

PRESIDENCY UNIVERSITY

DEPARTMENT OF INFORMATION SCIENCE

COMPUTER NETWORK LAB (BCA208)

BCA 4th Semester A.Y (2021-22)

Instructor Incharge : Ms. AKSHATHA Y

Course Credit Structure : 2-2-3 (3 Credits)

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.



The screenshot shows a Microsoft Windows Command Prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe". The window displays the following text:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 155.0.0.24

Pinging 155.0.0.24 with 32 bytes of data:
Reply from 155.0.0.24: bytes=32 time<1ms TTL=128

Ping statistics for 155.0.0.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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*

```
C:\Users\Codrut Neagu>ping www.digitalcitizen.life -t
Pinging www.digitalcitizen.life [2606:4700:20::681a:cfc] with 32 bytes of data:
Reply from 2606:4700:20::681a:cfc: time=10ms
Reply from 2606:4700:20::681a:cfc: time=85ms
Reply from 2606:4700:20::681a:cfc: time=10ms
Reply from 2606:4700:20::681a:cfc: time=18ms
Reply from 2606:4700:20::681a:cfc: time=10ms
Reply from 2606:4700:20::681a:cfc: time=11ms
Reply from 2606:4700:20::681a:cfc: time=21ms
Reply from 2606:4700:20::681a:cfc: time=64ms
Reply from 2606:4700:20::681a:cfc: time=10ms
Reply from 2606:4700:20::681a:cfc: time=14ms

Ping statistics for 2606:4700:20::681a:cfc:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 85ms, Average = 25ms
Control-Break
Reply from 2606:4700:20::681a:cfc: time=10ms

Ping statistics for 2606:4700:20::681a:cfc:
    Packets: Sent = 16, Received = 16, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 85ms, Average = 19ms
Control-C
^C
C:\Users\Codrut Neagu>
```

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.

```
Command Prompt  
C:\Users\Codrut Neagu>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . :  
IPv6 Address . . . . . : 2a02:2f01:730a:1300:107c:de5c:5f89:c00a  
Temporary IPv6 Address . . . . . : 2a02:2f01:730a:1300:254b:7d03:4a72:9b5c  
Link-local IPv6 Address . . . . . : fe80::107c:de5c:5f89:c00a%20  
IPv4 Address . . . . . : 192.168.50.239  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : fe80::6d9:f5ff:feb5:b1f0%20  
192.168.50.1  
  
Wireless LAN adapter Wi-Fi:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
  
Wireless LAN adapter Local Area Connection* 9:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
C:\Users\Codrut Neagu>
```

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

```
C:\WINDOWS\System32\cmd.exe  
C:\>ipconfig /all  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection 3:  
  
Connection-specific DNS Suffix . :  
IP Address . . . . . : 192.168.5.28  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.5.100
```

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.

```
Command Prompt  
C:\Users\Codrut Neagu>ipconfig /all  
  
Windows IP Configuration  
  
Host Name . . . . . : Codrut-PC  
Primary Dns Suffix . . . . .  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . . . . .  
Description . . . . . : Realtek PCIe 2.5GbE Family Controller  
Physical Address. . . . . : 04-D9-F5-34-B1-A3  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
IPv6 Address. . . . . : 2a02:2f01:730a:1300:107c:de5c:5f89:c00a(PREFERRED)  
Temporary IPv6 Address. . . . . : 2a02:2f01:730a:1300:254b:7d03:4a72:9b5c(PREFERRED)  
Link-local IPv6 Address . . . . . : fe80::107c:de5c:5f89:c00a%20(PREFERRED)  
IPv4 Address. . . . . : 192.168.50.239(PREFERRED)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Thursday, January 23, 2020 1:45:35 PM  
Lease Expires . . . . . : Friday, January 24, 2020 1:45:34 PM  
Default Gateway . . . . . : fe80::6d9:f5ff:feb5:b1f0%20  
                          192.168.50.1  
DHCP Server . . . . . : 192.168.50.1  
DHCIPv6 IAID . . . . . : 335862261  
DHCIPv6 Client DUID. . . . . : 00-01-00-01-25-21-90-1C-04-D9-F5-34-B1-A3  
DNS Servers . . . . . : 2a02:2f01:730a:1300::1  
                          192.168.50.1  
                          2a02:2f01:730a:1300::1  
NetBIOS over Tcpip. . . . . : Enabled  
  
Wireless LAN adapter Wi-Fi:  
  
Media State . . . . . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . .  
Description . . . . . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz  
Physical Address. . . . . . . . : 38-00-25-41-C3-F5  
DHCP Enabled. . . . . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes
```

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

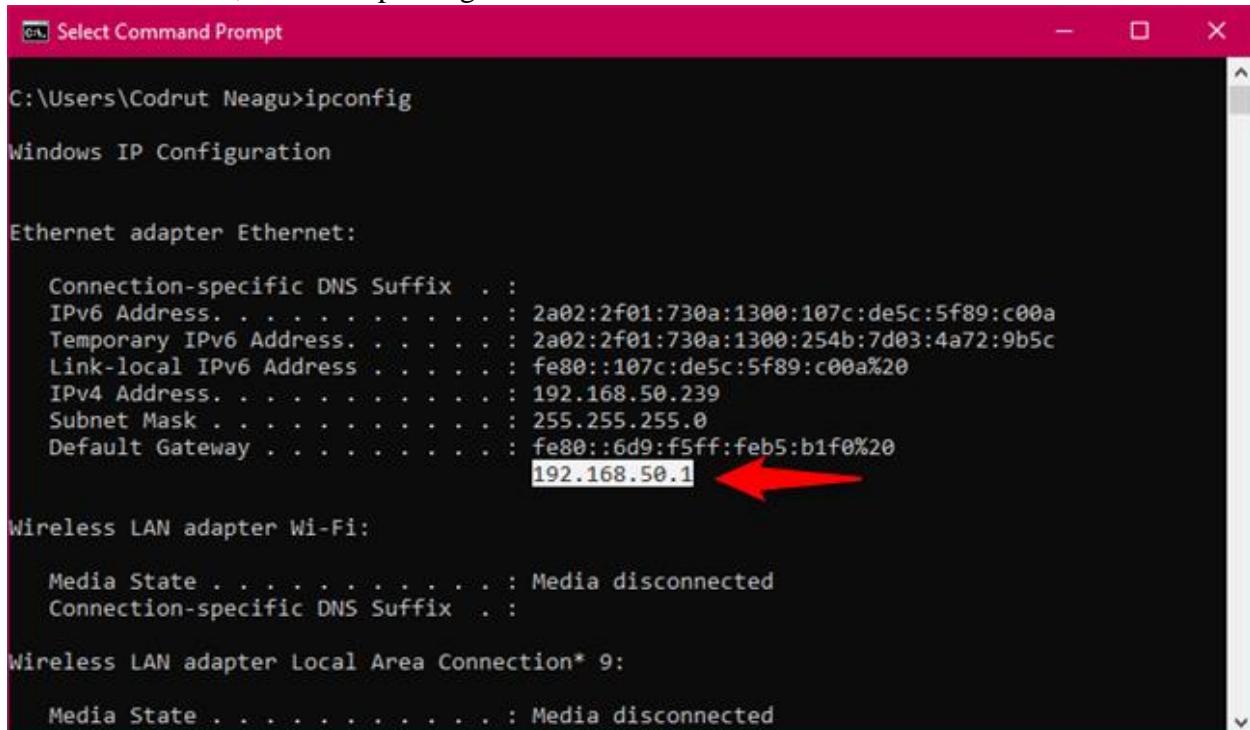
ipconfig /? -shows help

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.



```
C:\Users\Codrut Neagu>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . : 2a02:2f01:730a:1300:107c:de5c:5f89:c00a
  Temporary IPv6 Address. . . . . : 2a02:2f01:730a:1300:254b:7d03:4a72:9b5c
  Link-local IPv6 Address . . . . . : fe80::107c:de5c:5f89:c00a%20
  IPv4 Address. . . . . : 192.168.50.239
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::6d9:f5ff:feb5:b1f0%20
                                192.168.50.1

Wireless LAN adapter Wi-Fi:

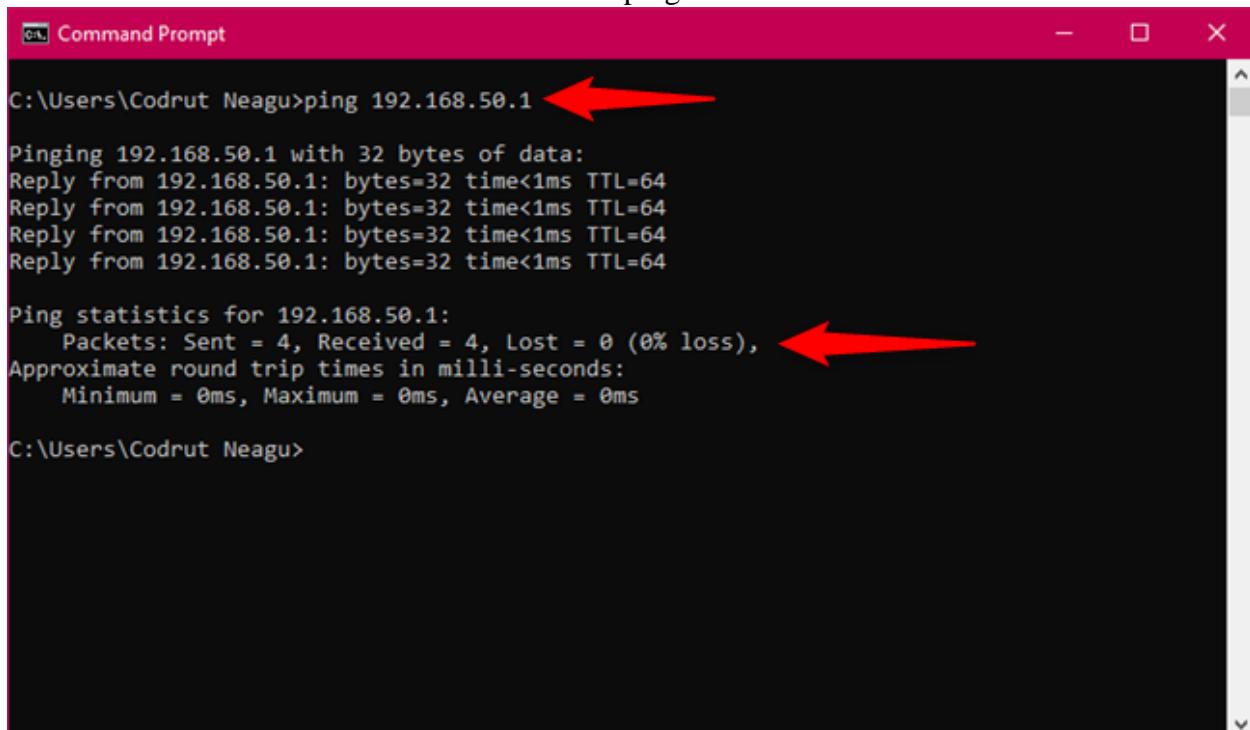
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:

  Media State . . . . . : Media disconnected
```

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.



```
C:\Users\Codrut Neagu>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

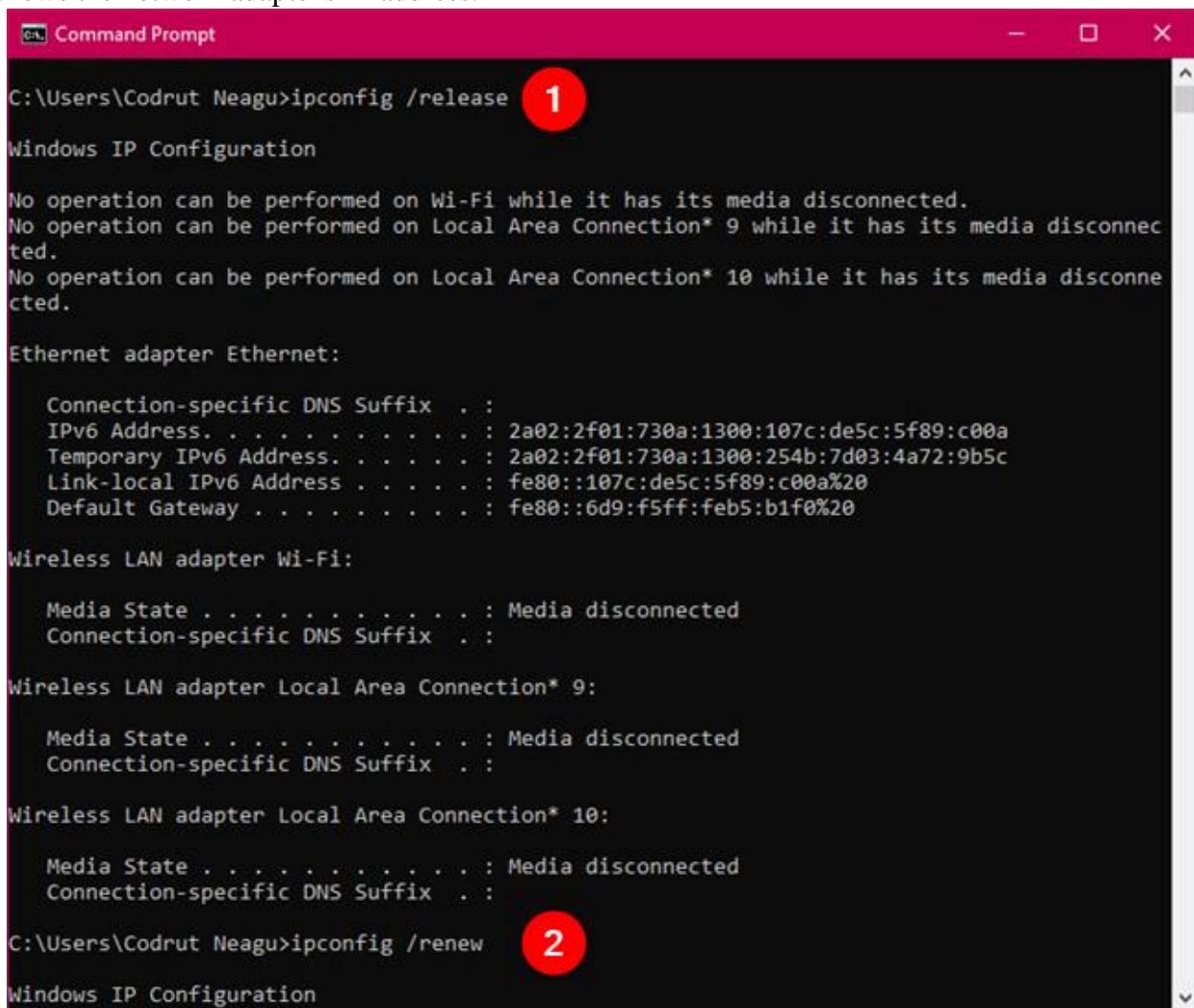
C:\Users\Codrut Neagu>
```

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.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window contains the following text:

```
C:\Users\Codrut Neagu>ipconfig /release 1
Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . .
IPv6 Address . . . . . : 2a02:2f01:730a:1300:107c:de5c:5f89:c00a
Temporary IPv6 Address . . . . . : 2a02:2f01:730a:1300:254b:7d03:4a72:9b5c
Link-local IPv6 Address . . . . . : fe80::107c:de5c:5f89:c00a%20
Default Gateway . . . . . : fe80::6d9:f5ff:feb5:b1f0%20

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . .

Wireless LAN adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . .

Wireless LAN adapter Local Area Connection* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . .

C:\Users\Codrut Neagu>ipconfig /renew 2
Windows IP Configuration
```

Two red circles with numbers are overlaid on the screenshot: circle 1 is over the "ipconfig /release" command, and circle 2 is over the "ipconfig /renew" command.

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

```
cmd C:\WINDOWS\system32\cmd.exe
C:\>Documents and Settings\Administrator>tracert google.com
Tracing route to google.com [72.14.207.99]
over a maximum of 30 hops:
  1 <1 ms <1 ms <1 ms 150.0.0.1
  2   1 ms <1 ms <1 ms ntc.net.pk [202.83.160.129]
  3   28 ms  29 ms  29 ms ntc.net.pk [202.83.160.129]
  4   24 ms  26 ms  26 ms gwish.ntc.net.pk [202.83.160.61]
  5   72 ms  231 ms  268 ms s8-1-0.rwp44d1.pie.net.pk [202.125.155.65]
  6   49 ms  52 ms  49 ms rwp44.pie.net.pk [202.125.148.133]
  7   80 ms  52 ms  49 ms pos2-2.khi77gsrc1.pie.net.pk [202.125.159.45]
  8   51 ms  46 ms  49 ms g3-0.khi77gw1.pie.net.pk [202.125.128.62]
  9   180 ms  181 ms  182 ms t2c2-ge7-0.uk-lon2.eu.bt.net [166.49.176.44]
  10  180 ms  181 ms  185 ms t2c2-ge7-0.uk-lon2.eu.bt.net [166.49.176.44]
  11  181 ms  181 ms  182 ms t2c1-ge4-2.uk-lon1.eu.bt.net [166.49.208.6]
  12  185 ms  185 ms  185 ms t2a1-pc1.uk-lon1.eu.bt.net [166.49.135.98]
  13  183 ms  185 ms  221 ms 195.66.226.125
  14  179 ms  182 ms  185 ms 72.14.238.242
  15  271 ms  267 ms  268 ms 72.14.236.216
  16  281 ms  268 ms  268 ms 72.14.236.213
  17  326 ms  270 ms  270 ms 72.14.236.215
  18  222 ms  281 ms  304 ms 66.249.94.96
  19  222 ms  272 ms  274 ms 66.249.94.118
  20  275 ms  274 ms  274 ms 72.14.207.99

Trace complete.
```

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

```
Command Prompt - netstat
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Codrut Neagu>netstat

Active Connections

Proto Local Address          Foreign Address        State
TCP   127.0.0.1:9012        Codrut-PC:49999      ESTABLISHED
TCP   127.0.0.1:9013        Codrut-PC:50162      ESTABLISHED
TCP   127.0.0.1:9487        Codrut-PC:49815      ESTABLISHED
TCP   127.0.0.1:49815       Codrut-PC:9487       ESTABLISHED
TCP   127.0.0.1:49856       Codrut-PC:49857      ESTABLISHED
TCP   127.0.0.1:49857       Codrut-PC:49856      ESTABLISHED
TCP   127.0.0.1:49860       Codrut-PC:49861      ESTABLISHED
TCP   127.0.0.1:49861       Codrut-PC:49860      ESTABLISHED
TCP   127.0.0.1:49870       Codrut-PC:49871      ESTABLISHED
TCP   127.0.0.1:49871       Codrut-PC:49870      ESTABLISHED
TCP   127.0.0.1:49872       Codrut-PC:49873      ESTABLISHED
TCP   127.0.0.1:49873       Codrut-PC:49872      ESTABLISHED
TCP   127.0.0.1:49876       Codrut-PC:49877      ESTABLISHED
TCP   127.0.0.1:49877       Codrut-PC:49876      ESTABLISHED
TCP   127.0.0.1:49999       Codrut-PC:9812       ESTABLISHED
TCP   127.0.0.1:50014       Codrut-PC:65001      ESTABLISHED
TCP   127.0.0.1:50030       Codrut-PC:50101      ESTABLISHED
TCP   127.0.0.1:50101       Codrut-PC:50030      ESTABLISHED
TCP   127.0.0.1:50162       Codrut-PC:9813       ESTABLISHED
TCP   127.0.0.1:56854       Codrut-PC:56855      ESTABLISHED
TCP   127.0.0.1:56855       Codrut-PC:56854      ESTABLISHED
TCP   127.0.0.1:56859       Codrut-PC:56860      ESTABLISHED
TCP   127.0.0.1:56860       Codrut-PC:56859      ESTABLISHED
TCP   127.0.0.1:57015       Codrut-PC:57016      ESTABLISHED
TCP   127.0.0.1:57016       Codrut-PC:57015      ESTABLISHED
TCP   127.0.0.1:57607       Codrut-PC:57608      ESTABLISHED
TCP   127.0.0.1:57608       Codrut-PC:57607      ESTABLISHED
TCP   127.0.0.1:57692       Codrut-PC:57693      ESTABLISHED
TCP   127.0.0.1:57693       Codrut-PC:57692      ESTABLISHED
TCP   127.0.0.1:65001       Codrut-PC:50014      ESTABLISHED
TCP   192.168.50.239:58685  51.105.249.228:https ESTABLISHED
TCP   192.168.50.239:58692  ec2-54-190-34-249:https ESTABLISHED
TCP   192.168.50.239:58696  136:http           ESTABLISHED
TCP   192.168.50.239:58706  51.105.249.228:https ESTABLISHED
TCP   192.168.50.239:58750  ec2-3-120-198-117:https ESTABLISHED
TCP   192.168.50.239:59957  53:https           ESTABLISHED
TCP   192.168.50.239:60094  do-1:https         ESTABLISHED
```

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.

```
C:\Users\Codrut Neagu>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Codrut-PC:0           LISTENING
  TCP    0.0.0.0:445            Codrut-PC:0           LISTENING
  TCP    0.0.0.0:902            Codrut-PC:0           LISTENING
  TCP    0.0.0.0:912            Codrut-PC:0           LISTENING
  TCP    0.0.0.0:5040           Codrut-PC:0           LISTENING
  TCP    0.0.0.0:5357           Codrut-PC:0           LISTENING
  TCP    0.0.0.0:7680           Codrut-PC:0           LISTENING
  TCP    0.0.0.0:9012           Codrut-PC:0           LISTENING
  TCP    0.0.0.0:9813           Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49664          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49665          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49666          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49667          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49670          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:49844          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:57621          Codrut-PC:0           LISTENING
  TCP    0.0.0.0:61688          Codrut-PC:0           LISTENING
  TCP    127.0.0.1:1042          Codrut-PC:0           LISTENING
  TCP    127.0.0.1:1043          Codrut-PC:0           LISTENING
  TCP    127.0.0.1:3213          Codrut-PC:0           LISTENING
  TCP    127.0.0.1:9012          Codrut-PC:49999         ESTABLISHED
  TCP    127.0.0.1:9013          Codrut-PC:50162         ESTABLISHED
  TCP    127.0.0.1:9487          Codrut-PC:0           LISTENING
  TCP    127.0.0.1:9487          Codrut-PC:49815         ESTABLISHED
  TCP    127.0.0.1:13010         Codrut-PC:0           LISTENING
  TCP    127.0.0.1:13030         Codrut-PC:0           LISTENING
  TCP    127.0.0.1:17945         Codrut-PC:0           LISTENING
  TCP    127.0.0.1:49815         Codrut-PC:9487          ESTABLISHED
  TCP    127.0.0.1:49856         Codrut-PC:49857         ESTABLISHED
  TCP    127.0.0.1:49857         Codrut-PC:49856         ESTABLISHED
  TCP    127.0.0.1:49860         Codrut-PC:49861         ESTABLISHED
  TCP    127.0.0.1:49861         Codrut-PC:49860         ESTABLISHED
  TCP    127.0.0.1:49870         Codrut-PC:49871         ESTABLISHED
  TCP    127.0.0.1:49871         Codrut-PC:49870         ESTABLISHED
  TCP    127.0.0.1:49872         Codrut-PC:49873         ESTABLISHED
  TCP    127.0.0.1:49873         Codrut-PC:49872         ESTABLISHED
  TCP    127.0.0.1:49876         Codrut-PC:49877         ESTABLISHED
  TCP    127.0.0.1:49877         Codrut-PC:49876         ESTABLISHED
  TCP    127.0.0.1:49999         Codrut-PC:9012          ESTABLISHED
  TCP    127.0.0.1:50014         Codrut-PC:65001          ESTABLISHED
  TCP    127.0.0.1:50030         Codrut-PC:0             LISTENING
  TCP    127.0.0.1:50030         Codrut-PC:50101          ESTABLISHED
  TCP    127.0.0.1:50101         Codrut-PC:50030          ESTABLISHED
  TCP    127.0.0.1:50162         Codrut-PC:9013          ESTABLISHED
  TCP    127.0.0.1:56854         Codrut-PC:56855          ESTABLISHED
  TCP    127.0.0.1:56855         Codrut-PC:56854          ESTABLISHED
  TCP    127.0.0.1:56859         Codrut-PC:56860          ESTABLISHED
  TCP    127.0.0.1:56860         Codrut-PC:56859          ESTABLISHED
  TCP    127.0.0.1:57015         Codrut-PC:57816          ESTABLISHED
  TCP    127.0.0.1:57816         Codrut-PC:57815          ESTABLISHED
  TCP    127.0.0.1:57607         Codrut-PC:57608          ESTABLISHED
  TCP    127.0.0.1:57608         Codrut-PC:57607          ESTABLISHED
  TCP    127.0.0.1:57692         Codrut-PC:57693          ESTABLISHED
  TCP    127.0.0.1:57693         Codrut-PC:57692          ESTABLISHED
  TCP    127.0.0.1:65001         Codrut-PC:0             LISTENING
  TCP    127.0.0.1:65001         Codrut-PC:50014          ESTABLISHED
  TCP    192.168.58.239:139      Codrut-PC:0             LISTENING
  TCP    192.168.58.239:58685     51.105.249.228:https   ESTABLISHED
```

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.

```
Command Prompt  
C:\Users\Codrut Neagu>arp -a  
  
Interface: 192.168.50.239 --- 0x14  
Internet Address Physical Address Type  
192.168.50.1 04-d9-f5-b5-b1-f0 dynamic  
192.168.50.4 90-94-97-c6-42-62 dynamic  
192.168.50.60 ac-e4-b5-e0-5c-57 dynamic  
192.168.50.96 00-28-f8-3c-eb-5a dynamic  
192.168.50.169 54-25-ea-a0-0a-51 dynamic  
192.168.50.205 04-d9-f5-b5-dd-10 dynamic  
192.168.50.247 b0-6e-bf-10-d1-62 dynamic  
192.168.50.255 ff-ff-ff-ff-ff-ff static  
224.0.0.22 01-00-5e-00-00-16 static  
224.0.0.251 01-00-5e-00-00-fb static  
224.0.0.252 01-00-5e-00-00-fc static  
239.255.255.250 01-00-5e-7f-ff-fa static  
255.255.255.255 ff-ff-ff-ff-ff-ff static  
  
C:\Users\Codrut Neagu>
```

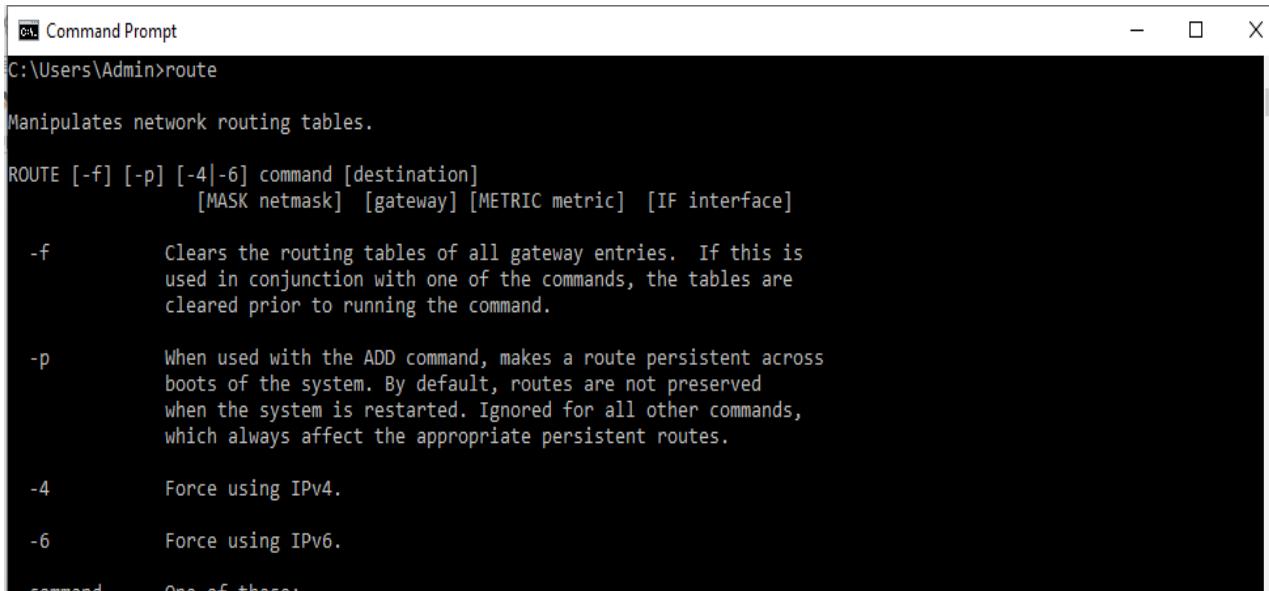
```
C:\WINDOWS\system32\cmd.exe  
  
C:\Users\Brien>arp -a 147.100.100.151  
  
Interface: 147.100.100.224 --- 0x2  
Internet Address Physical Address Type  
147.100.100.151 68-05-ca-19-1c-d2 dynamic  
  
C:\Users\Brien>
```

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.



```
Command Prompt
C:\Users\Admin>route
Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
      [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f           Clears the routing tables of all gateway entries. If this is
            used in conjunction with one of the commands, the tables are
            cleared prior to running the command.

-p           When used with the ADD command, makes a route persistent across
            boots of the system. By default, routes are not preserved
            when the system is restarted. Ignored for all other commands,
            which always affect the appropriate persistent routes.

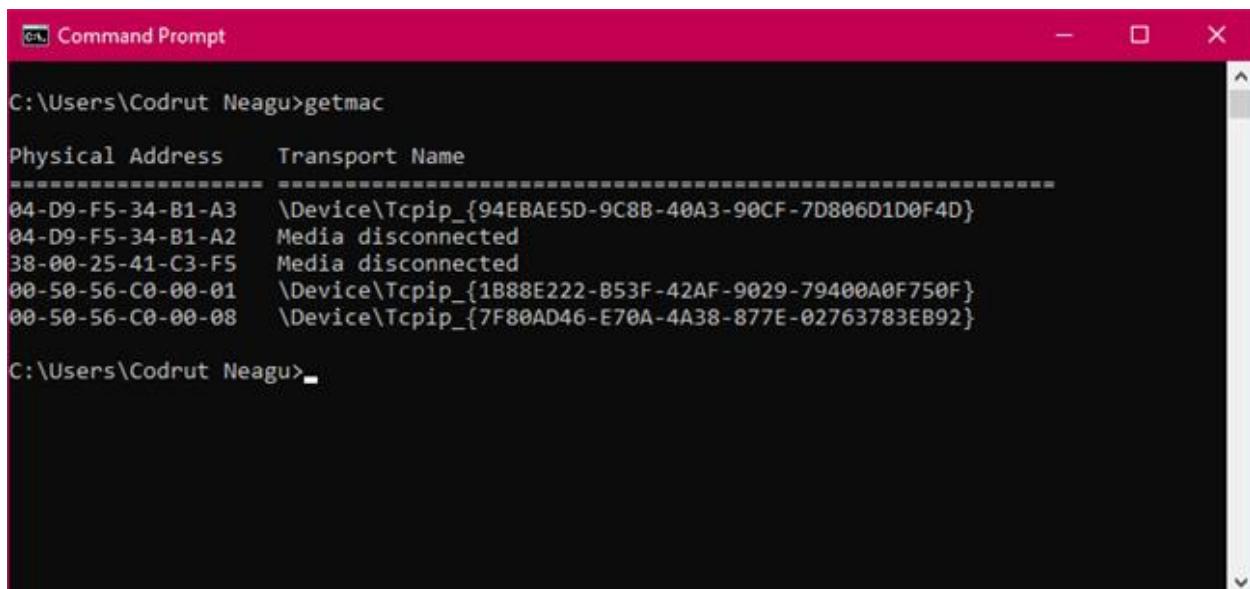
-4           Force using IPv4.

-6           Force using IPv6.

command      One of these:
```

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.



```
Command Prompt
C:\Users\Codrut Neagu>getmac

Physical Address      Transport Name
-----
04-D9-F5-34-B1-A3    \Device\Tcpip_{94EBAE5D-9C8B-40A3-90CF-7D806D1D0F4D}
04-D9-F5-34-B1-A2    Media disconnected
38-00-25-41-C3-F5    Media disconnected
00-50-56-C0-00-01    \Device\Tcpip_{1B88E222-B53F-42AF-9029-79400A0F750F}
00-50-56-C0-00-08    \Device\Tcpip_{7F80AD46-E70A-4A38-877E-02763783EB92}

C:\Users\Codrut Neagu>
```

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

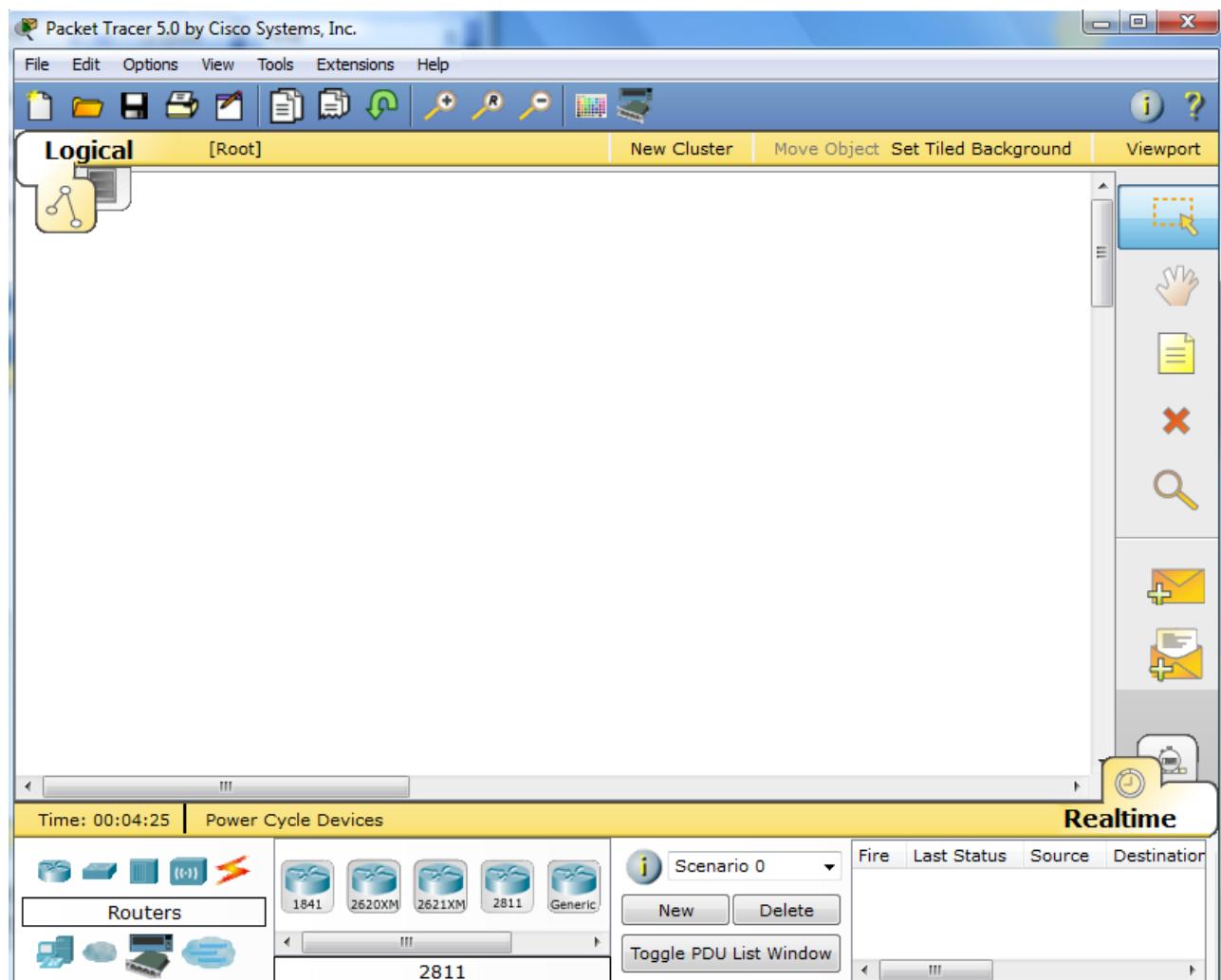
Packet Tracer – Creating a New Topology

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

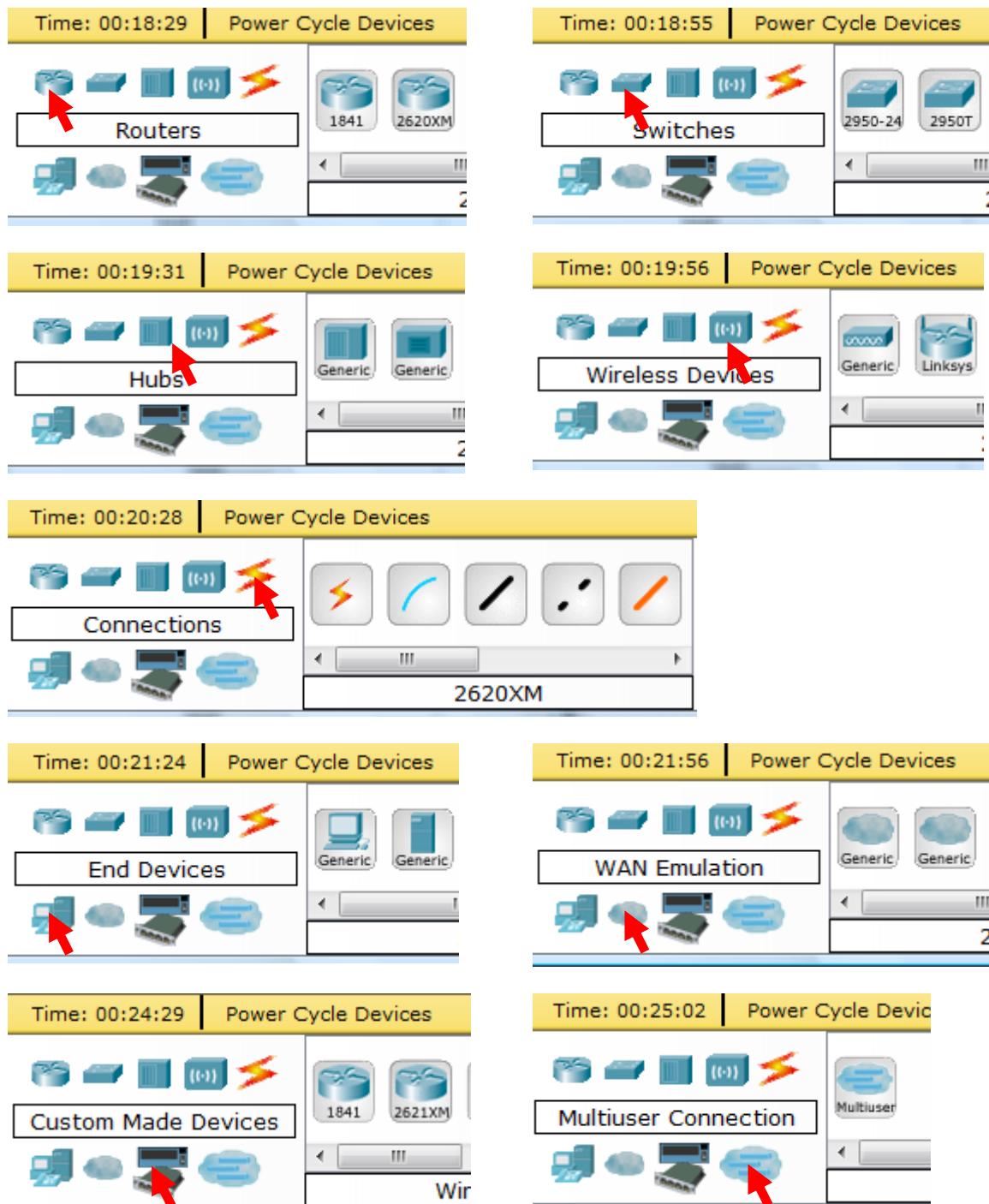
Step 1: Start Packet Tracer



Step 2: Choosing Devices and Connections

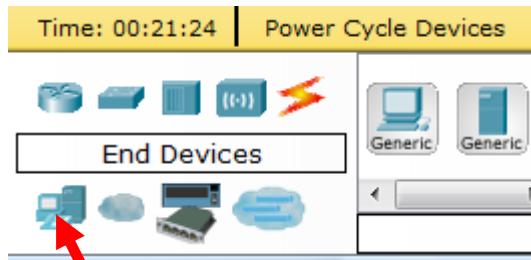
We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using **End Devices**, **Switches**, **Hubs**, and **Connections**.

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

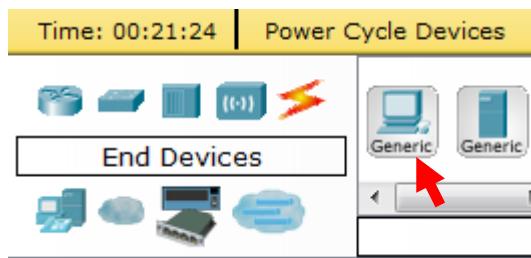


Step 3: Building the Topology – Adding Hosts

Single click on the **End Devices**.



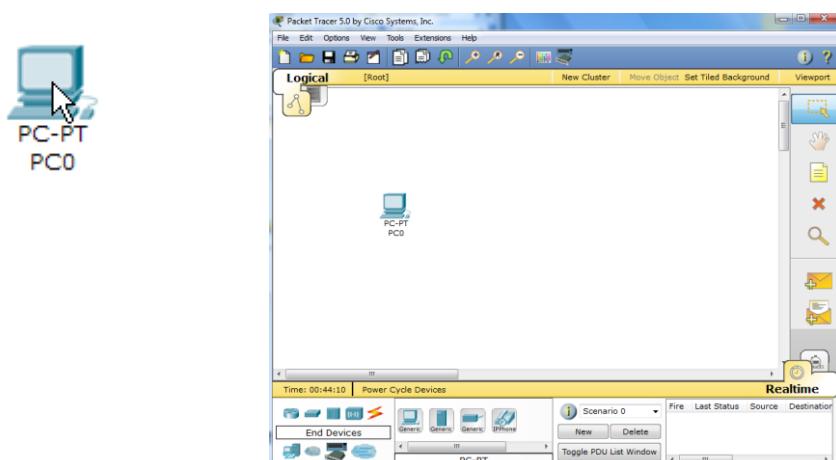
Single click on the **Generic** host.



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.



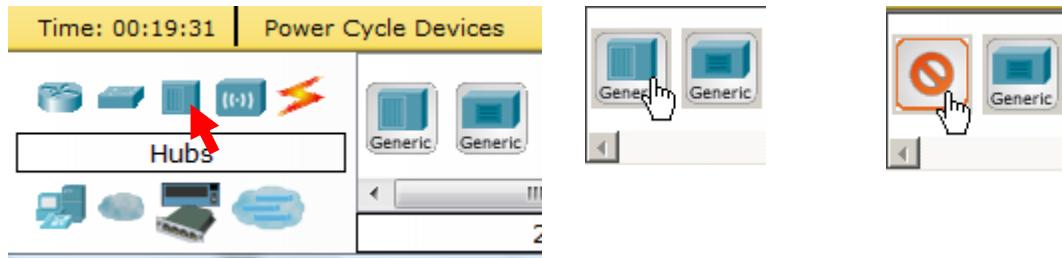
Add three more hosts.



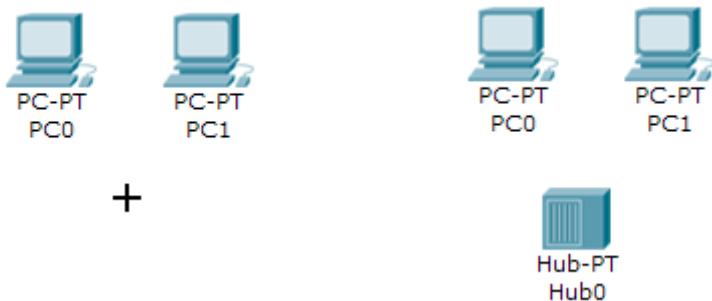
Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

Adding a Hub

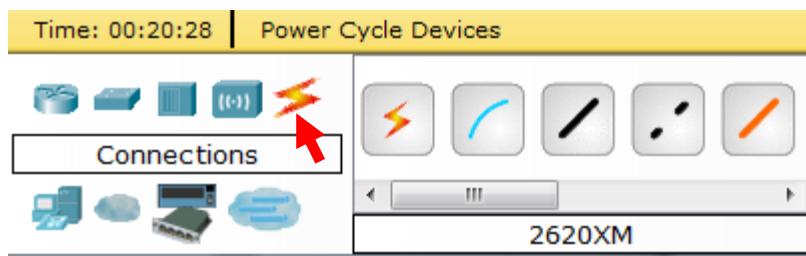
Select a hub, by clicking once on **Hubs** and once on a **Generic** hub.



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



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



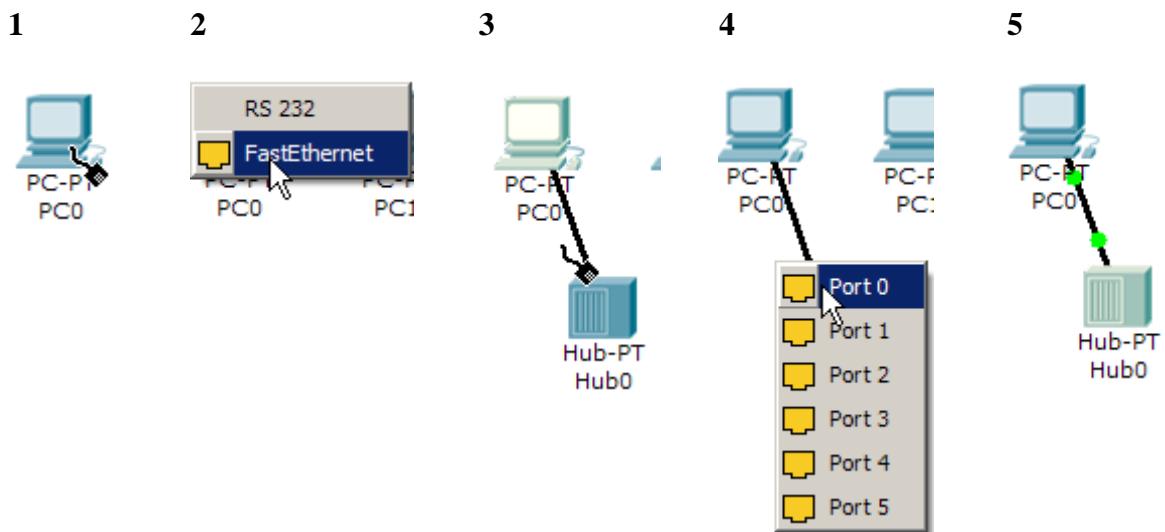
Click once on the **Copper Straight-through** cable.



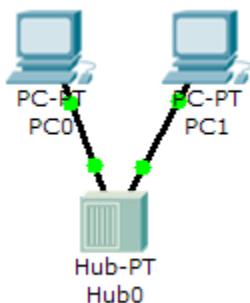
Perform the following steps to connect **PC0** to **Hub0**:

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.

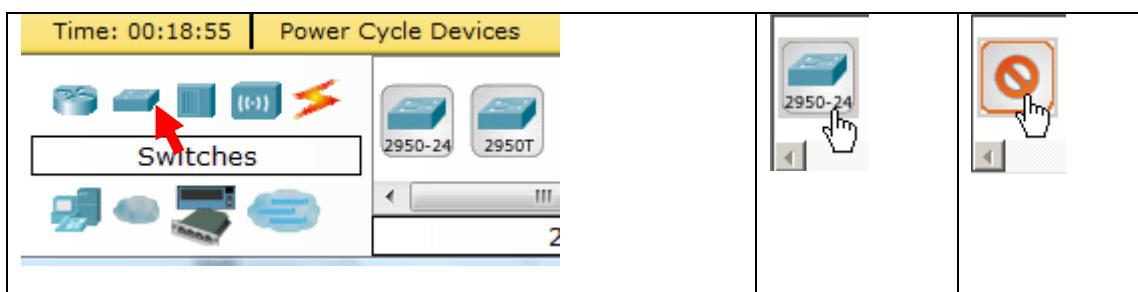


Repeat the steps above for **PC1** connecting it to **Port 1** on **Hub0**. (The actual hub port you choose does not matter.)

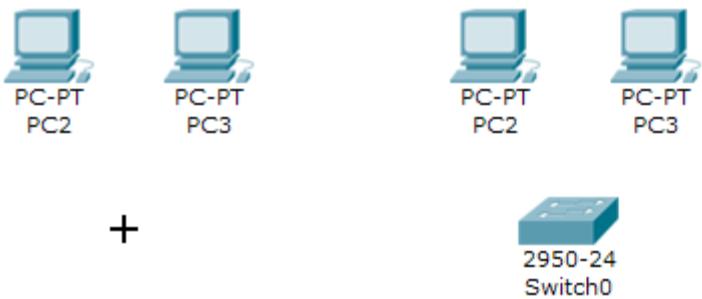


Adding a Switch

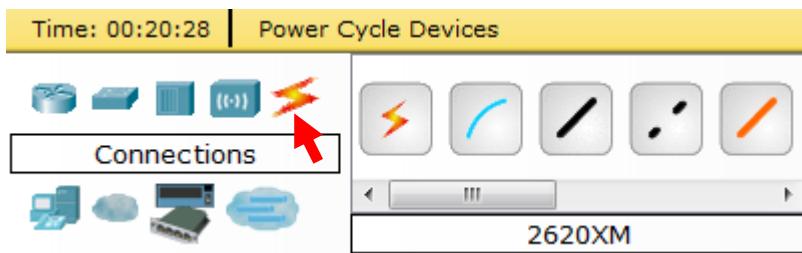
Select a switch, by clicking once on **Switches** and once on a **2950-24** switch.



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 about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now be forwarded out the switch port.

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

1

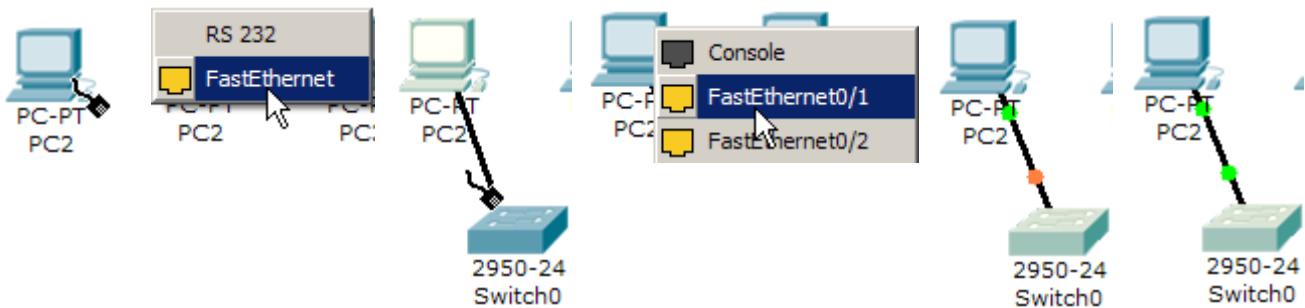
2

3

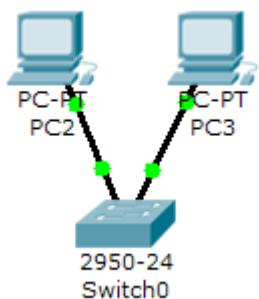
4

5

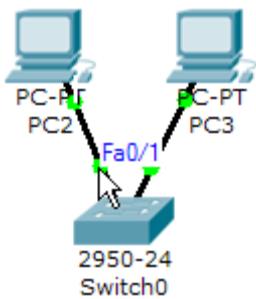
6



Repeat the steps above for **PC3** connecting it to **Port 3** on **Switch0** on port **FastEthernet0/2**. (The actual switch port you choose does not matter.)



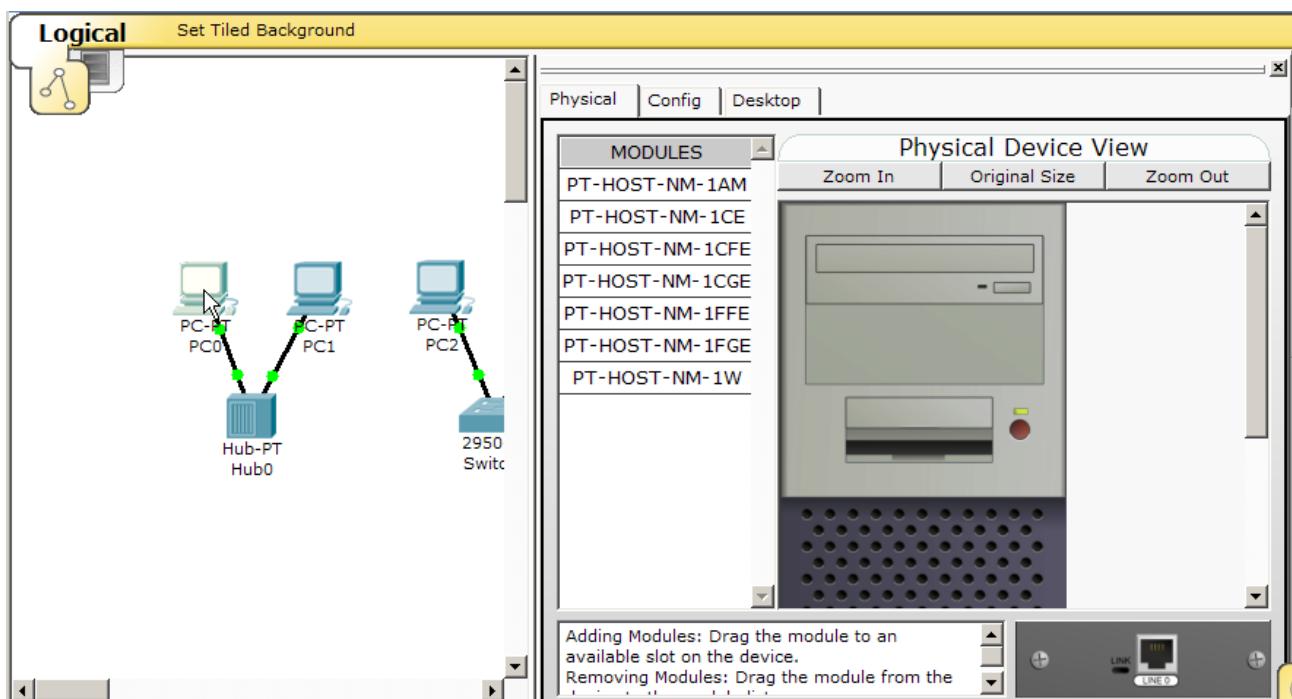
Move the cursor over the link light to view the port number. **Fa** means FastEthernet, 100 Mbps Ethernet.



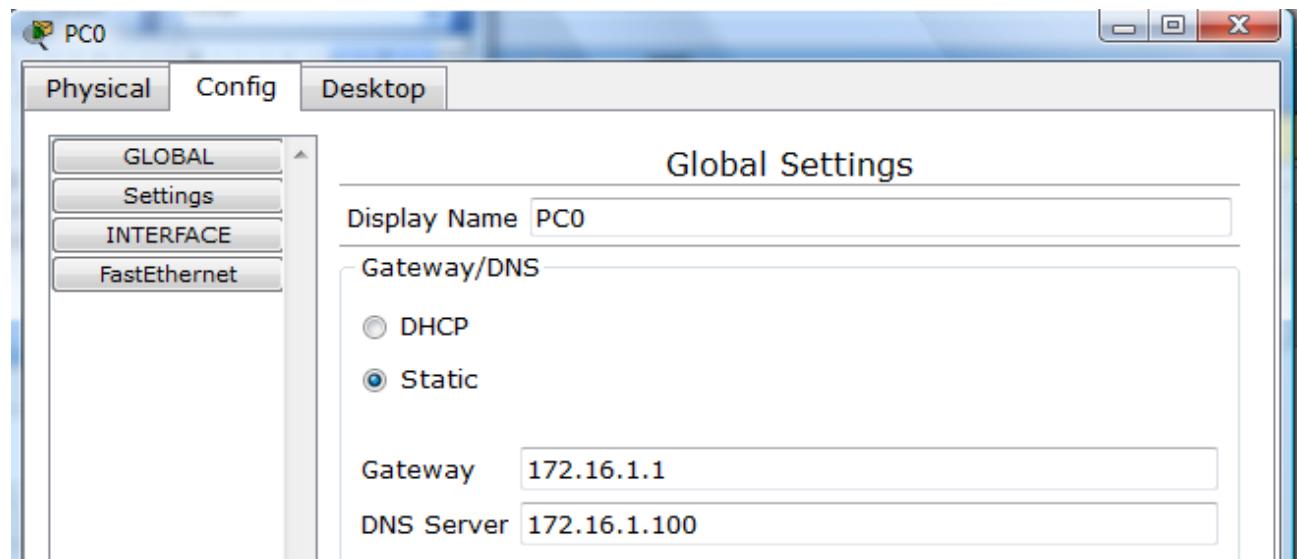
Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

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

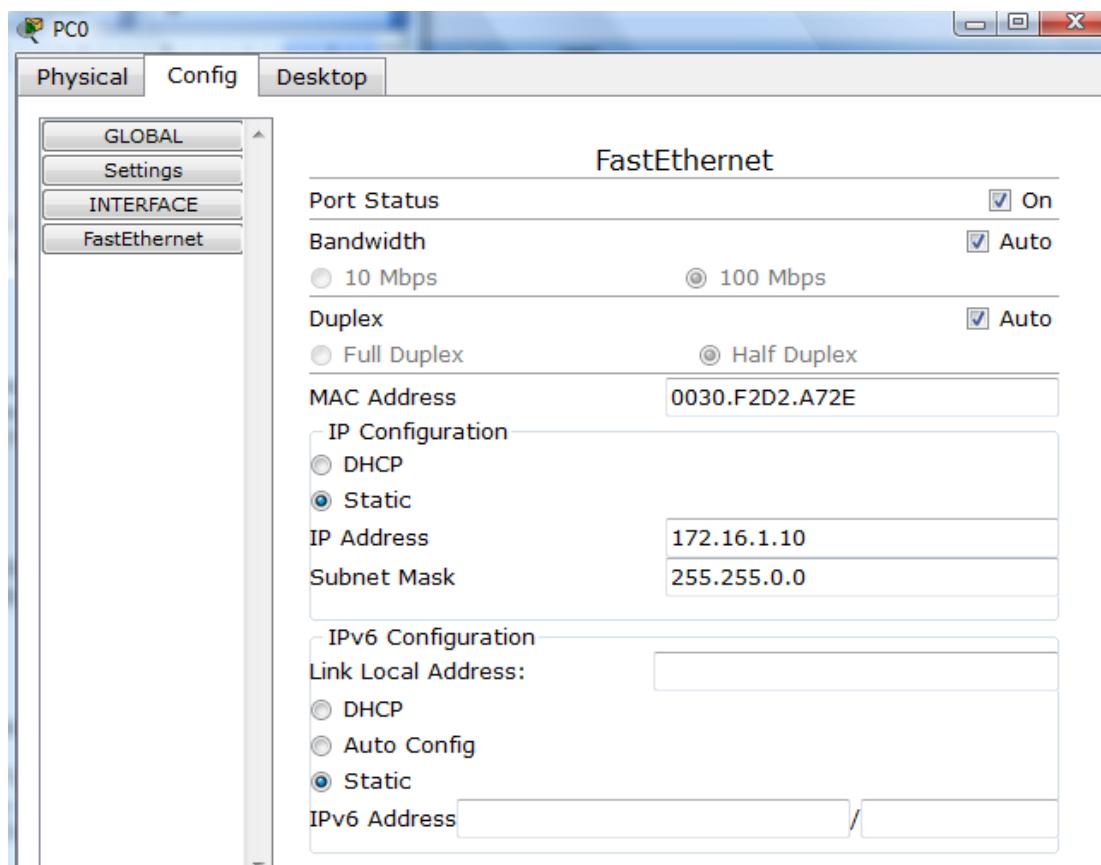
Click once on PC0.



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.

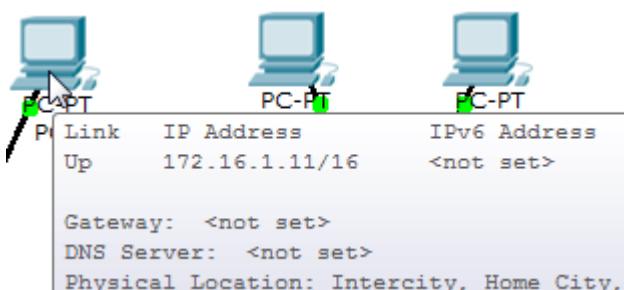


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

<u>Host</u>	<u>IP Address</u>	<u>Subnet Mask</u>
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.



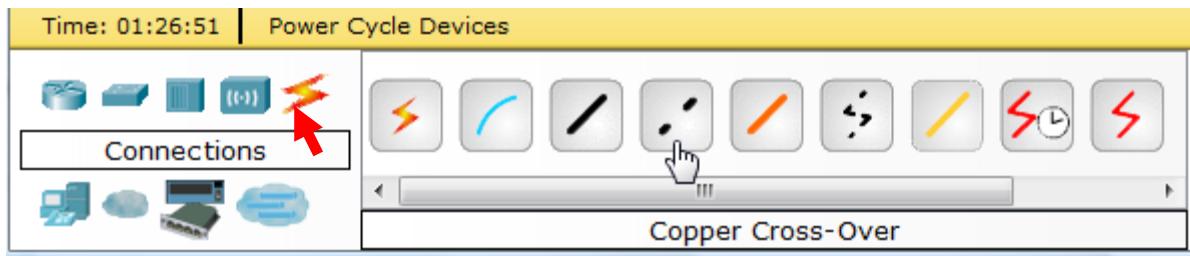
Deleting a Device or Link

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

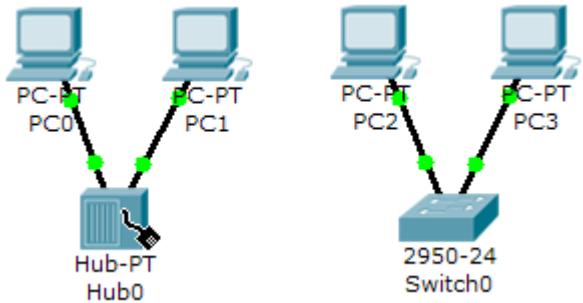


Step 6: Connecting Hub0 to Switch0

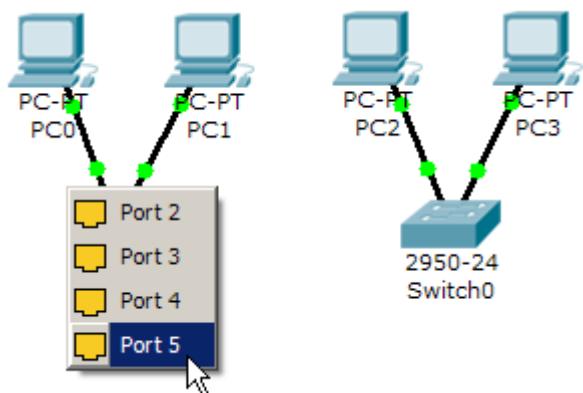
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the **Cross-over** Cable from the **Connections** options.



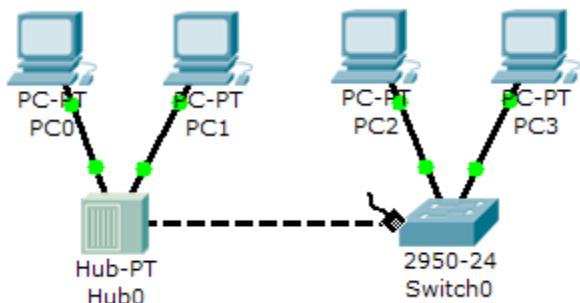
Move the Connections cursor over **Hub0** and click once.



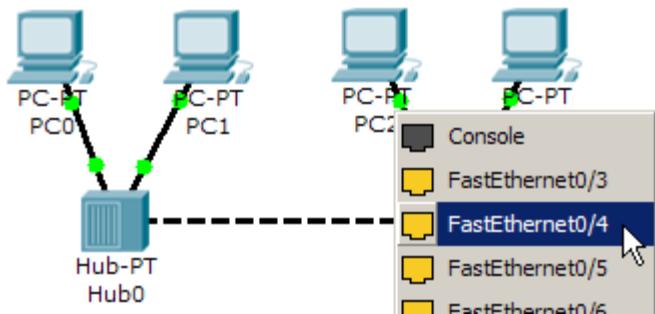
Select **Port 5** (actual port does not matter).



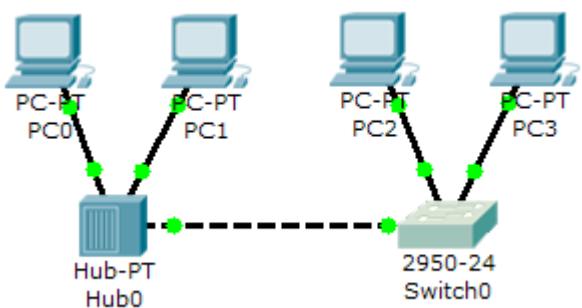
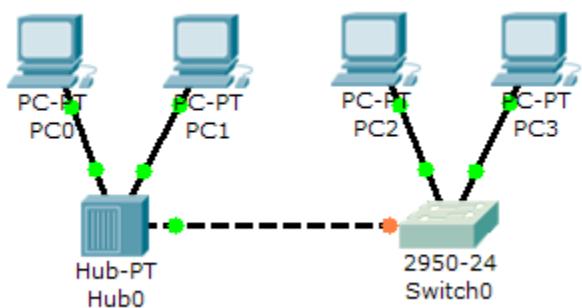
Move the Connections cursor to **Switch0**.



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

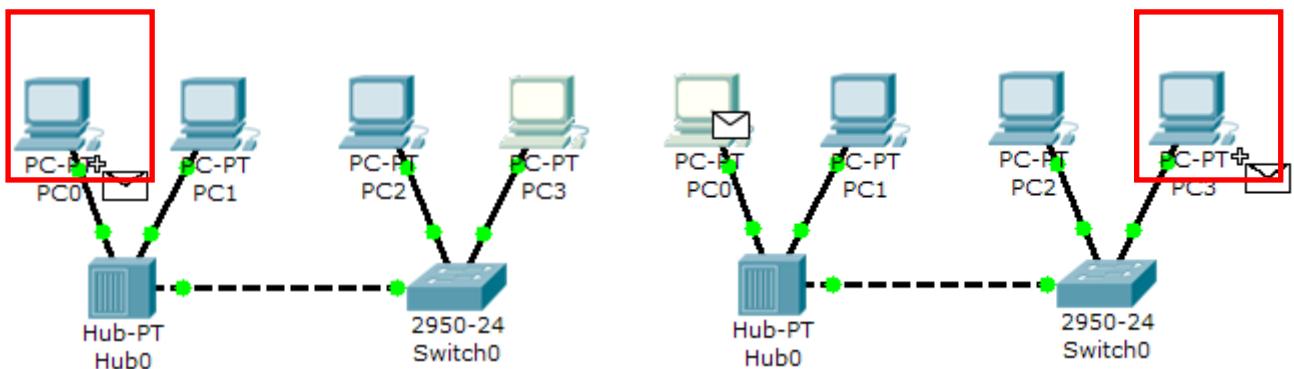
Be sure you are in **Realtime** mode.



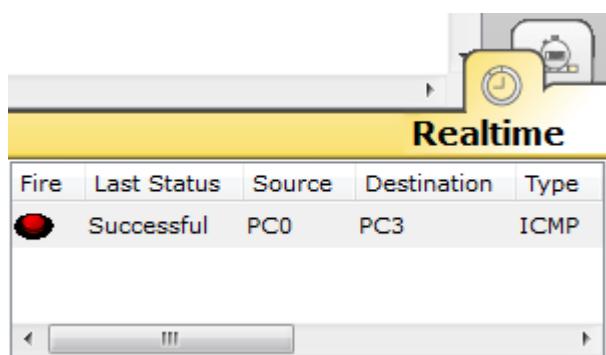
Select the **Add Simple PDU** tool used to ping devices..



Click once on PC0, then once on PC3.



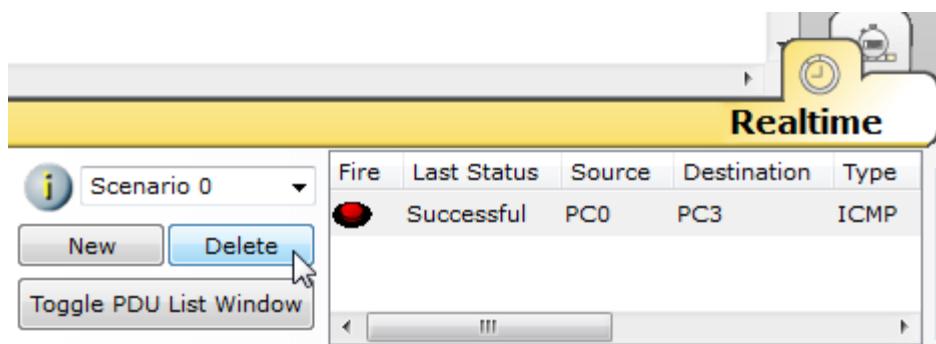
The PDU Last Status should show as **Successful**.



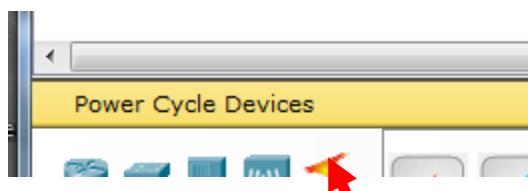
Resetting the Network

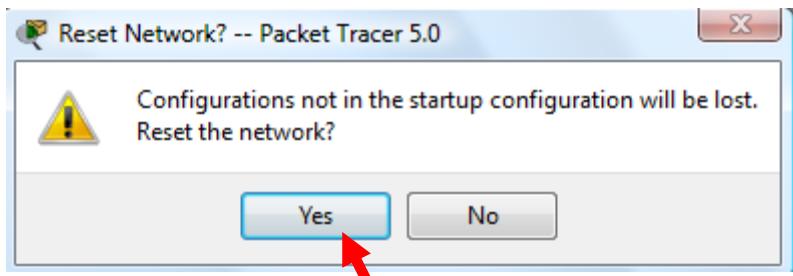
At this point we will want to reset the network. Whenever you want to reset the network and begin the simulation again, perform the following tasks:

Click **Delete** in the PDU area.



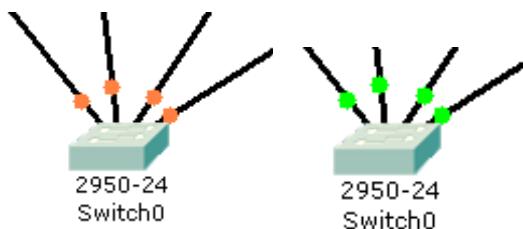
Now, Power Cycle Devices and confirm the action.





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.

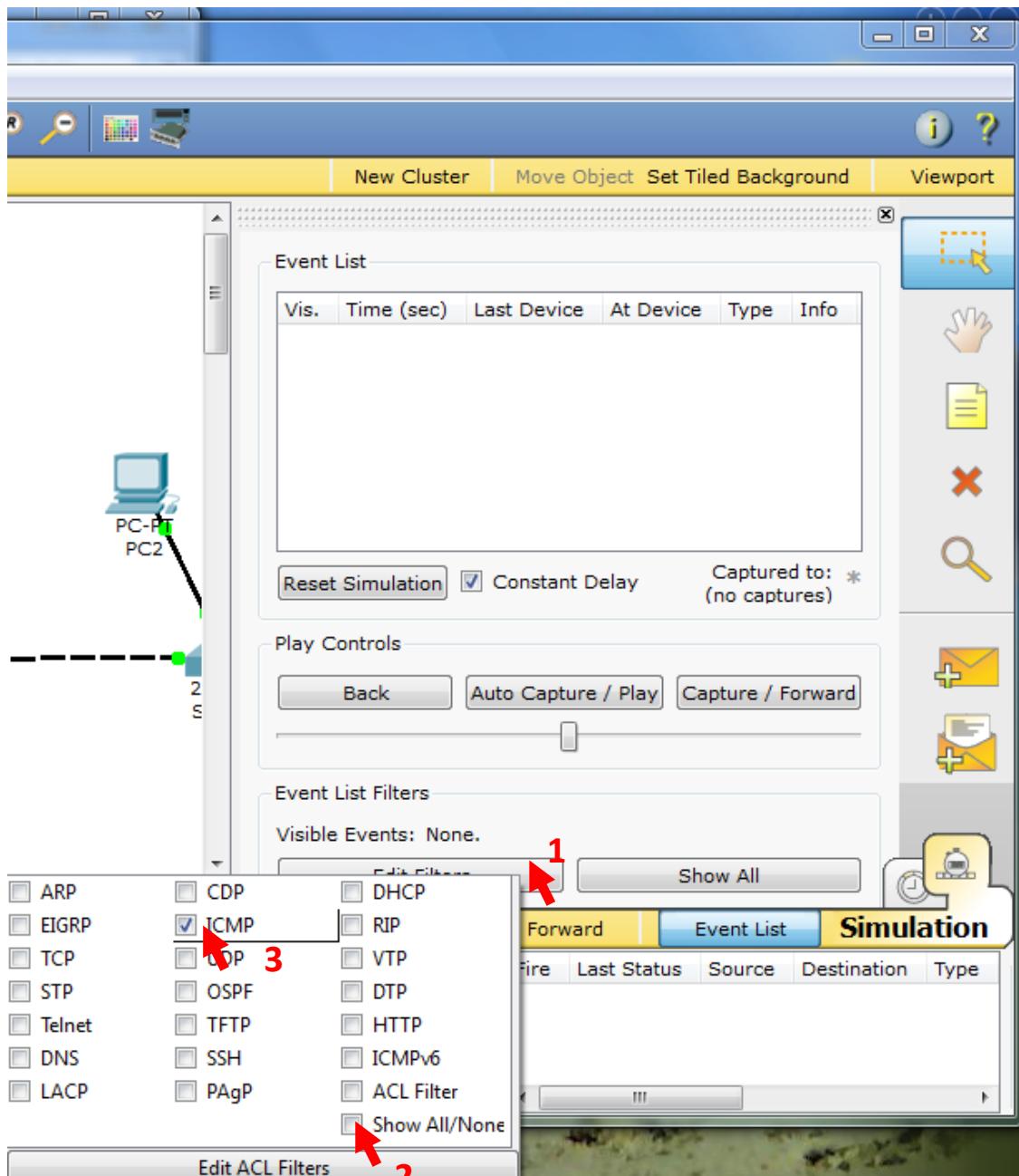


Step 8: Verifying Connectivity in Simulation Mode

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



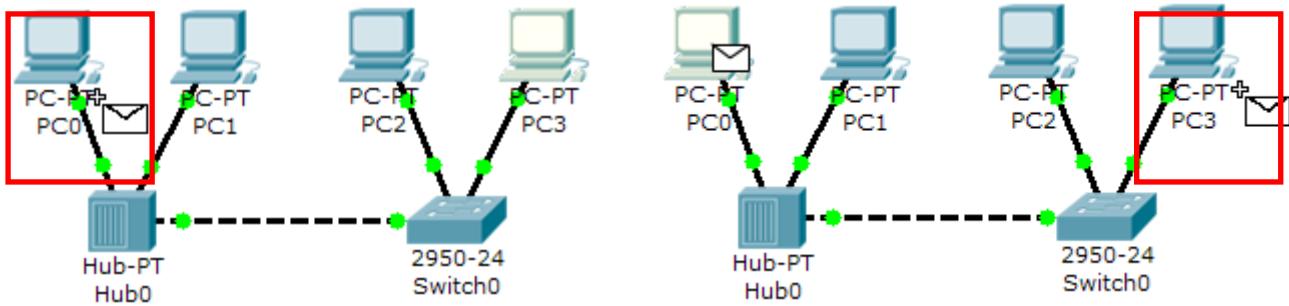
Deselect all filters (All/None) and select only **ICMP**.



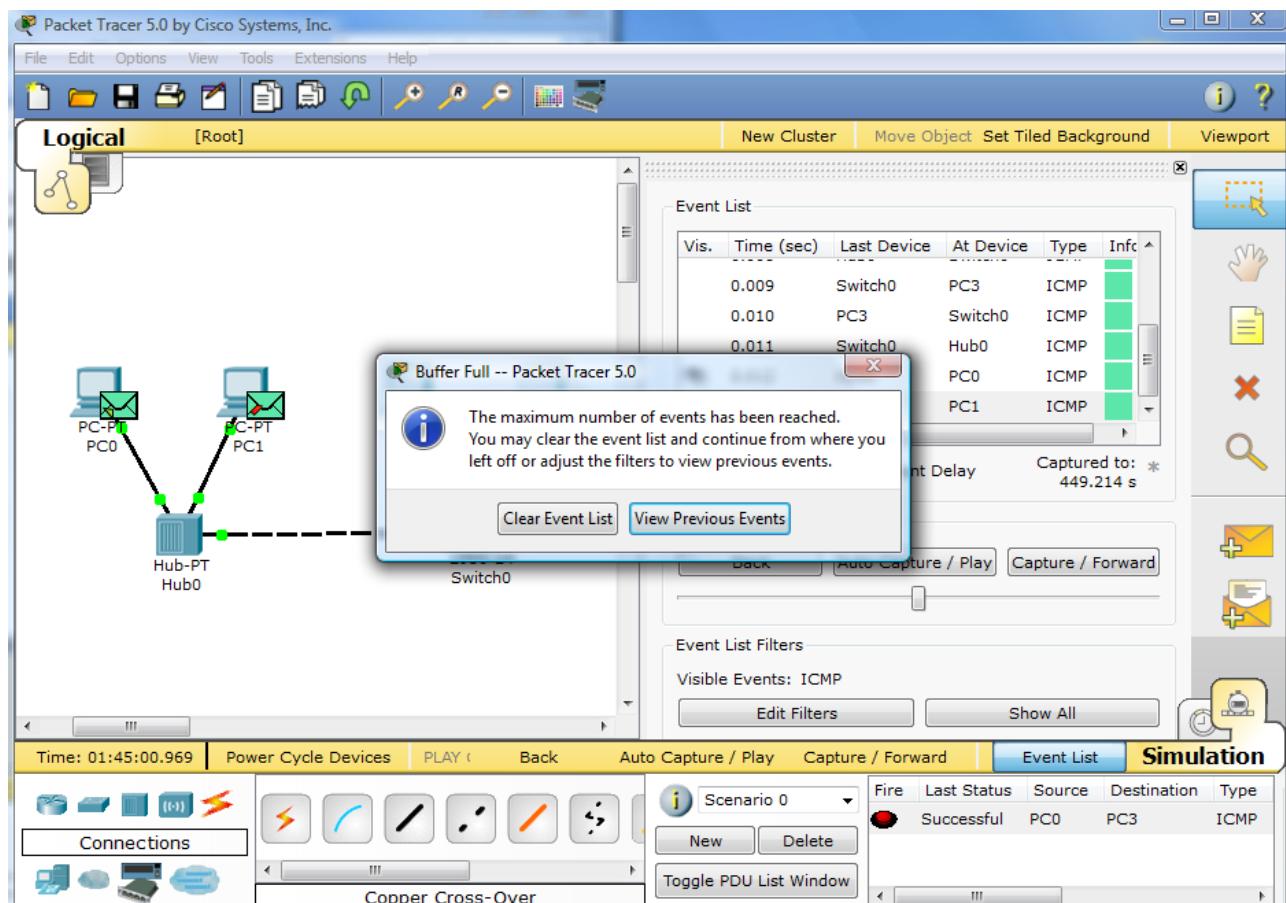
Select the **Add Simple PDU** tool used to ping devices..



Click once on PC0, then once on PC3.

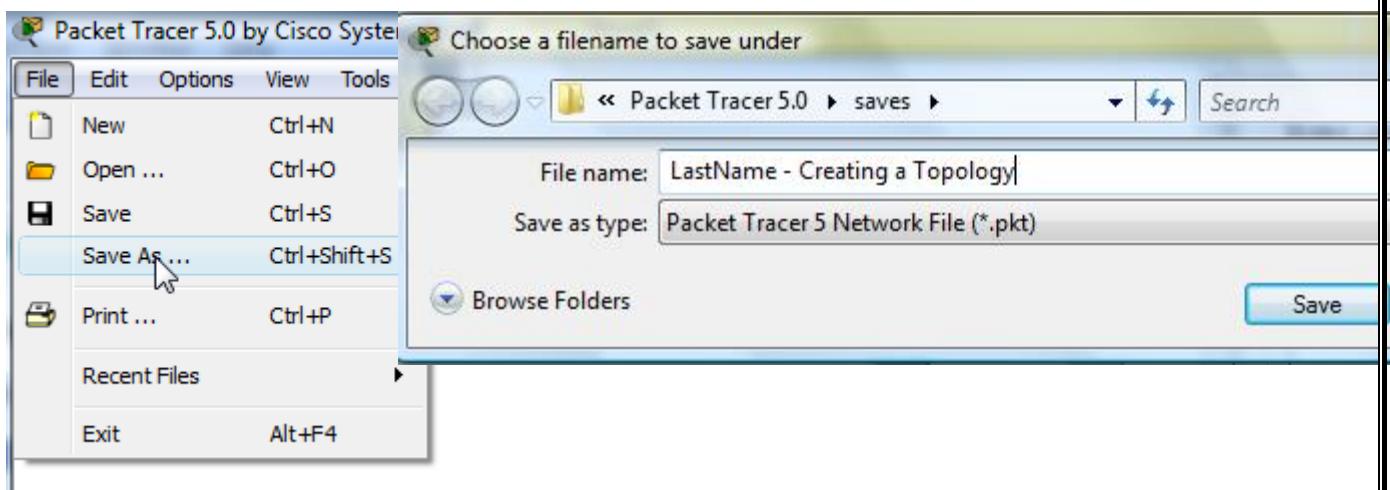


Continue clicking **Capture/Forward** button until the ICMP ping is completed. You should see the ICMP messages move between the hosts, hub and switch. The PDU **Last Status** should show as **Successful**. Click on **Clear Event List** if you do not want to look at the events or click **Preview Previous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

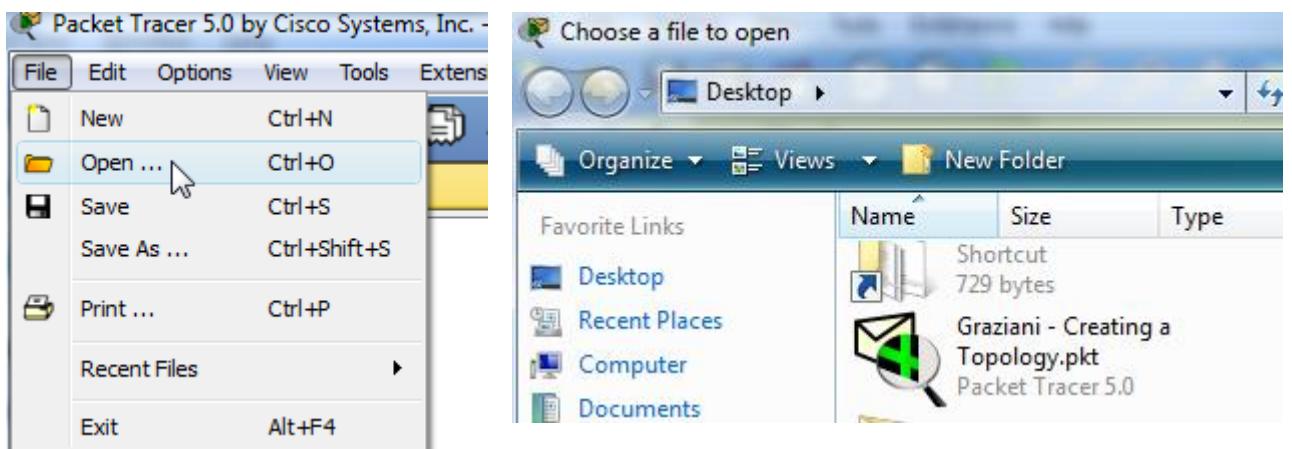


Step 9: Saving the Topology

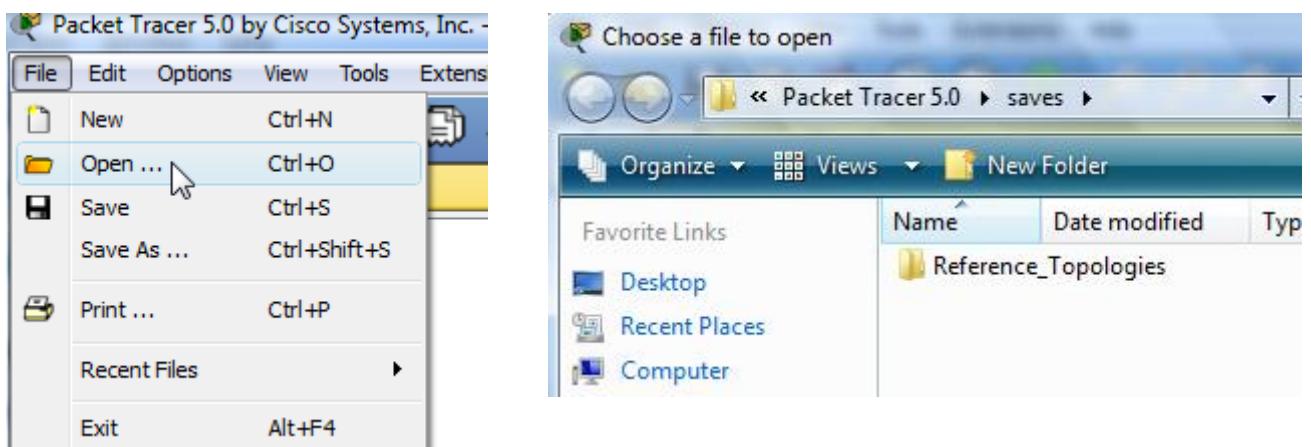
Perform the following steps to save the topology (uses .pkt file extension).

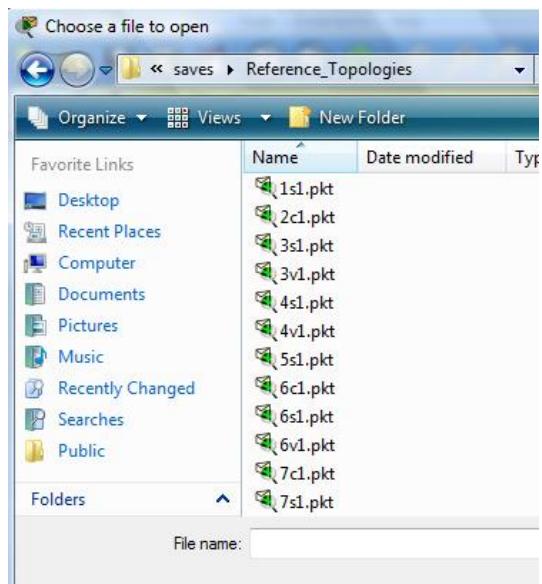


Opening Existing Topologies



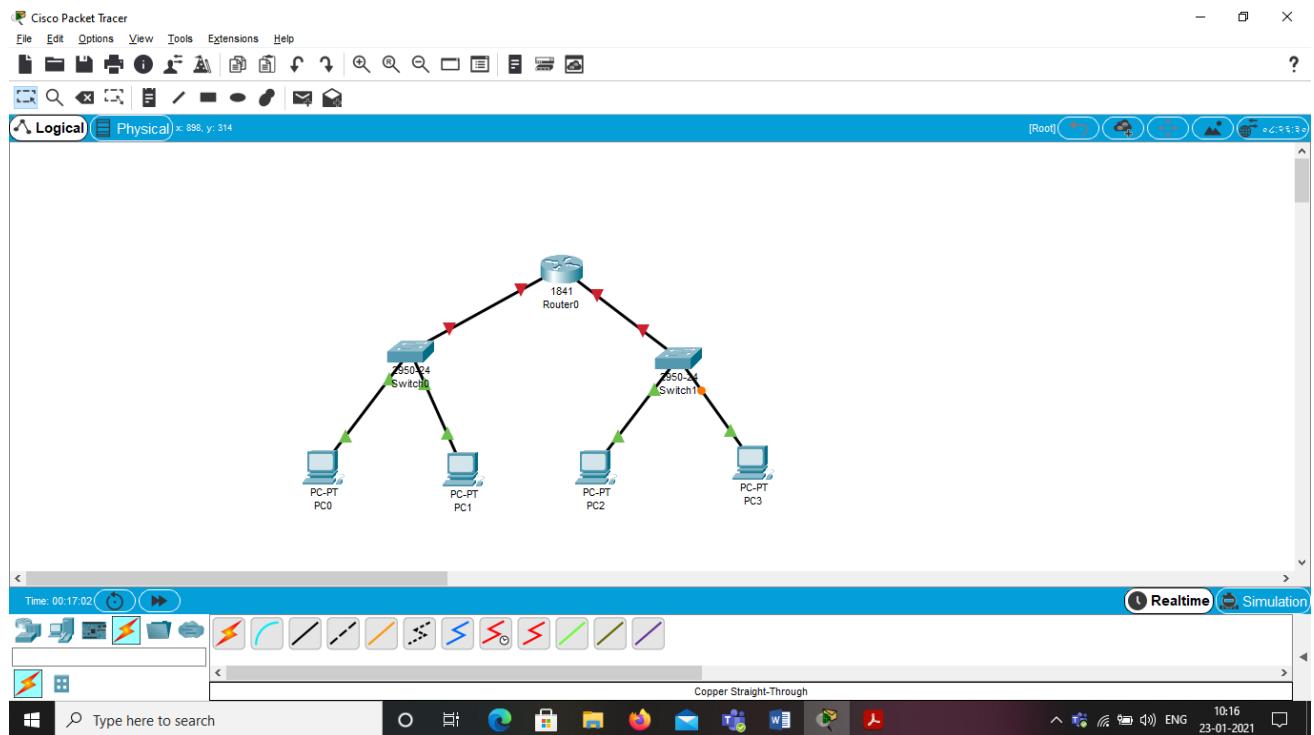
Opening Existing PT Topologies



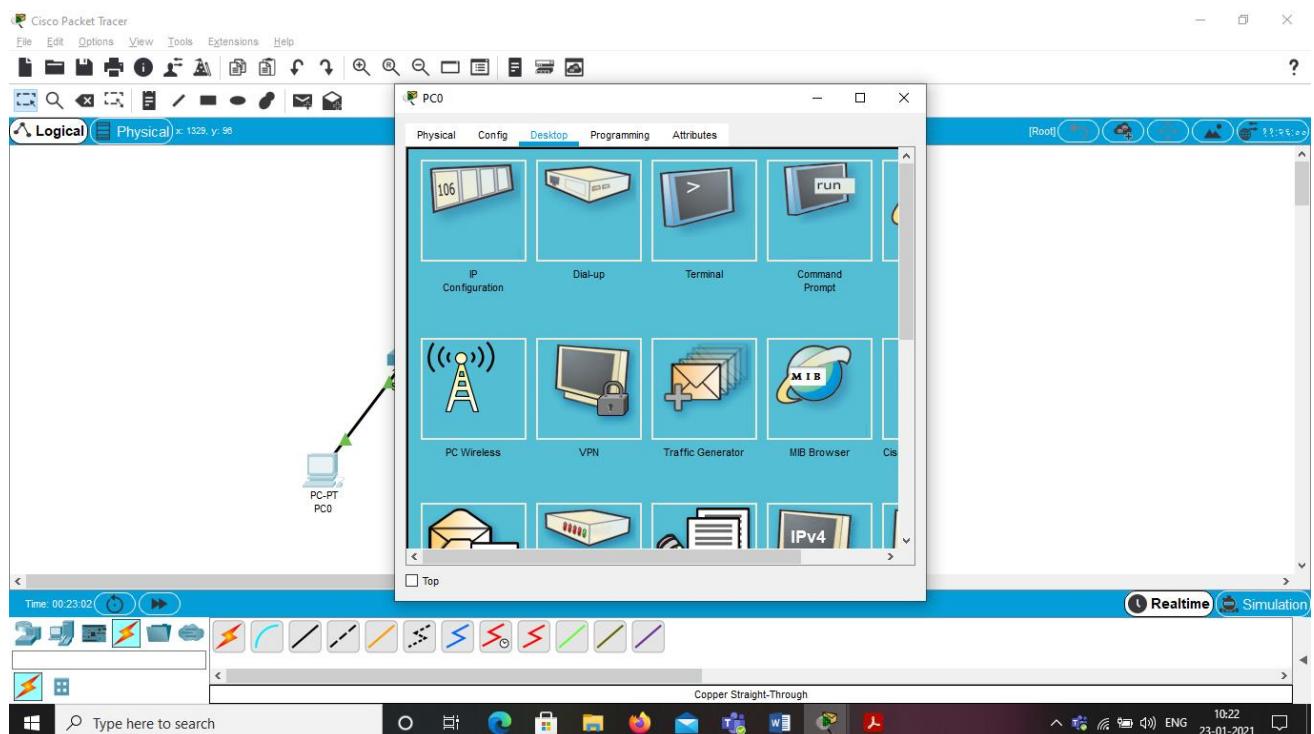


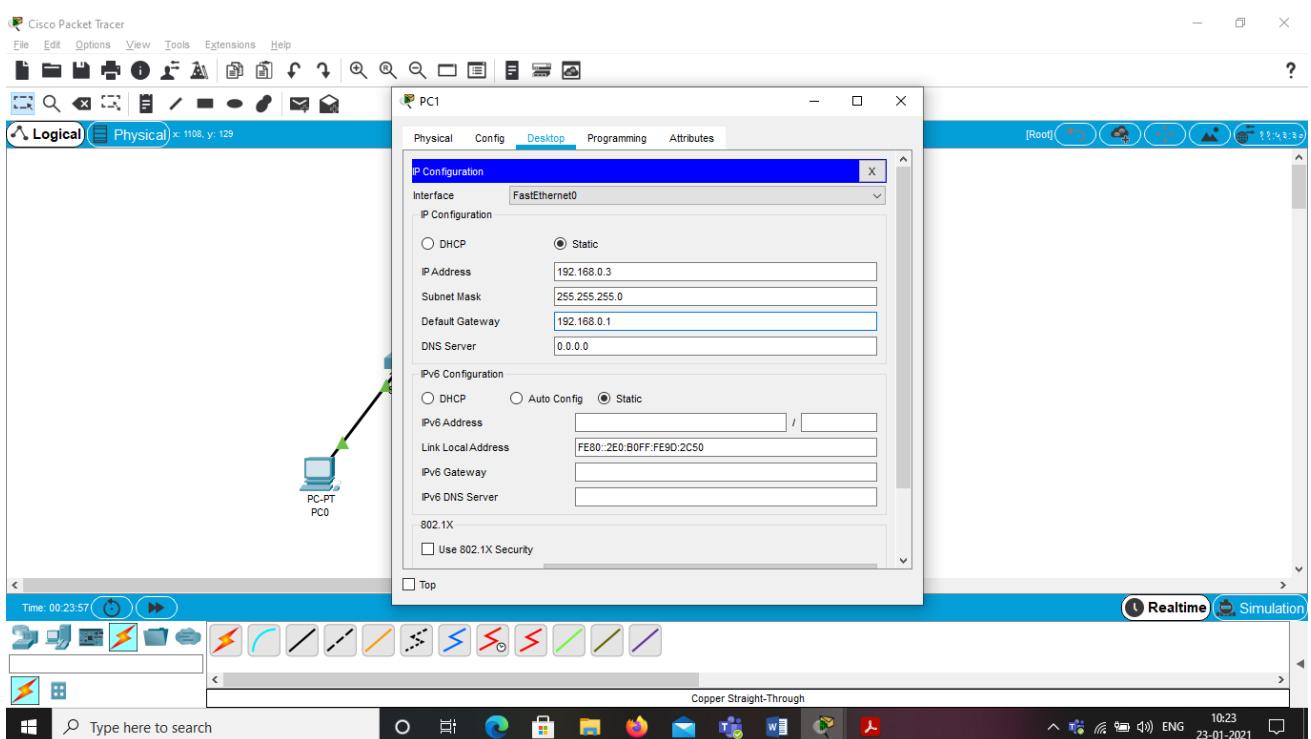
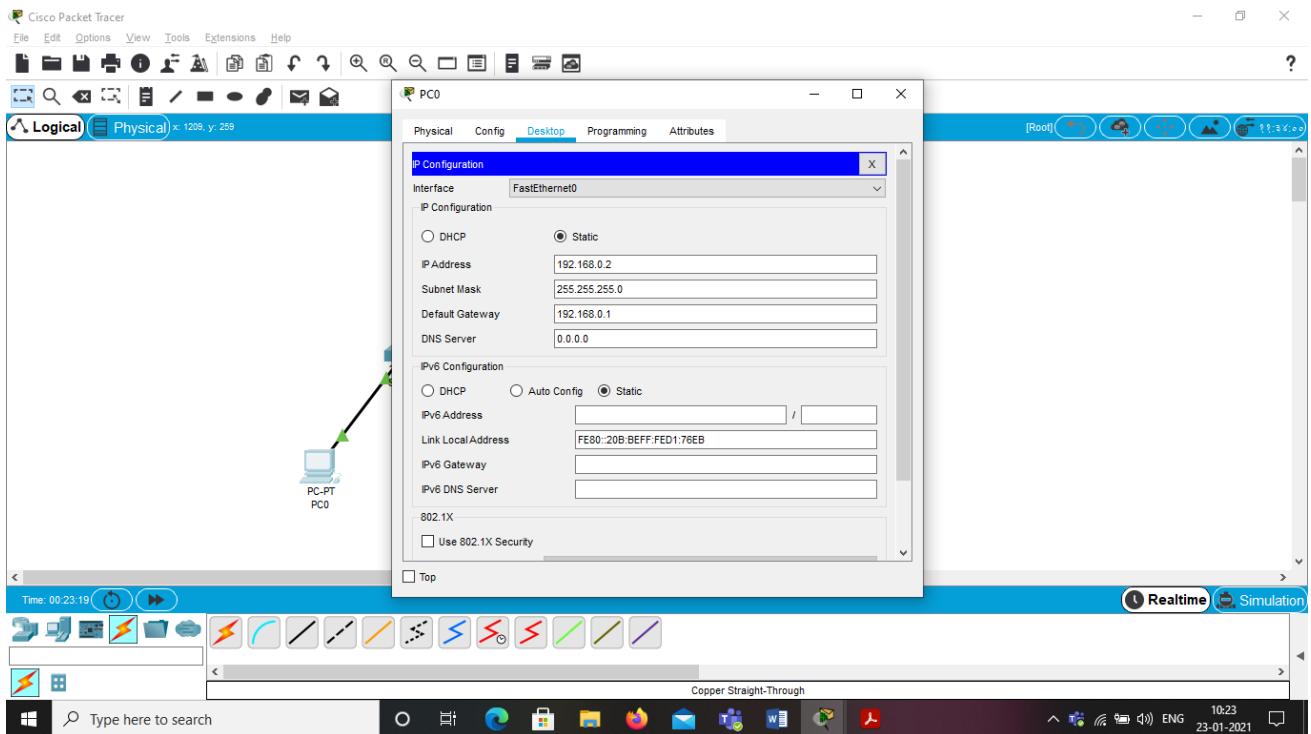
Exp 1: Configuration of Router using cisco packet tracer

Step 1: Construct the topology

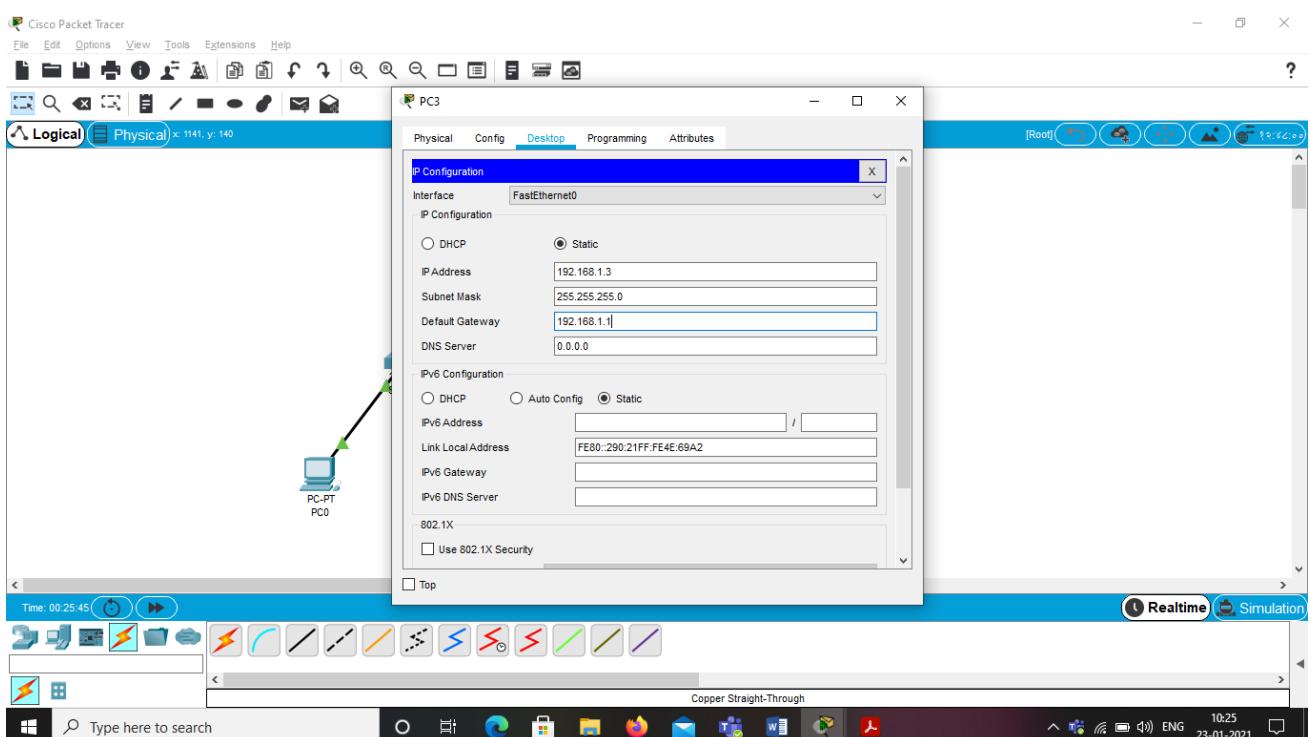
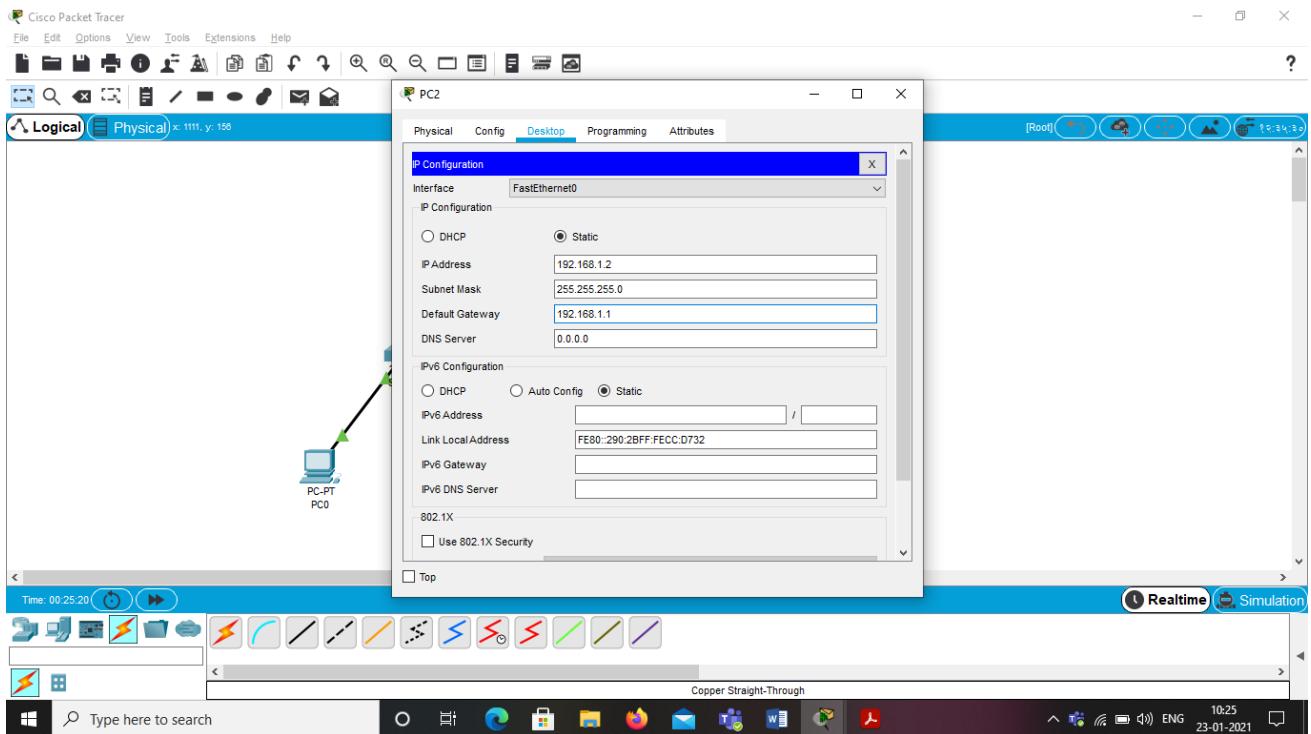


Step 2: Assign IP addresses to all PC's.



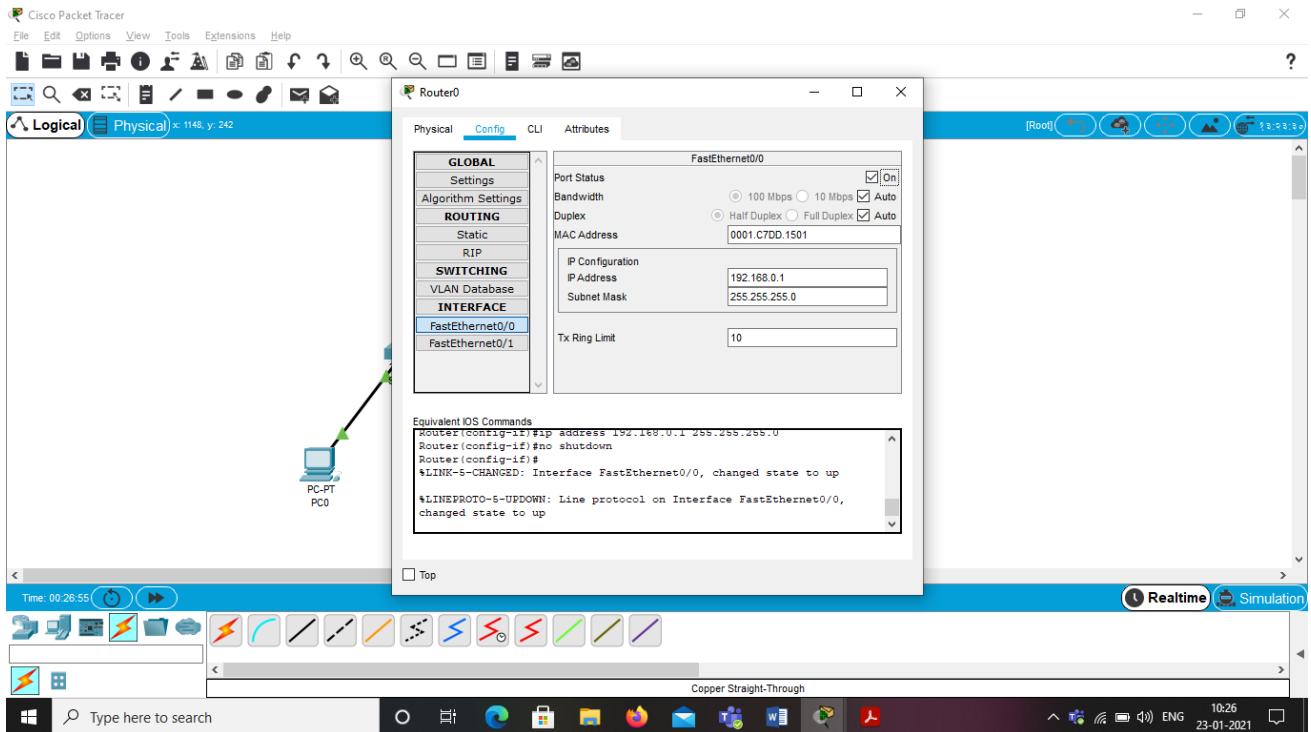


Use another network address for second network.

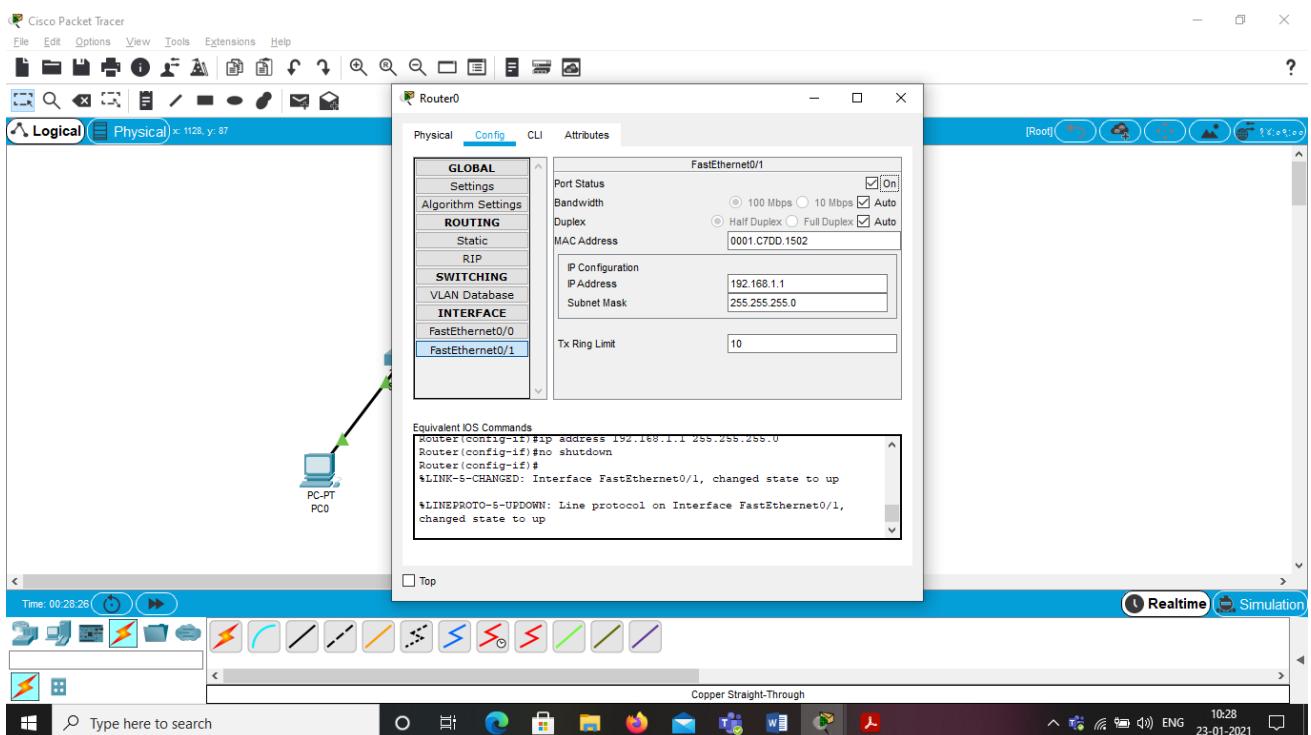


Step 3: Assign the IP address for router

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

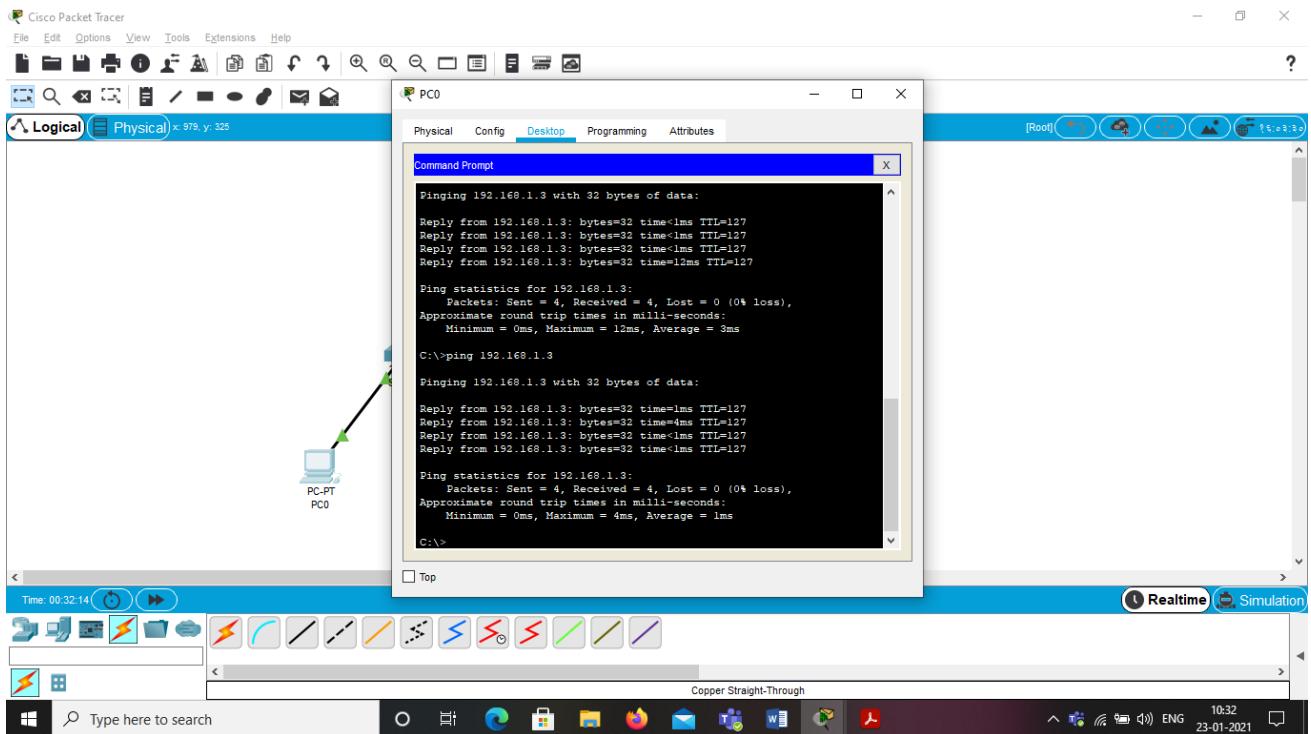


Assign the gateway address of 2nd network for FastEthernet0/1 interface

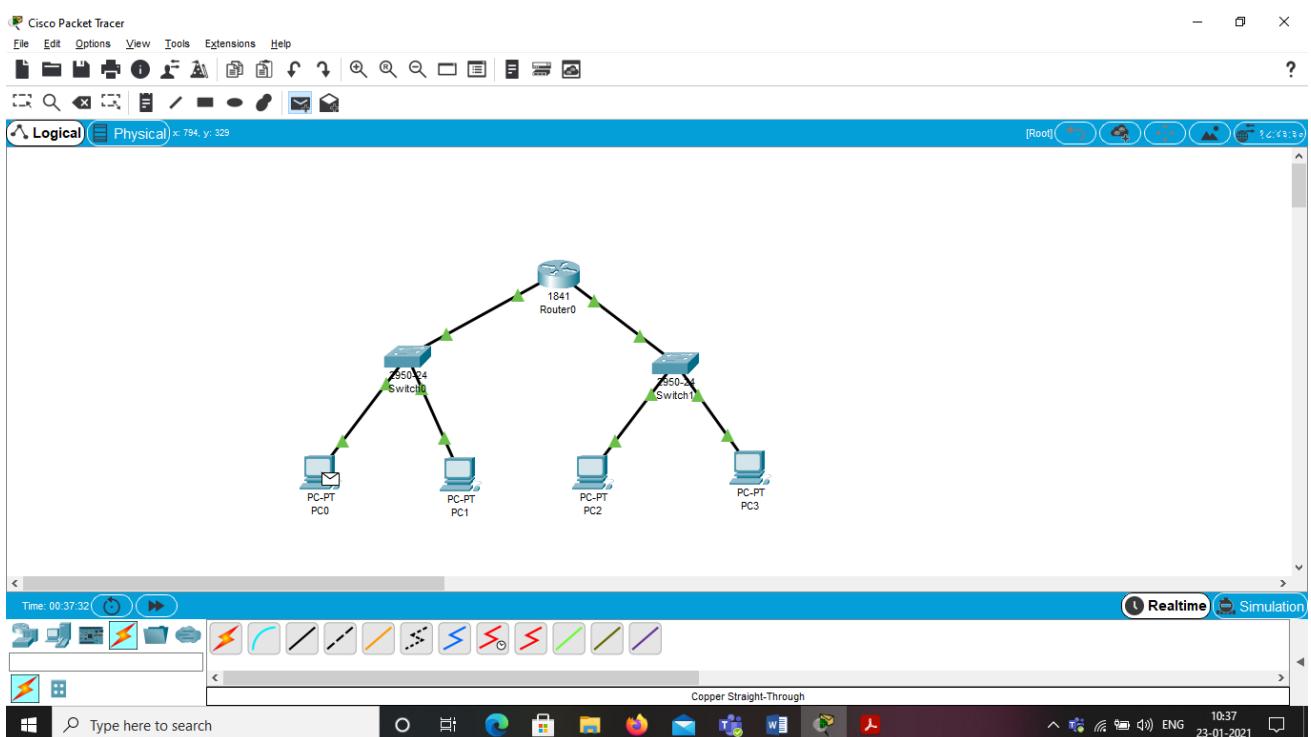


Step 3: Check the connectivity from one network to another network

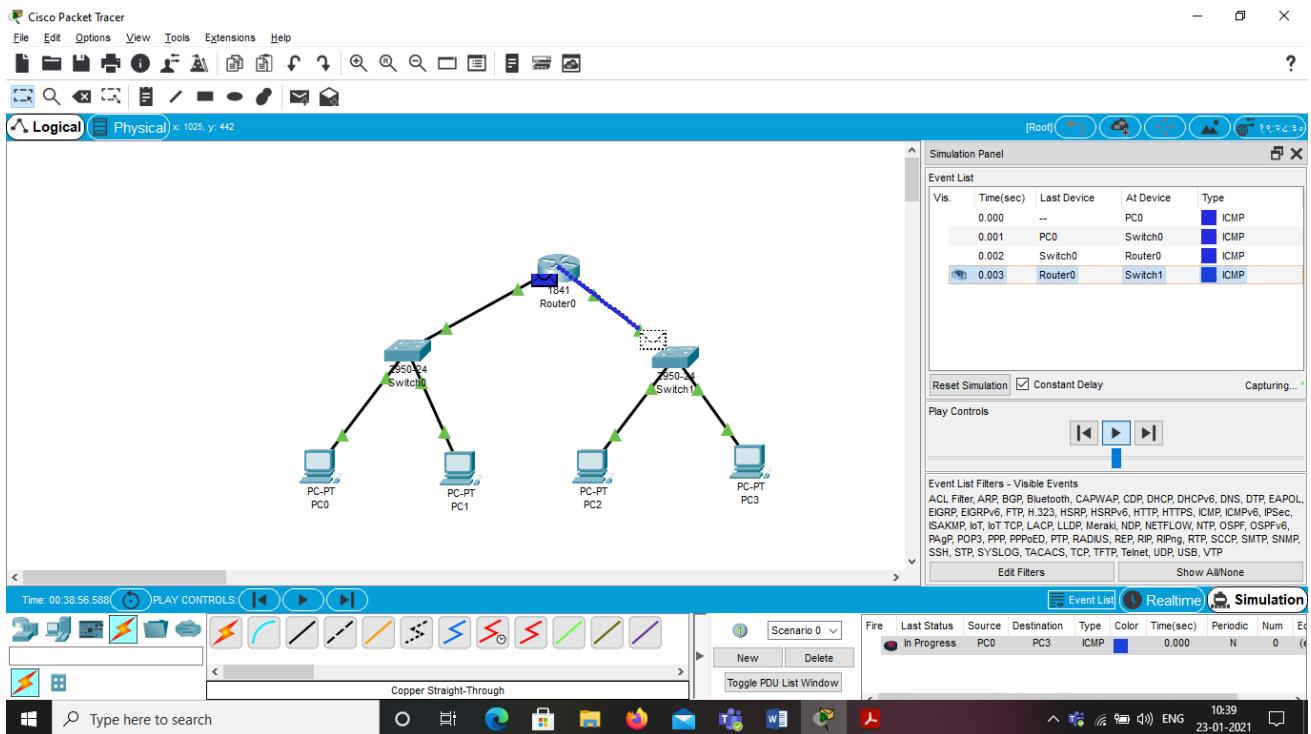
Select any PC from 1st network go to Desktop tab->Command Prompt->execute ping command for the 2nd network.



Step 4: Send Simple PDU.



Step 5: Check in simulation mode



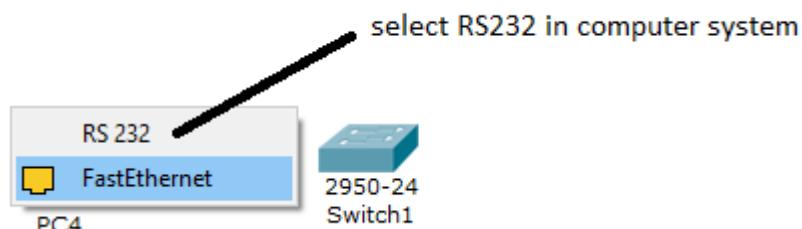
Exp 2: Configuration of Switch using cisco packet tracer



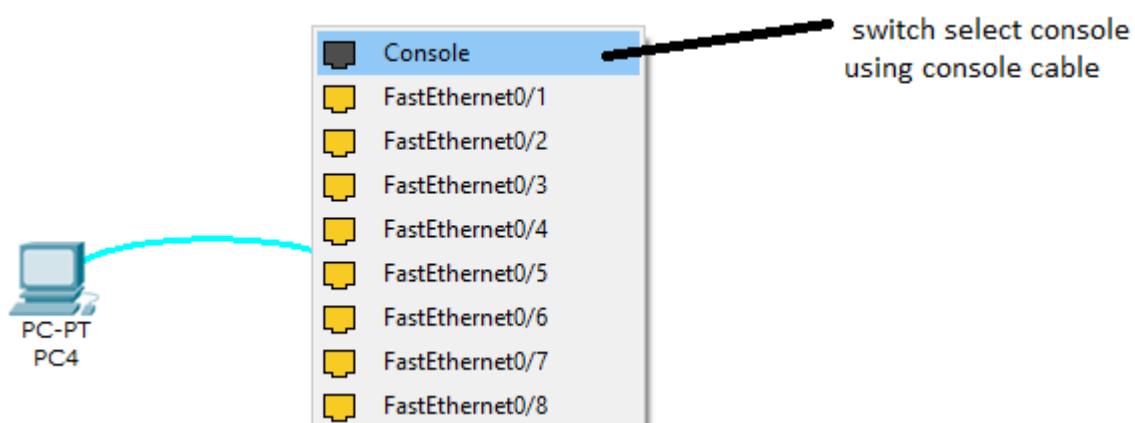
Step 1:



Step 2:



Step 3:





Step 4:

Physical Config Desktop Software/Services

double click PC and select terminal

Terminal Configuration

Port Configuration

Bits Per Second:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

Command Prompt

Web Browser

MIB Browser

Cisco IP Communicator

OK

select ok

this screen display

```

Switch>
Switch>
Switch>
Switch>
Switch>
Switch>|
```

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.

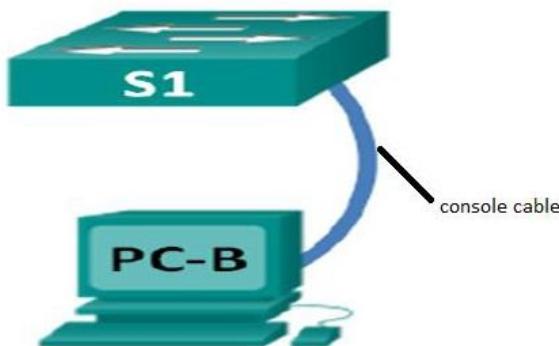
S1# show ip interface brief

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

```
Press RETURN to get started!
User Access Verification
Password:
Password:
Switch>|
```

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
```

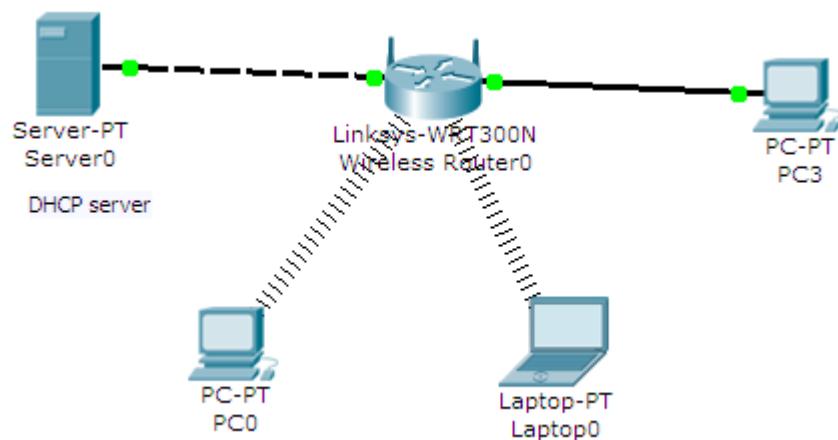
```
Username: network
```

```
Password:
```

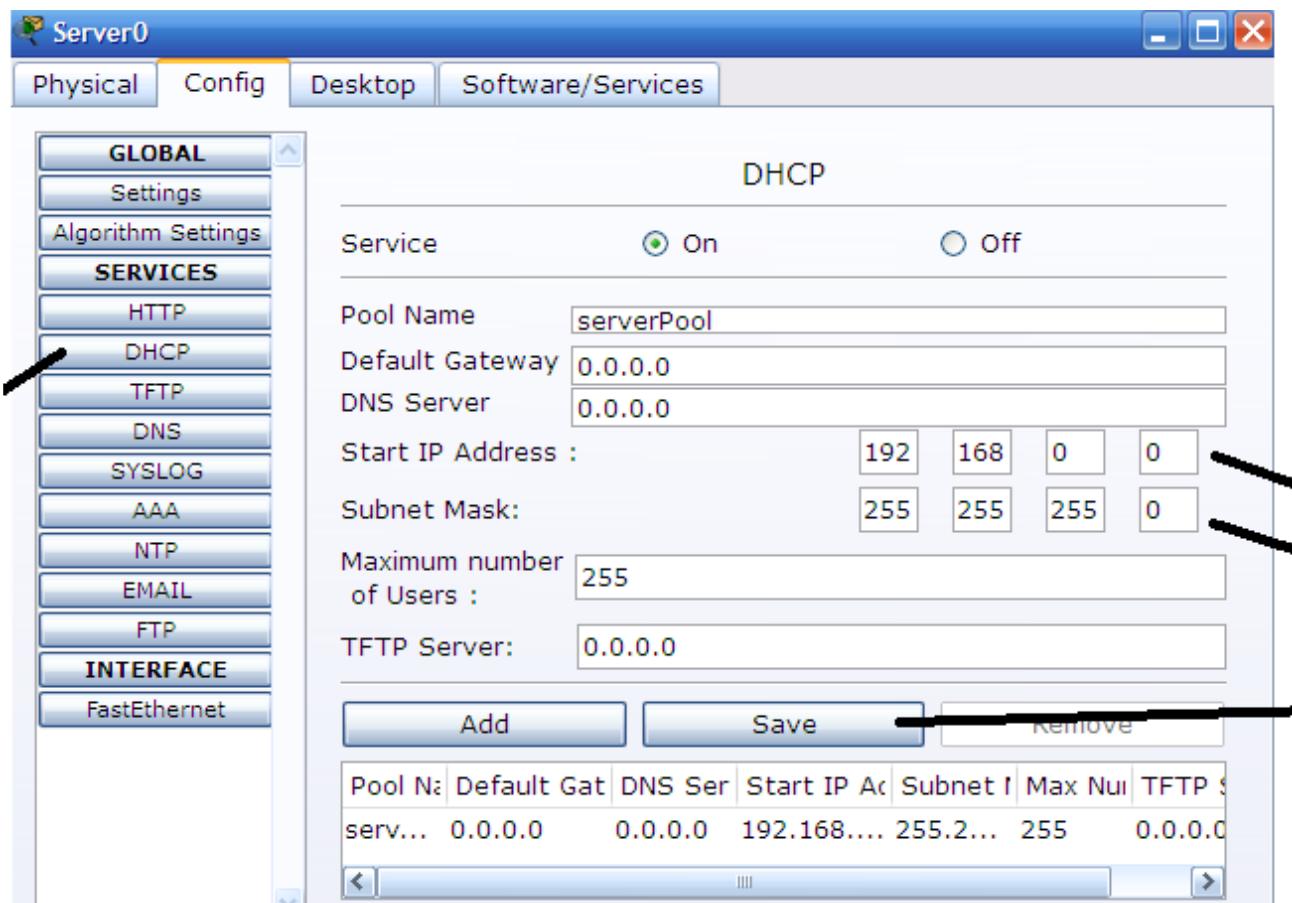
```
CISCO> enable
```

```
Password:
```

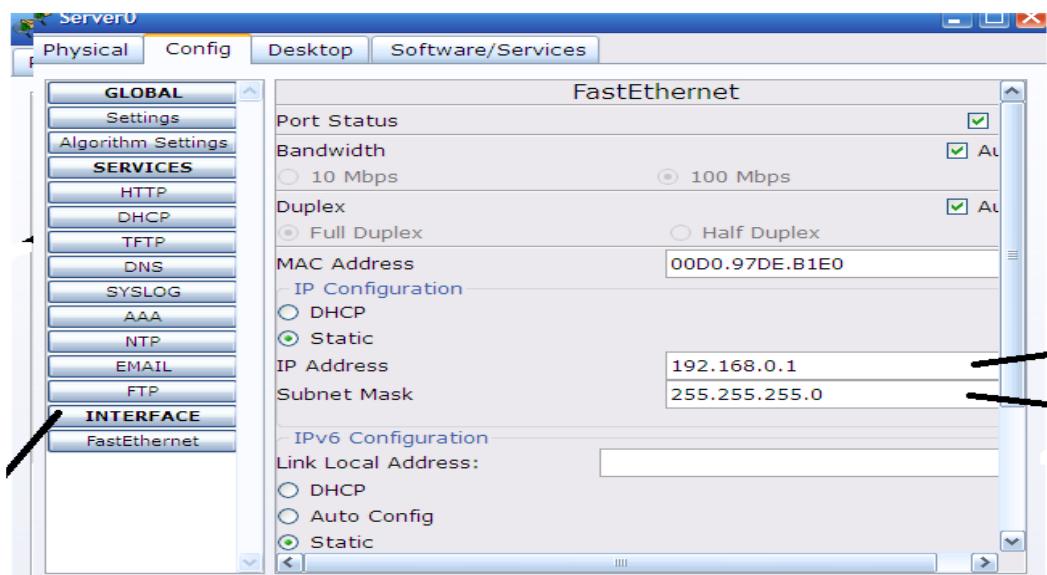
Exp 4: Configure the DHCP Server and wireless router and check the connectivity



Step1 :configure the DHCP server



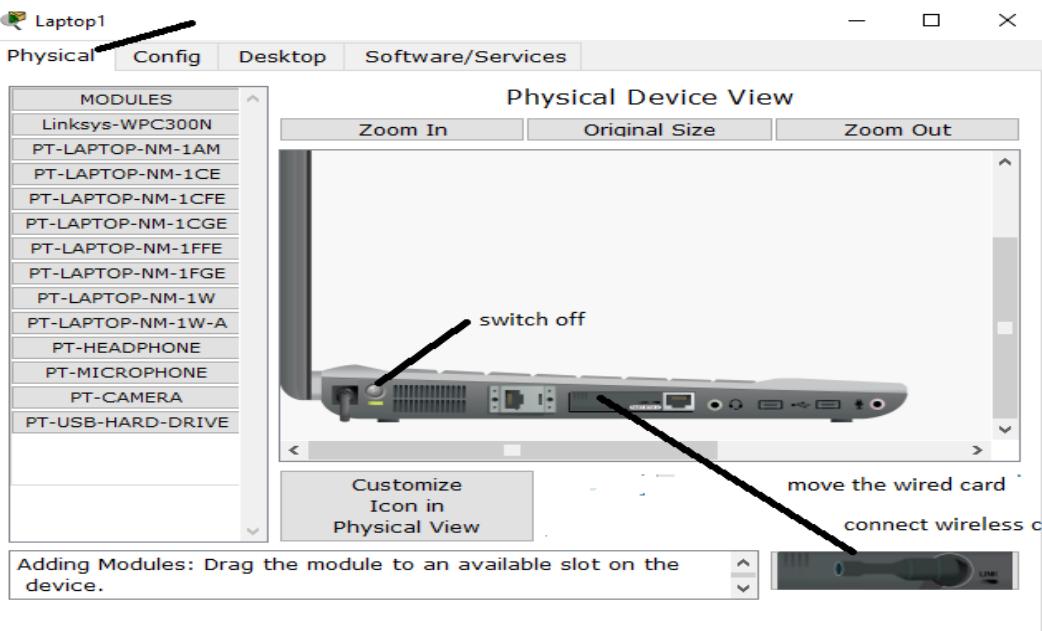
Step2: In server configure the fast Ethernet



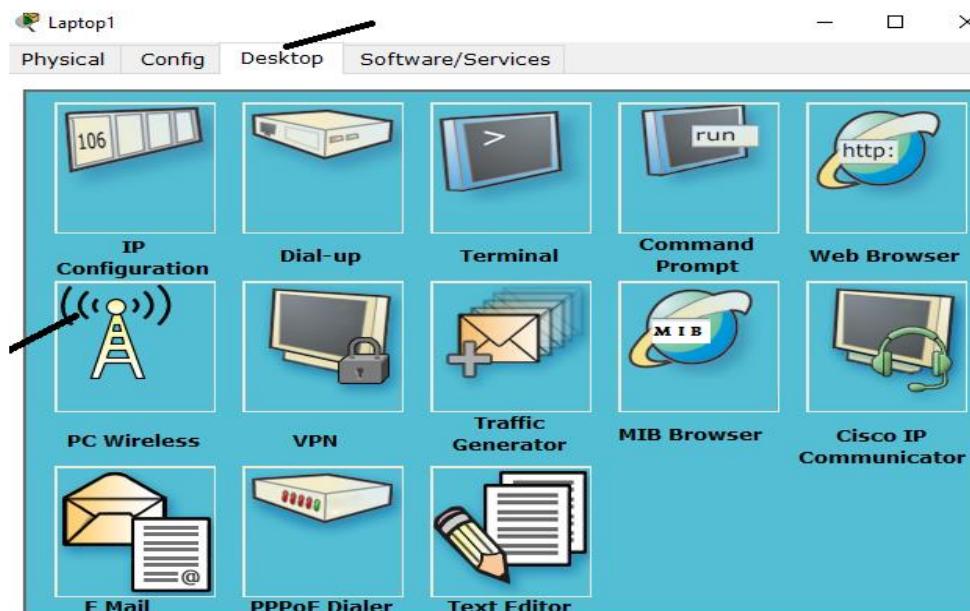
Step 3: configure the wireless router



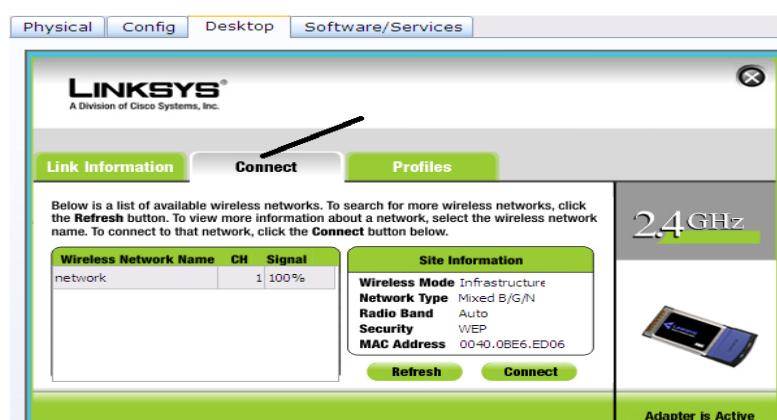
Step4 :Laptop remove the wired NIC card to wireless card



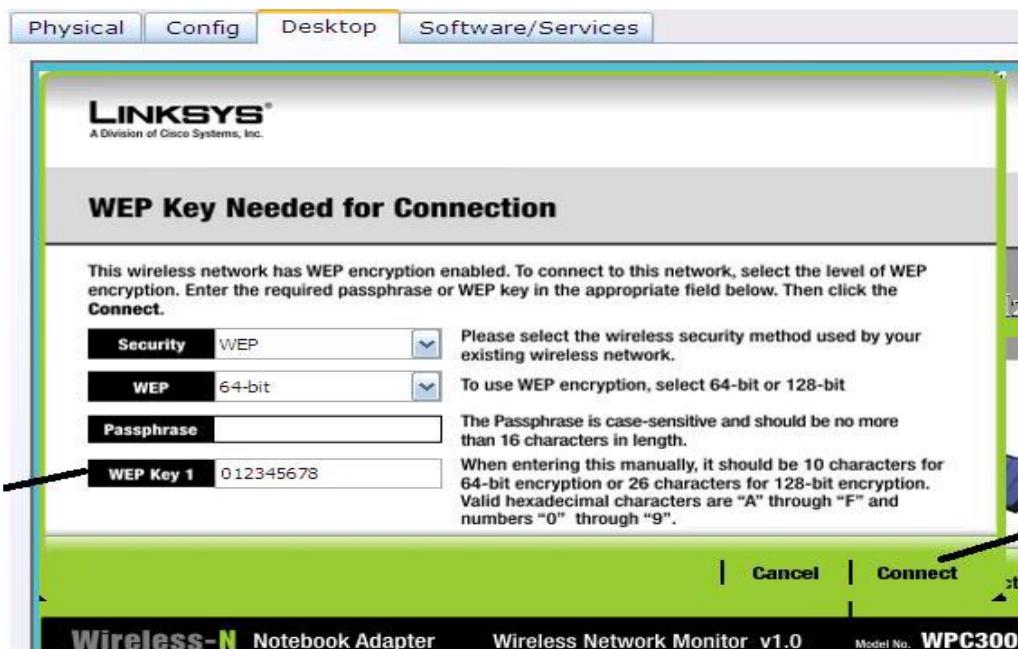
Step 5: Laptop connect the wireless



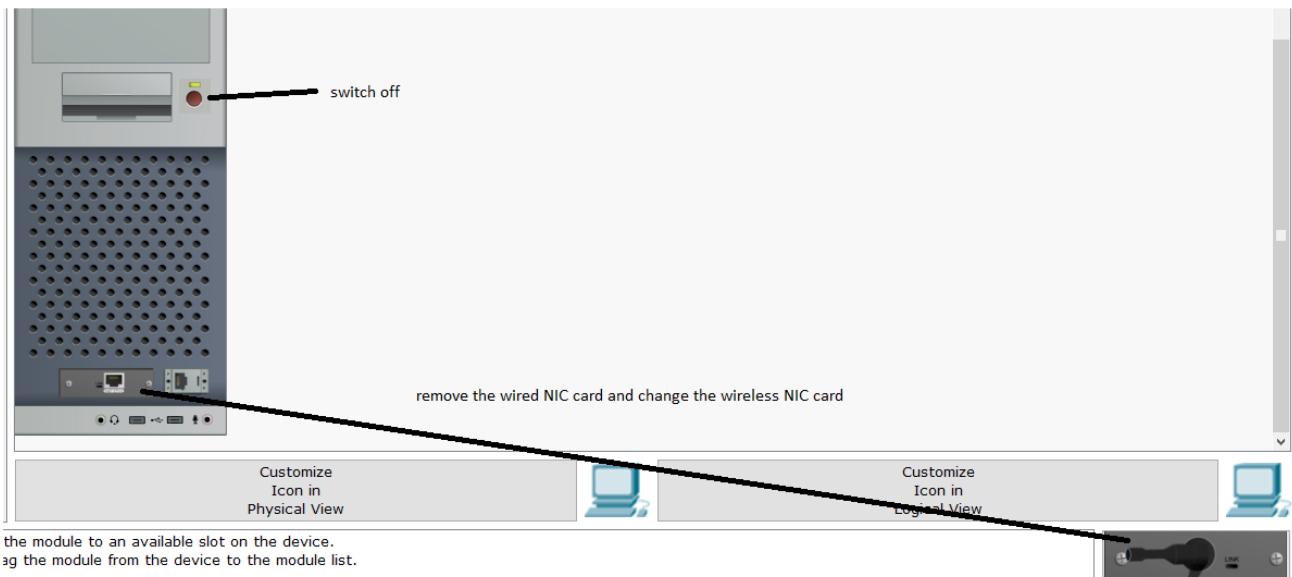
Step 6 : connect Laptop with wireless router



Step 7 :enter web key

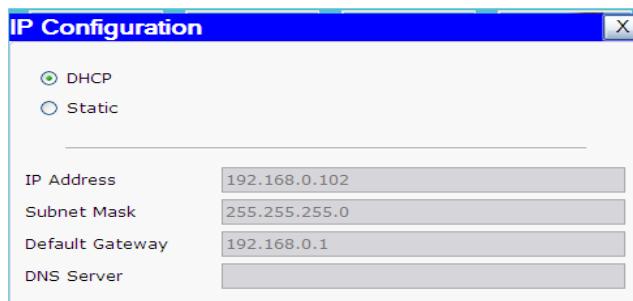


Step8 : PC remove the wired NIC card to wireless card

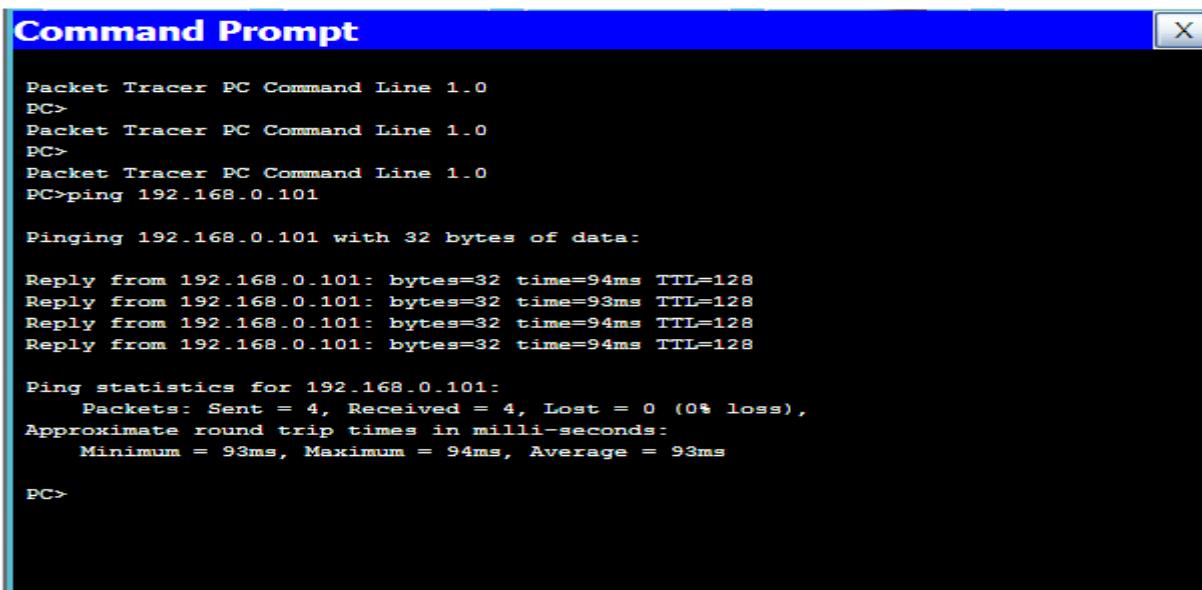


Note : Same steps 5,6,7

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



Step10 check the connectivity



The image shows a Command Prompt window titled "Command Prompt". The window has a blue header bar with the title and a close button (X) in the top right corner. The main body of the window is black and contains white text. The text shows the output of a ping command. It starts with three "Packet Tracer PC Command Line 1.0" prompts, followed by a "PC>" prompt. Then it shows the ping command being entered: "PC>ping 192.168.0.101". Below this, the text "Pinging 192.168.0.101 with 32 bytes of data:" is displayed. Four replies are shown, each with "bytes=32 time=94ms TTL=128". After the replies, the text "Ping statistics for 192.168.0.101:" is displayed, followed by "Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)", "Approximate round trip times in milli-seconds:", and "Minimum = 93ms, Maximum = 94ms, Average = 93ms". Finally, another "PC>" prompt is shown at the bottom.

```
Packet Tracer PC Command Line 1.0
PC>
Packet Tracer PC Command Line 1.0
PC>
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:

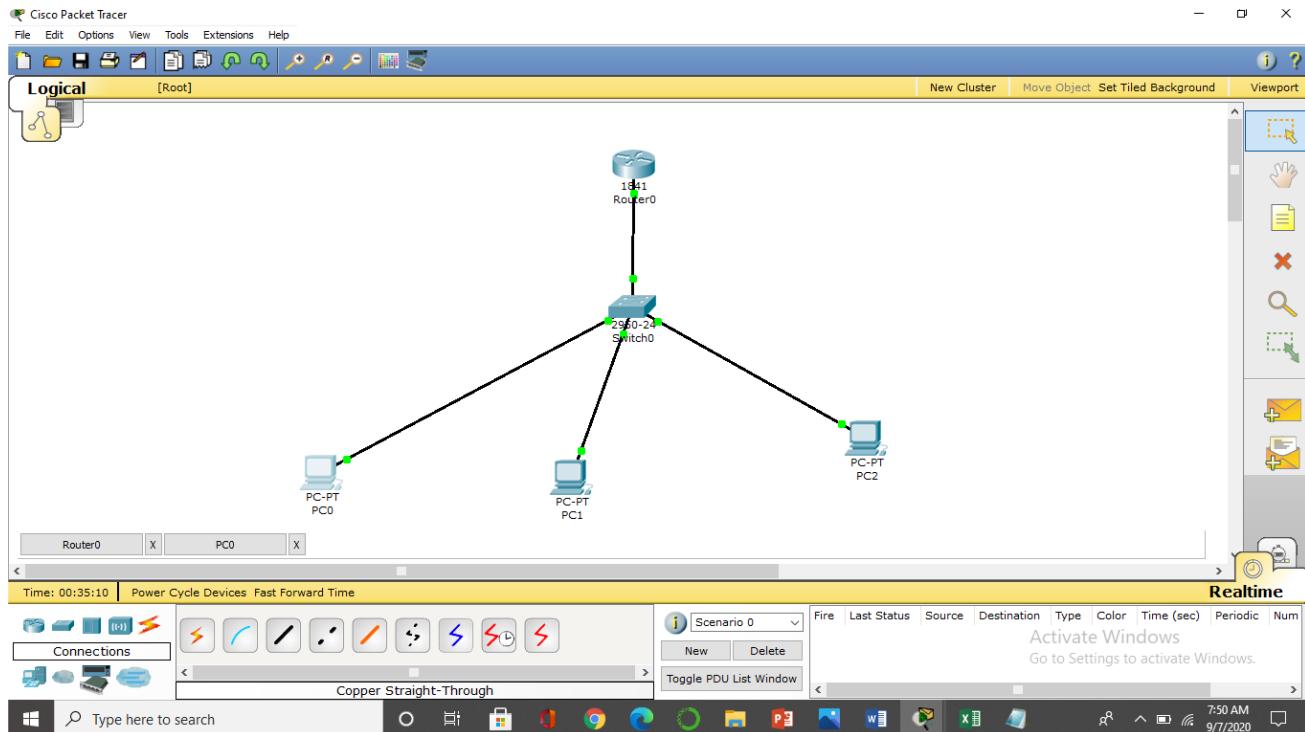
Reply from 192.168.0.101: bytes=32 time=94ms TTL=128
Reply from 192.168.0.101: bytes=32 time=93ms TTL=128
Reply from 192.168.0.101: bytes=32 time=94ms TTL=128
Reply from 192.168.0.101: bytes=32 time=94ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 94ms, Average = 93ms

PC>
```

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#

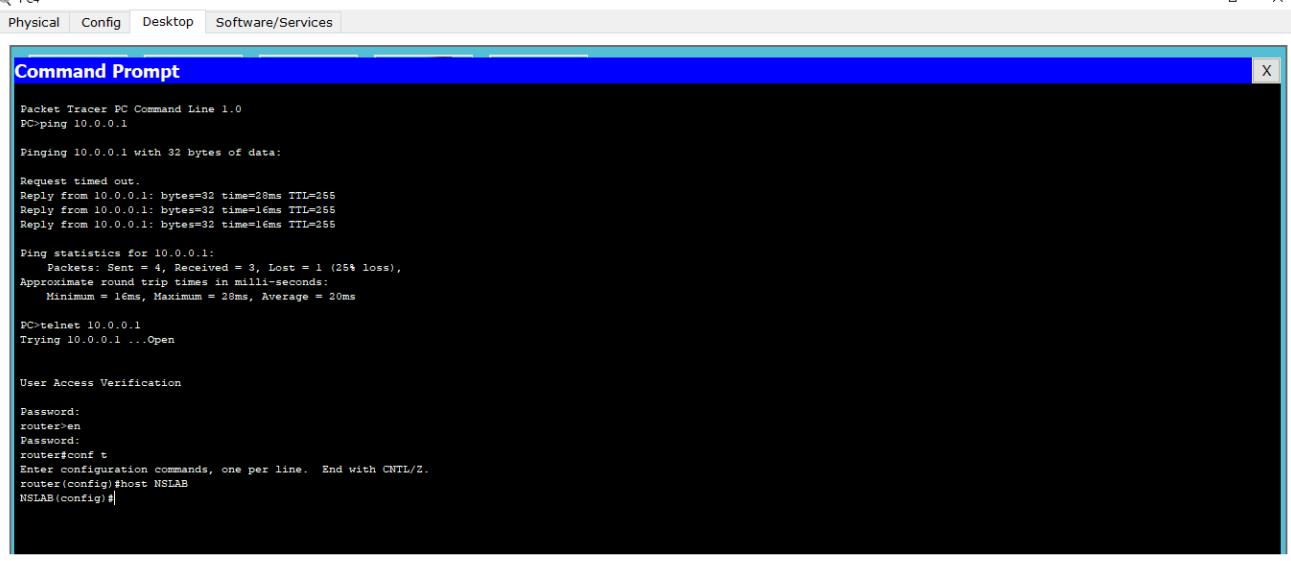
We can change hostname of router in PC command prompt.

Router#conf t

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

Router(config)#host nslab

nslab(config)#



The screenshot shows a Windows desktop environment with a Command Prompt window open. The window title is "Command Prompt". Inside the window, the following text is displayed:

```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 10.0.0.1: bytes=32 time=28ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 28ms, Average = 20ms

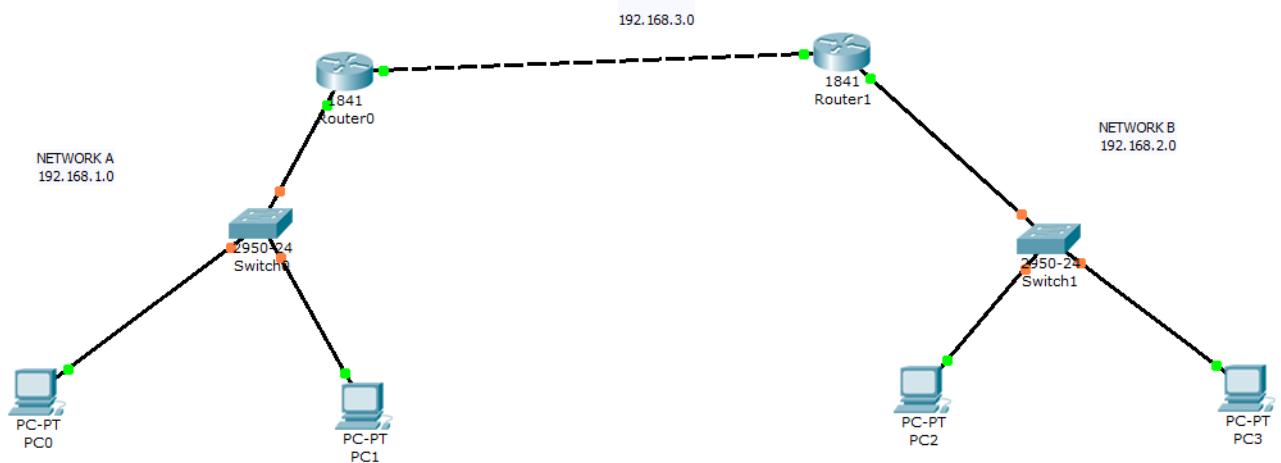
PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Password:
router>en
Password:
router>conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#host NSLAB
NSLAB(config)#
```

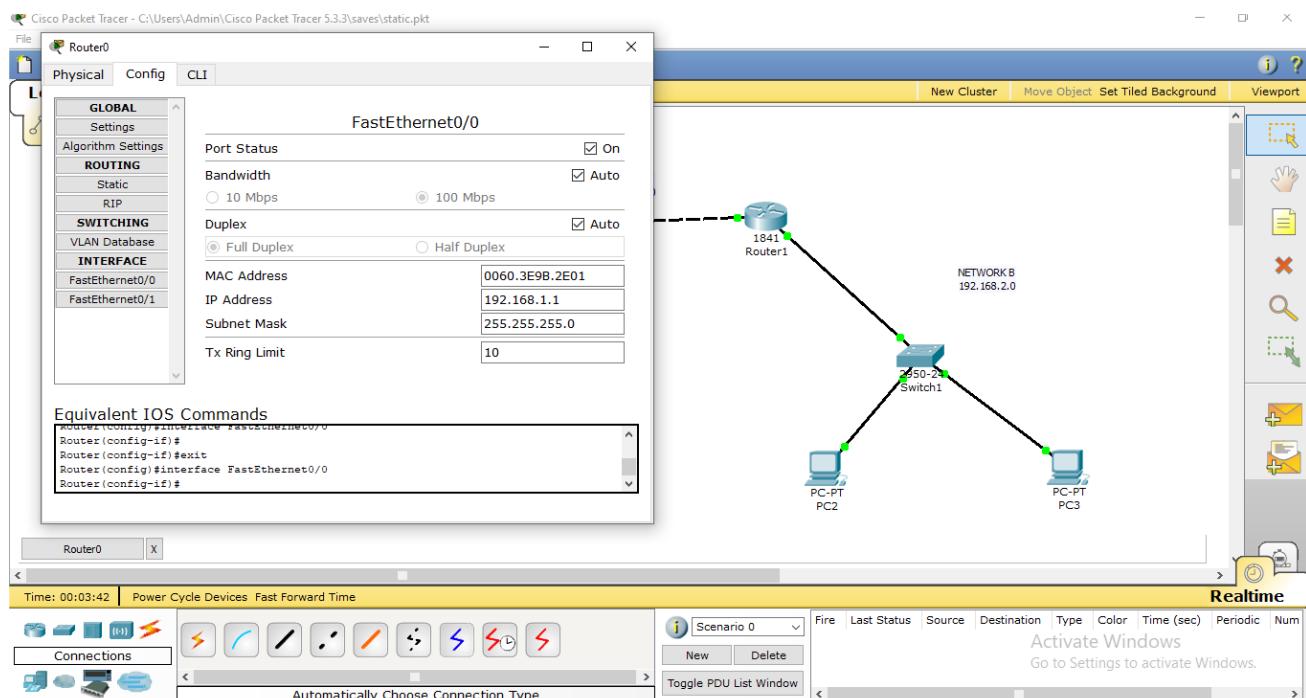
Exp 6: Configure the static routing using cisco packet tracer.

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

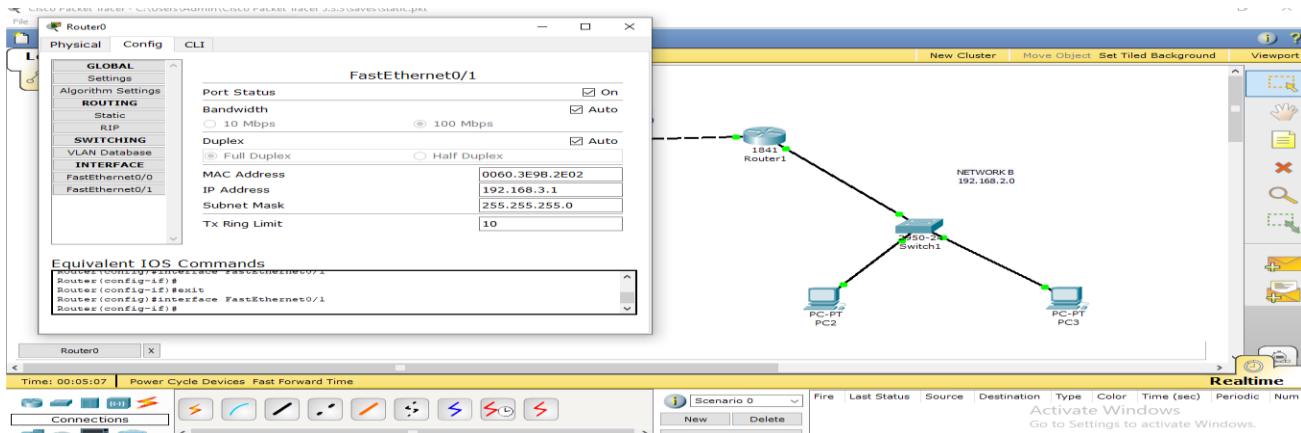


Step 2: Configure IP address to router1.

For Fastethernet 0/0

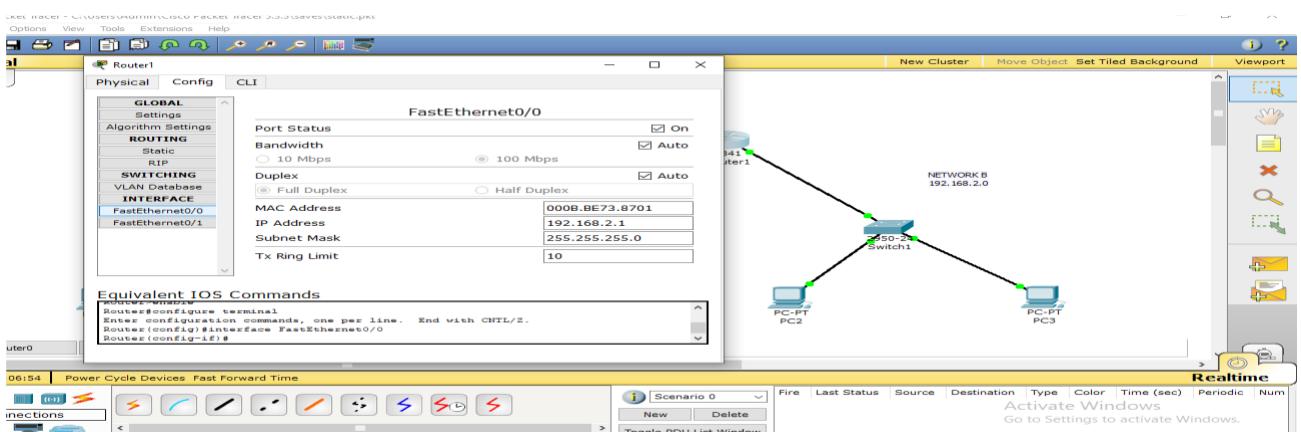


For Fastethernet 0/1

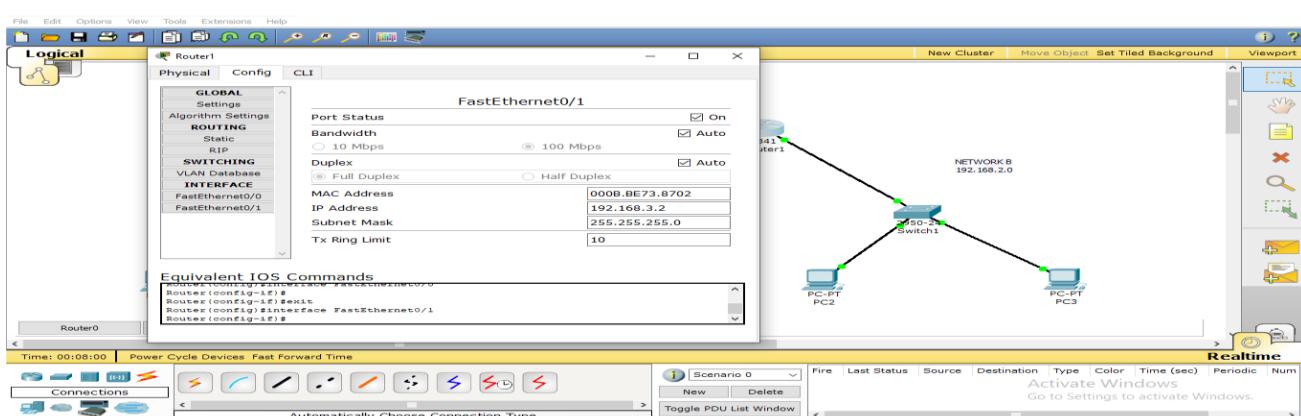


Step 3 :Configure IP address to router2

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
```



```
PC1
Physical Config Desktop Software/Services

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

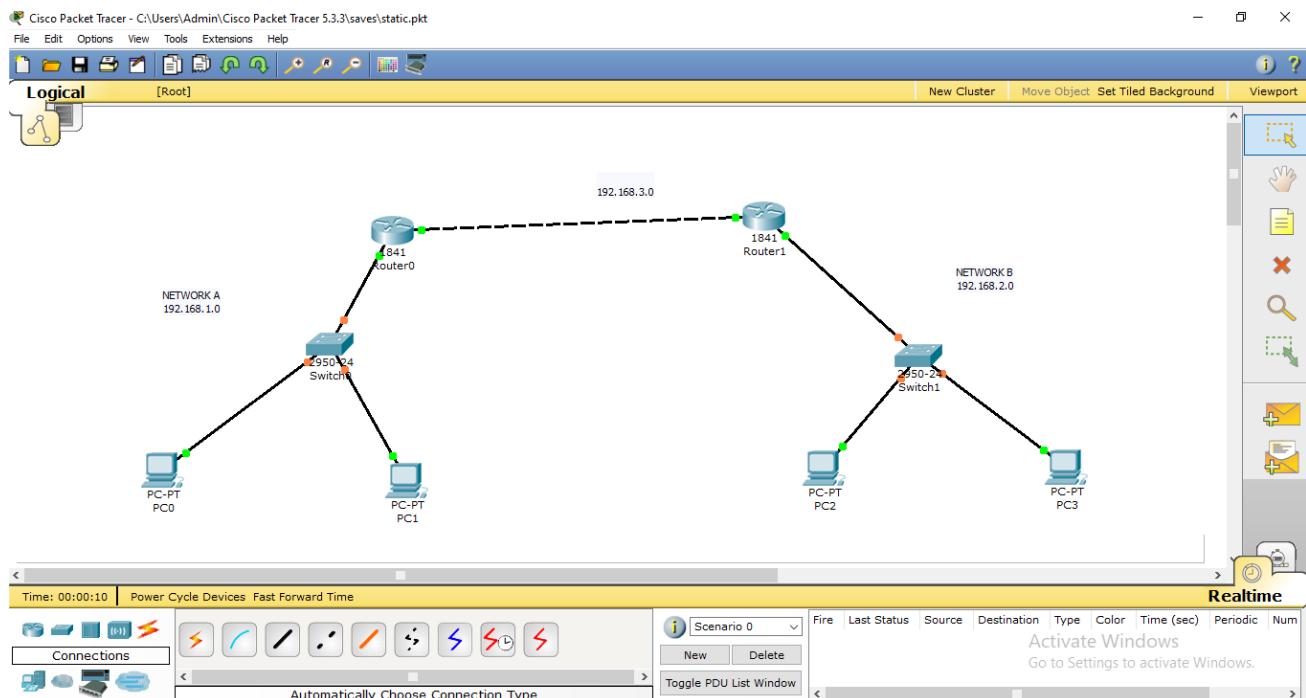
Reply from 192.168.2.1: bytes=32 time=147ms TTL=254
Reply from 192.168.2.1: bytes=32 time=84ms TTL=254
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

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

PC>
PC>
PC>
```

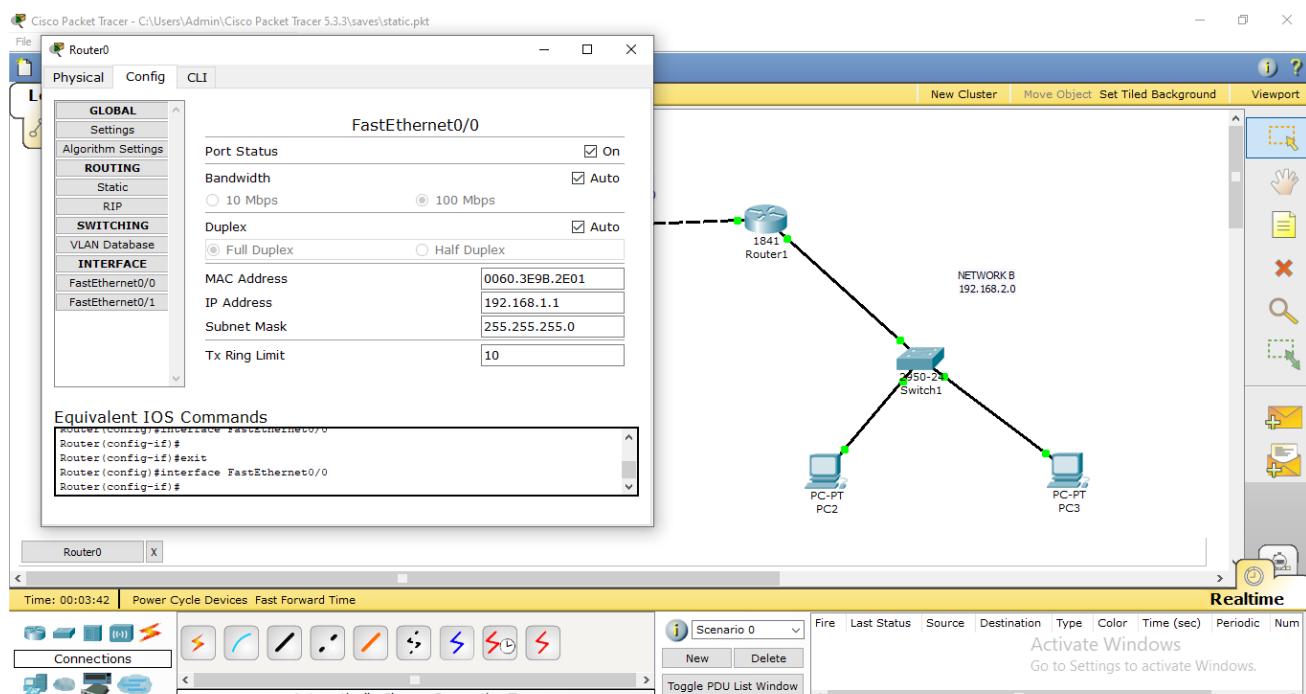
Exp 7: Configure the RIP routing using cisco packet tracer.

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

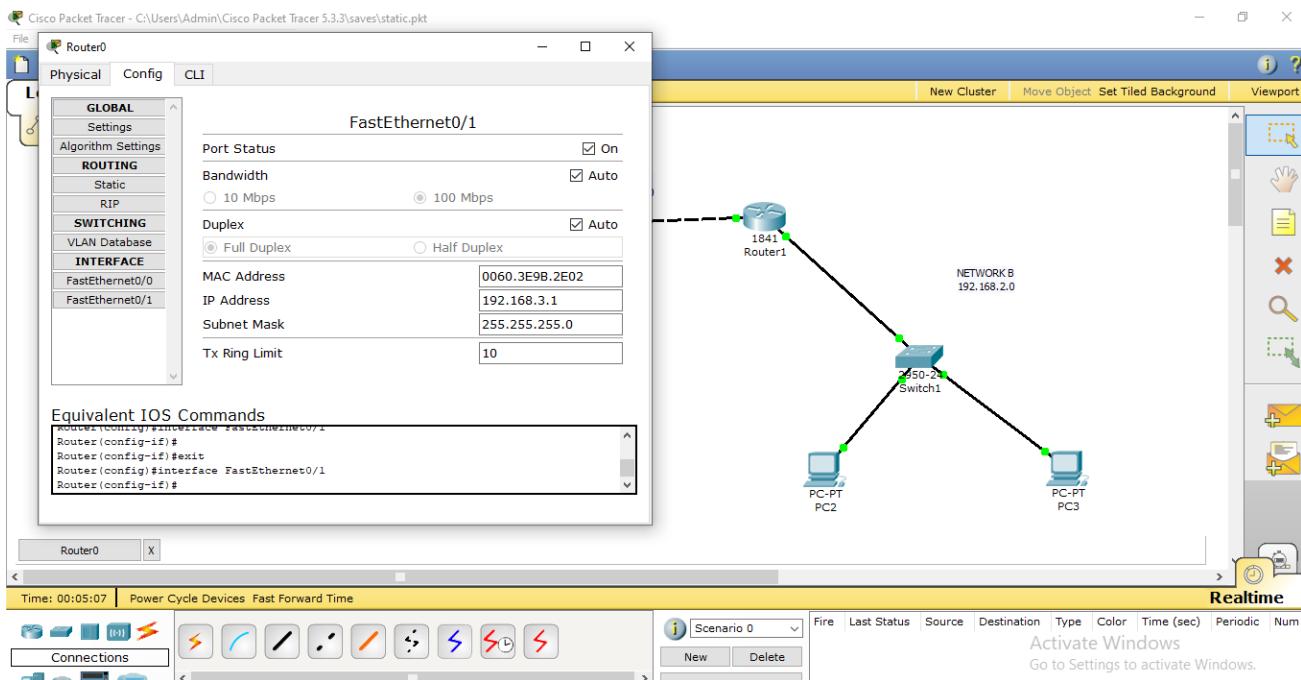


Step 2: Configure IP address to router1.

For Fastethernet 0/0

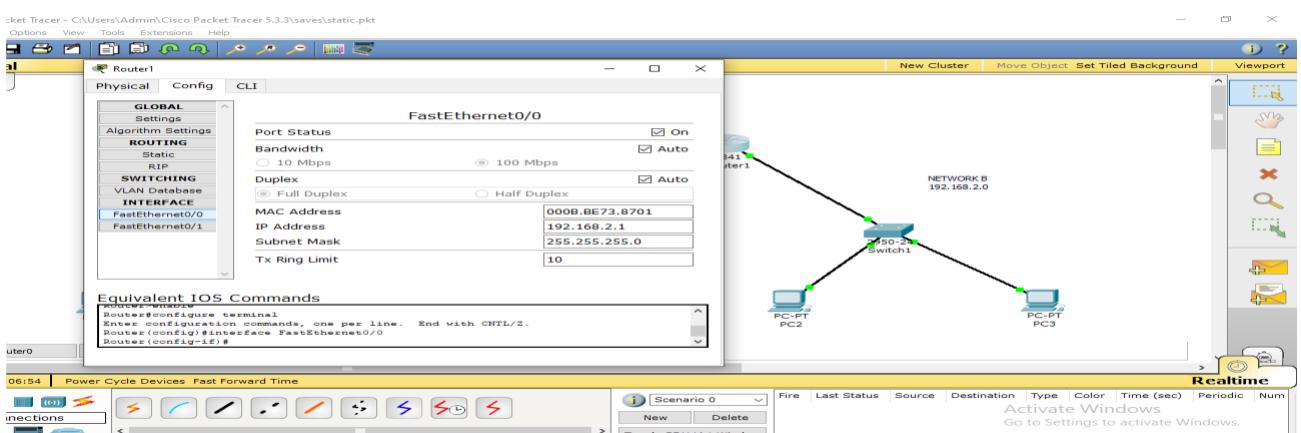


For Fastethernet 0/1

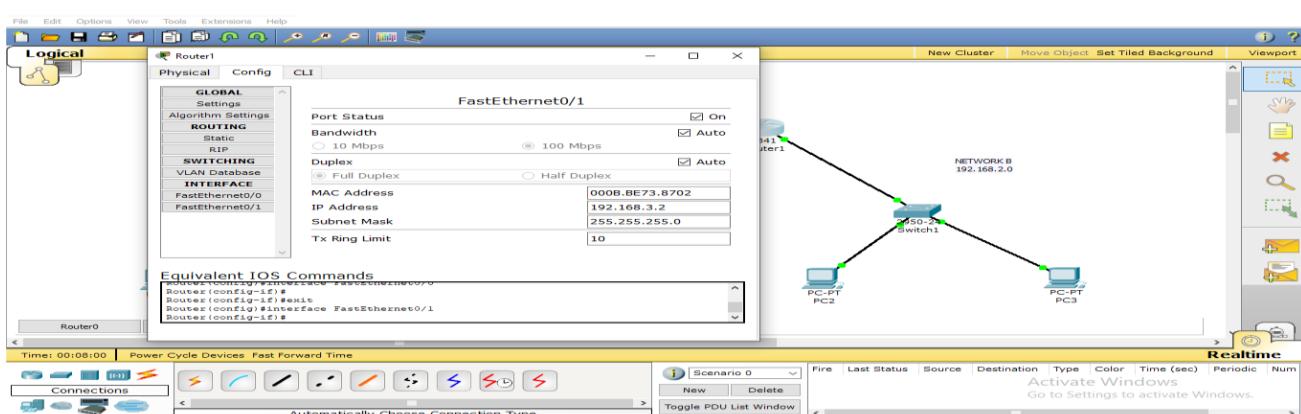


Step 3 :Configure IP address to router2

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

PC1

Physical Config Desktop Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
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

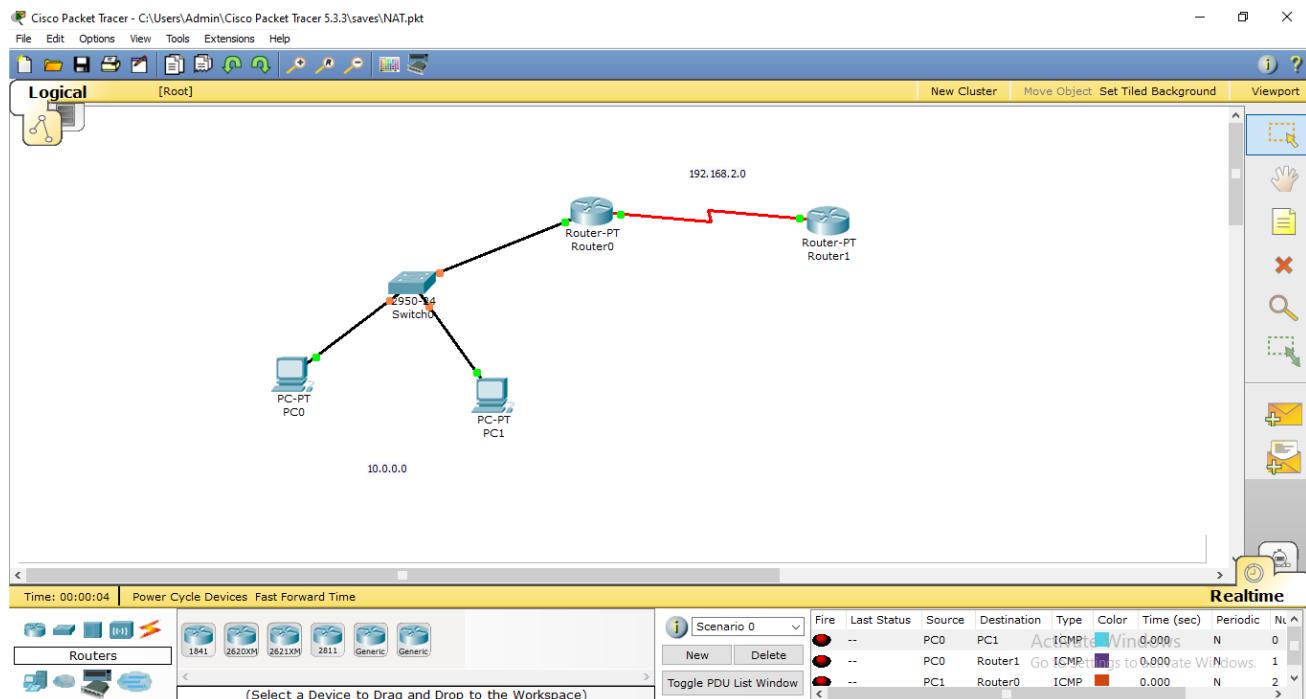
PC>
PC>
PC>
```

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

NAT(NETWORK ADDRESS TRANSLATION)

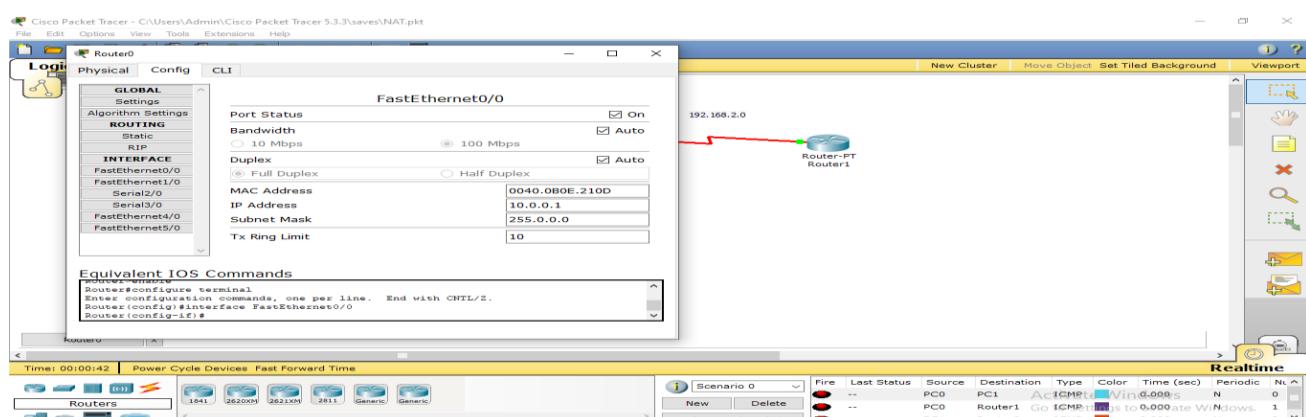
It is a Process in which one or more Local ip address is translated into global ip address or vice versa in order to provide internet access to the host. It Allows multiple devices to access internet through single public ip address.

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

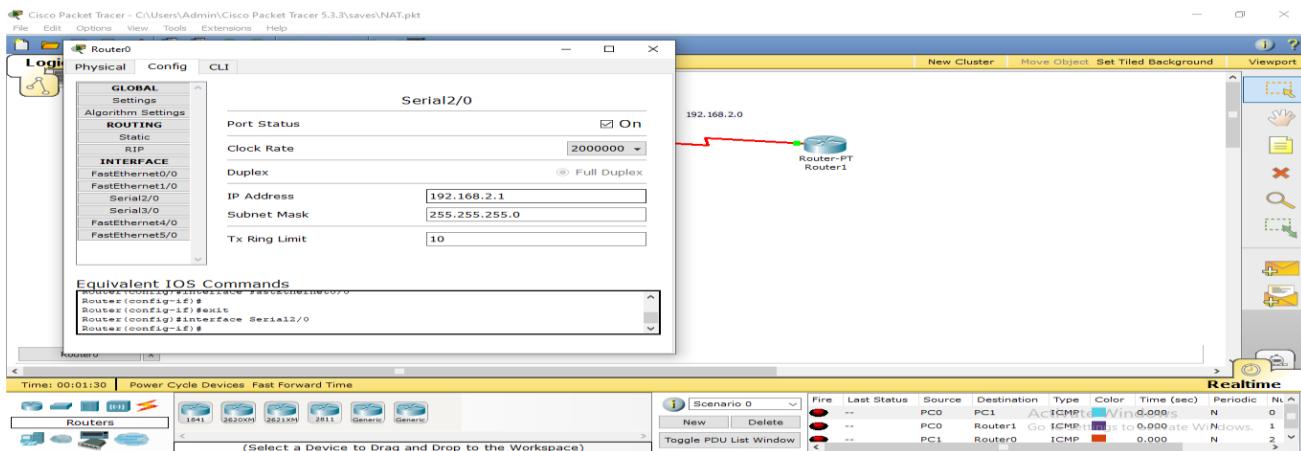


Step 2: Configure IP address to router1.

For Fastethernet 0/0

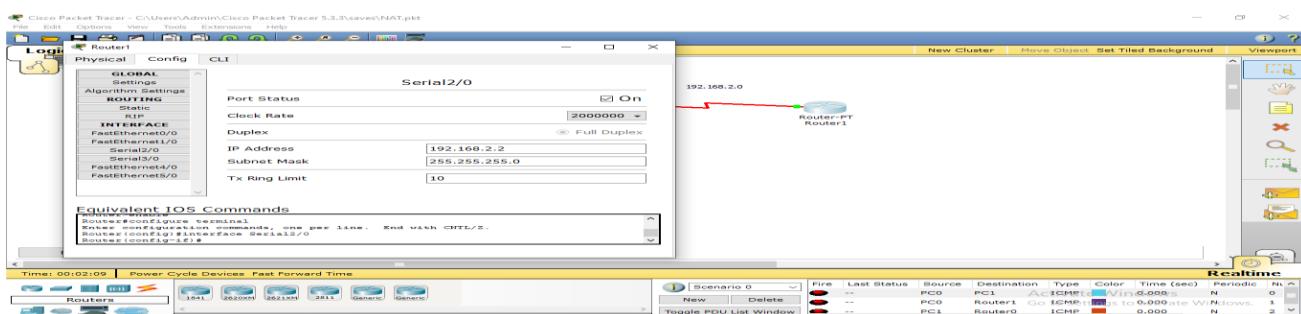


For Serial2/0



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

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

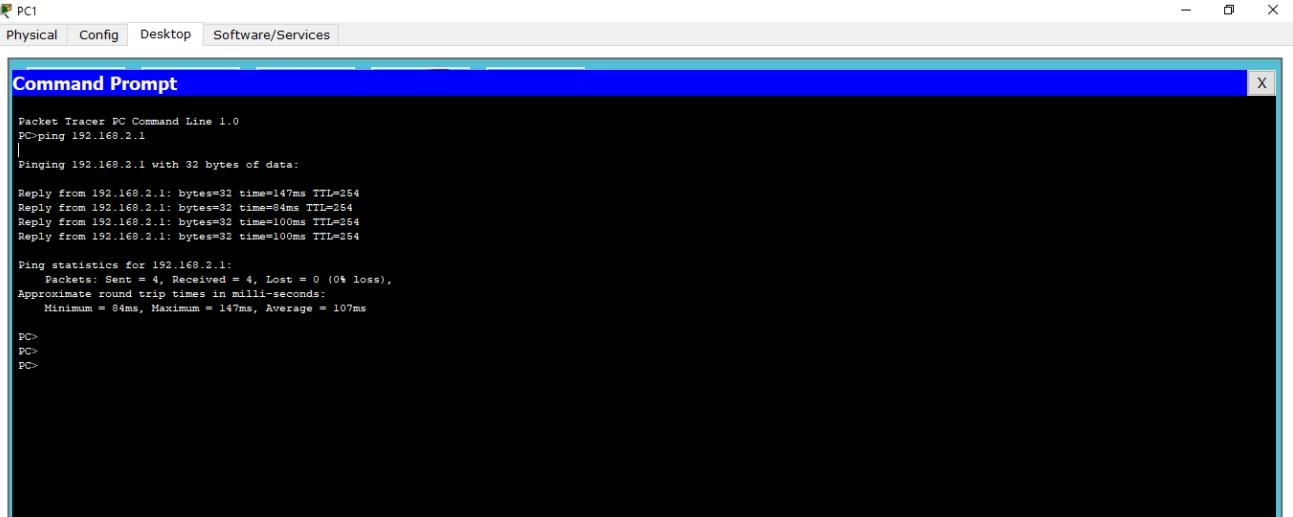
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

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



The screenshot shows a Windows-style Command Prompt window titled "Command Prompt". The window has a title bar with icons for minimize, maximize, and close, and tabs for "Physical", "Config", "Desktop", and "Software/Services". The main area of the window displays the output of a ping command. The output is as follows:

```
Packet Tracer PC Command Line 1.0
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

PC>
PC>
PC>
```

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: -

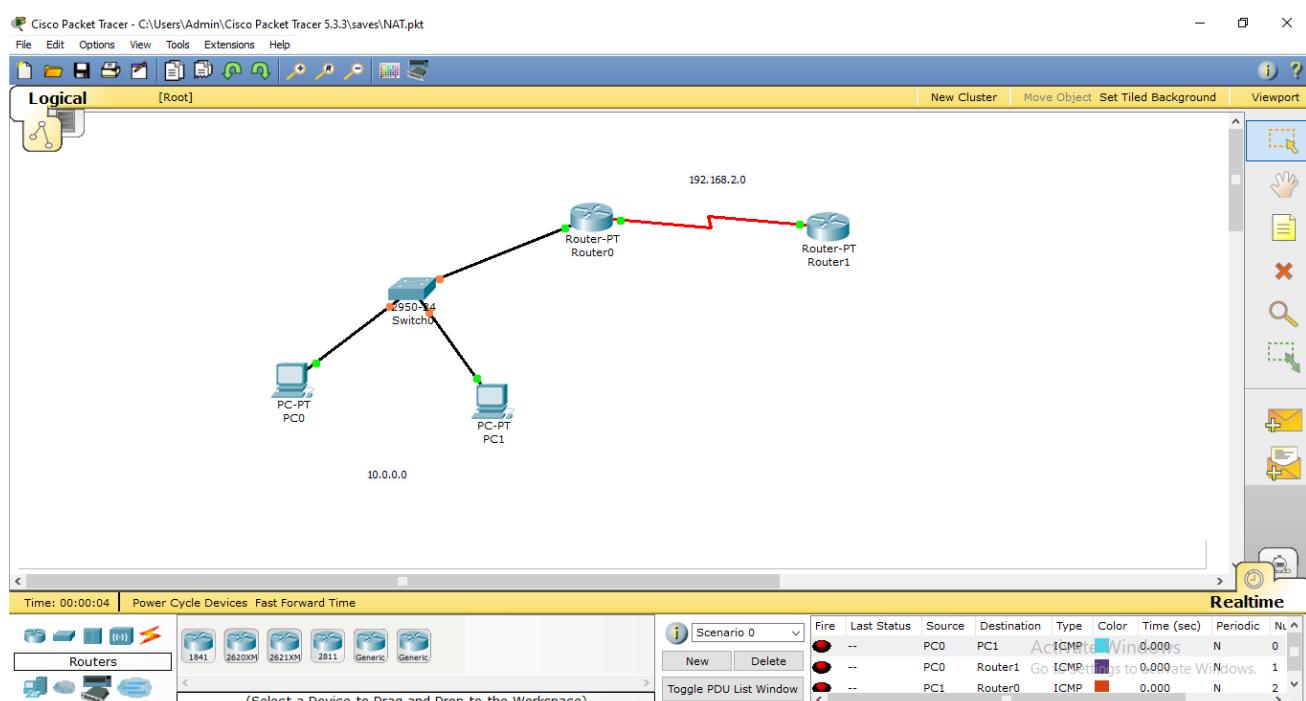
Step1: Create an access list of IP addresses which need translation(ACL range 1 to 99 and 1300 to 1999)

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

Step3: Map access list with pool

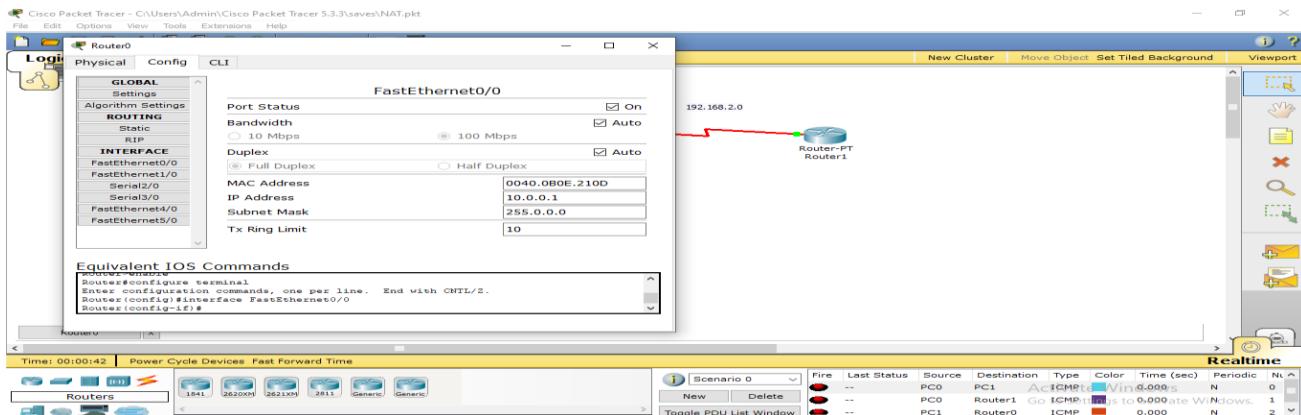
Step4: Define inside and outside interfaces

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

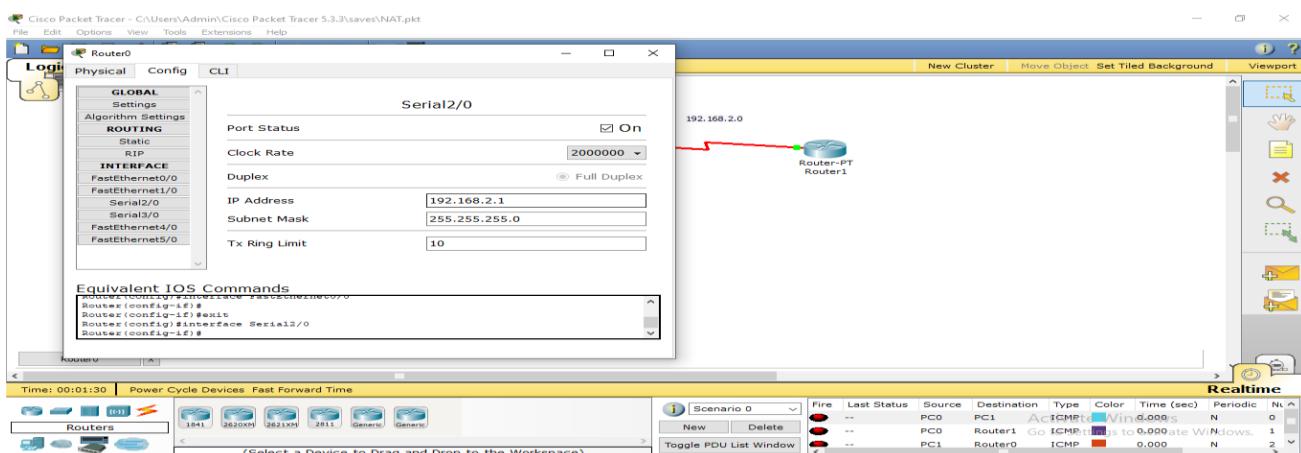


Step 2: Configure IP address to router1.

For Fastethernet 0/0

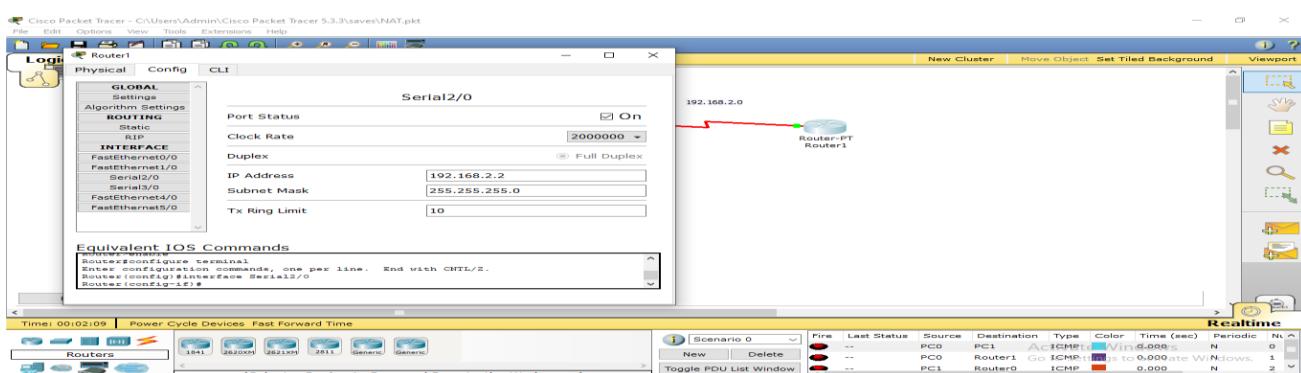


For Serial2/0



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

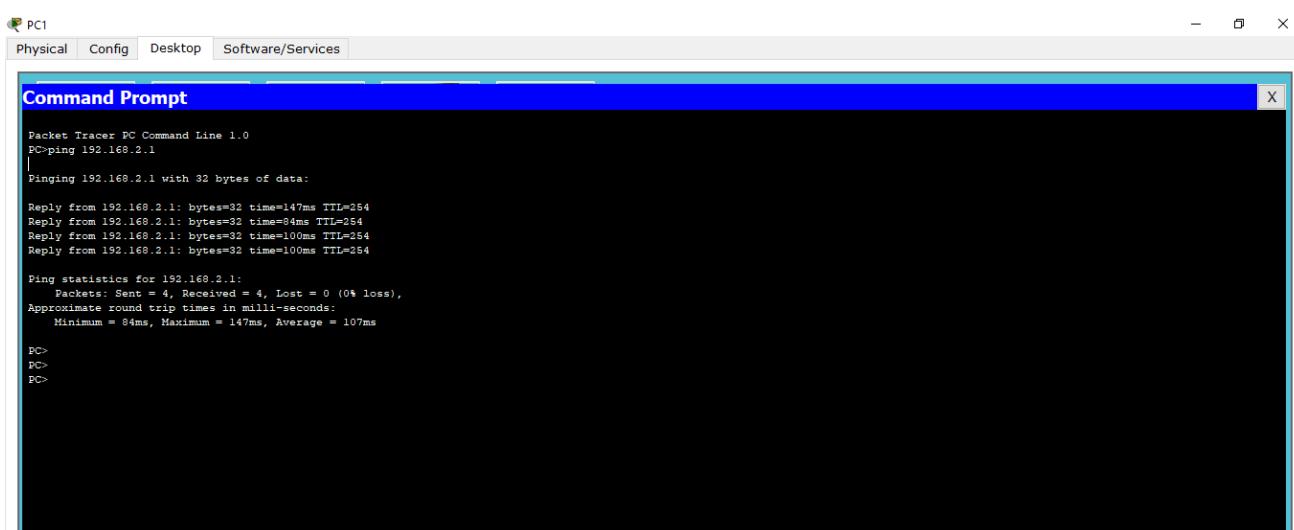
Reply from 192.168.2.1: bytes=32 time=100ms TTL=254

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



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window has tabs at the top: "Physical", "Config", "Desktop", and "Software/Services". The "Config" tab is selected. The main area of the window displays the output of a ping command. The output is as follows:

```
Packet Tracer PC Command Line 1.0  
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  
  
PC>  
PC>  
PC>
```

Module-3

NS2 Simulator

Exp 1: THREE NODE POINT TO POINT NETWORK

Aim: Simulate a three node point to point network with duplex links between them. Set queue size and vary the bandwidth and find number of packets dropped.

```
set ns [new Simulator]      # Letter S is capital
set nf [open PA1.nam w]      # open a nam trace file in write mode
$ns namtrace-all $nf # nf nam filename
set tf [open PA1.tr w] # tf trace filename
$ns trace-all $tf
proc finish { } {
global ns nf tf
$ns flush-trace# clears trace file contents
close $nf
close $tf
exec nam PA1.nam &
exit 0
}
set n0 [$ns node]          # creates 3 nodes
set n2 [$ns node]
set n3 [$ns node]
$ns duplex-link $n0 $n2 200Mb 10ms DropTail  # establishing links
$ns duplex-link $n2 $n3 1Mb 1000ms DropTail
$ns queue-limit $n0 $n2 10
set udp0 [new Agent/UDP]    # attaching transport layer protocols
$ns attach-agent $n0 $udp0
set cbr0 [new Application/Traffic/CBR]    # attaching application layer protocols
$cbr0 set packetSize_ 500
$cbr0 set interval_ 0.005
$cbr0 attach-agent $udp0
set null0 [new Agent/Null]
$ns attach-agent $n3 $null0
$ns connect $udp0 $null0

$ns at 0.1 "$cbr0 start"
$ns at 1.0 "finish"
$ns run
```

AWK file: (Open a new editor using “vi command” and write awk file and save with “.awk” extension)

```
#immediately after BEGIN should open braces {
```

```
BEGIN{ c=0;}
```

```

{
if($1=="d")
{c++;
printf("%s\t%s\n",$5,$11);
}
}
END{ printf("The number of packets dropped =%d\n",c); }

```

Steps for execution

- Open gedit editor and type program. Program name should have the extension “ .tcl ”

[root@localhost ~]# gedit lab1.tcl

- Open gedit editor and type awk program. Program name should have the extension “.awk ”

[root@localhost ~]# gedit lab1.awk

- Run the simulation program

[root@localhost~]# ns lab1.tcl

- Here “ns” indicates network simulator. We get the topology shown in the snapshot.

- Now press the play button in the simulation window and the simulation will begins.

- After simulation is completed run awk file to see the output ,

[root@localhost~]# awk -f lab1.awk lab1.tr

- To see the trace file contents open the file as ,

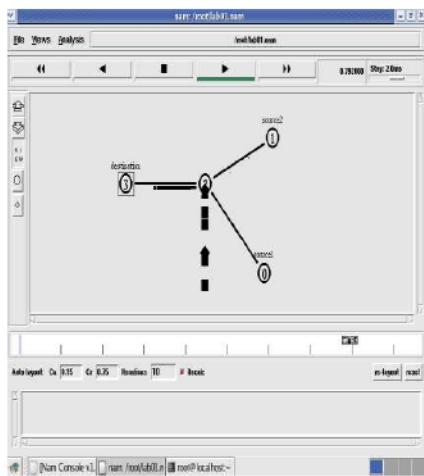
[root@localhost~]# gedit lab1.tr

Trace file contains 12 columns:

Event type, Event time, From Node, To Node, Packet Type, Packet Size, Flags (indicated by -----), Flow ID, Source address, Destination address, Sequence ID, Packet ID

```
root@localhost:~# 
File Edit View Terminal Tabs Help
+ 0.1 0 2 cbr 500 ----- 0 0.0 3.0 0 0
- 0.1 0 2 cbr 500 ----- 0 0.0 3.0 0 0
r 0.10108 0 2 cbr 500 ----- 0 0.0 3.0 0 0
+ 0.10108 2 3 cbr 500 ----- 0 0.0 3.0 0 0
- 0.10108 2 3 cbr 500 ----- 0 0.0 3.0 0 0
+ 0.105 0 2 cbr 500 ----- 0 0.0 3.0 1 1
- 0.105 0 2 cbr 500 ----- 0 0.0 3.0 1 1
r 0.10608 0 2 cbr 500 ----- 0 0.0 3.0 1 1
+ 0.10608 2 3 cbr 500 ----- 0 0.0 3.0 1 1
- 0.10608 2 3 cbr 500 ----- 0 0.0 3.0 1 1
+ 0.11 0 2 cbr 500 ----- 0 0.0 3.0 2 2
- 0.11 0 2 cbr 500 ----- 0 0.0 3.0 2 2
r 0.11108 0 2 cbr 500 ----- 0 0.0 3.0 2 2
+ 0.11108 2 3 cbr 500 ----- 0 0.0 3.0 2 2
- 0.11108 2 3 cbr 500 ----- 0 0.0 3.0 2 2
+ 0.115 0 2 cbr 500 ----- 0 0.0 3.0 3 3
- 0.115 0 2 cbr 500 ----- 0 0.0 3.0 3 3
r 0.11608 0 2 cbr 500 ----- 0 0.0 3.0 3 3
+ 0.11608 2 3 cbr 500 ----- 0 0.0 3.0 3 3
- 0.11608 2 3 cbr 500 ----- 0 0.0 3.0 3 3
+ 0.12 0 2 cbr 500 ----- 0 0.0 3.0 4 4
- 0.12 0 2 cbr 500 ----- 0 0.0 3.0 4 4
r 0.12108 0 2 cbr 500 ----- 0 0.0 3.0 4 4
+ 0.12108 2 3 cbr 500 ----- 0 0.0 3.0 4 4
```

Contents of Trace File



Topology

```
File Edit View Terminal Tabs Help
[root@localhost ~]# vi lab01.tcl
[root@localhost ~]# awk -f PA1.awk lab01.tr
cbr 139
cbr 143
cbr 130
cbr 149
cbr 151
cbr 154
cbr 139
cbr 159
cbr 163
cbr 145
cbr 169
cbr 171
cbr 174
cbr 177
cbr 179
cbr 182
The number of packets dropped =16
[root@localhost ~]#
```

Output

Exp 2: TRANSMISSION OF PING MESSAGE

Aim: Simulate the transmission of ping messages over a network topology consisting of 6 nodes and find the number of packets dropped due to congestion.

```
set ns [ new Simulator ]
set nf [ open lab4.nam w ]
$ns namtrace-all $nf
set tf [ open lab4.tr w ]
$ns trace-all $tf
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
set n5 [$ns node]
$ns duplex-link $n0 $n4 1005Mb 1ms DropTail
$ns duplex-link $n1 $n4 50Mb 1ms DropTail
$ns duplex-link $n2 $n4 2000Mb 1ms DropTail
$ns duplex-link $n3 $n4 200Mb 1ms DropTail
$ns duplex-link $n4 $n5 1Mb 1ms DropTail
set p1 [new Agent/Ping] # letters A and P should be capital
$ns attach-agent $n0 $p1
$p1 set packetSize_ 50000
$p1 set interval_ 0.0001
set p2 [new Agent/Ping] # letters A and P should be capital
$ns attach-agent $n1 $p2
set p3 [new Agent/Ping] # letters A and P should be capital
$ns attach-agent $n2 $p3
$p3 set packetSize_ 30000
$p3 set interval_ 0.00001
set p4 [new Agent/Ping] # letters A and P should be capital
$ns attach-agent $n3 $p4
set p5 [new Agent/Ping] # letters A and P should be capital
$ns attach-agent $n5 $p5
$ns queue-limit $n0 $n4 5
$ns queue-limit $n2 $n4 3
$ns queue-limit $n4 $n5 2
Agent/Ping instproc recv {from rtt} {
$self instvar node_
puts "node [$node_ id]received answer from $from with round trip time $rtt msec" }

# please provide space between $node_ and id. No space between $ and from. No space
between and $ and rtt */

$ns connect $p1 $p5
$ns connect $p3 $p4
proc finish { } {
global ns nf tf
$ns flush-trace
```

```
close $nf
close $tf
exec nam lab4.nam &
exit 0
}
$ns at 0.1 "$p1 send"
$ns at 0.2 "$p1 send"
$ns at 0.3 "$p1 send"
$ns at 0.4 "$p1 send"
$ns at 0.5 "$p1 send"
$ns at 0.6 "$p1 send"
$ns at 0.7 "$p1 send"
$ns at 0.8 "$p1 send"
$ns at 0.9 "$p1 send"
$ns at 1.0 "$p1 send"
$ns at 1.1 "$p1 send"
$ns at 1.2 "$p1 send"
$ns at 1.3 "$p1 send"
$ns at 1.4 "$p1 send"
$ns at 1.5 "$p1 send"
$ns at 1.6 "$p1 send"
$ns at 1.7 "$p1 send"
$ns at 1.8 "$p1 send"
$ns at 1.9 "$p1 send"
$ns at 2.0 "$p1 send"
$ns at 2.1 "$p1 send"
$ns at 2.2 "$p1 send"
$ns at 2.3 "$p1 send"
$ns at 2.4 "$p1 send"
$ns at 2.5 "$p1 send"
$ns at 2.6 "$p1 send"
$ns at 2.7 "$p1 send"
$ns at 2.8 "$p1 send"
$ns at 2.9 "$p1 send"

$ns at 0.1 "$p3 send"
$ns at 0.2 "$p3 send"
$ns at 0.3 "$p3 send"
$ns at 0.4 "$p3 send"
$ns at 0.5 "$p3 send"
$ns at 0.6 "$p3 send"
$ns at 0.7 "$p3 send"
$ns at 0.8 "$p3 send"
$ns at 0.9 "$p3 send"
$ns at 1.0 "$p3 send"
$ns at 1.1 "$p3 send"
$ns at 1.2 "$p3 send"
$ns at 1.3 "$p3 send"
$ns at 1.4 "$p3 send"
$ns at 1.5 "$p3 send"
```

```

$ns at 1.6 "$p3 send"
$ns at 1.7 "$p3 send"
$ns at 1.8 "$p3 send"
$ns at 1.9 "$p3 send"
$ns at 2.0 "$p3 send"
$ns at 2.1 "$p3 send"
$ns at 2.2 "$p3 send"
$ns at 2.3 "$p3 send"
$ns at 2.4 "$p3 send"
$ns at 2.5 "$p3 send"
$ns at 2.6 "$p3 send"
$ns at 2.7 "$p3 send"
$ns at 2.8 "$p3 send"
$ns at 2.9 "$p3 send"

$ns at 3.0 "finish"
$ns run

```

AWK file: (Open a new editor using “vi command” and write awk file and save with “.awk” extension)

```

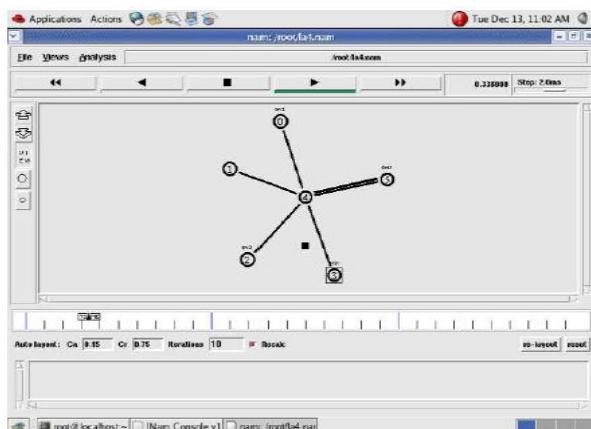
BEGIN{
drop=0;
}
{
if($1=="d" )
{
drop++;
}
}
END{
printf("Total number of %s packets dropped due to congestion =%d\n",$5,drop);
}

```

Steps for execution:

- 1) Open gedit editor and type program. Program name should have the extension “ .tcl ”
 - a. [root@localhost ~]# gedit lab4.tcl
2. Open gedit editor and type awk program. Program name should have the extension “.awk”
 - a. [root@localhost ~]# vi lab4.awk
3. Run the simulation program
 - a. [root@localhost~]# ns lab4.tcl
 - i) Here “ns” indicates network simulator. We get the topology shown in the snapshot.

- ii) Now press the play button in the simulation window and the simulation will begins.
 - 4) After simulation is completed run awk file to see the output,
- ```
[root@localhost~]# awk -f lab4.awk lab4.tr
```
- 5) To see the trace file contents open the file as ,
- ```
[root@localhost~]# gedit lab4.tr
```



Topology

```
root@localhost:~# Tue Dec 13, 10:41 AM
root@localhost:~# awk -f lab4.awk lab4.tr
root@localhost:~#
```

The screenshot shows a terminal window with the command 'awk -f lab4.awk lab4.tr' entered and its output displayed. The output consists of multiple lines of text showing the round trip times for each node (0, 1, 2, 3, 5) receiving answers from node 3. The time values fluctuate between 72.1 and 88.1 nsec.

Output

```
root@localhost:~# Tue Dec 13, 11:04 AM
root@localhost:~# awk -f lab4.awk lab4.tr
root@localhost:~# Number of ping packets dropped due to congestion are 20
root@localhost:~#
```

This screenshot shows a terminal window with the command 'awk -f lab4.awk lab4.tr' entered. The output includes the command itself, the message 'Number of ping packets dropped due to congestion are 20', and then the prompt '[root@localhost ~]#'. This indicates that the awk script processed the trace file and reported on congestion issues.

Output

Exp 3: ETHERNET LAN USING N-NODES

Aim: Simulate an Ethernet LAN using n nodes, change error rate and data rate and compare throughput.

```
set ns [new Simulator]
set tf [open lab5.tr w]
$ns trace-all $tf
set nf [open lab5.nam w]
$ns namtrace-all $nf
$ns color 0 blue
set n0 [$ns node]
$n0 color "red"
set n1 [$ns node]
$n1 color "red"
set n2 [$ns node]
$n2 color "red"
set n3 [$ns node]
$n3 color "red"
set n4 [$ns node]
$n4 color "magenta"
set n5 [$ns node]
$n5 color "magenta"
set n6 [$ns node]
$n6 color "magenta"
set n7 [$ns node]
$n7 color "magenta"
$ns make-lan "$n0 $n1 $n2 $n3" 100Mb 300ms LL Queue/ DropTail Mac/802_3 $ns make-lan "$n4
$n5 $n6 $n7" 100Mb 300ms LL Queue/ DropTail Mac/802_3
$ns duplex-link $n3 $n4 100Mb 300ms DropTail $ns duplex-link-op $n3 $n4 color "green"

#      set error rate. Here ErrorModel is a class and it is single word and space should not be given
between Error and Model

#      lossmodel is a command and it is single word. Space should not be given between loss and
model

set err [new ErrorModel]
$ns lossmodel $err $n3 $n4
$err set rate_ 0.1

# error rate should be changed for each output like 0.1,0.3,0.5.... */

set udp [new Agent/UDP]
$ns attach-agent $n1 $udp
set cbr [new Application/Traffic/CBR]
$cbr attach-agent $udp
$cbr set fid_ 0
$cbr set packetSize_ 1000
```

```

$cbr set interval_ 0.0001
set null [new Agent/Null]
$ns attach-agent $n7 $null
$ns connect $udp $null
proc finish { } {
    global ns nf tf
    $ns flush-trace
    close $nf
    close $tf
    exec nam lab5.nam &
    exit 0
}
$ns at 0.1 "$cbr start"
$ns at 3.0 "finish"
$ns run

```

AWK file: (Open a new editor using “vi command” and write awk file and save with “.awk” extension)

```

BEGIN{
pkt=0;
time=0;
}
{
if($1=="r" && $3=="9" && $4=="7"){
pkt = pkt + $6;
time =$2;
}
}
END {
printf("throughput:%fMbps",(( pkt / time) * (8 / 1000000)));
}

```

Steps for execution

- Open gedit editor and type program. Program name should have the extension “ .tcl ”
[*root@localhost ~]*# gedit lab5.tcl
- Open gedit editor and type awk program. Program name should have the extension “.awk ”
[*root@localhost ~]*# gedit lab5.awk
- Run the simulation program
[*root@localhost~*]# ns lab5.tcl
 - o Here “ns” indicates network simulator. We get the topology shown in the snapshot.
 - o Now press the play button in the simulation window and the simulation will begins.

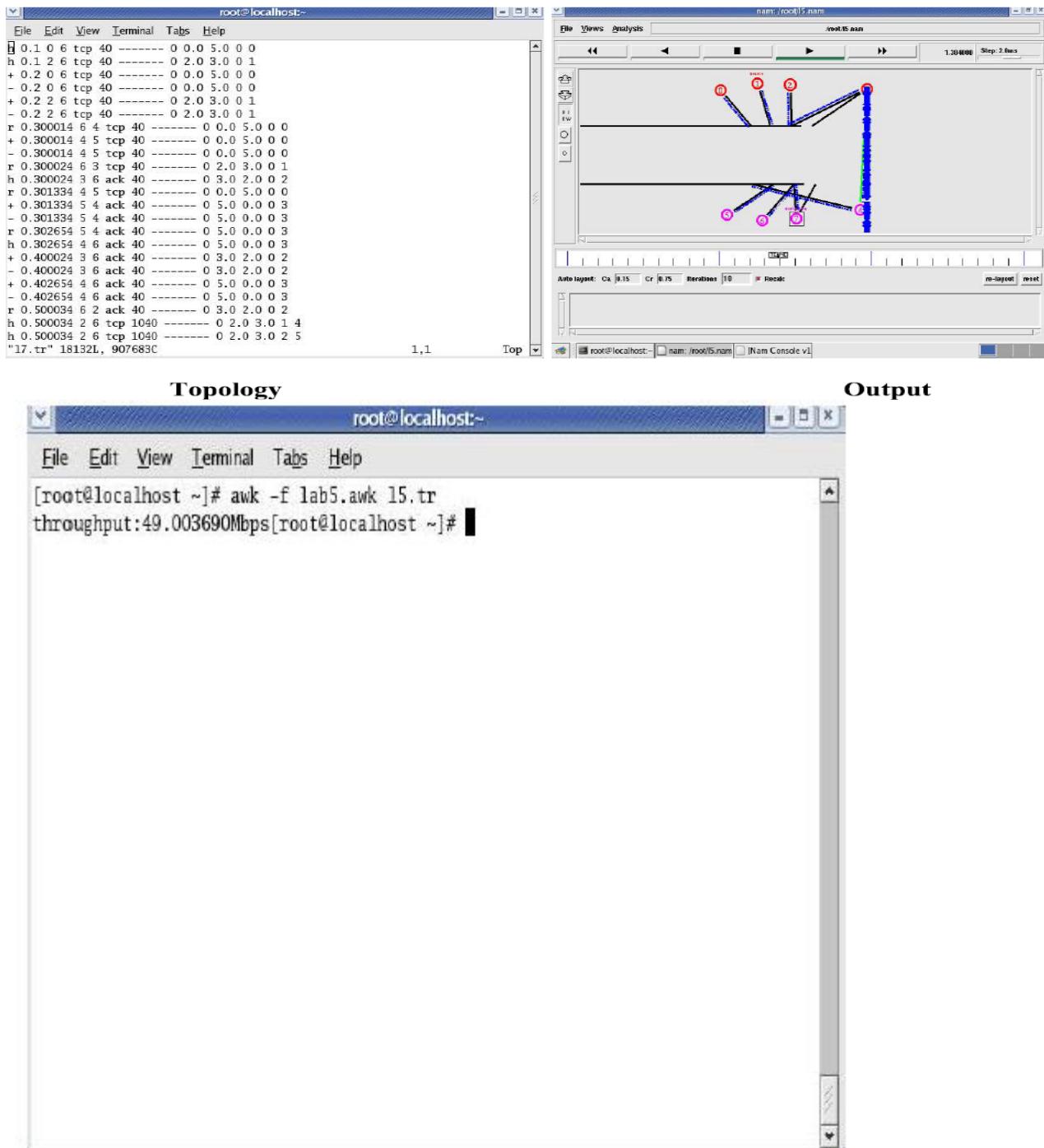
- After simulation is completed run awk file to see the output ,

```
[root@localhost~]# awk -f lab5.awk lab5.tr
```

- To see the trace file contents open the file as ,

```
[root@localhost~]# gedit lab5.tr
```

Here "h" indicates host.



This above output is for error rate 0.1. During next execution of simulation change error rate to 0.3, 0.5....., and check its effect on throughput.

Exp 4: ETHERNET LAN USING N-NODES WITH MULTIPLE TRAFFIC

Aim: Simulate an Ethernet LAN using n nodes and set multiple traffic nodes and plot congestion window for different source / destination

```
set ns [new Simulator]
set tf [open pgm7.tr w]
$ns trace-all $tf
set nf [open pgm7.nam w]
$ns namtrace-all $nf
set n0 [$ns node]
$n0 color "magenta"
$n0 label "src1"
set n1 [$ns node]
set n2 [$ns node]
$n2 color "magenta"
$n2 label "src2"
set n3 [$ns node]
$n3 color "blue"
$n3 label "dest2"
set n4 [$ns node]
set n5 [$ns node]
$n5 color "blue"
$n5 label "dest1"
$ns make-lan "$n0 $n1 $n2 $n3 $n4" 100Mb 100ms LL Queue/ DropTail Mac/802_3
```

#should come in single line

```
$ns duplex-link $n4 $n5 1Mb 1ms DropTail
set tcp0 [new Agent/TCP]
$ns attach-agent $n0 $tcp0
set ftp0 [new Application/FTP]
$ftp0 attach-agent $tcp0
$ftp0 set packetSize_ 500
$ftp0 set interval_ 0.0001
set sink5 [new Agent/TCPSink]
$ns attach-agent $n5 $sink5
$ns connect $tcp0 $sink5
set tcp2 [new Agent/TCP]
$ns attach-agent $n2 $tcp2
set ftp2 [new Application/FTP]
$ftp2 attach-agent $tcp2
$ftp2 set packetSize_ 600
$ftp2 set interval_ 0.001
set sink3 [new Agent/TCPSink]
$ns attach-agent $n3 $sink3
$ns connect $tcp2 $sink3
set file1 [open file1.tr w]
```

```

$tcp0 attach $file1
set file2 [open file2.tr w]
$tcp2 attach $file2
$tcp0 trace cwnd_      # must put underscore ( _ ) after cwnd and no space between them $tcp2 trace
cwnd_
proc finish { } {
global ns nf tf
$ns flush-trace
close $tf
close $nf
exec nam pgm7.nam &
exit 0
}
$ns at 0.1 "$ftp0 start"
$ns at 5 "$ftp0 stop"
$ns at 7 "$ftp0 start"
$ns at 0.2 "$ftp2 start"
$ns at 8 "$ftp2 stop"
$ns at 14 "$ftp0 stop"
$ns at 10 "$ftp2 start"
$ns at 15 "$ftp2 stop"
$ns at 16 "finish"
$ns run

```

AWK file: (Open a new editor using “vi command” and write awk file and save with “.awk” extension)

cwnd:- means congestion window

```

BEGIN {
}
{
if($6=="cwnd_")          # don't leave space after writing cwnd_
printf("%f\t%f\n",$1,$7); # you must put \n in printf
}
END {
}

```

Steps for execution

- Open gedit editor and type program. Program name should have the extension “.tcl ”

[root@localhost ~]# gedit lab7.tcl

- Open gedit editor and type awk program. Program name should have the extension “.awk ”

[root@localhost ~]# gedit lab7.awk

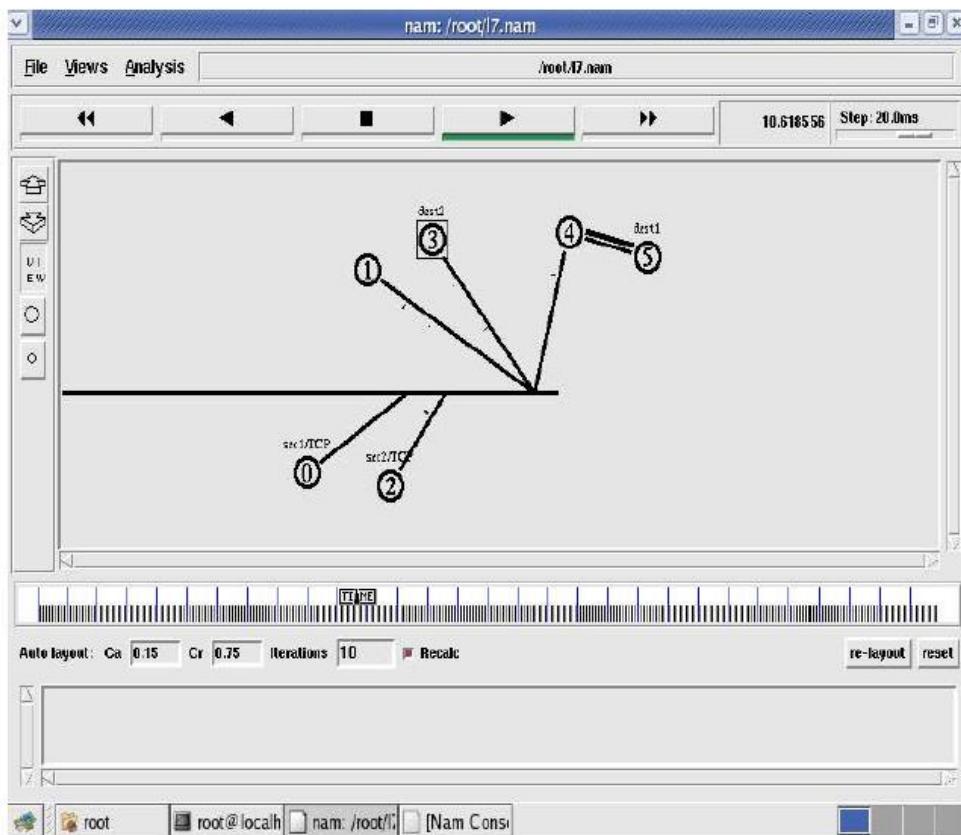
- Run the simulation program

```
[root@localhost~]# ns lab7.tcl
```

- After simulation is completed run awk file to see the output , [root@localhost~]# awk –f lab7.awk file1.tr > a1 [root@localhost~]# awk –f lab7.awk file2.tr > a2 [root@localhost~]# xgraph a1 a2
- Here we are using the congestion window trace files i.e. file1.tr and file2.tr and we are redirecting the contents of those files to new files say a1 and a2 using output redirection operator (>).
- To see the trace file contents open the file as ,

```
[root@localhost~]# gedit lab7.tr
```

Topology:



Output:

