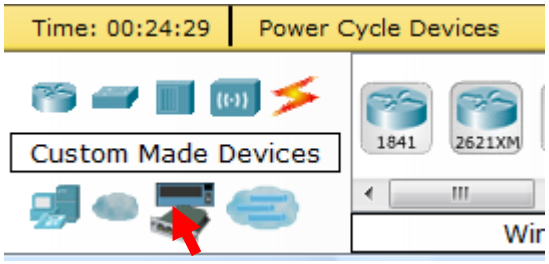

Time: 00:19:31
Power Cycle Devices
Hubs
Generic
Generic

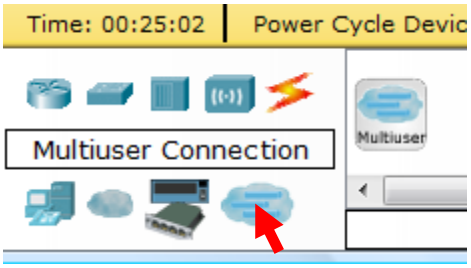

Time: 00:19:56
Power Cycle Devices
Wireless Devices
Generic
Linksys


Time: 00:20:28
Power Cycle Devices
Connections
2620XM


Time: 00:21:24
Power Cycle Devices
End Devices
Generic
Generic

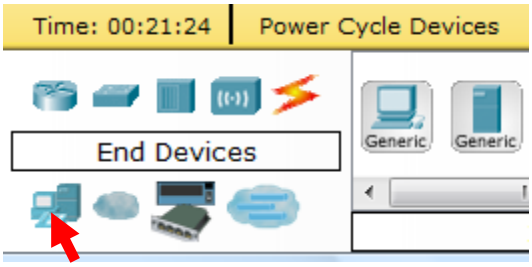

Time: 00:21:56
Power Cycle Devices
WAN Emulation
Generic
Generic


Time: 00:24:29
Power Cycle Devices
Custom Made Devices
1841
2621XM

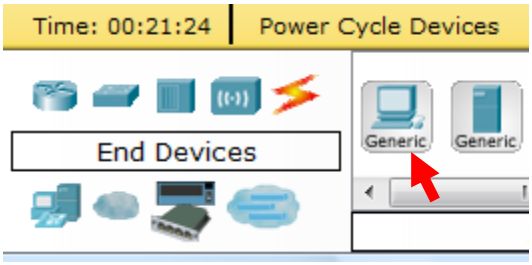

Time: 00:25:02
Power Cycle Devic
Multiuser Connection
Multiuser

Step 3: Building the Topology – Adding Hosts

Single click on the **End Devices**.



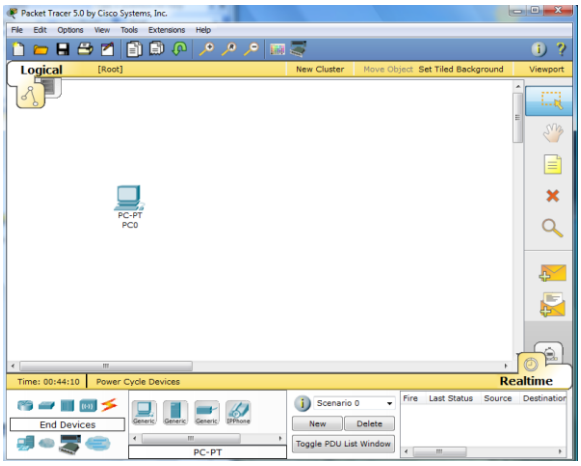
Single click on the **Generic** host.



Move the cursor into topology area. You will notice it turns into a plus "+" sign.

+

Single click in the topology area and it copies the device.

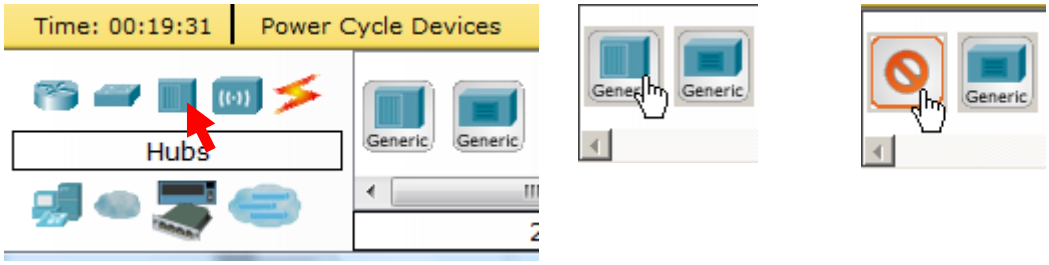


Add three more hosts.

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

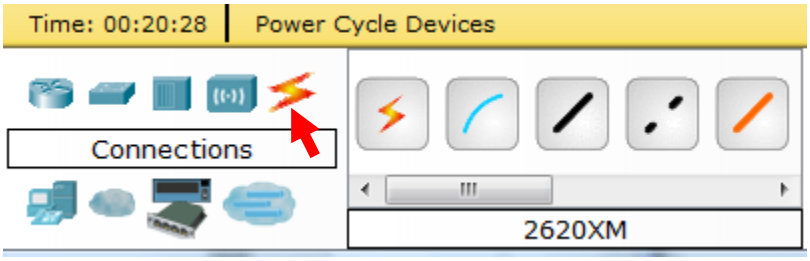
Adding a Hub

Select a hub, by clicking once on **Hubs** and once on a **Generic** hub.

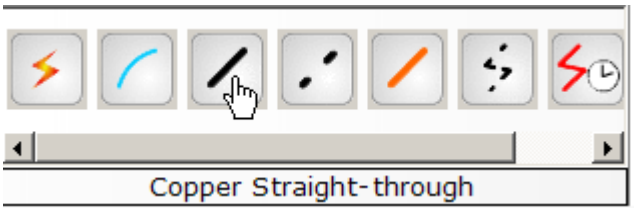


Add the hub by moving the plus sign "+" below PC0 and PC1 and click once.

Connect PC0 to Hub0 by first choosing **Connections.**



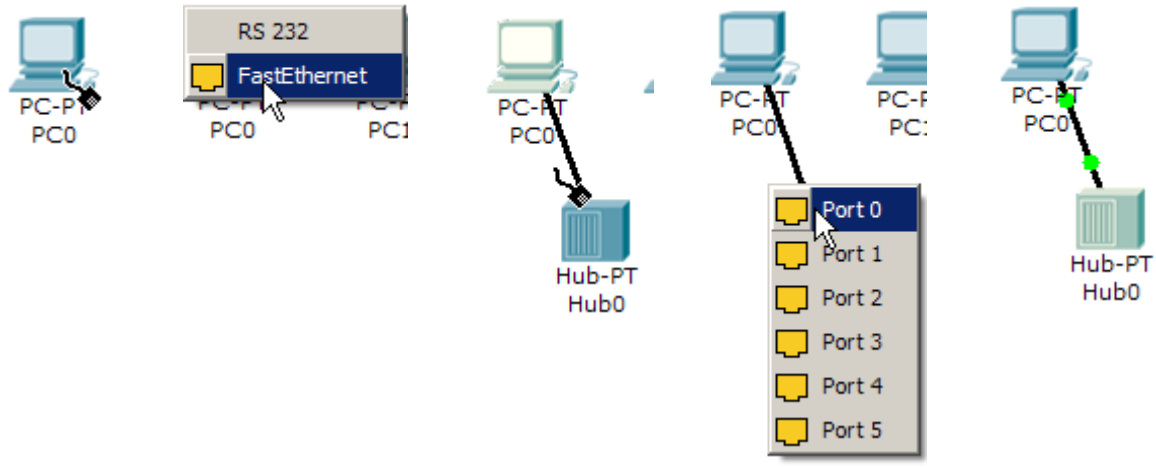
Click once on the **Copper Straight-through** cable.



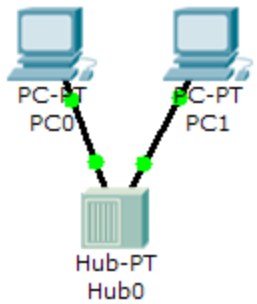
Perform the following steps to connect **PC0** to **Hub0**:

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.

1 **2** **3** **4** **5**

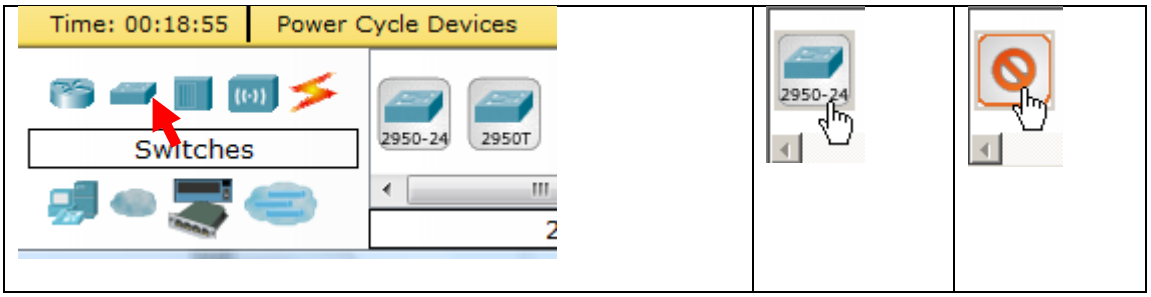


Repeat the steps above for **PC1** connecting it to **Port 1** on **Hub0**. (The actual hub port you choose does not matter.)



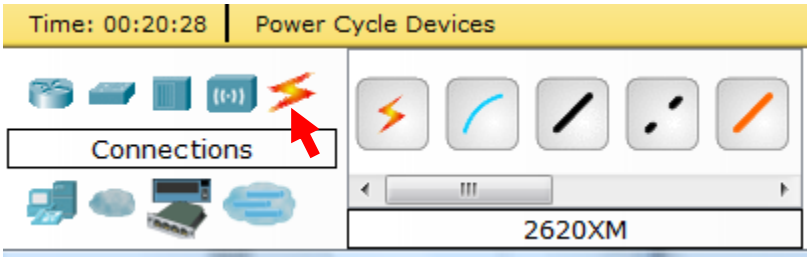
Adding a Switch

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

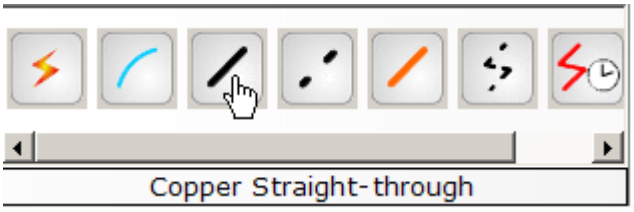


Add the switch by moving the plus sign "+" below PC2 and PC3 and click once.

Connect PC2 to Hub0 by first choosing **Connections.**



Click once on the **Copper Straight-through** cable.

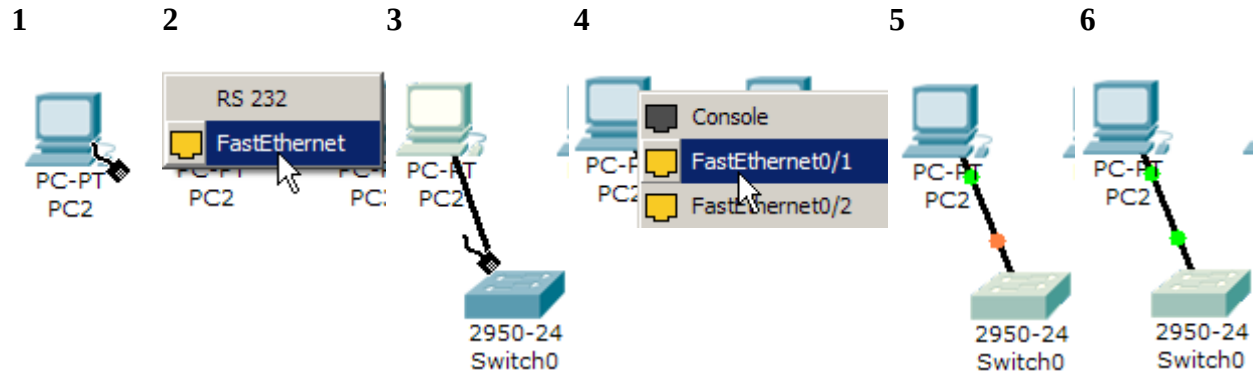


Perform the following steps to connect **PC2** to **Switch0**:

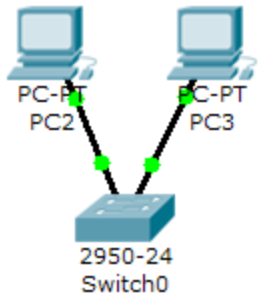
1. Click once on **PC2**
2. Choose **FastEthernet**
3. Drag the cursor to **Switch0**
4. Click once on **Switch0** and choose **FastEthernet0/1**

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.

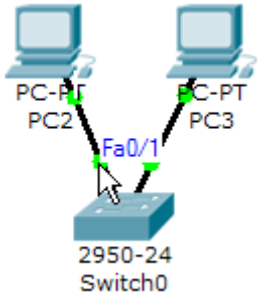
Note: Spanning Tree Protocol (STP) is discussed later.



Repeat the steps above for **PC3** connecting it to **Port 3** on **Switch0** on port **FastEtherent0/2**. (The actual switch port you choose does not matter.)



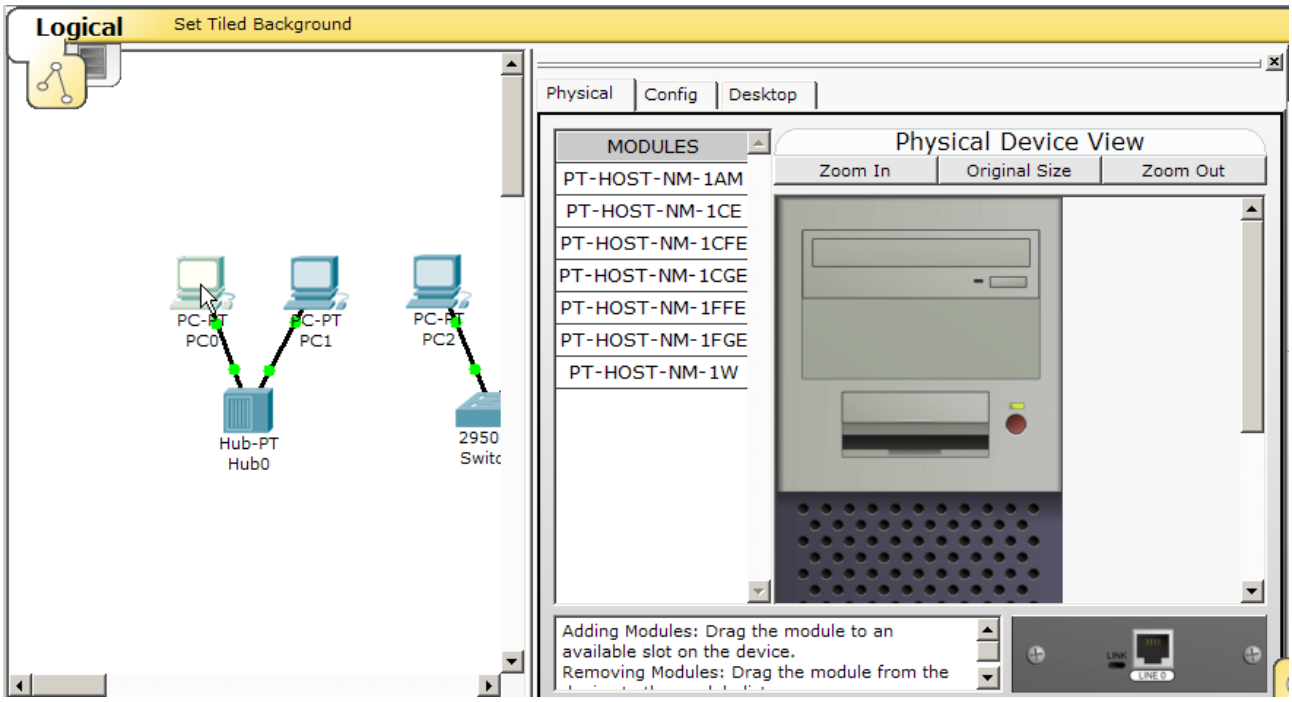
Move the cursor over the link light to view the port number. **Fa** means FastEthernet, 100 Mbps Ethernet.



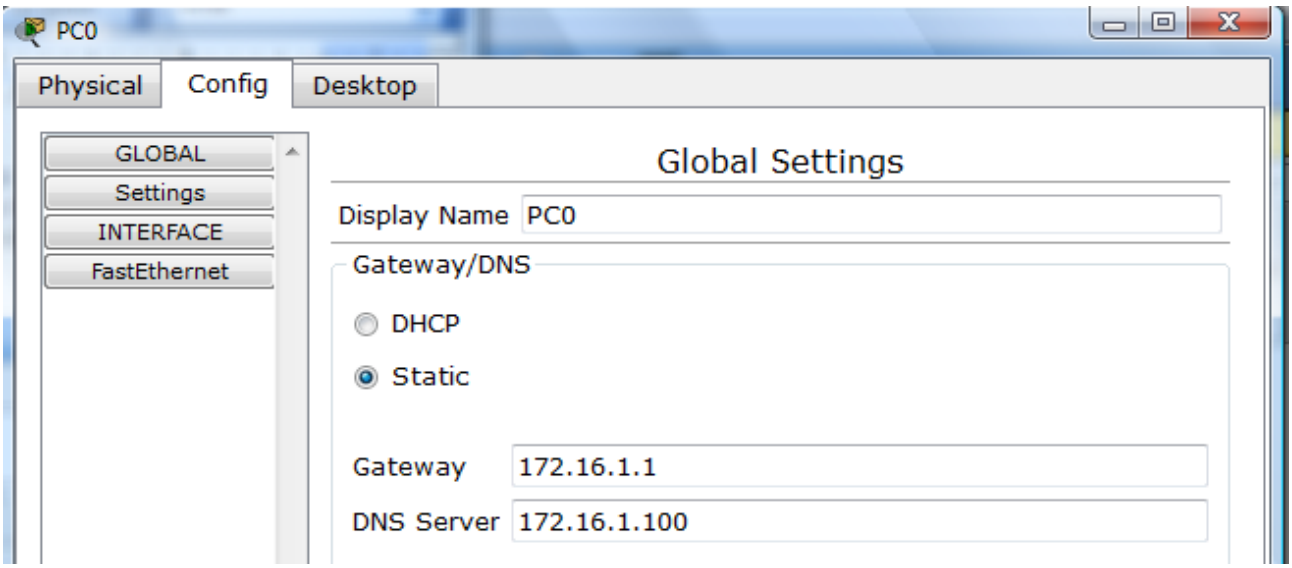
Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

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

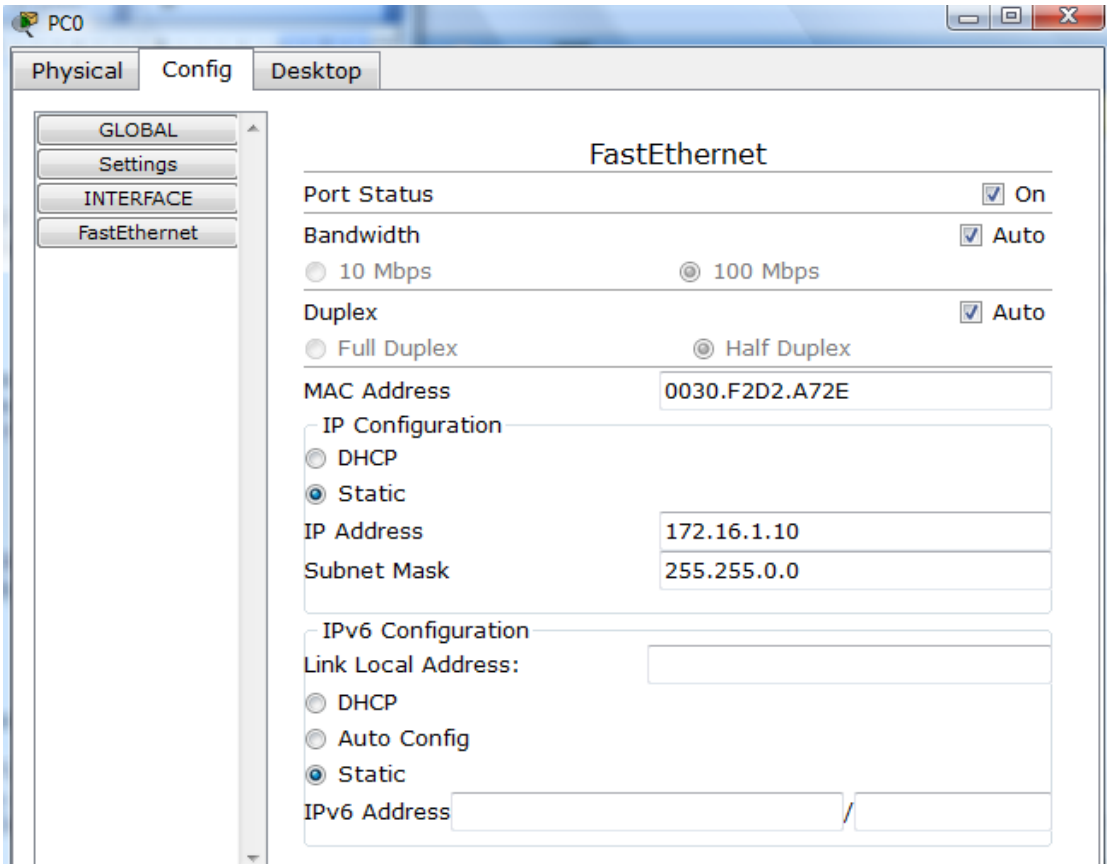
Click once on PC0.



Choose the **Config** tab and click on **Settings**. 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 and the **DNS Server** IP Address. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the Gateway IP Address 172.16.1.1 and DNS Server IP Address 172.16.1.100, although it will not be used in this lab.



Click on **Interface** and then **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

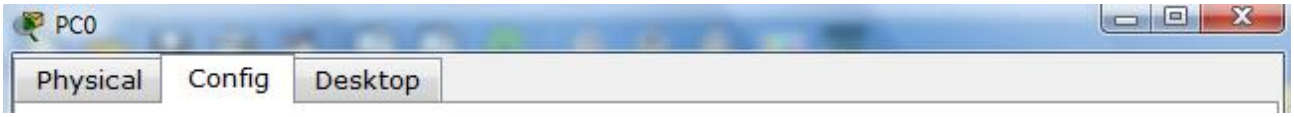
Hub: If the host is connected to a hub, then the Ethernet NIC on the host will choose Half Duplex.

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.

To close this dialog box, click the "**X**" in the upper right.

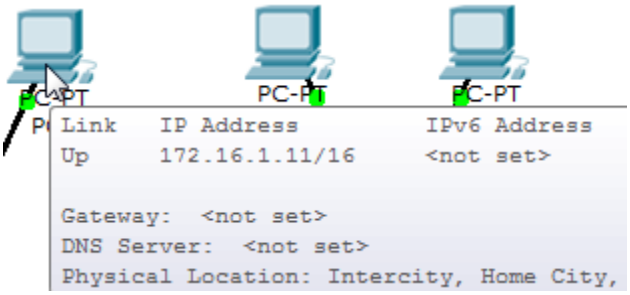


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

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.

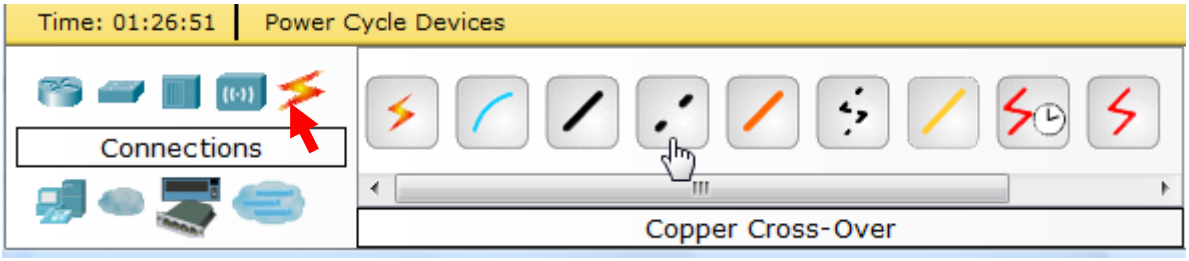


Deleting a Device or Link

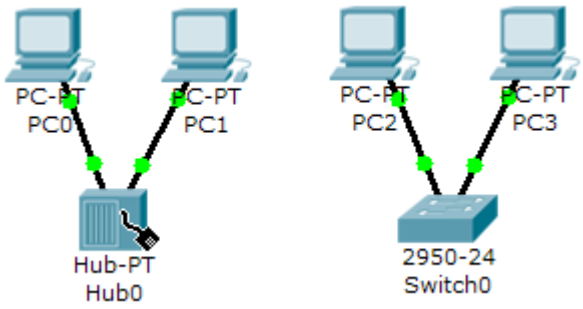
To delete a device or link, choose the **Delete** tool and click on the item you wish to delete.

Step 6: Connecting Hub0 to Switch0

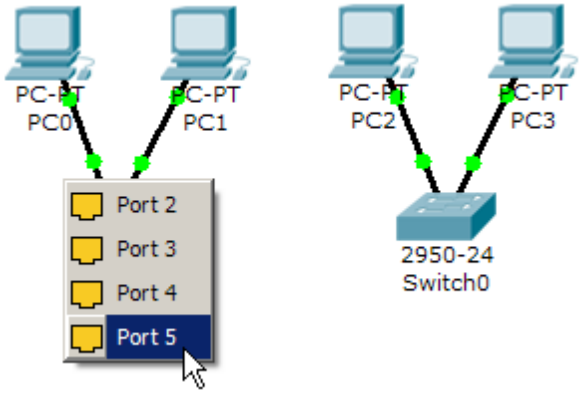
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the **Cross-over** Cable from the **Connections** options.



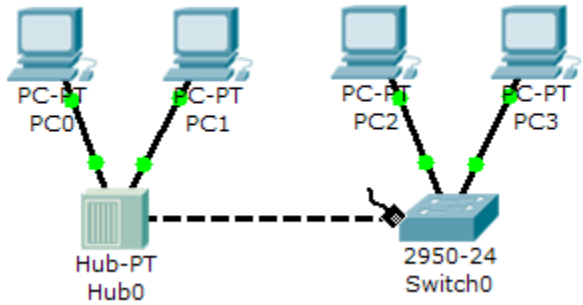
Move the Connections cursor over **Hub0** and click once.



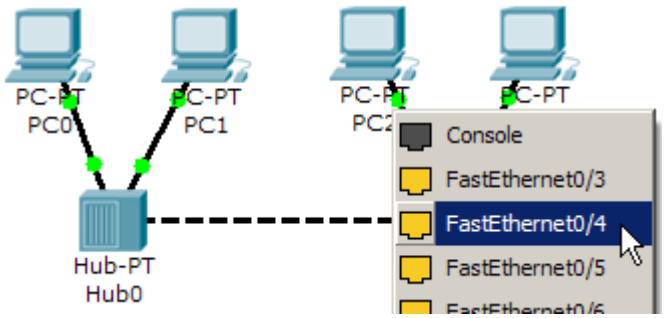
Select **Port 5** (actual port does not matter).



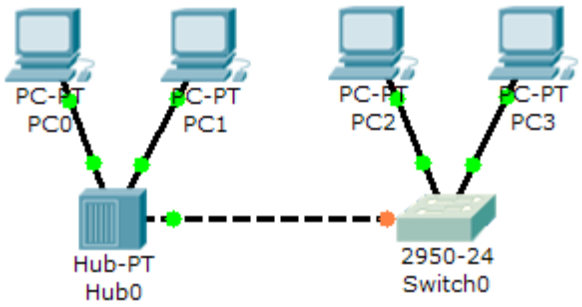
Move the Connections cursor to **Switch0**.

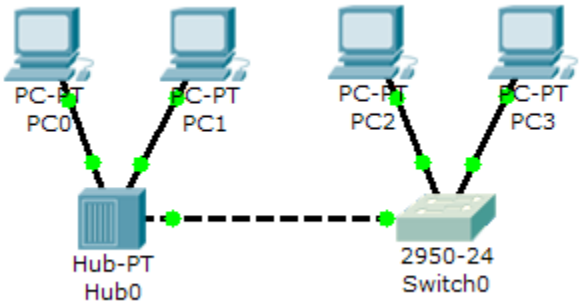


Click once on **Switch0** and choose **FastEthernet0/4** (actual port does not matter).



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.



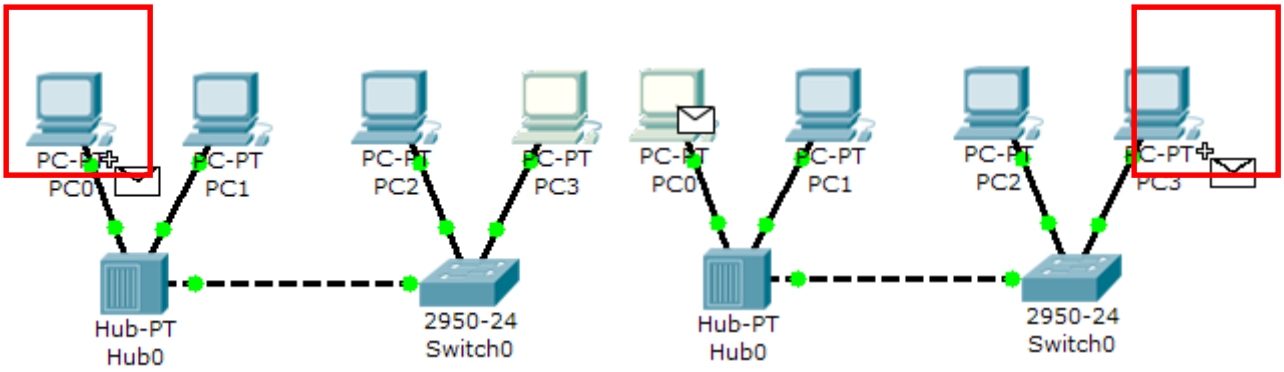


Step 7: Verifying Connectivity in Realtime Mode

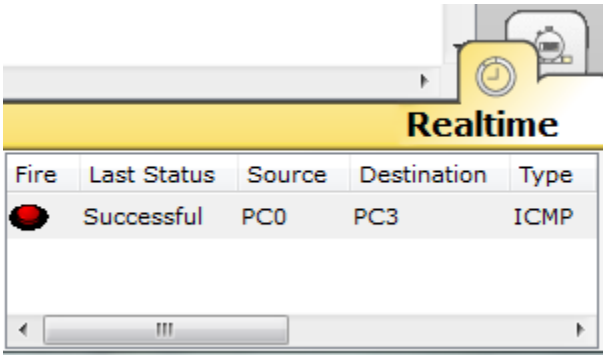
Be sure you are in **Realtime** mode.

Select the **Add Simple PDU** tool used to ping devices..

Click once on PC0, then once on PC3.



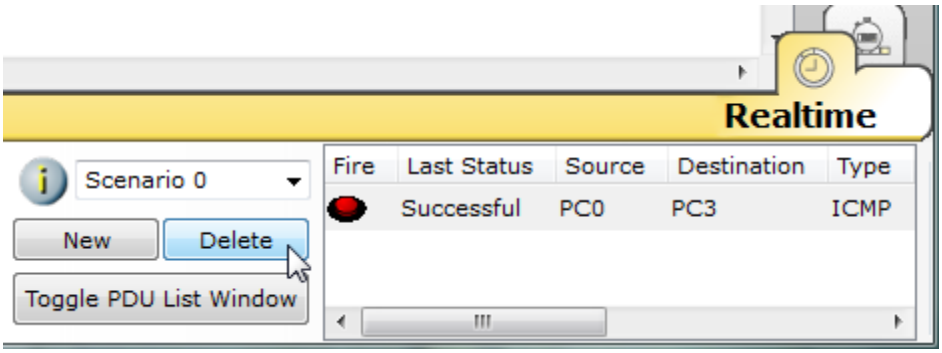
The PDU **Last Status** should show as **Successful**.



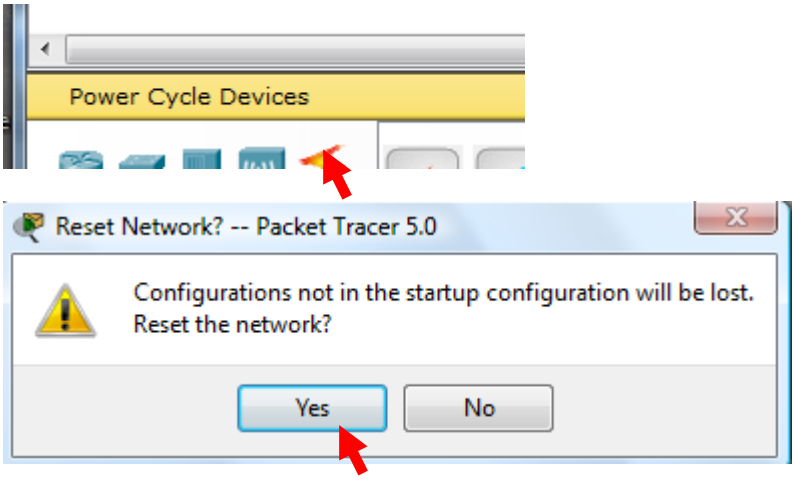
Resetting the Network

At this point we will want to reset the network, Whenever you want to reset the network and begin the simulation again, perform the following tasks:

Click **Delete** in the PDU area.

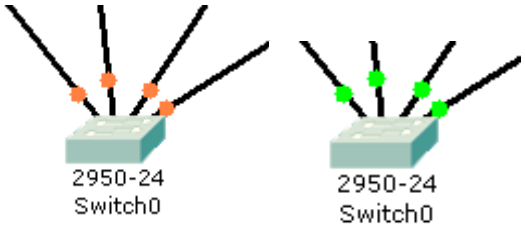


Now, Power Cycle Devices and confirm the action.



Waiting for Spanning Tree Protocol (STP)

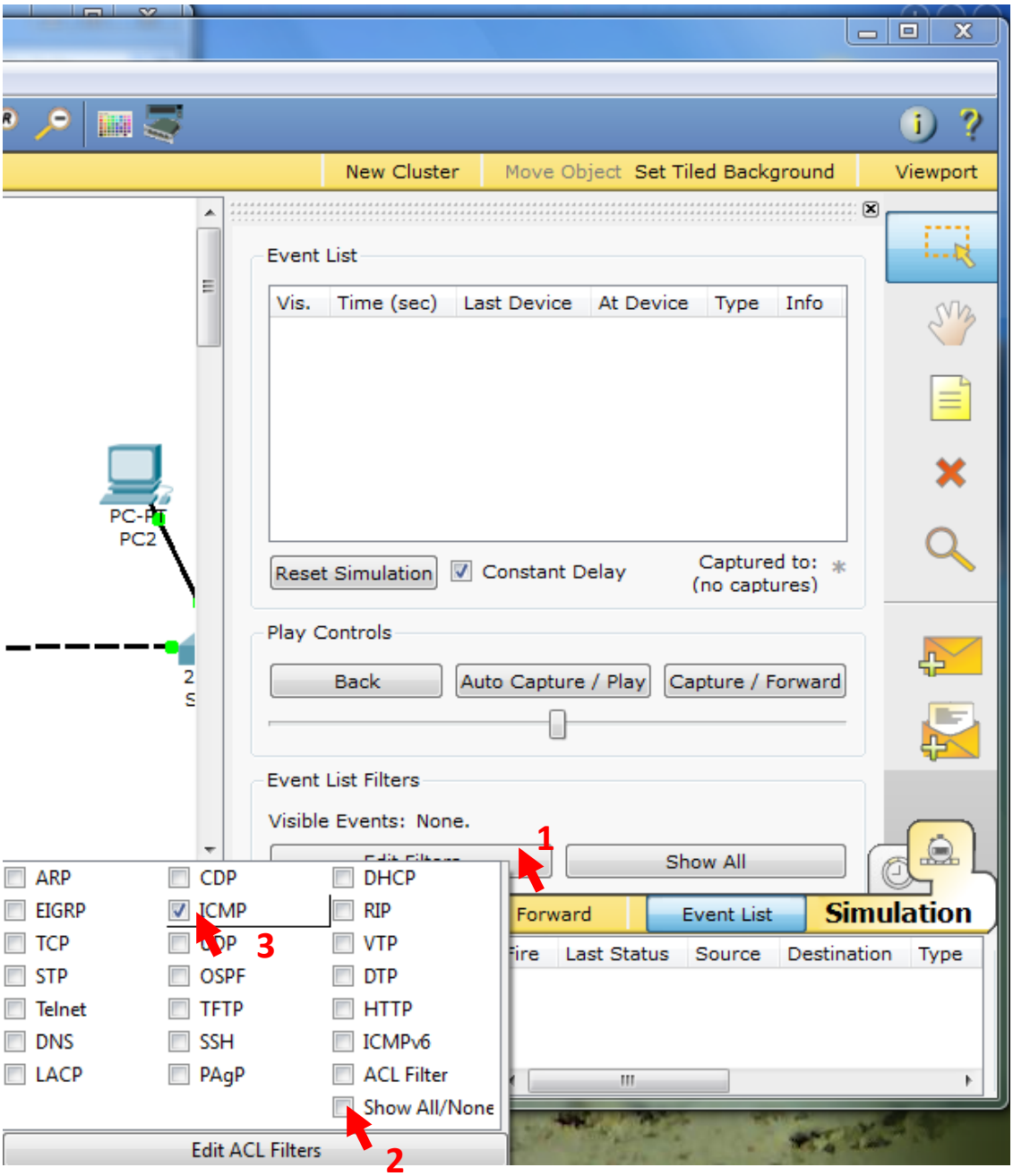
Note: Because Packet Tracer also simulates the Spanning Tree Protocol (later), at times the switch may show amber lights on its interfaces. You will need to wait for the lights to turn green on the switches before they will forward any Ethernet frames.



Step 8: Verifying Connectivity in Simulation Mode

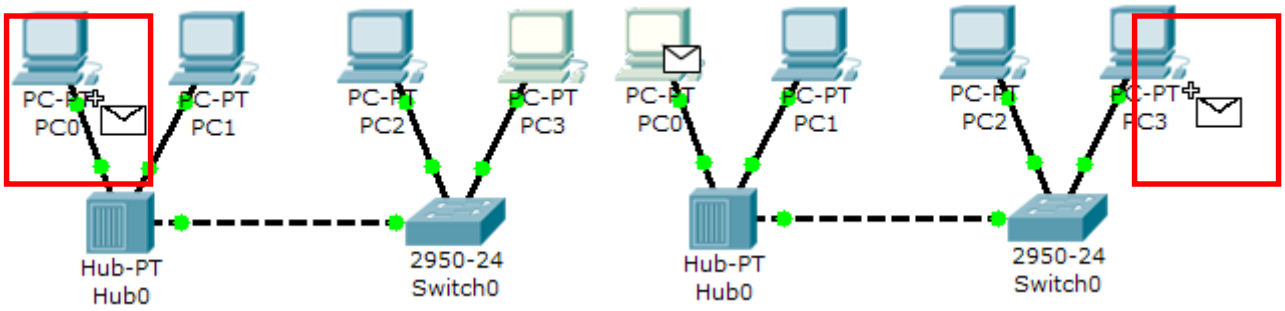
Be sure you are in **Simulation** mode.

Deselect all filters (All/None) and select only **ICMP**.

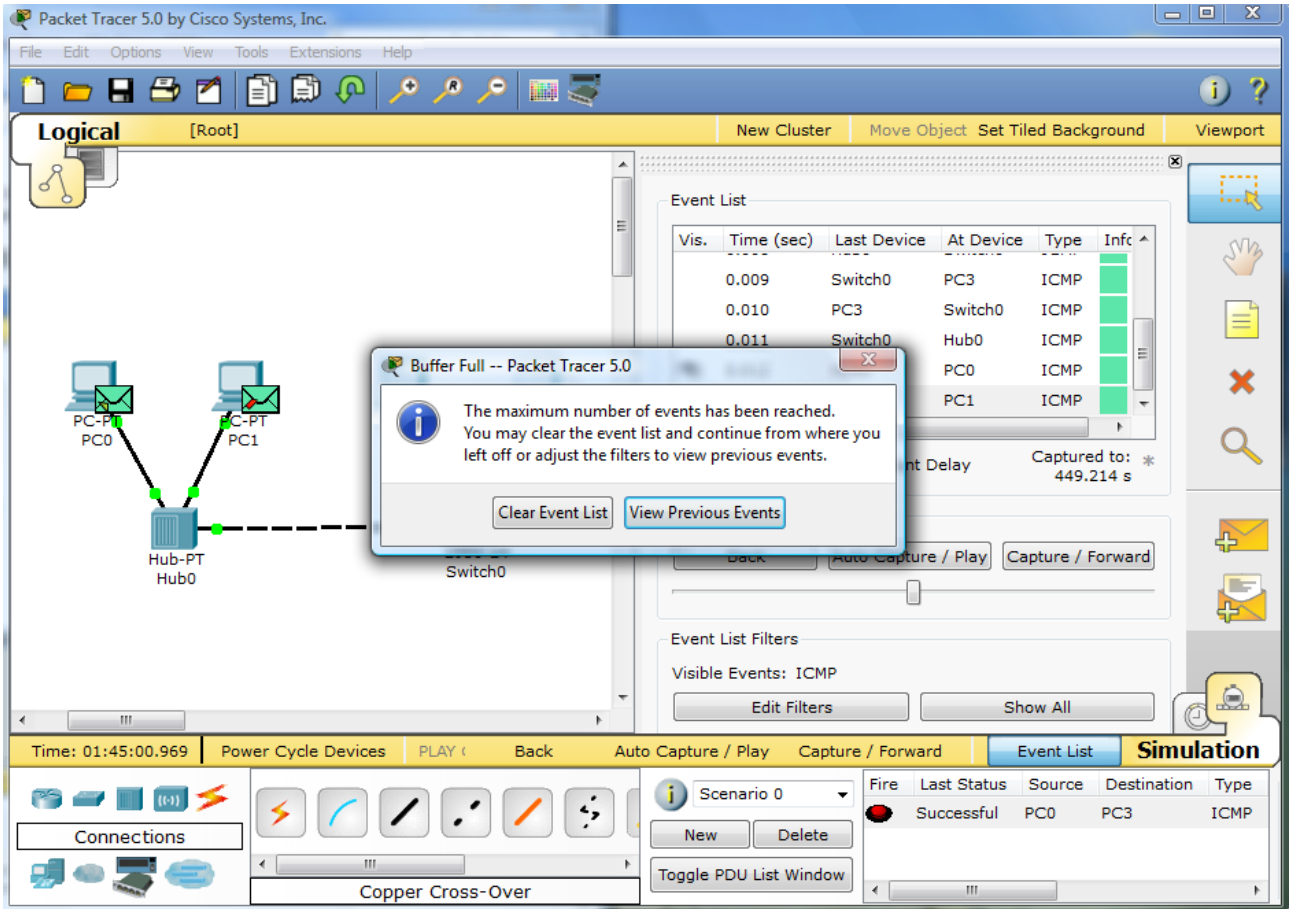


Select the **Add Simple PDU** tool used to ping devices..

Click once on PC0, then once on PC3.

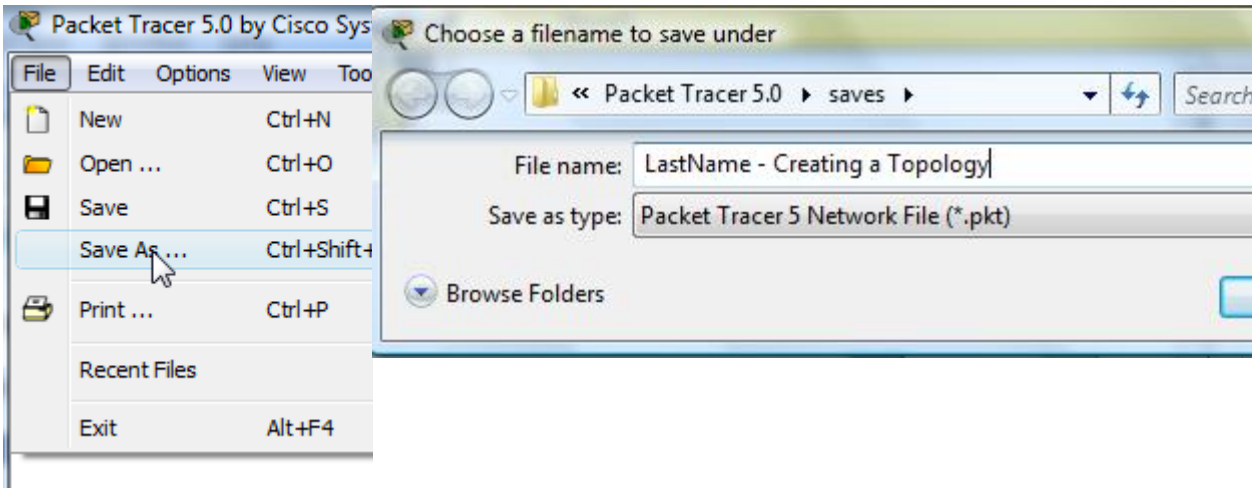


Continue clicking **Capture/Forward** button until the ICMP ping is completed. You should see the ICMP messages move between the hosts, hub and switch. The PDU **Last Status** should show as **Successful**. Click on **Clear Event List** if you do not want to look at the events or click **Preview Previous Events** if you do. For this exercise it does not matter.

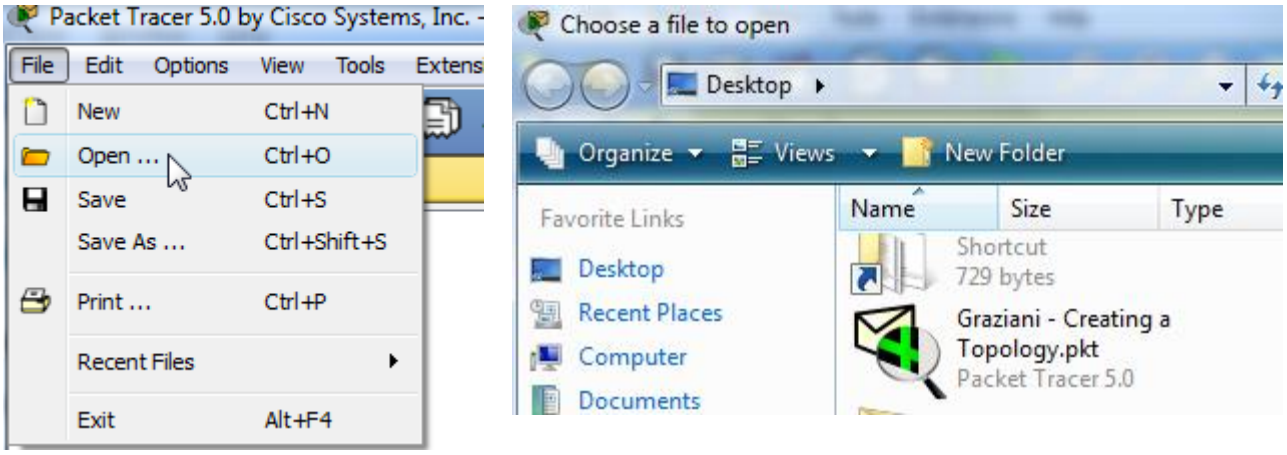


Step 9: Saving the Topology

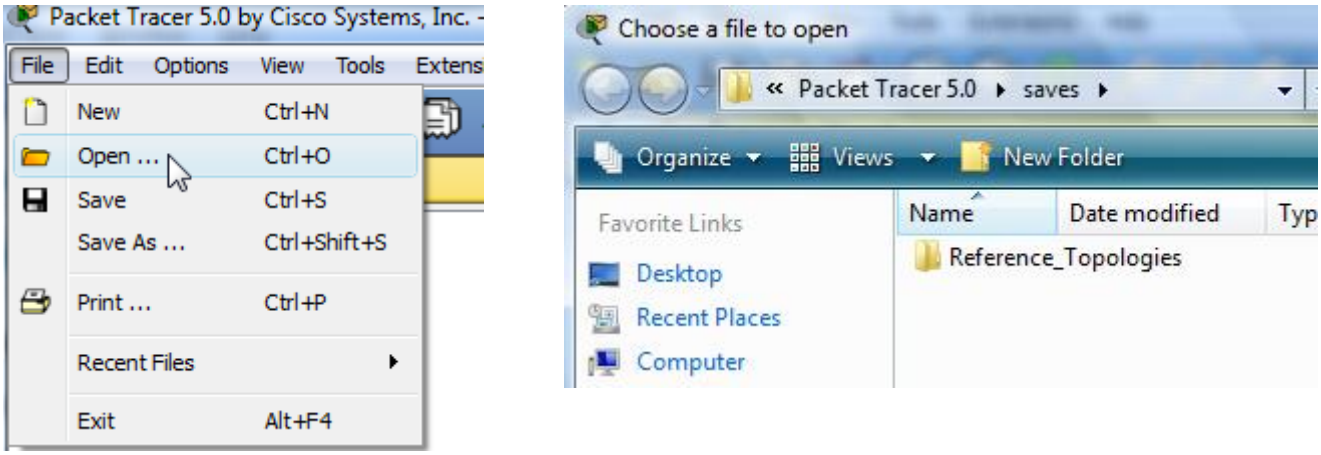
Perform the following steps to save the topology (uses .pkt file extension).

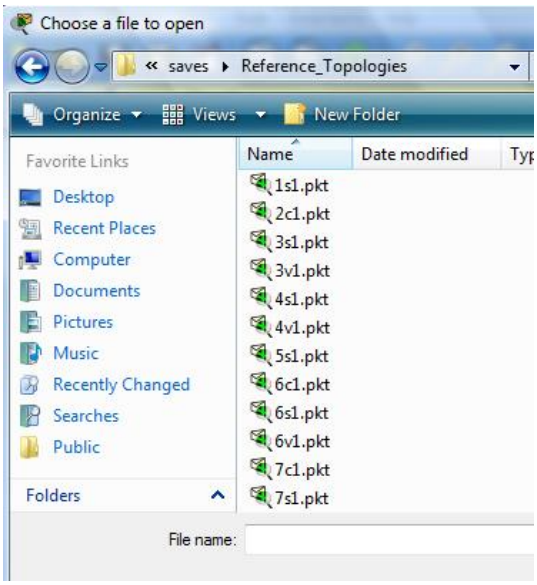


Opening Existing Topologies



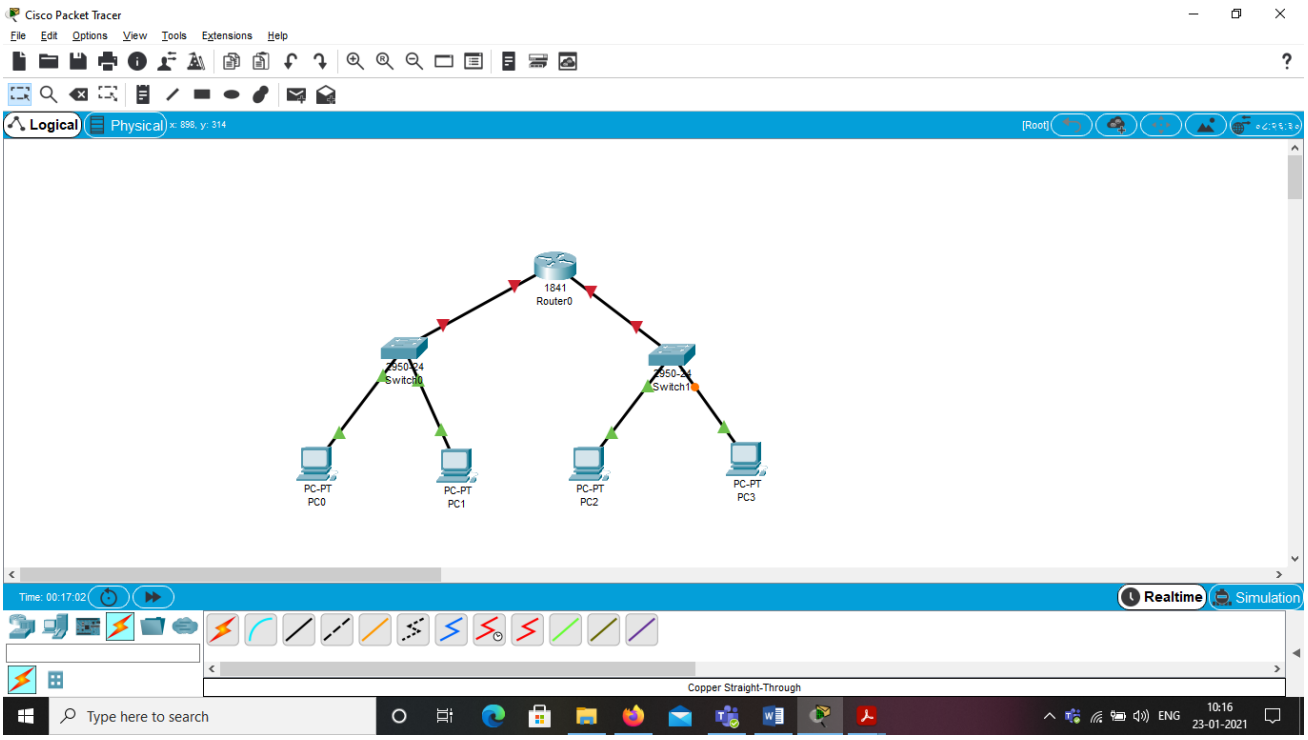
Opening Existing PT Topologies



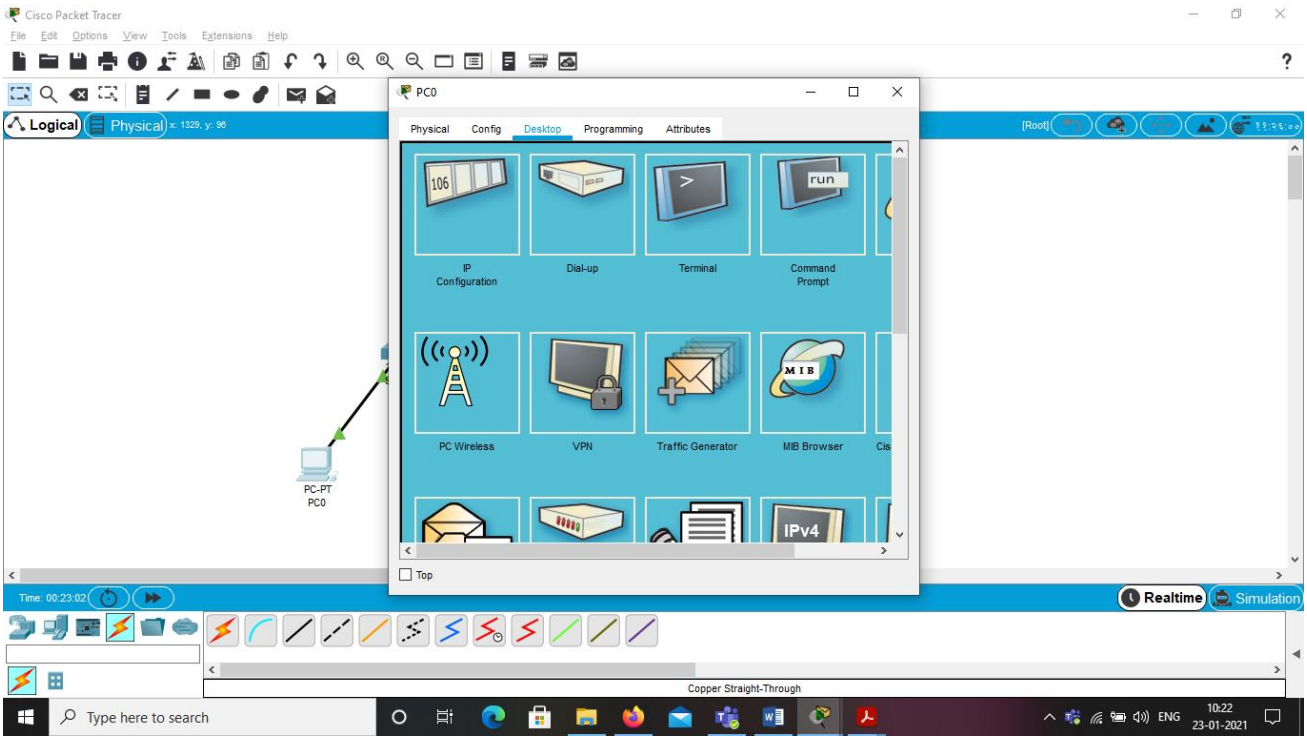

Choose a file to open
« saves ▸ Reference_Topologies
Organize
Views
New Folder
Favorite Links
Desktop
Recent Places
Computer
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
Name
Date modified
Typ
1s1.pkt
2c1.pkt
3s1.pkt
3v1.pkt
4s1.pkt
4v1.pkt
5s1.pkt
6c1.pkt
6s1.pkt
6v1.pkt
7c1.pkt
7s1.pkt
File name:

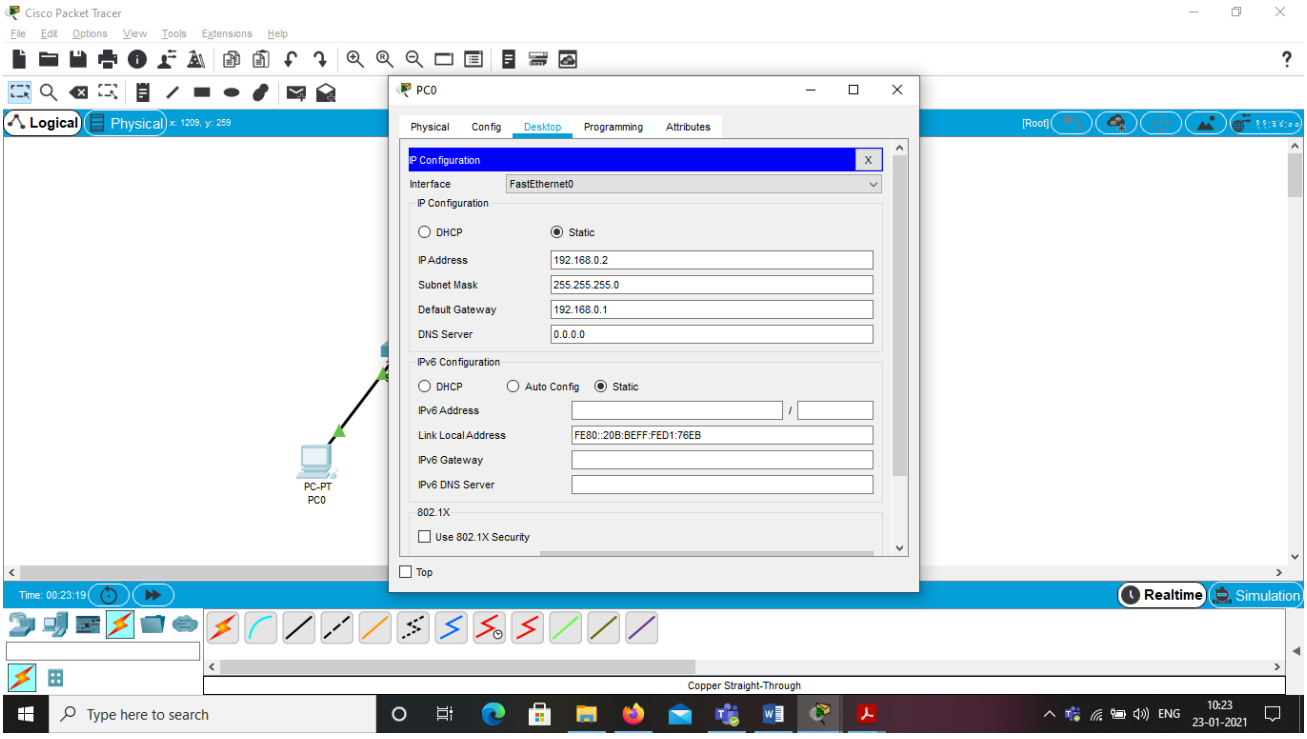
Exp 1: Configuration of Router using cisco packet tracer

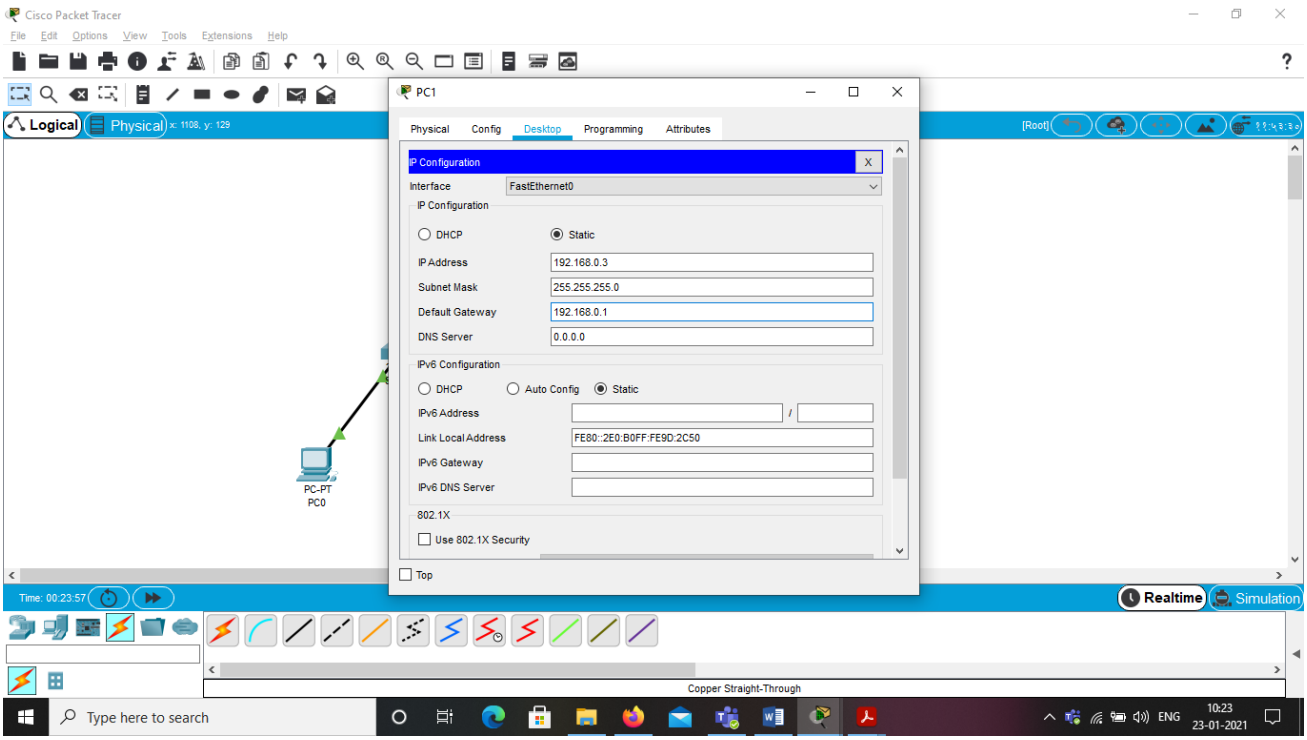
Step 1: Construct the topology



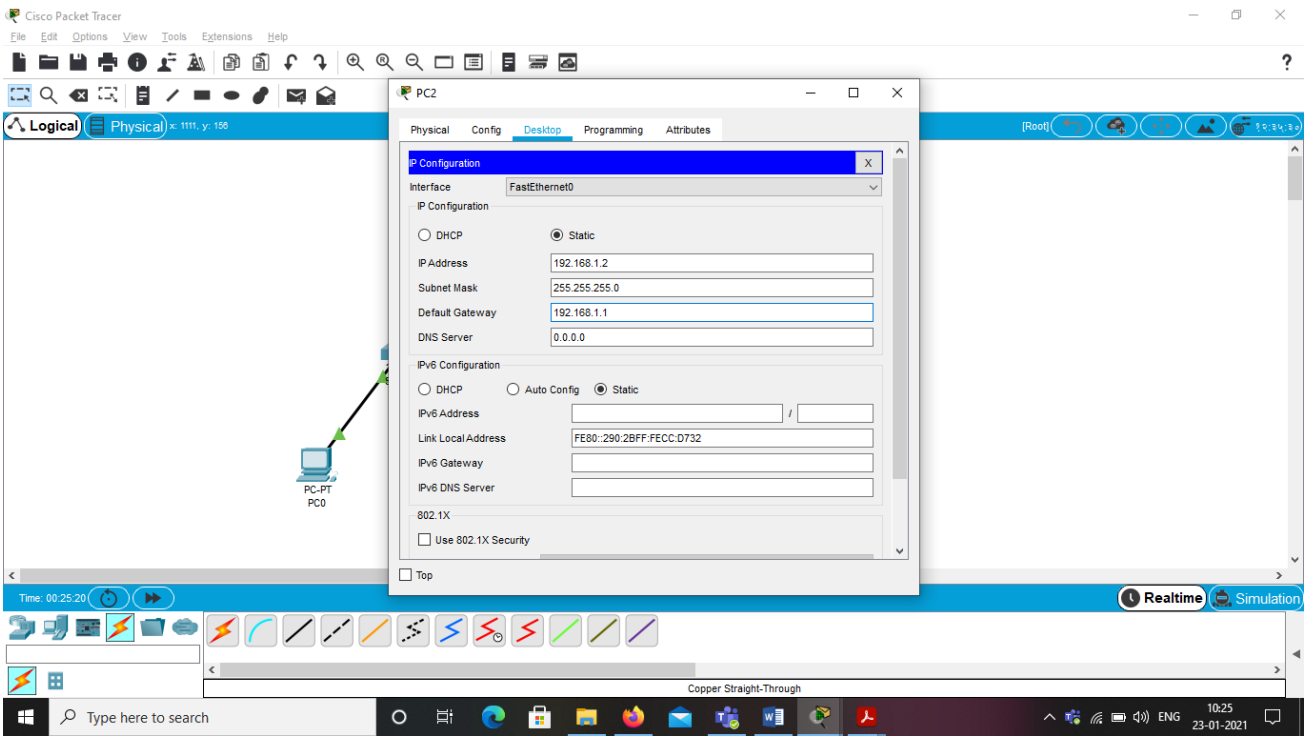
Step 2: Assign IP addresses to all PC's.

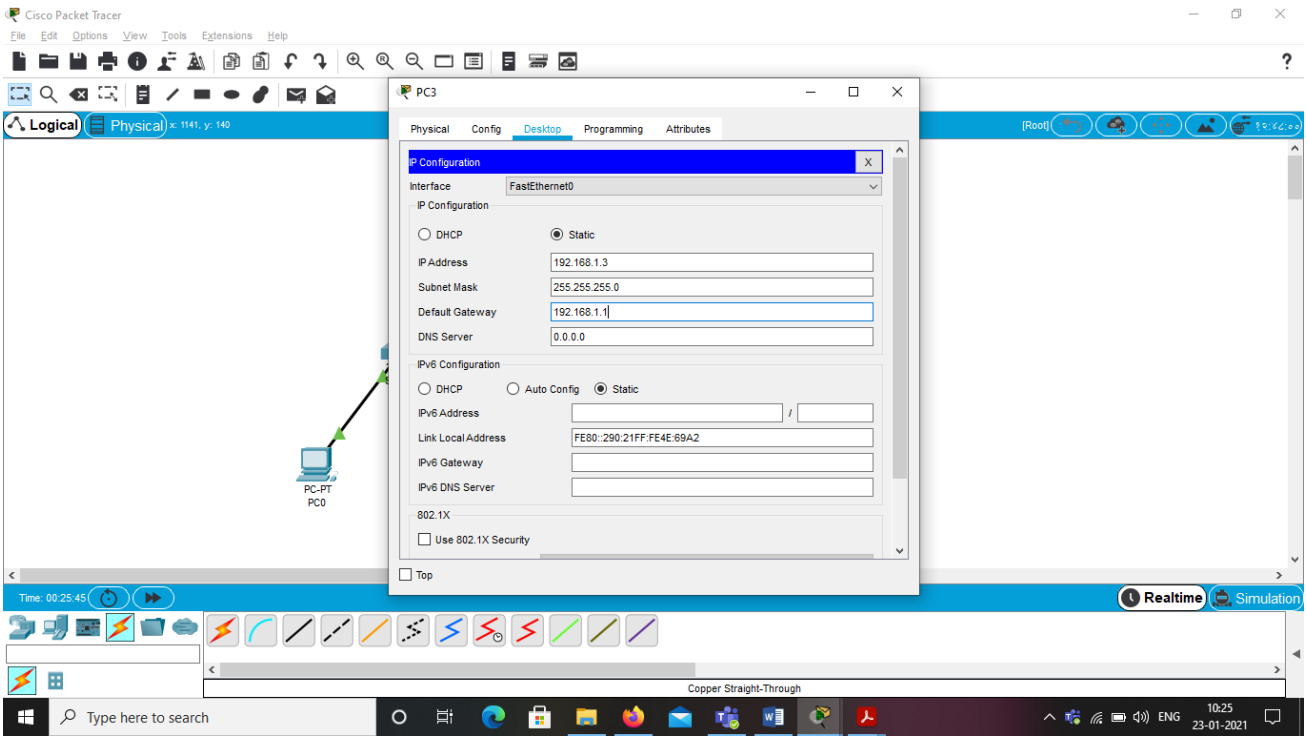

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 1329, y: 96
[Root]
PC0
Physical Config Desktop Programming Attributes
IP Configuration
Dial-up
Terminal
Command Prompt
PC Wireless
VPN
Traffic Generator
MIB Browser
IPv4
Top
PC-PT PC0
Time: 00:23:02
Realtime Simulation
Copper Straight-Through
Type here to search
ENG 10:22 23-01-2021


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 1209, y: 259
[Root]
PC0
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IP Address 192.168.0.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.0.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::20B:BEFF:FED1:76EB
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
PC-PT PC0
Time: 00:23:19
Realtime Simulation
Copper Straight-Through
Type here to search
ENG 10:23 23-01-2021



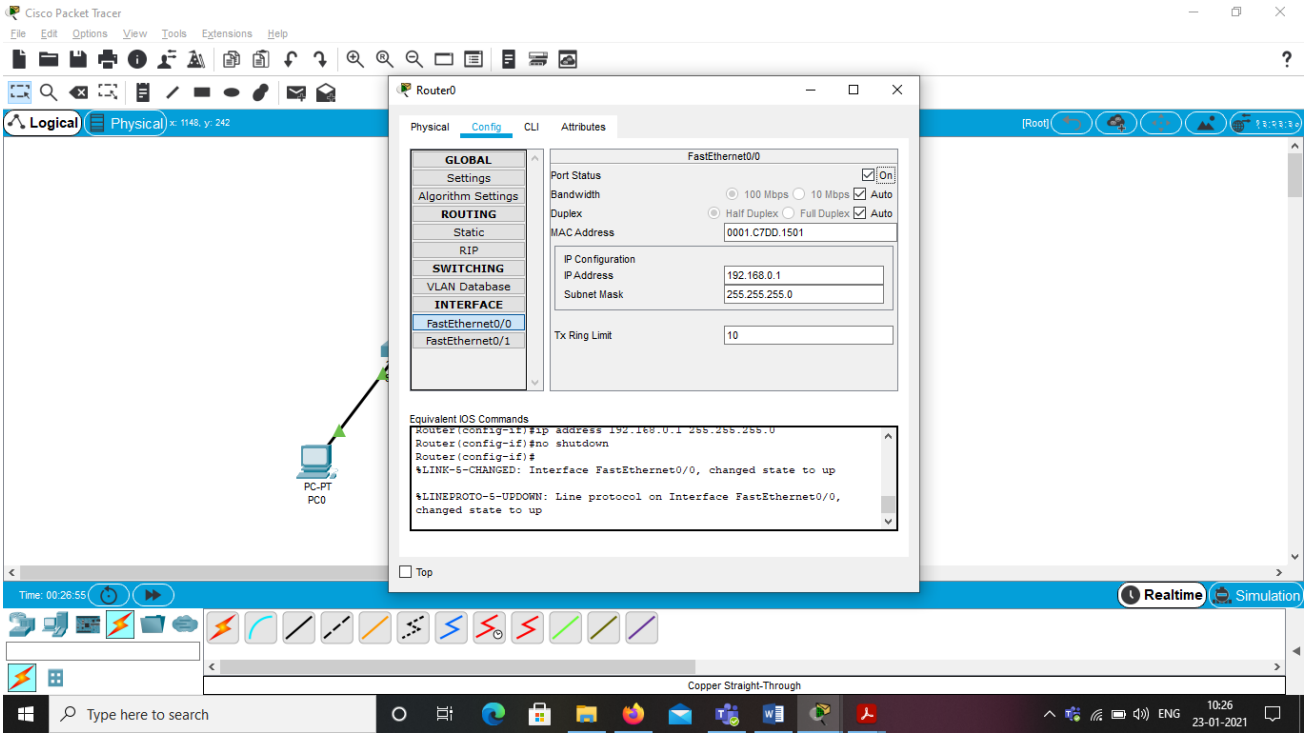
Use another network address for second network.



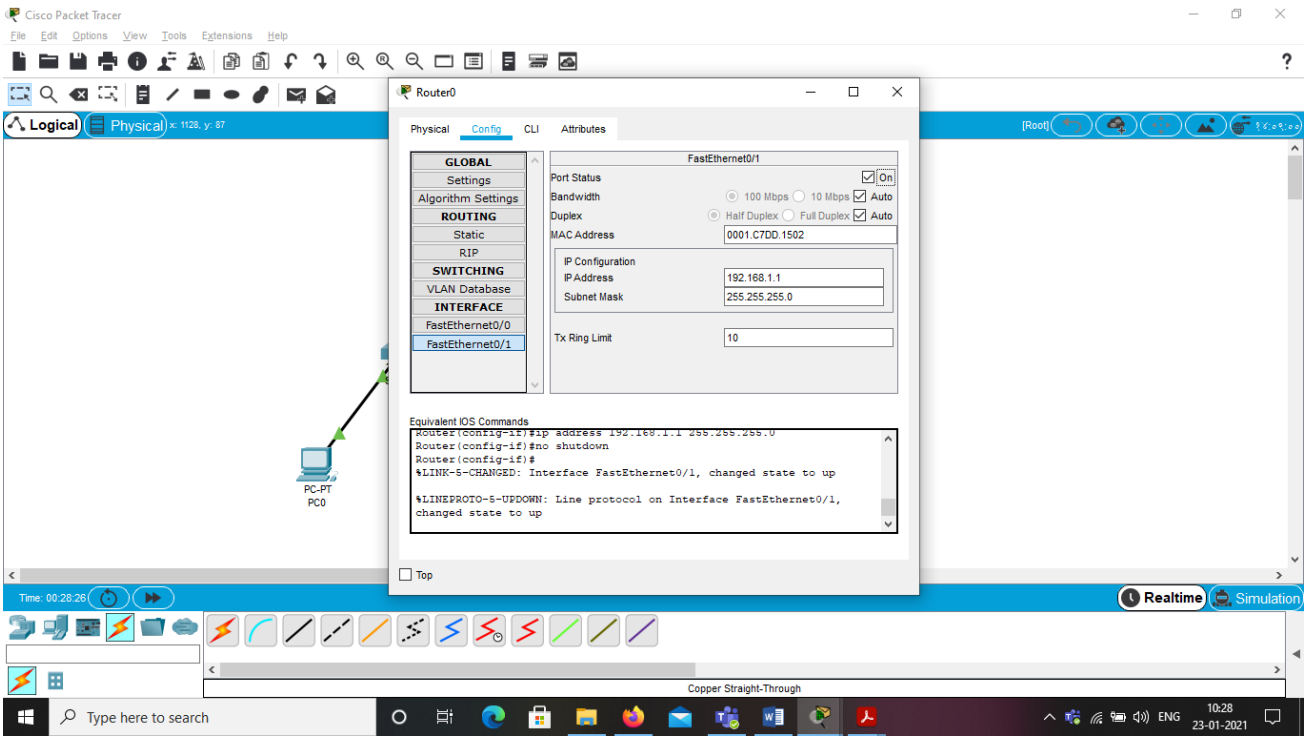


Step 3: Assign the IP address for router

Assign the gateway address of 1st network and don't forget to turn on the port status

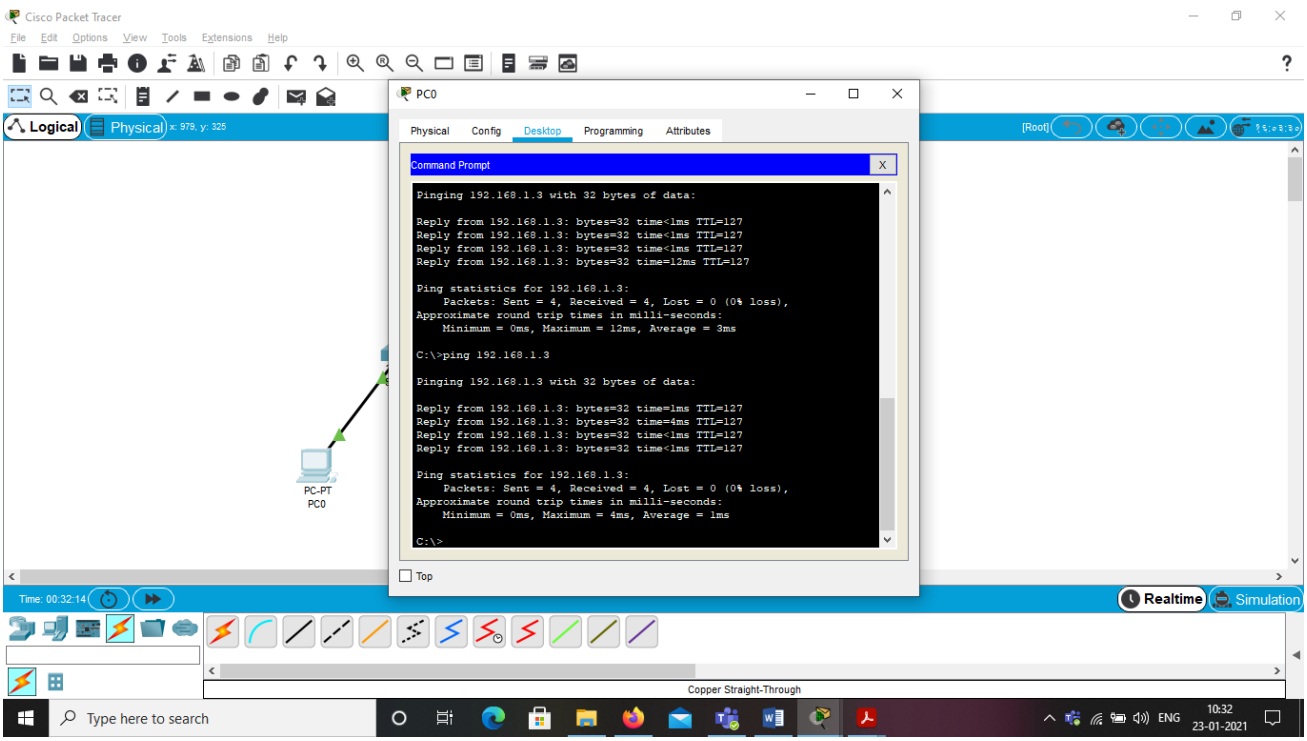


Assign the gateway address of 2nd network for FastEthernet0/1 interface

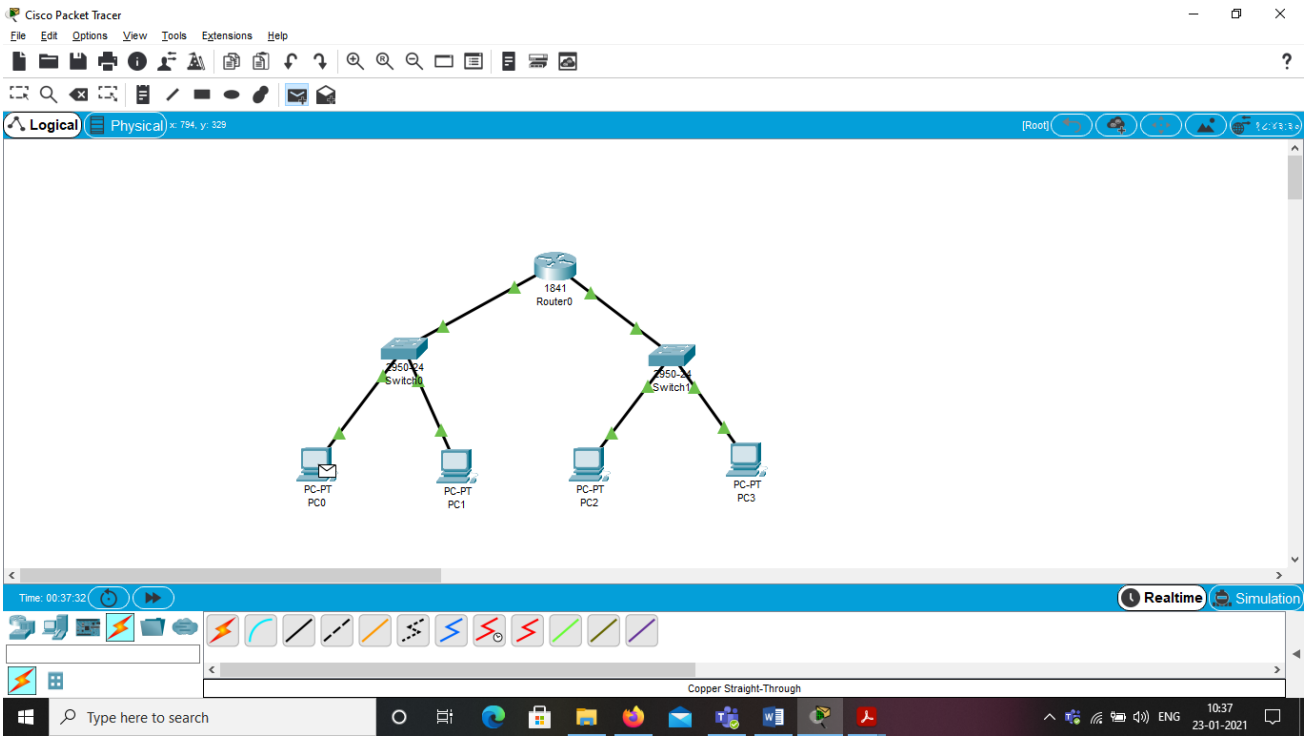


Step 3: Check the connectivity from one network to another network

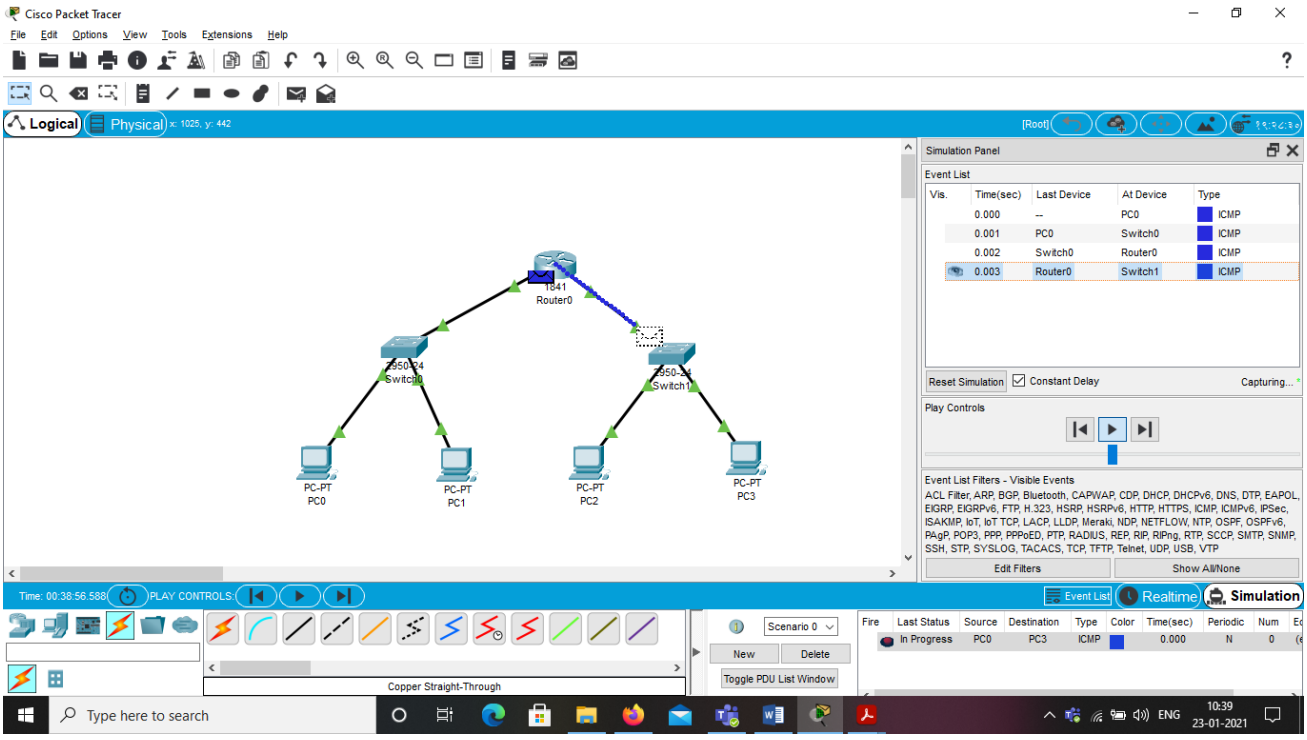
Select any PC from 1st network go to Desktop tab->Command Prompt->execute ping command for the 2nd network.



Step 4: Send Simple PDU.



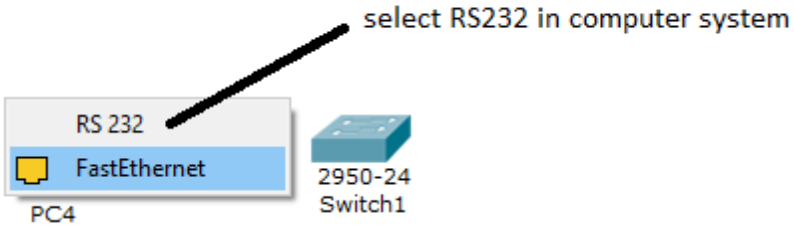
Step 5: Check in simulation mode



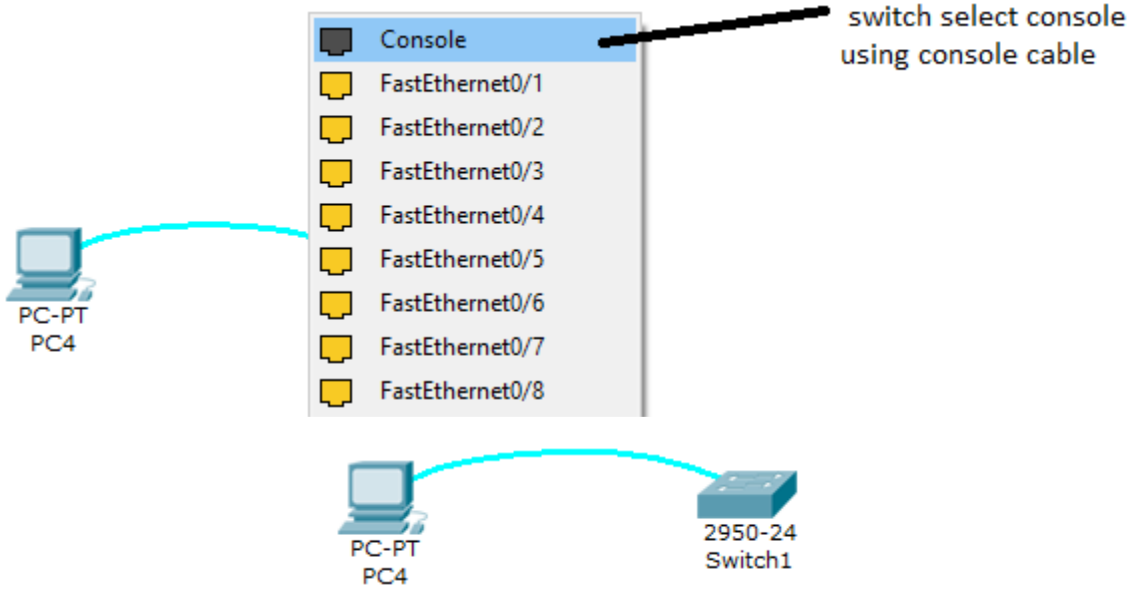
Exp 2: Configuration of Switch using cisco packet tracer

Step 1:

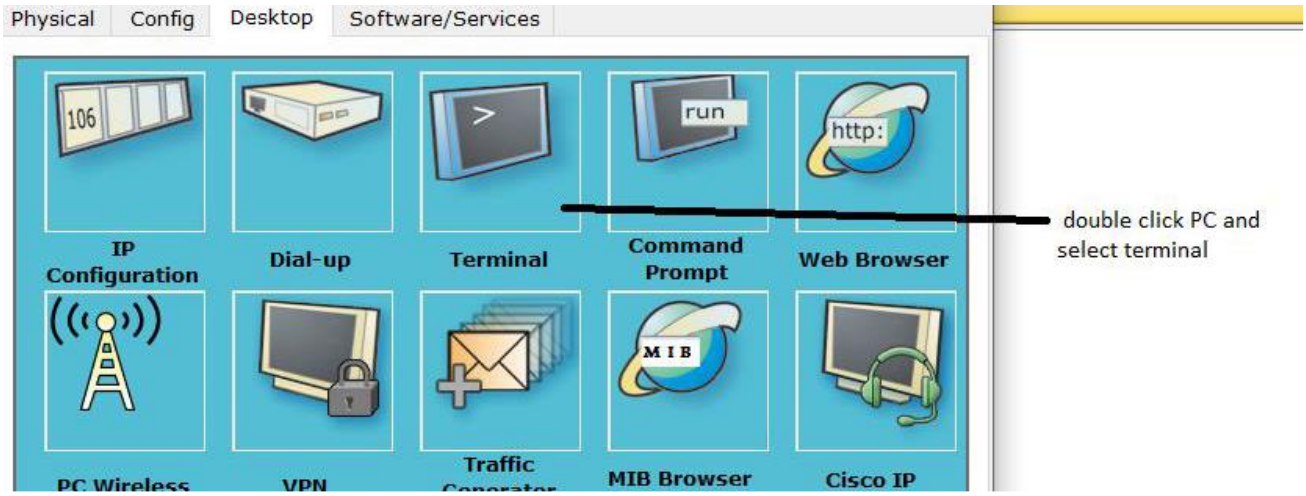
Step 2:

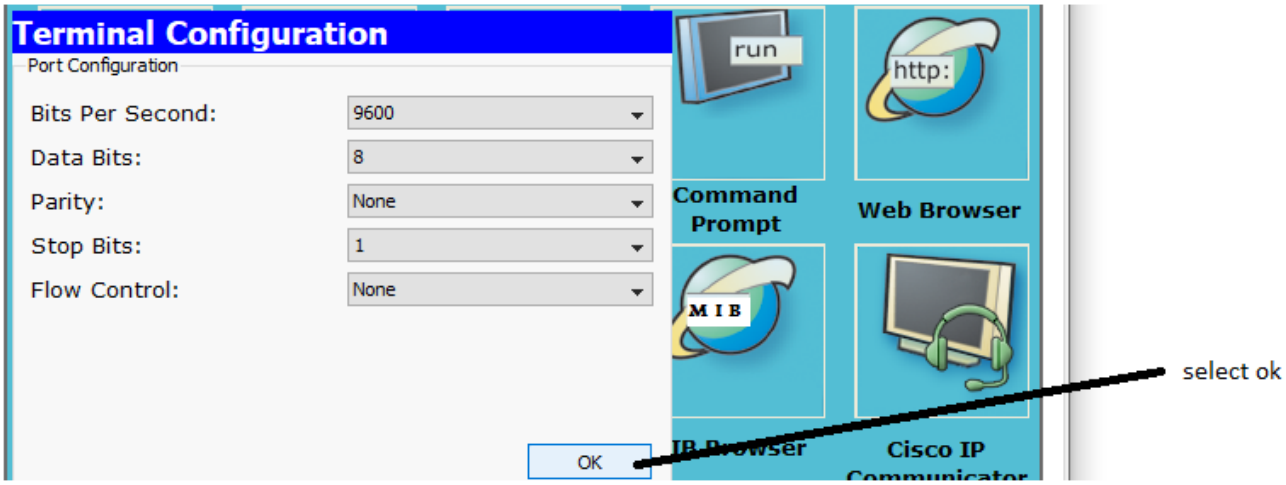


Step 3:



Step 4:





Basic commands:

switch> ---> User Mode

switch>enable --> Enters into the Privilege mode

switch# --> Privilege mode

switch# configure terminal (or) conf t --> Enable Configuration Mode

switch(config)# --> Configuration Mode

Helping commands

switch> ? --> Help to list the available commands in this mode

switch>te? --> Lists all the commands starts with "tel"

switch# ? --> Help

Step 1: Erase the startup configuration file from NVRAM.

Type the erase startup-config command to remove the startup configuration from nonvolatile random access memory (NVRAM).

Switch # erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Router#

Step 2: Reload the switch.

Issue the reload command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

switch# reload

Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing no and press Enter.

System configuration has been modified. Save? [yes/no]: no

Step 3:

Use the show flash command to determine if any VLANs have been created on the switch.

Switch# show flash

Directory of flash:/

2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text

3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text

4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs

5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)

Switch#

Step 4

Switch#

Switch> show version

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE

(fc1)

Switch uptime is 2 minutes

System returned to ROM by power-on

System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"

<output omitted>

Which IOS image version is currently in use by your switch?

Step 5 : Configure the clock.

As you learn more about networking, you will see that configuring the correct time on a Cisco switch can be helpful when you are troubleshooting problems. The following steps manually configure the internal clock of the switch.

a. Display the current clock settings.

Switch> **show clock**

*00:30:05.261 UTC Mon Mar 1 1993

b. Configure the clock setting. The question mark (?) provides help and allows you to determine the expected input for configuring the current time, date, and year. Press Enter to complete the clock configuration.

Switch# **clock set ?**

hh:mm:ss Current Time

Switch# **clock set 15:08:00 ?**

<1-31> Day of the month

MONTH Month of the year

Switch# **clock set 15:08:00 Oct 26 ?**

<1993-2035> Year

Switch# **clock set 15:08:00 Oct 26 2012**

Switch#

*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43

UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by

console.

c. Enter the show clock command to verify that the clock setting has updated.

Switch# **show clock**

15:08:07.205 UTC Fri Oct 26 2012

Step 6 : Give the switch a name.

Use the hostname command to change the switch name to S1.

Switch(config)# hostname S1

S1(config)#

Step 7:Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated. The banner motd command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the #, are often used.

S1(config)# banner motd #

Enter TEXT message. End with the character '#'

Unauthorized access is strictly prohibited and prosecuted to the full extent

of the law. #

S1(config)# exit

S1#

Step 8: Save the configuration.

Use the copy command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

S1# copy running-config startup-config

Destination filename [startup-config]? [Enter]

Building configuration...

[OK]

S1#

Step 9 : Display the current configuration.

The show running-config command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

S1# show running-config

Building configuration...

Current configuration : 1409 bytes

!

! Last configuration change at 03:49:17 UTC Mon Mar 1 1993

Step 10 : Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the show ip interface brief command. Press the spacebar to advance to the end of the list.

S1# **show ip interface brief**

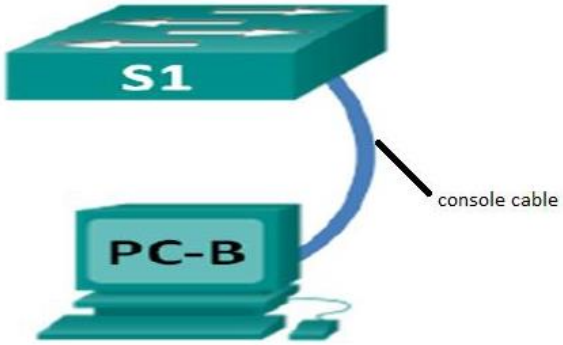
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned YES unset up up
FastEthernet0/1 unassigned YES unset up up
FastEthernet0/2 unassigned YES unset down down
FastEthernet0/3 unassigned YES unset down down
FastEthernet0/4 unassigned YES unset down down
FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset up up
FastEthernet0/7 unassigned YES unset down down
FastEthernet0/8 unassigned YES unset down down
FastEthernet0/9 unassigned YES unset down down

Step 11: Show vlan:

Show vlan command will display the VLANs. For administrative purpose, switch automatically create VLAN 1 and assign all its interfaces to it. You can create custom VLANs from global configuration mode and then assign them to interfaces.

Exp 3: Configure the privilege level password and user authentication in switch.



I How to Set Hostname and Configure Console Password

1. To set the host name

Switch(config)# hostname CISCO

2. To set console password

CISCO((config)#

CISCO((config)#line console 0

CISCO((config-line)#password cisco123

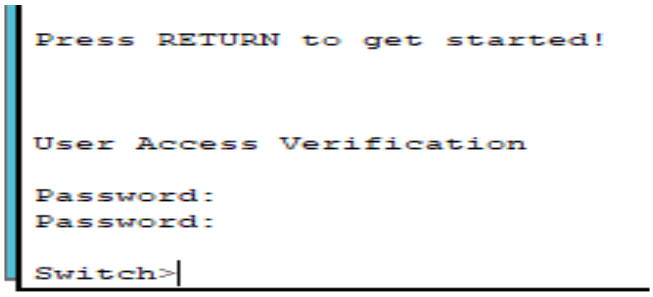
CISCO((config-line)#login

CISCO((config-line)#exit

CISCO((config)#exit

CISCO(#exit

Check the Console Password



II How to Set Privilege level password

1)Set a privilege password

!!! Clear Text Password not encrypted(less priority)

CISCO(config)# enable password muscat

!!! Encrypted password (more Priority)

CISCO(config)# enable secret nizwa

2) Verify the privilege Password

CISCO(config)# exit

CISCO# exit

CISCO con0 is now available

Press RETURN to get started.

User Access Verification

!!! TYPE HERE LINE CONSOLE Password

Password:

CISCO>enable

!!! TYPE HERE Privilege Level Password

Password:

III How to Set User Authentication in Switch

1)Set user authentication

CISCO# conf t

CISCO(config)# line console 0

CISCO(config-line)# login local

CISCO(config-line)# exit

CISCO(config)#username network password pwd

2) Verify the Authentication

CISCO(config)# exit

CISCO# exit

User Access Verification

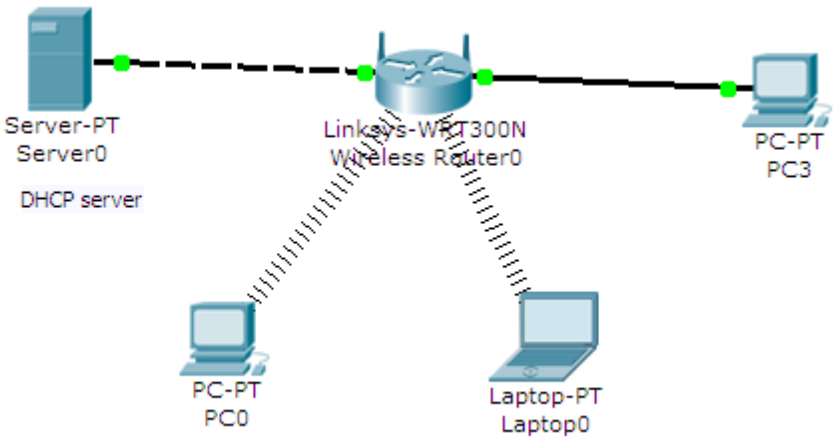
Username: network

Password:

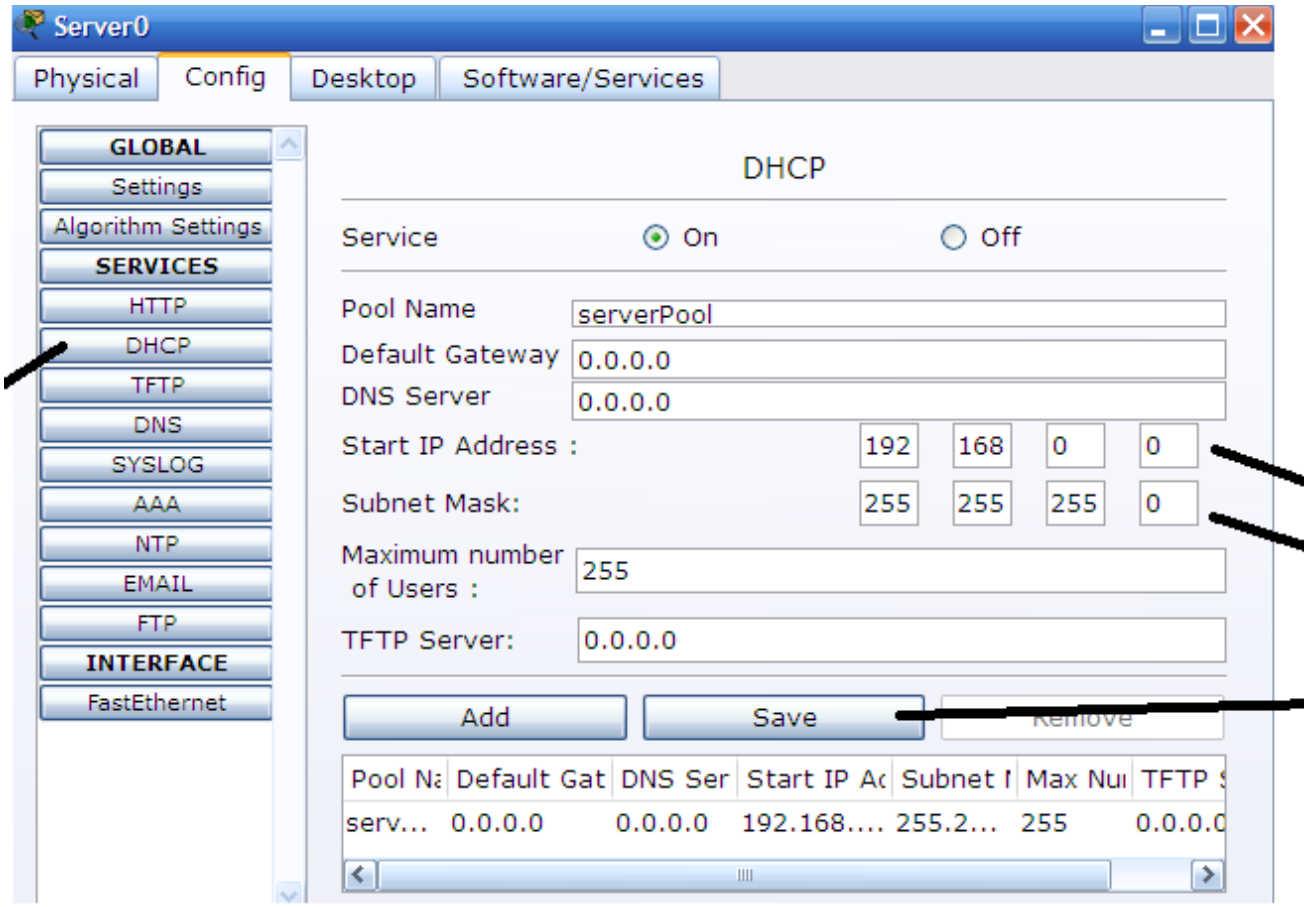
CISCO> enable

Password:

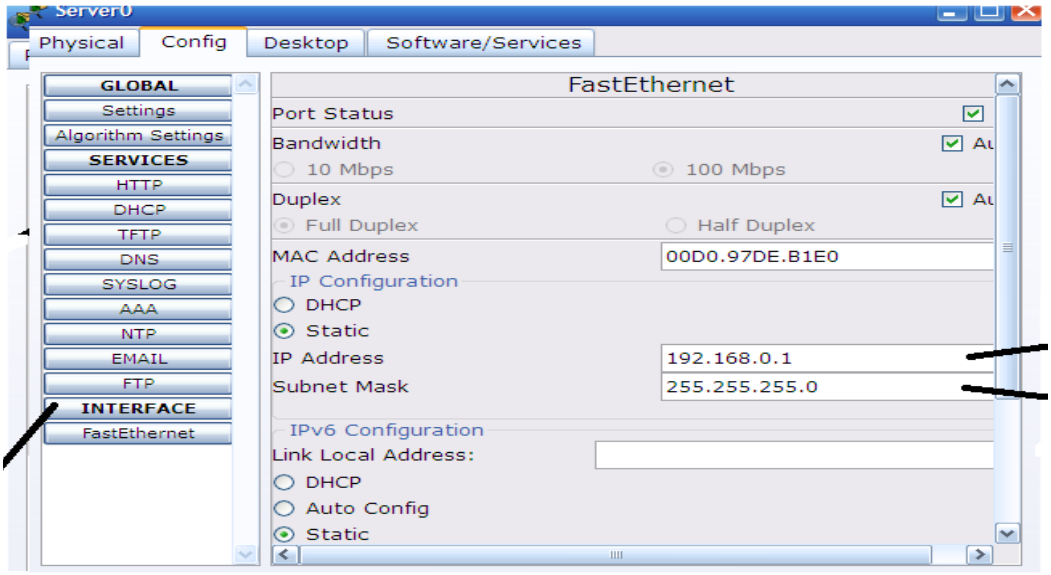
Exp 4: Configure the DHCP Server and wireless router and check the connectivity



Step1 :configure the DHCP server

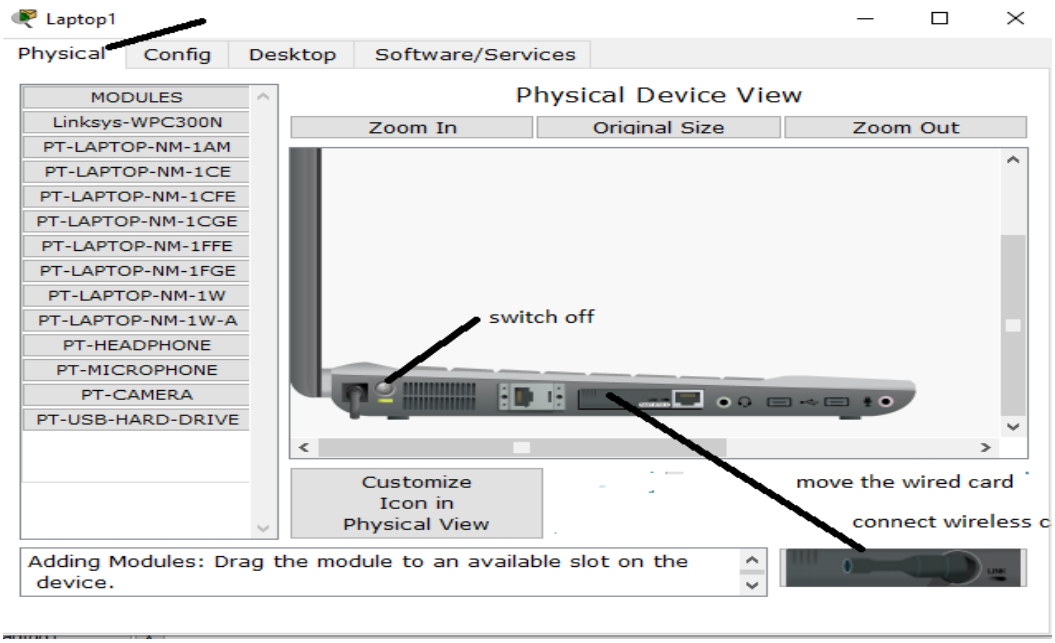


Step2: In server configure the fast Ethernet

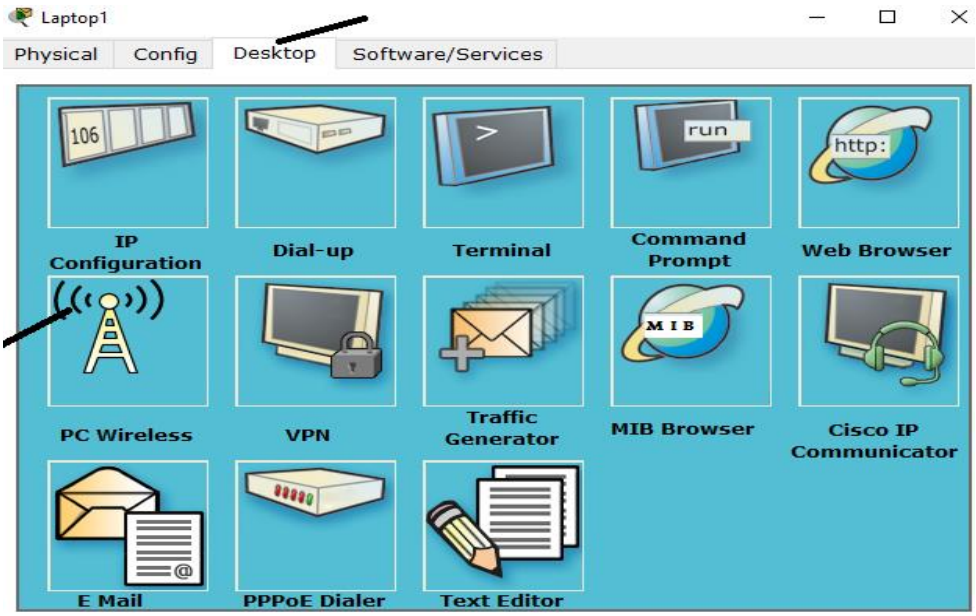


Step 3: configure the wireless router

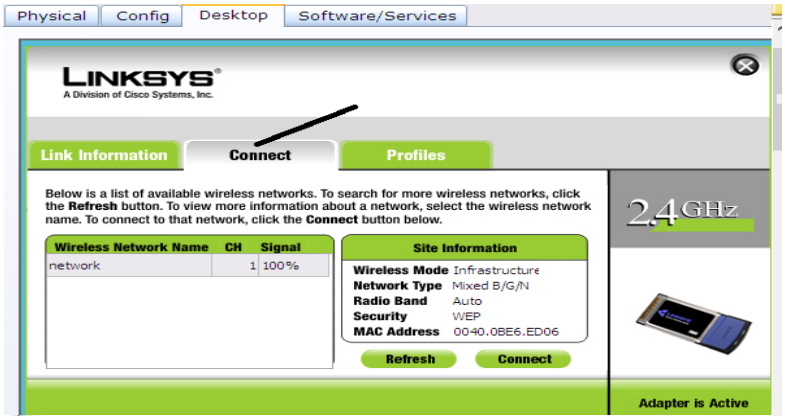
Step4 :Laptop remove the wired NIC card to wireless card



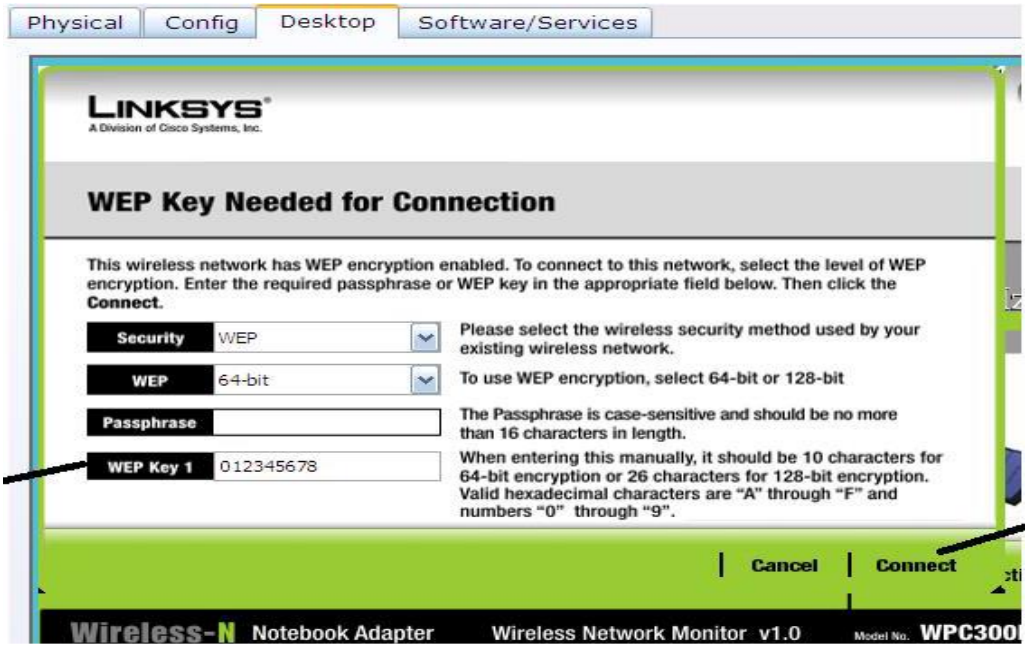
Step 5: Laptop connect the wireless



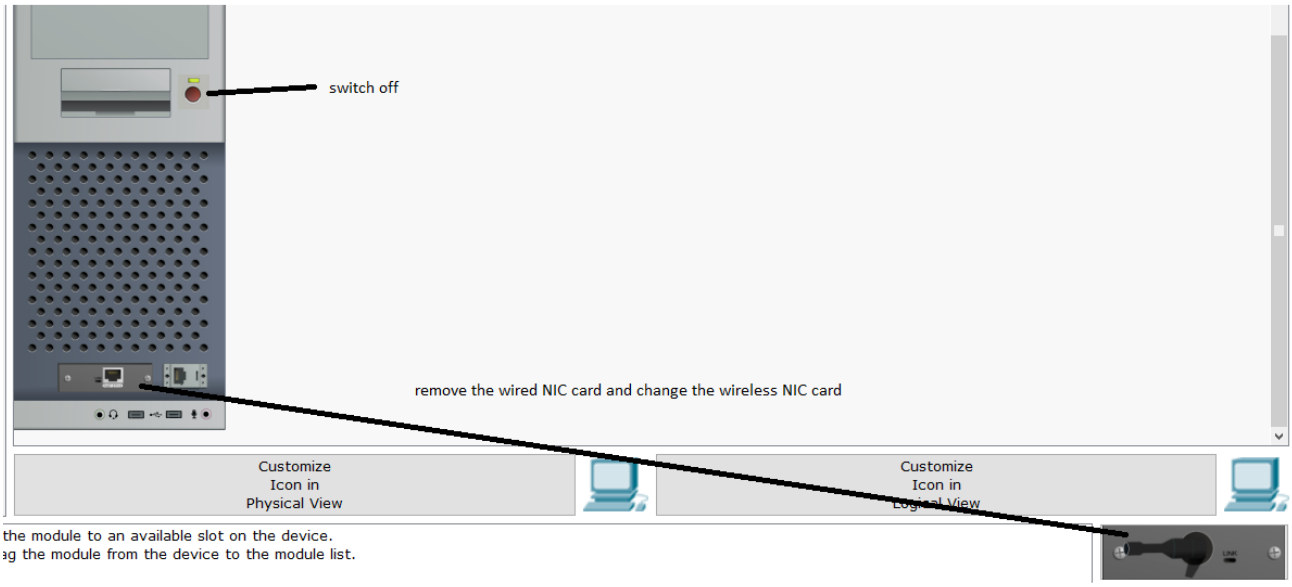
Step 6 : connect Laptop with wireless router



Step 7 :enter web key

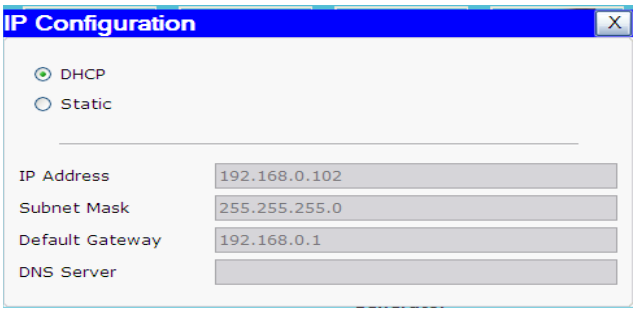


Step8 : PC remove the wired NIC card to wireless card

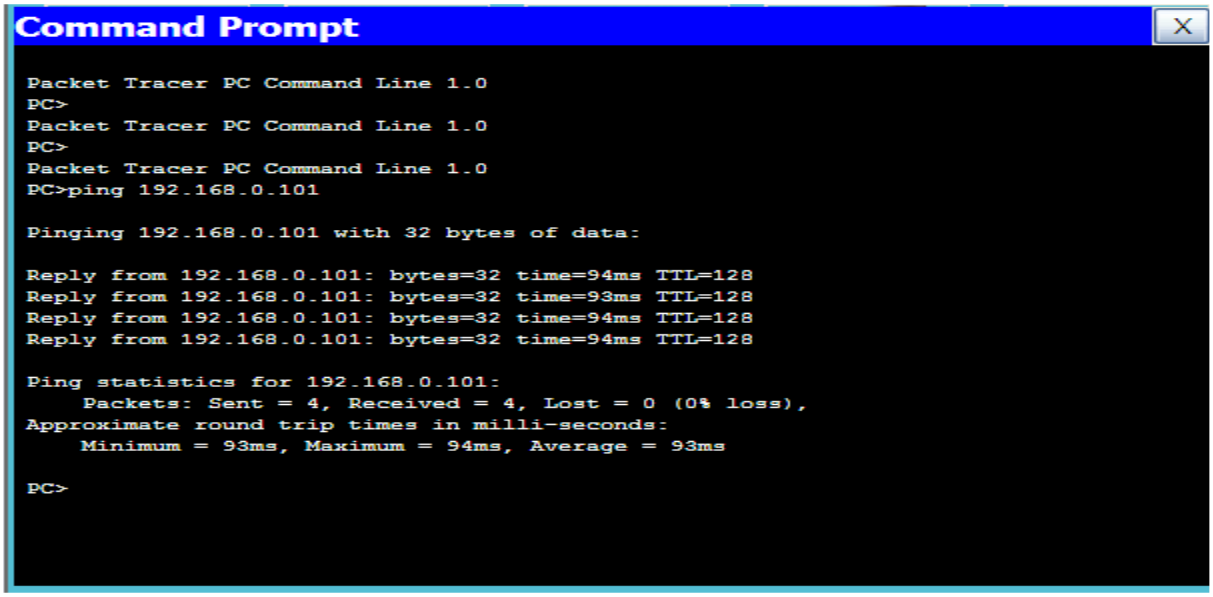


Note : Same steps 5,6,7

Step 9 : check the Pc and laptop for the DHCP ip address

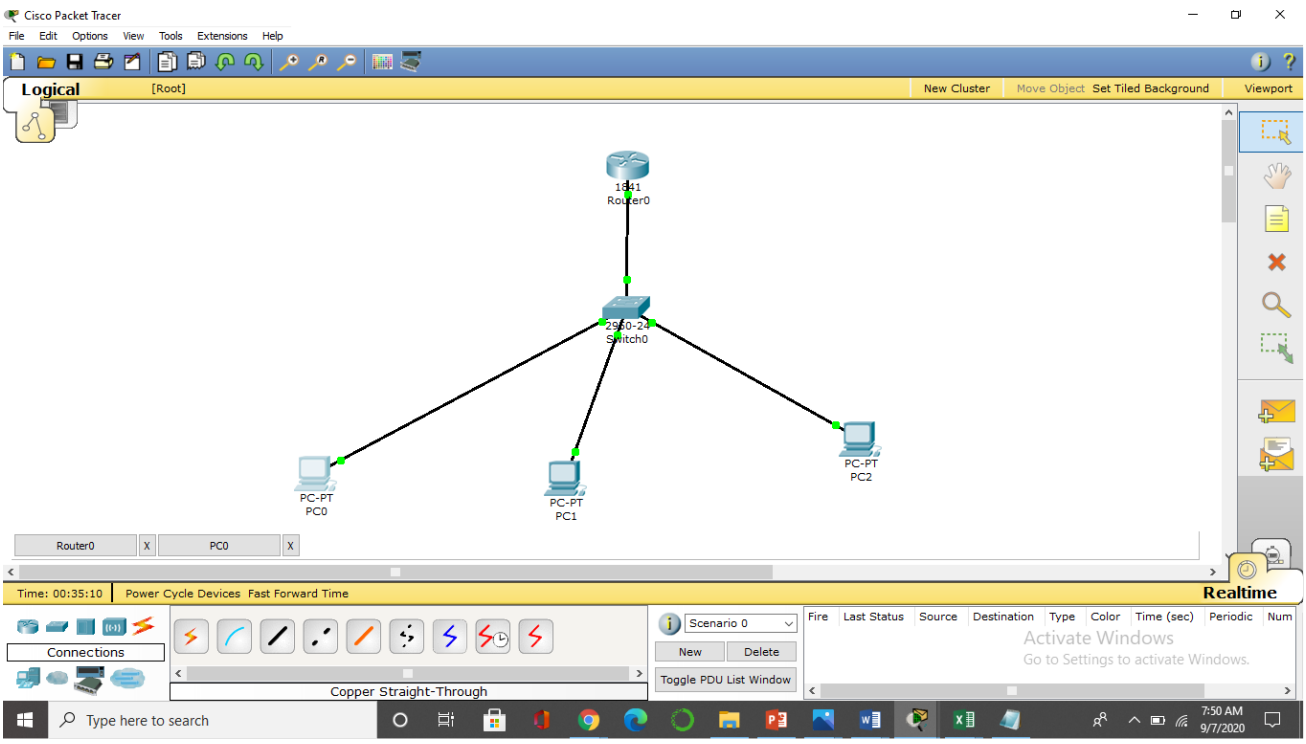


Step10 check the connectivity



Exp 5: Configure the telnet protocol using cisco packet tracer

Step 1: Draw a topology as shown below and assign IP address to all PC's.



Step 2:Configure IP address to router.

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 10.0.0.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Step 3:To set privilege mode password

Click on Router and go to CLI tab and type below.

Router(config)#enable password 1234

Router(config)#exit

Step 4:To configure telnet.

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#line vty 0 4

Router(config-line)#password cisco

Router(config-line)#login

Router(config-line)#exit

Step 5:To check telnet configuration.

Router#sh run

Building configuration...

Current configuration : 556 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

!

!

enable password 1234

!

!

ODD SEM 2020-21 PRESIDENCY UNIVERSITY, BENGALURU

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

interface FastEthernet0/0

ip address 10.0.0.1 255.0.0.0

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

!

!

!

!

!

!

line con 0

line vty 0 4

password cisco

login

line vty 5 6

password cisco

login

!

!

!

End

Step 6:To access cisco router via telnet connection from any PC.

Click on any PC>click on desktop>select command prompt and then type below commands

PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=13ms TTL=255

Reply from 10.0.0.1: bytes=32 time=16ms TTL=255

Reply from 10.0.0.1: bytes=32 time=16ms TTL=255

Reply from 10.0.0.1: bytes=32 time=16ms TTL=255

Ping statistics for 10.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 13ms, Maximum = 16ms, Average = 15ms

PC>telnet 10.0.0.1

Trying 10.0.0.1 ...Open

User Access Verification

Password:

Router>en

Password:

Router#

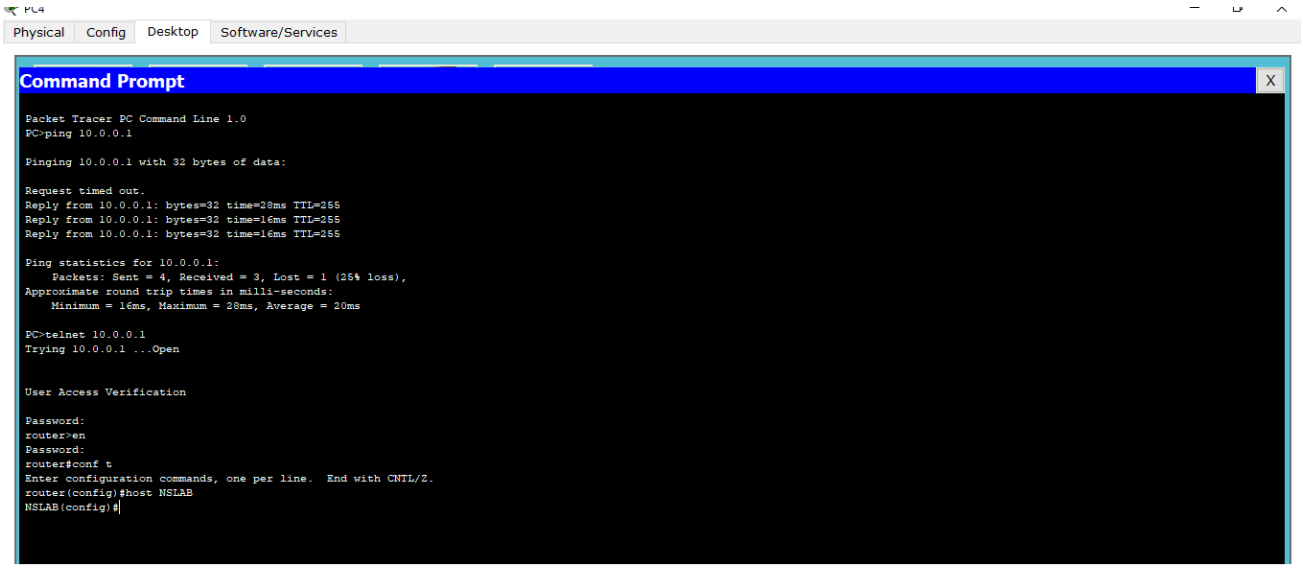
We can change hostname of router in PC command prompt.

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

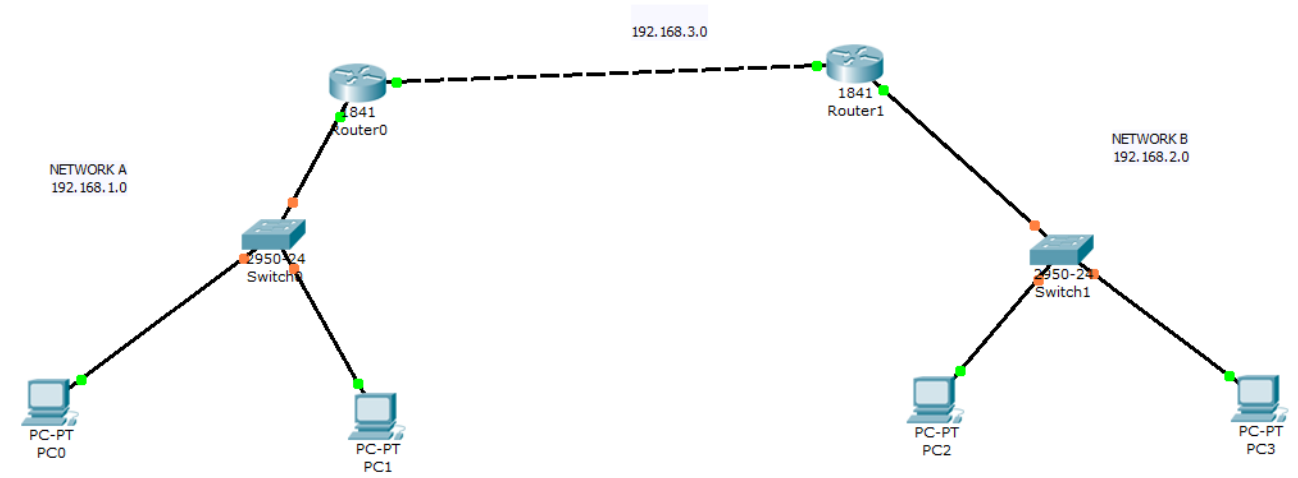
Router(config)#host nslab

nslab(config)#



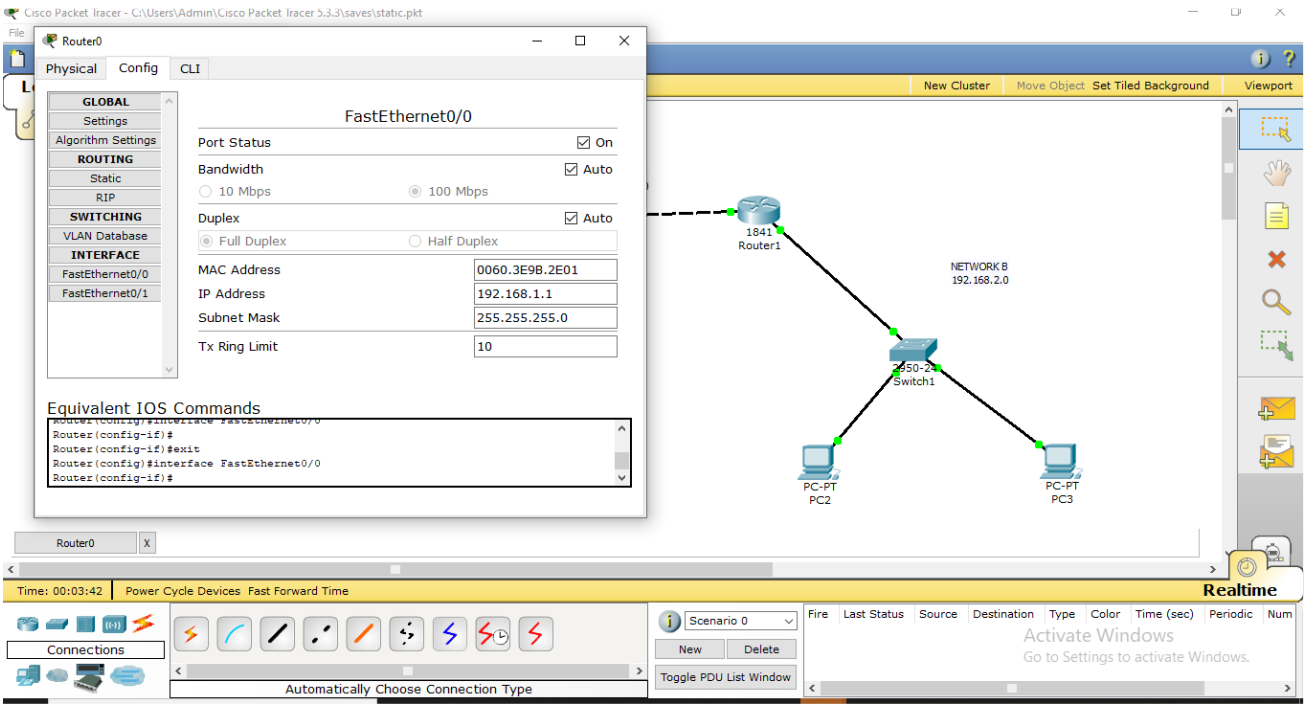
Exp 6: Configure the static routing using cisco packet tracer.

Step 1: Draw a topology as shown below and assign IP address to all PC's.

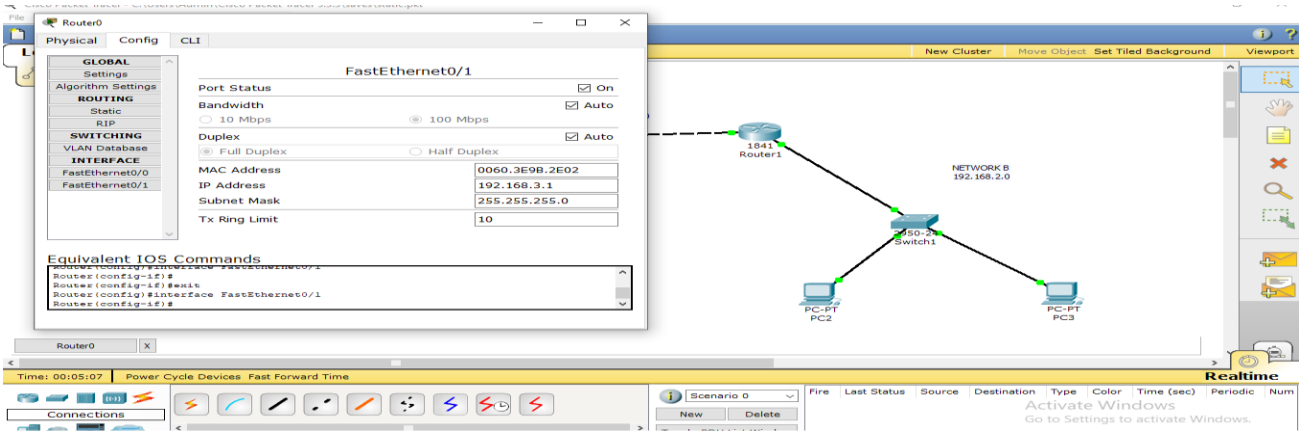


Step 2:Configure IP address to router1.

For Fastethernet 0/0

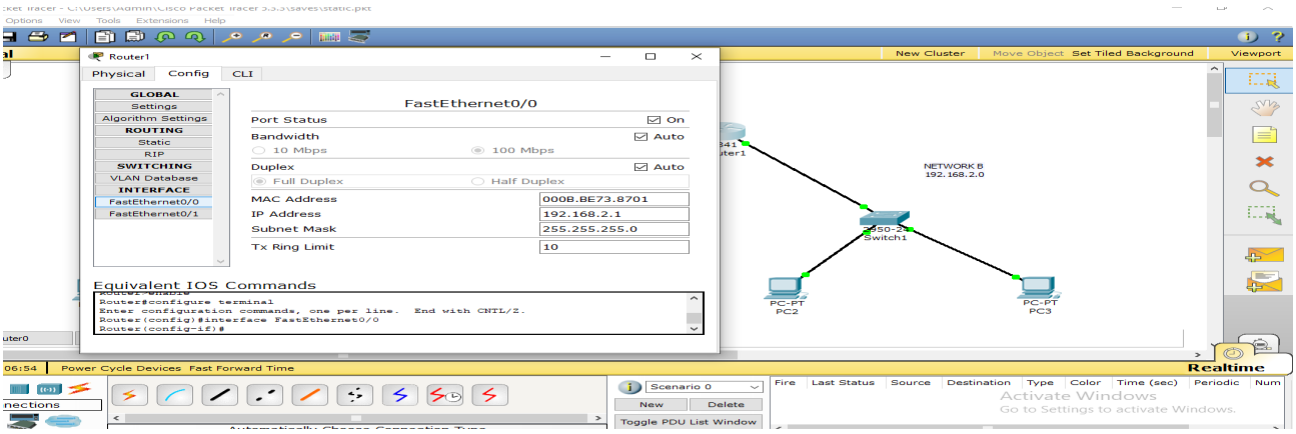


For Fastethernet 0/1

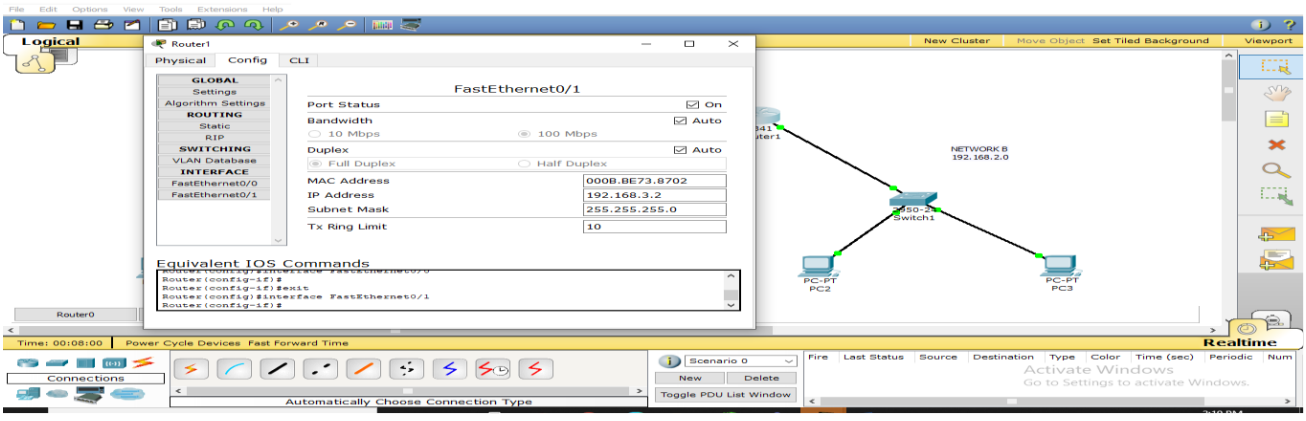


Step 3 :Configure IP address to router2

For Fastethernet 0/0



For FastEthernet 0/1



Step 4:To set up Static Routing

For Router 1:

In CLI:

Router(config)#

Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

In Config Window:

Click on Static

Then Add Opposite Network Address 192.168.2.0 and Next Hop address 192.168.3.1 Along with Subnet Mask Address 255.255.255.0

For Router 2:

In CLI:

Router(config)#

Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1

In Config Window:

Click on Static

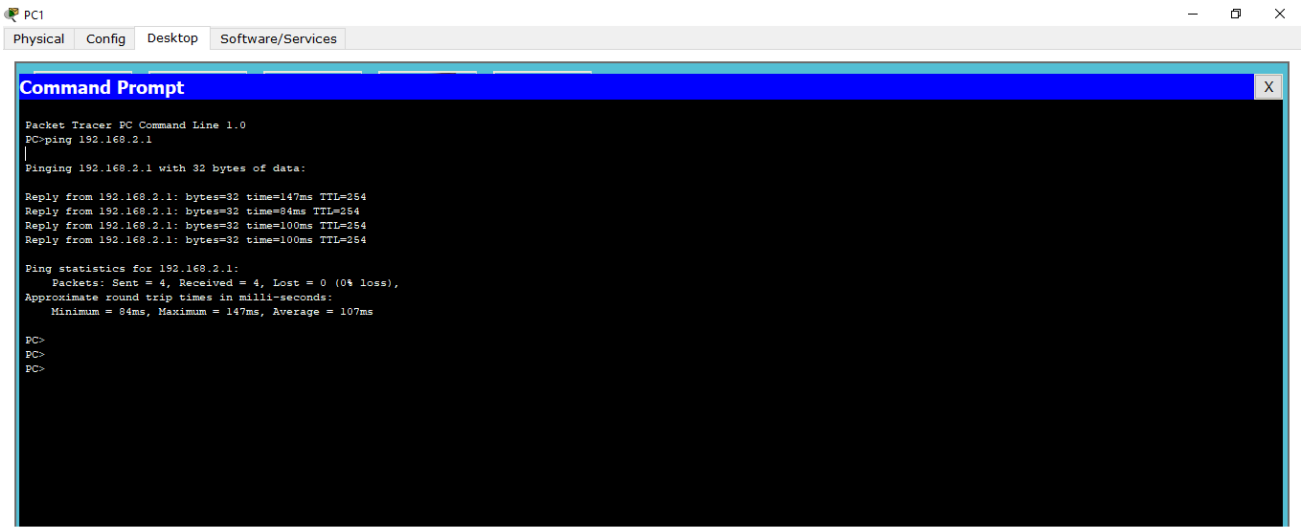
Then Add Opposite Network Address 192.168.1.0 and Next Hop address 192.168.3.2 Along with Subnet Mask Address 255.255.255.0

Step 5 :To Check Connectivity between two network using Static Routing

Click on any PC>click on desktop>select command prompt and then type below commands

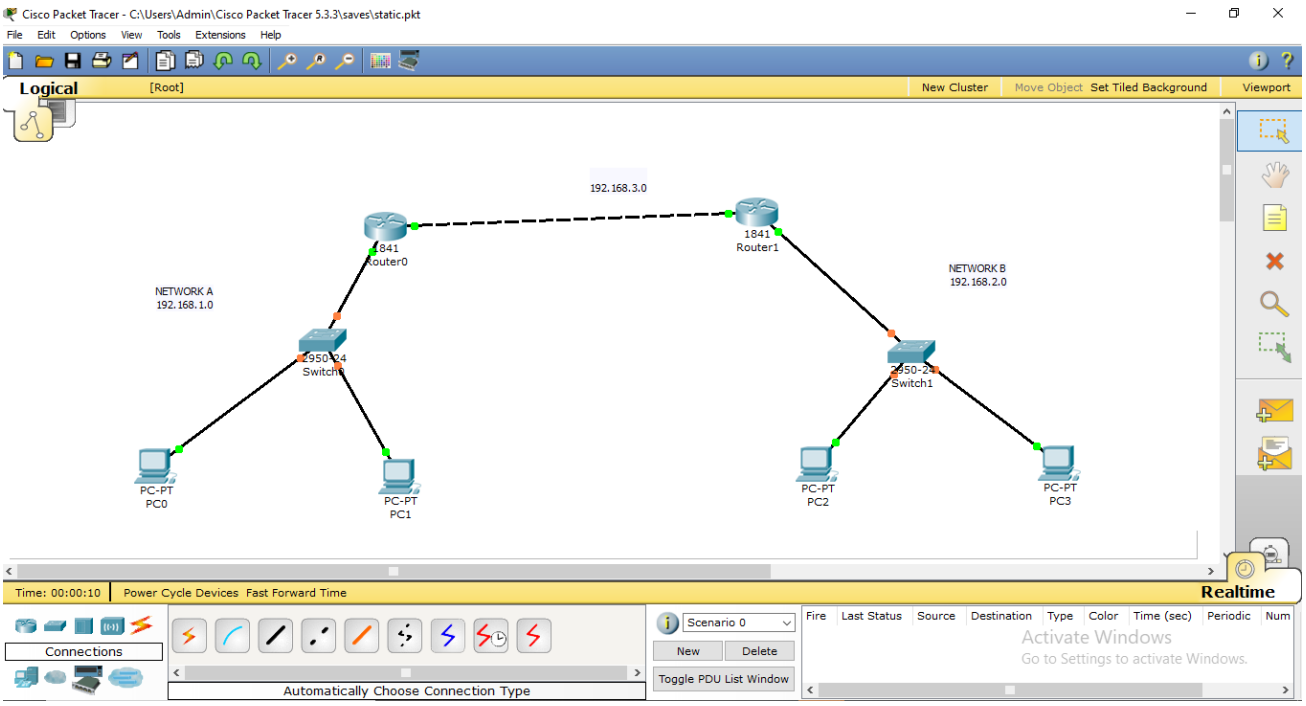
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=147ms TTL=254
Reply from 192.168.2.1: bytes=32 time=84ms TTL=254
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 84ms, Maximum = 147ms, Average = 107ms



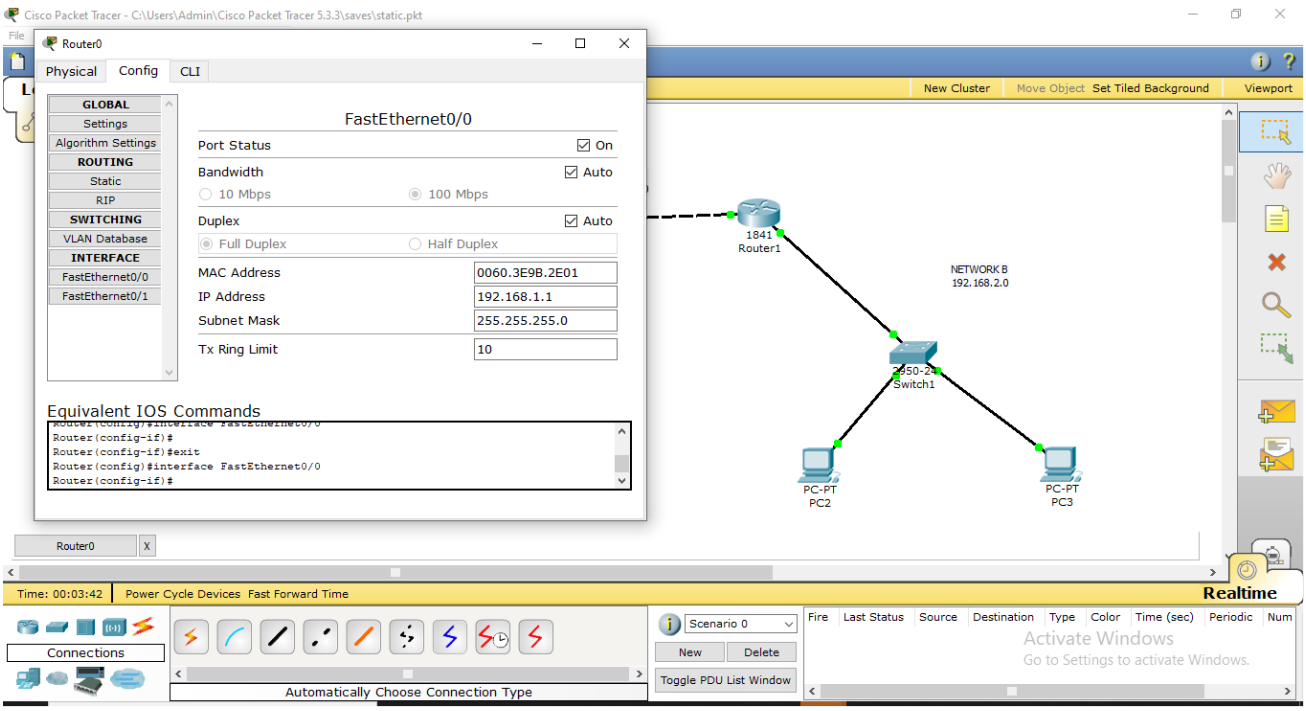
Exp 7: Configure the RIP routing using cisco packet tracer.

Step 1: Draw a topology as shown below and assign IP address to all PC's.

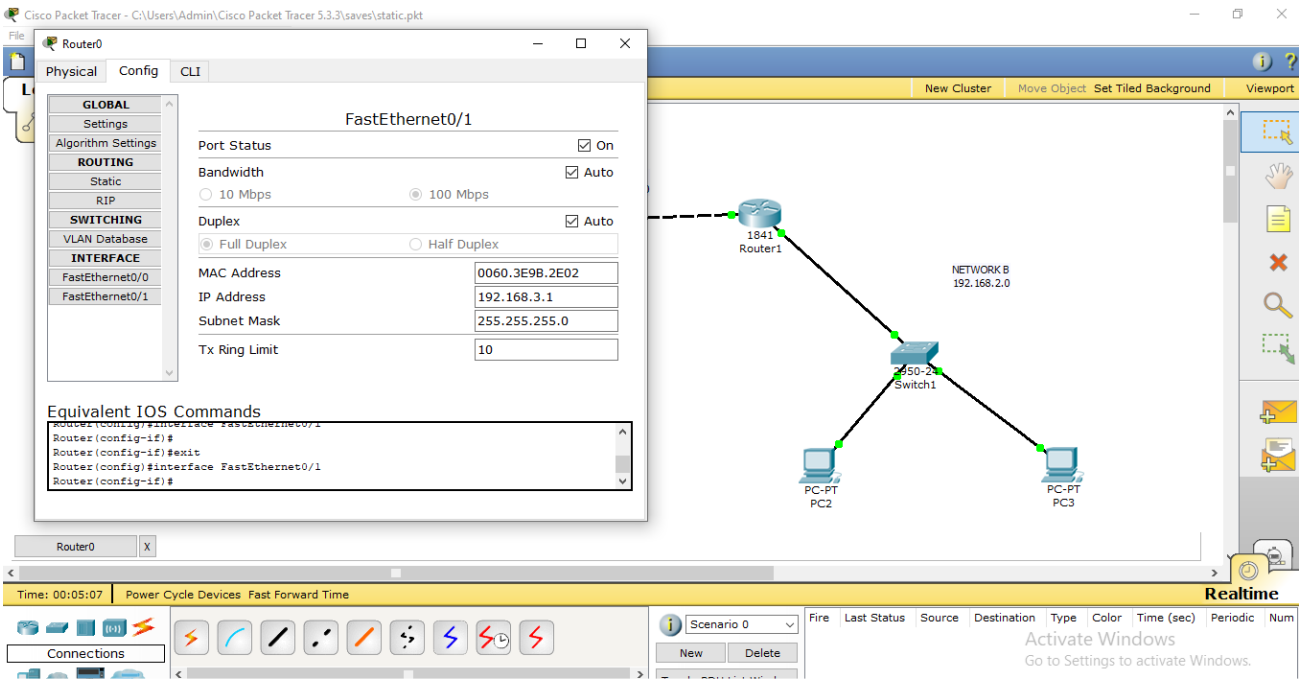


Step 2:Configure IP address to router1.

For Fastethernet 0/0

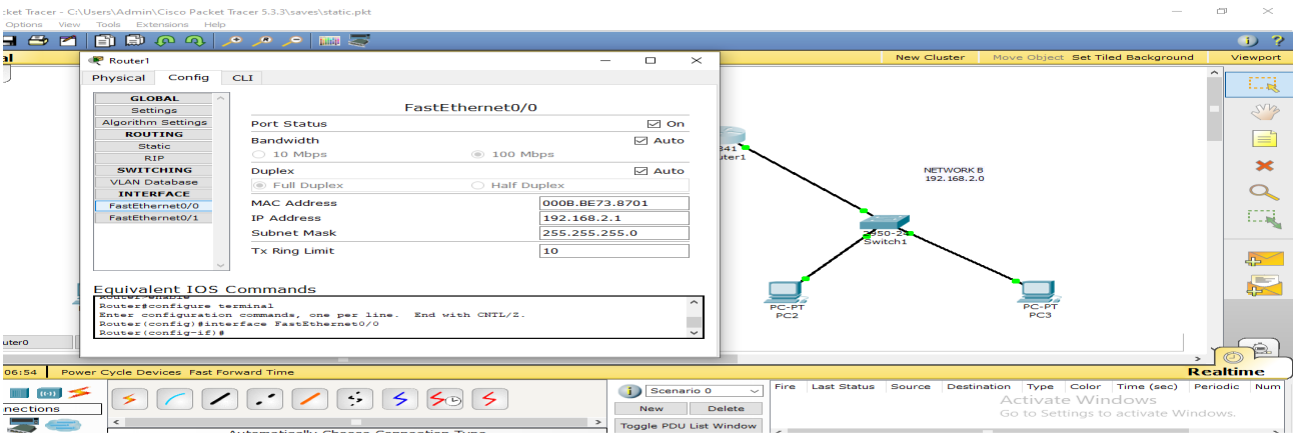


For Fastethernet 0/1

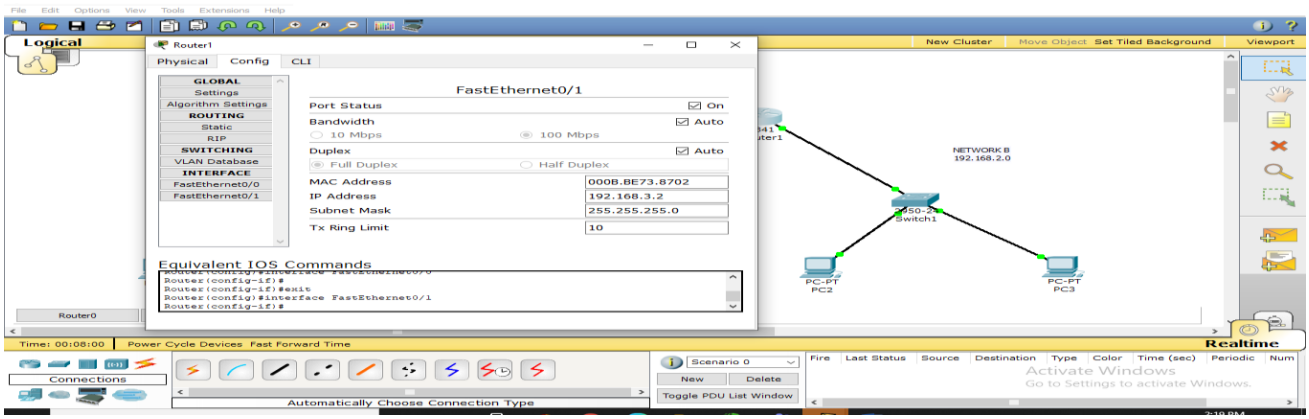


Step 3 :Configure IP address to router2

For Fastethernet 0/0



For FastEthernet 0/1



Step 4:To set up Dynamic Routing

For Router 1:

In CLI:

Router(config)#router rip

Router(config-router)#network 192.168.3.0

Router(config-router)#network 192.168.2.0

In Config Window:

Click on RIP

Then Add Opposite Network Address 192.168.2.0 and 192.168.3.0

For Router 2:

In CLI:

Router(config)#router rip

Router(config-router)#network 192.168.3.0

Router(config-router)#network 192.168.1.0

In Config Window:

Click on RIP

Then Add Opposite Network Address 192.168.1.0 and 192.168.3.0

Step 5 :To Check Connectivity between two network using RIP routing

Click on any PC>click on desktop>select command prompt and then type below commands

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=147ms TTL=254

Reply from 192.168.2.1: bytes=32 time=84ms TTL=254

Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

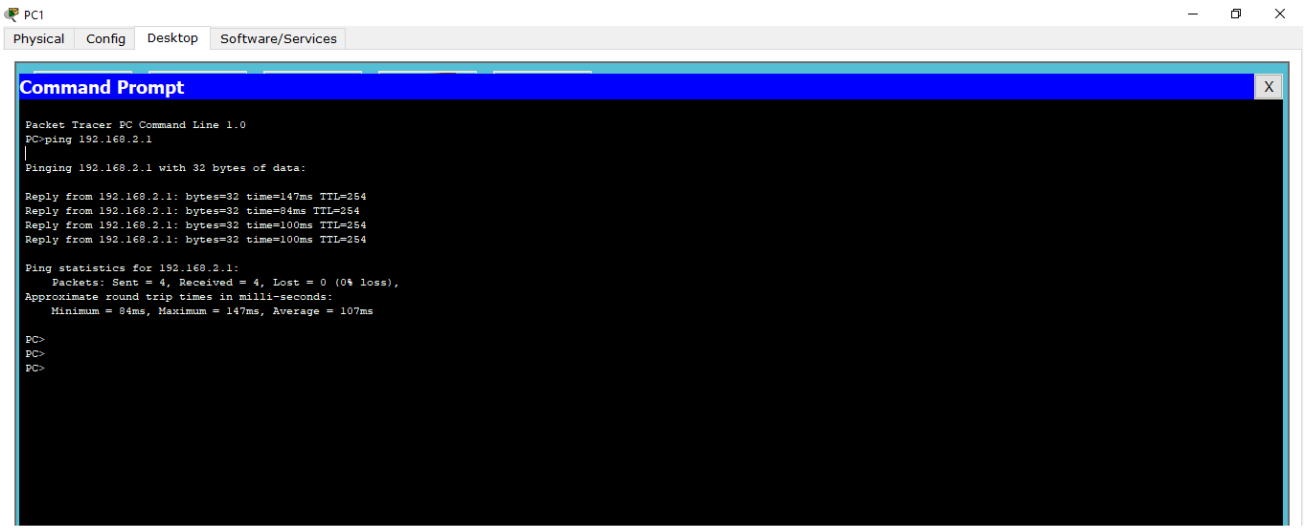
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 84ms, Maximum = 147ms, Average = 107ms

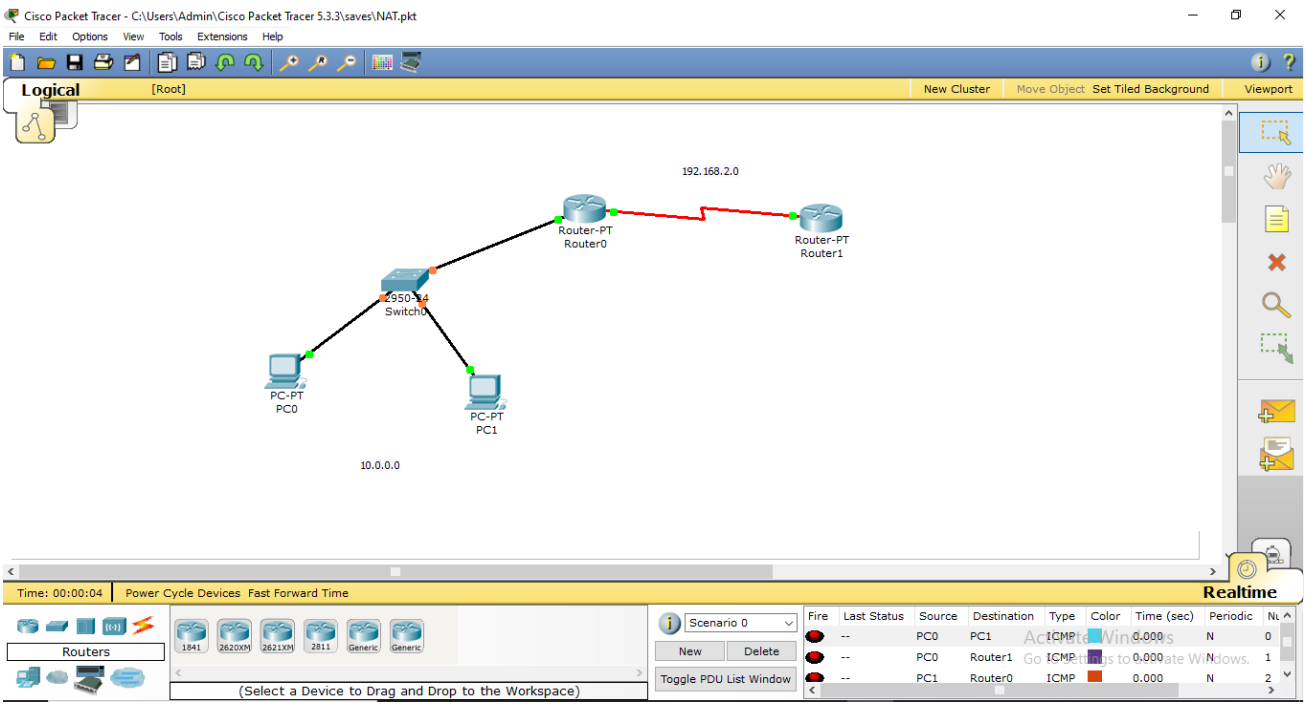


Exp 8: Configure the Static NAT using cisco packet tracer.

NAT(NETWORK ADDRESS TRANSLATION)

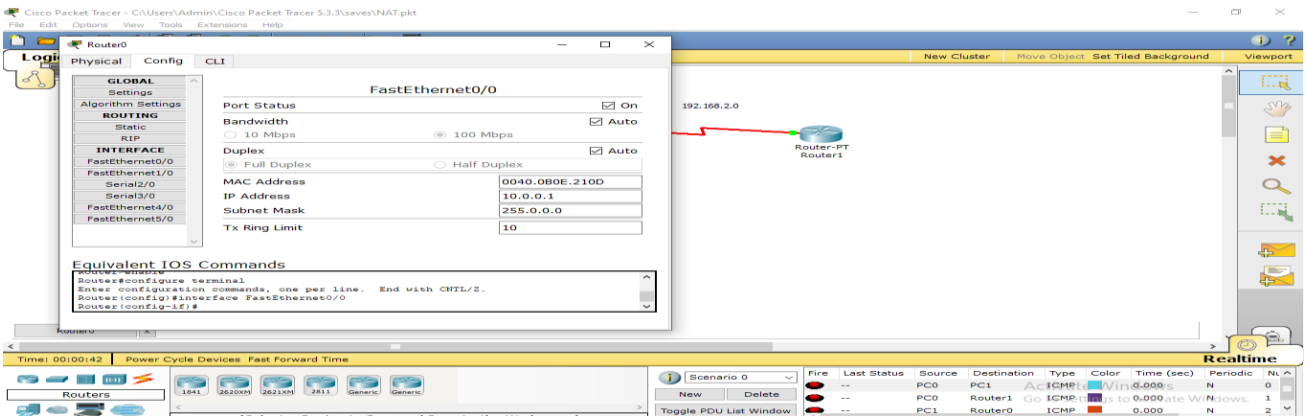
It is a Process in which one or more Local ip address is translated into global ip address or vice versa in order to provide internet access to the host. It Allows multiple devices to access internet through single public ip address.

Step 1: Draw a topology as shown below and assign IP address to all PC's.

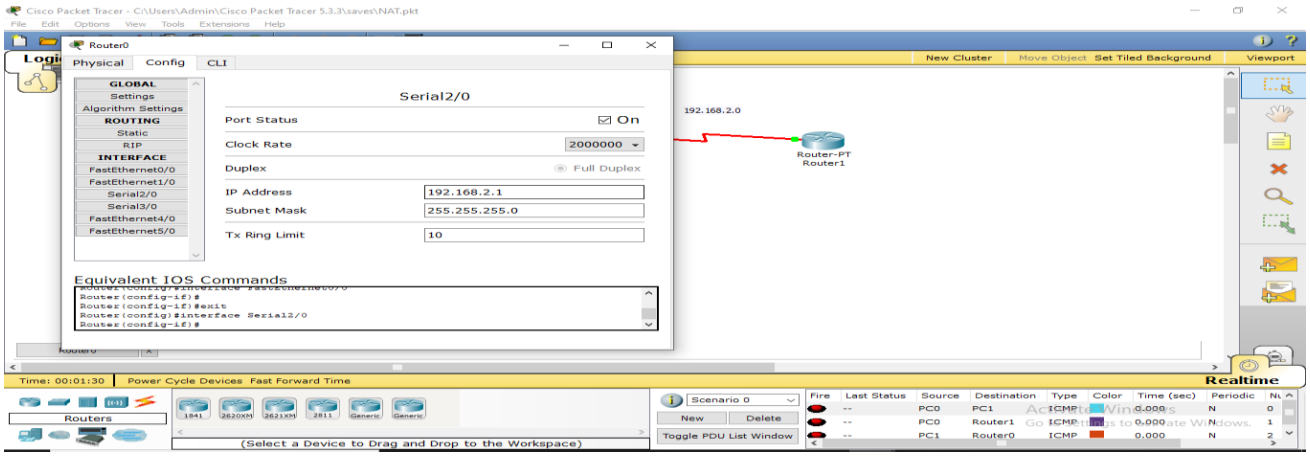


Step 2:Configure IP address to router1.

For Fastethernet 0/0

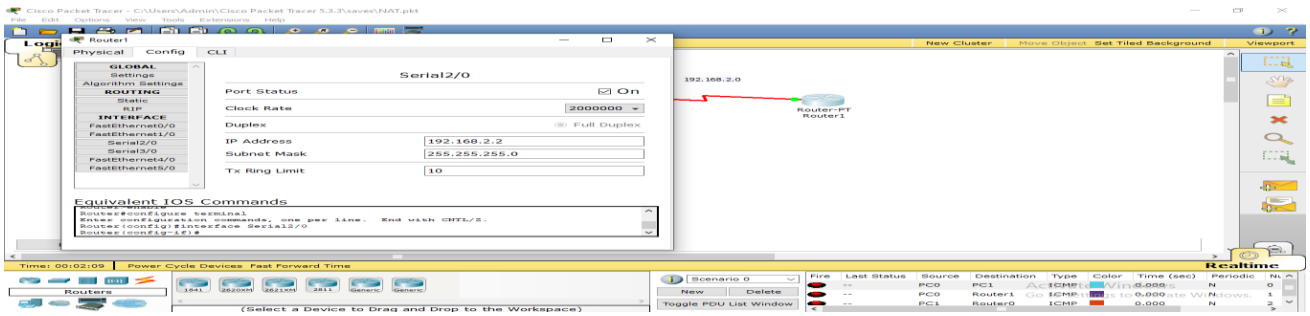


For Serial2/0



Step 3 :Configure IP address to router2

For Serial 2/0



Step 4:To set up Static NAT:

Router# sh ip nat translation

Router# config t

Router(config)#ip nat inside source static 10.0.0.2 192.168.1.3

Provide interface for NAT cable

Router(config)# int fa0/0

Router(config-if)# ip nat inside

exit

Router(config)# int serial2/0

Router(config-if)# ip nat outside

exit

exit

Router#sh ip nat translation

Step 5 :To Check Connectivity between two network

Click on any PC>click on desktop>select command prompt and then type below commands

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=147ms TTL=254

Reply from 192.168.2.1: bytes=32 time=84ms TTL=254

Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

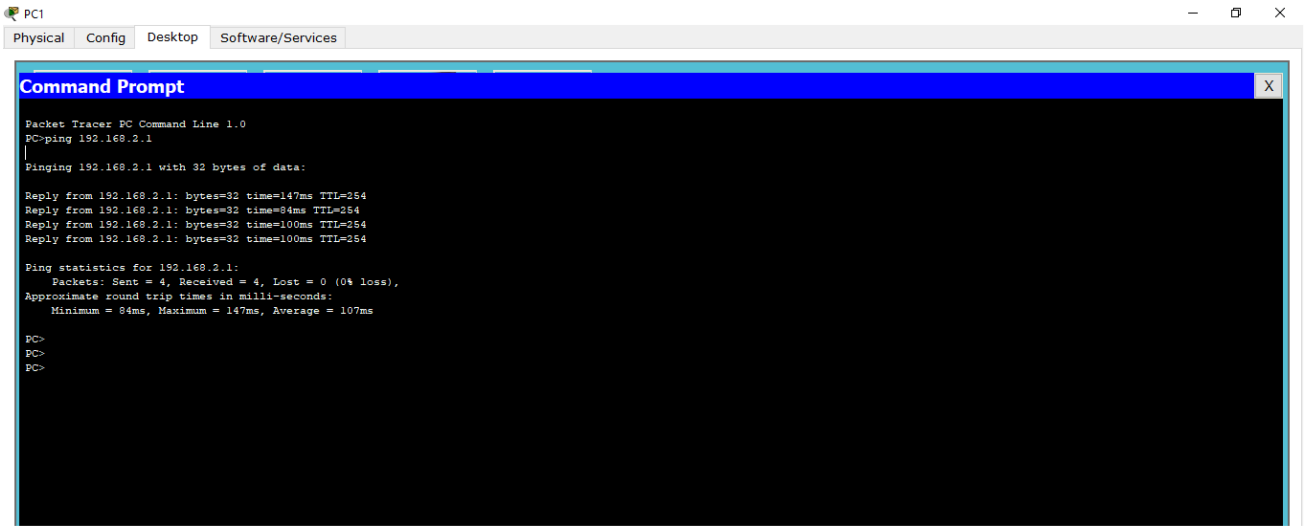
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 84ms, Maximum = 147ms, Average = 107ms



Exp 9: Configure the Dynamic NAT using cisco packet tracer.

NAT(NETWORK ADDRESS TRANSLATION)

It is a Process in which one or more Local ip address is translated into global ip address or vice versa in order to provide internet access to the host.

It Allows multiple devices to access internet through single public ip address.

Dynamic NAT configuration requires four steps: -

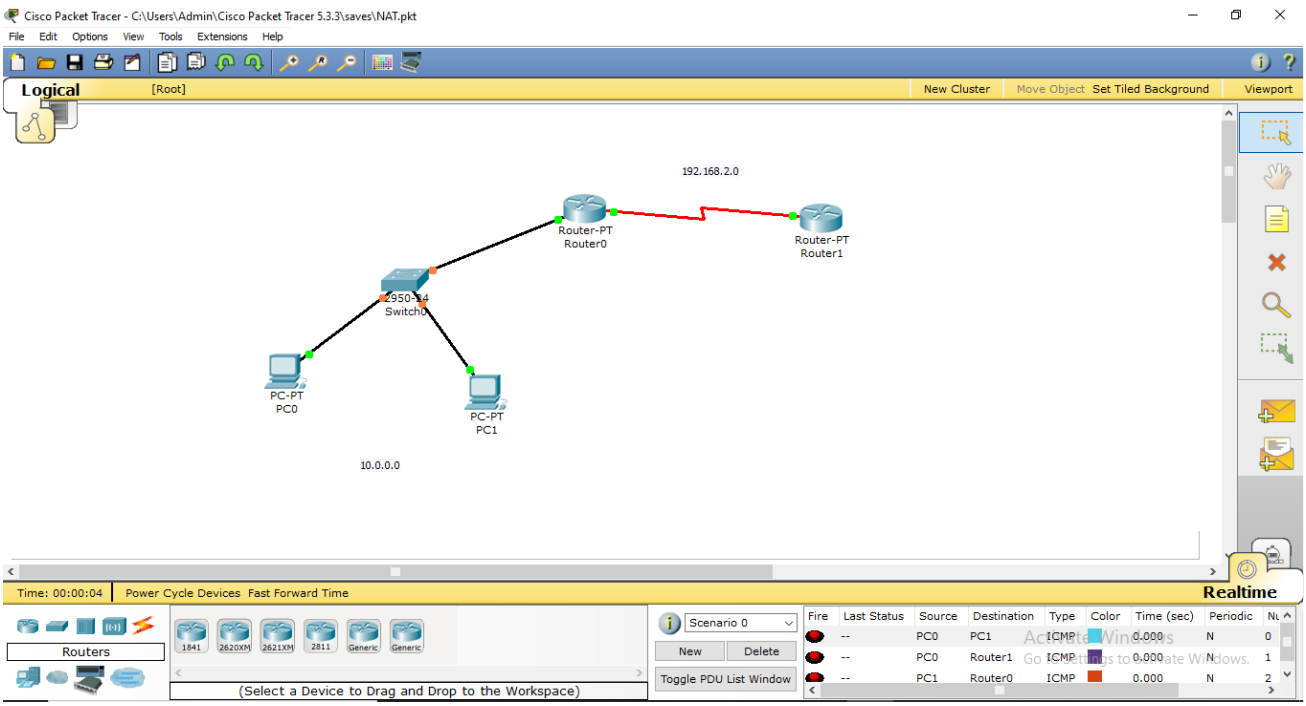
Step1: Create an access list of IP addresses which need translation(ACL range 1 to 99 and 1300 to 1999)

Step2 : Create a pool of all IP address which are available for translation

Step3: Map access list with pool

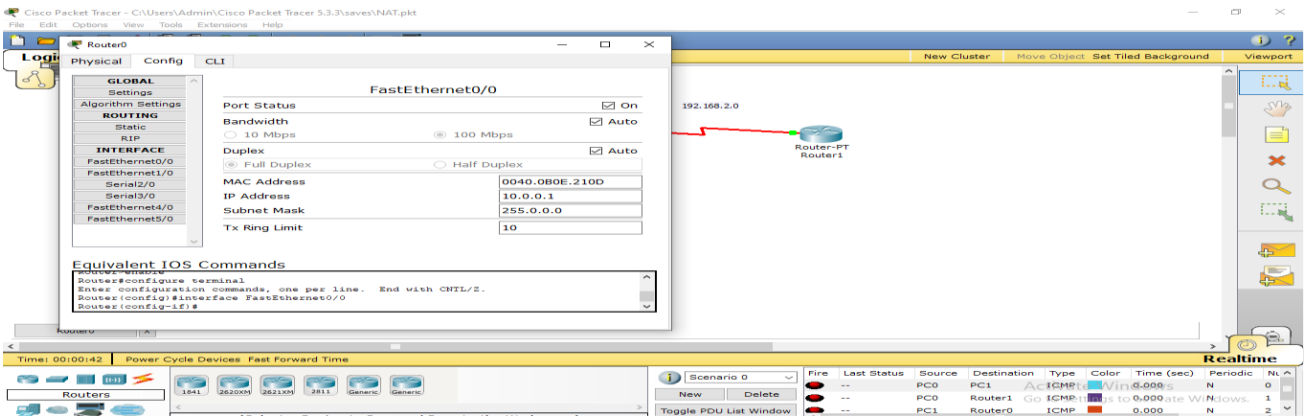
Stpe4: Define inside and outside interfaces

Step 1: Draw a topology as shown below and assign IP address to all PC's.

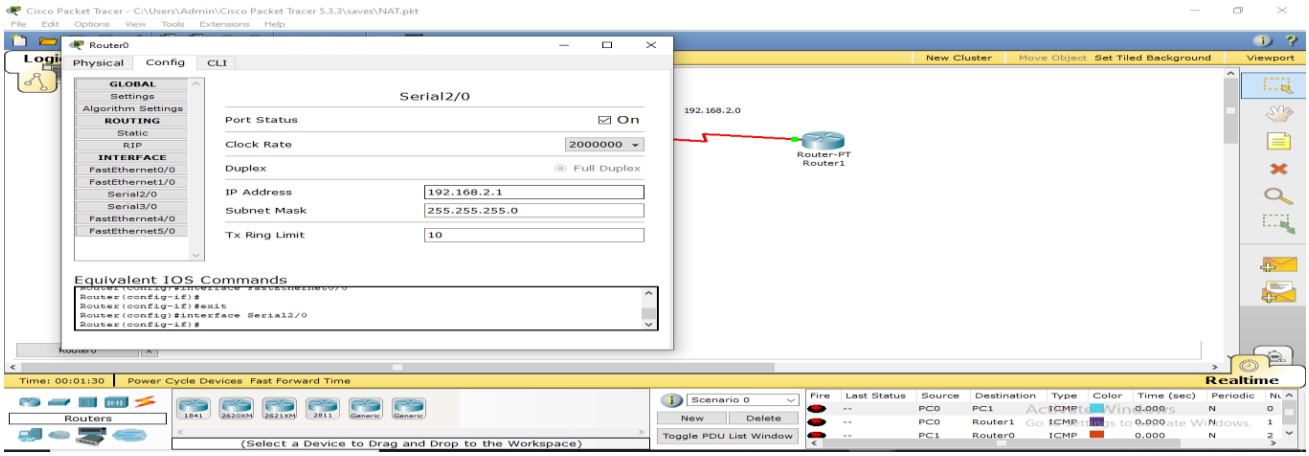


Step 2:Configure IP address to router1.

For Fastethernet 0/0

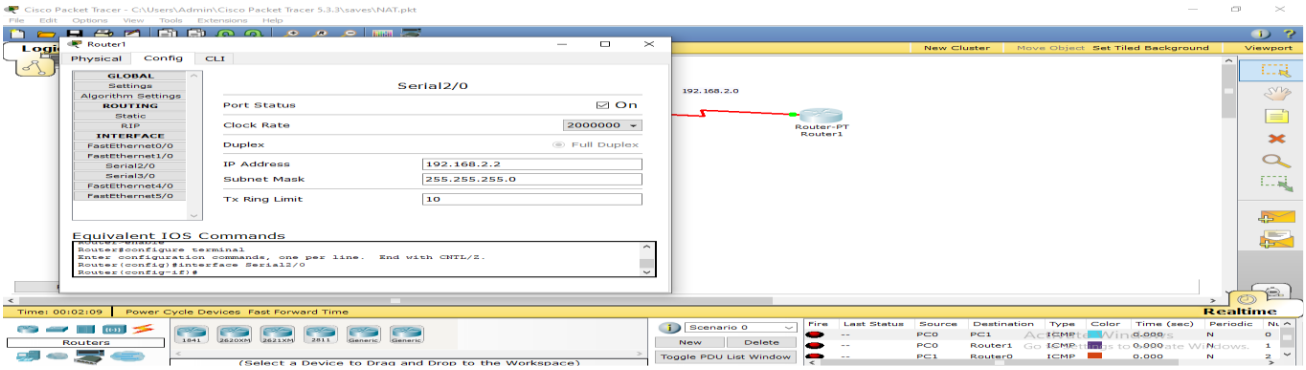


For Serial2/0



Step 3 :Configure IP address to router2

For Serial 2/0



Step 4:To set up Dynamic NAT:

router(config)#access-list 1 permit 10.0.0.2 0.0.0.0

router(config)#access-list 1 permit 10.0.0.3 0.0.0.0

router(config)#ip nat pool nslab 192.168.2.3 192.168.2.4 netmask 255.255.255.0

router(config)#ip nat inside source list 1 pool nslab

router(config)#int fa0/0

router(config-if)#ip nat inside

router(config-if)#exit

router(config)#int serial2/0

router(config-if)ip nat outside

router#sh ip nat translation

Step 5 :To Check Connectivity between two network

Click on any PC>click on desktop>select command prompt and then type below commands

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=147ms TTL=254

Reply from 192.168.2.1: bytes=32 time=84ms TTL=254

Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 84ms, Maximum = 147ms, Average = 107ms