PRESIDENCY UNIVERSITY BENGALURU

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CSE3155 DATA COMMUNICATION AND COMPUTER NETWORK LAB MANUAL

III B.Tech 3rd Semester A.Y (2024-25)

Instructor Incharge: Dr.Akshatha Y, Ms.Soumya

Course Credit Structure: 3-2-4 (4 Credits)

DOS COMMANDS

1. PING Command

How to check internet connection in CMD

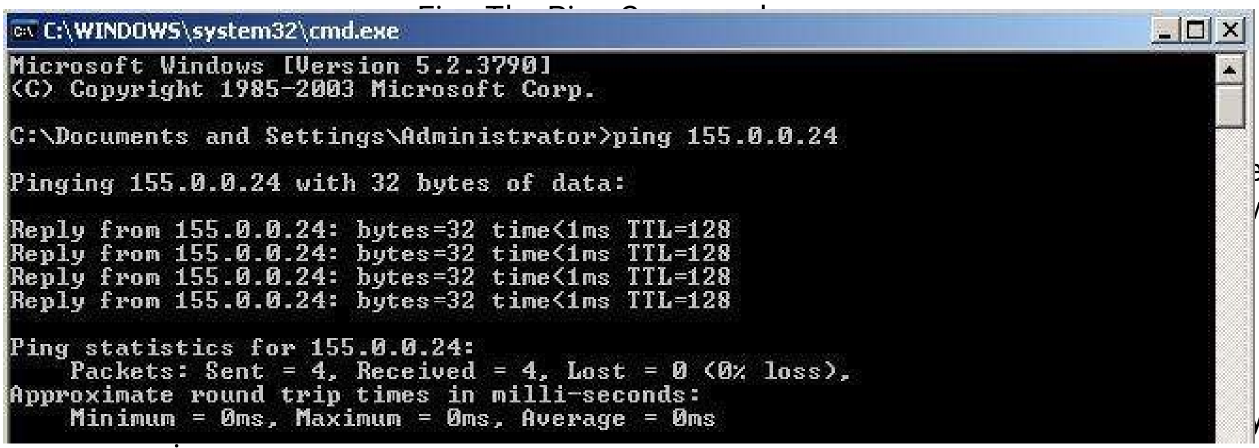
To check whether your internet connection works, you can use Command Prompt to test your connection to a certain website or internet location. To do that, you can use the ping network command, followed by a web address or IP address. For instance, you can check the connectivity to GOOGLE without opening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

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

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

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

Fig: The Ping Command



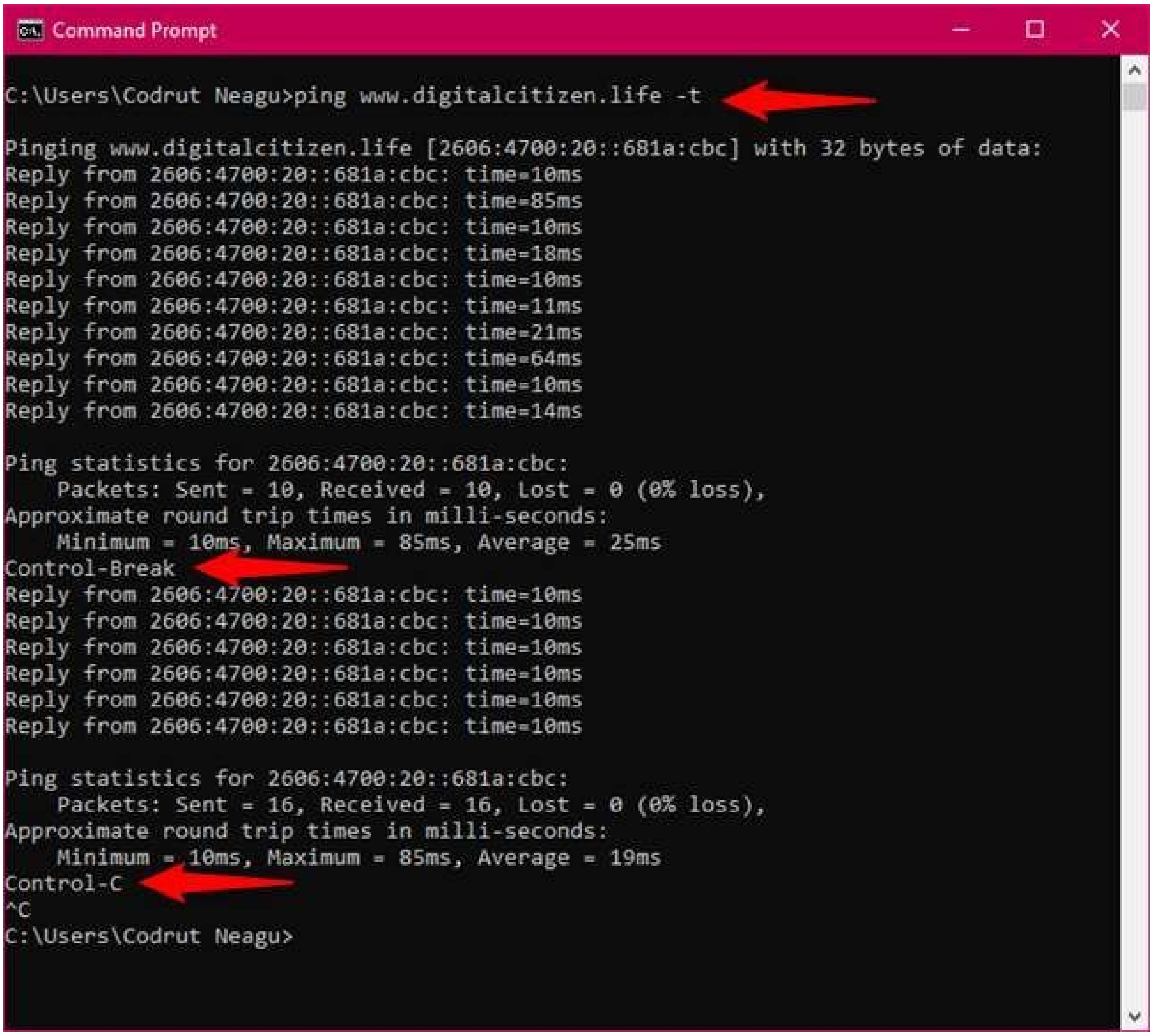
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

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
Reply from 155.0.0.24: bytes=32 time<1ms TTL=128
Reply from 155.0.0.24: bytes=32 time<1ms TTL=128
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
```

es

we

y

pressing
Ctrl + C

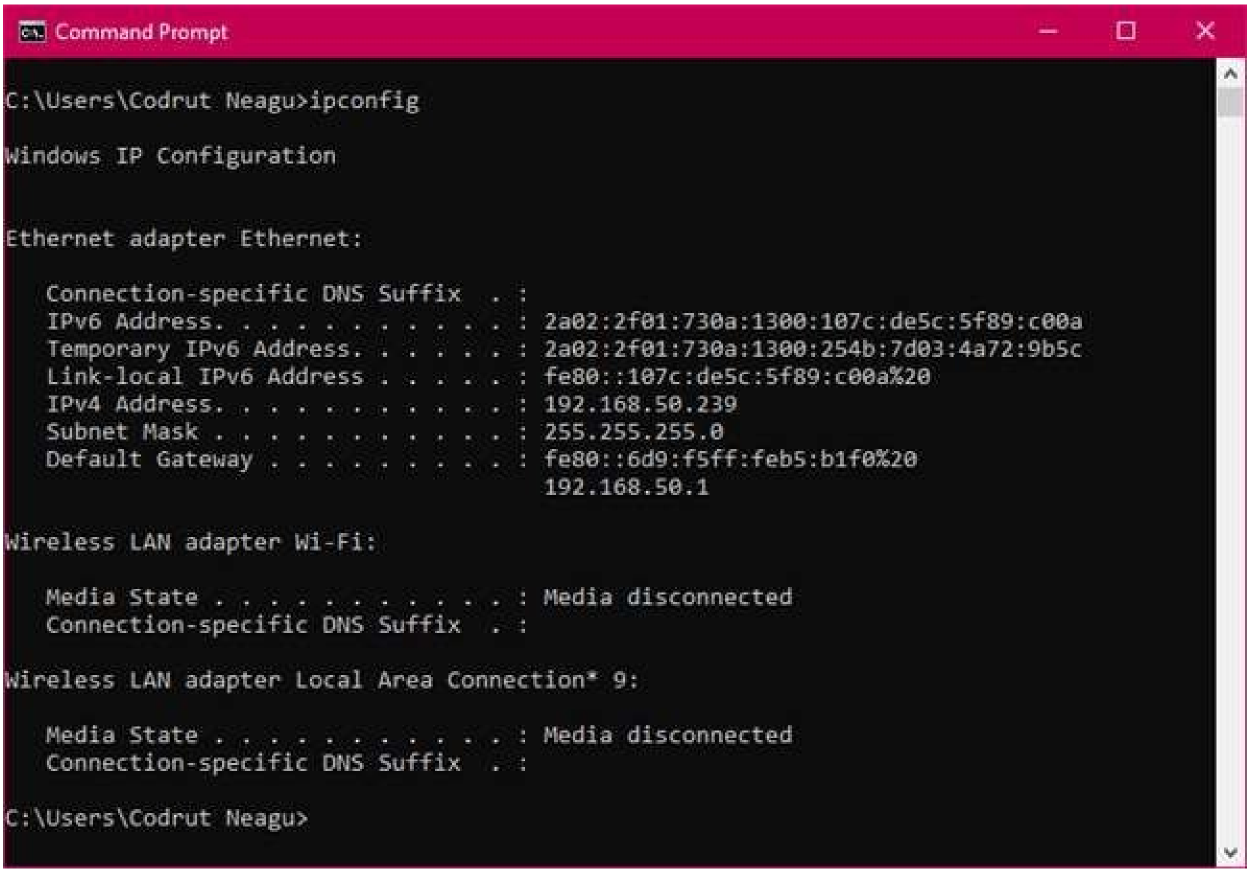


```
C:\Users\Codrut Neagu>ping www.digitalcitizen.life -t

Pinging www.digitalcitizen.life [2606:4700:20::681a:cbc] with 32 bytes of data:
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=85ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=18ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=11ms
Reply from 2606:4700:20::681a:cbc: time=21ms
Reply from 2606:4700:20::681a:cbc: time=64ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=14ms

Ping statistics for 2606:4700:20::681a:cbc:
    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:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=10ms
Reply from 2606:4700:20::681a:cbc: time=10ms

Ping statistics for 2606:4700:20::681a:cbc:
    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?

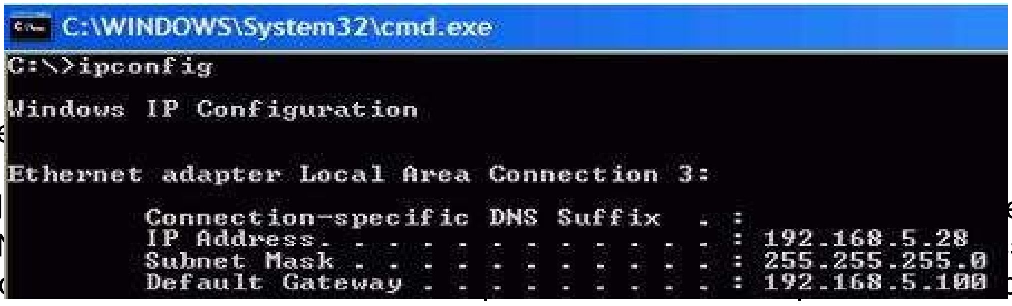
To obtain detailed information about your network adapters and connections, use the ipconfig command. Open Command Prompt, type ipconfig, and press Enter. As you can see in the screenshot below, when you run this command, Windows displays the list of all the active network devices, whether they're connected 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.



```
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.

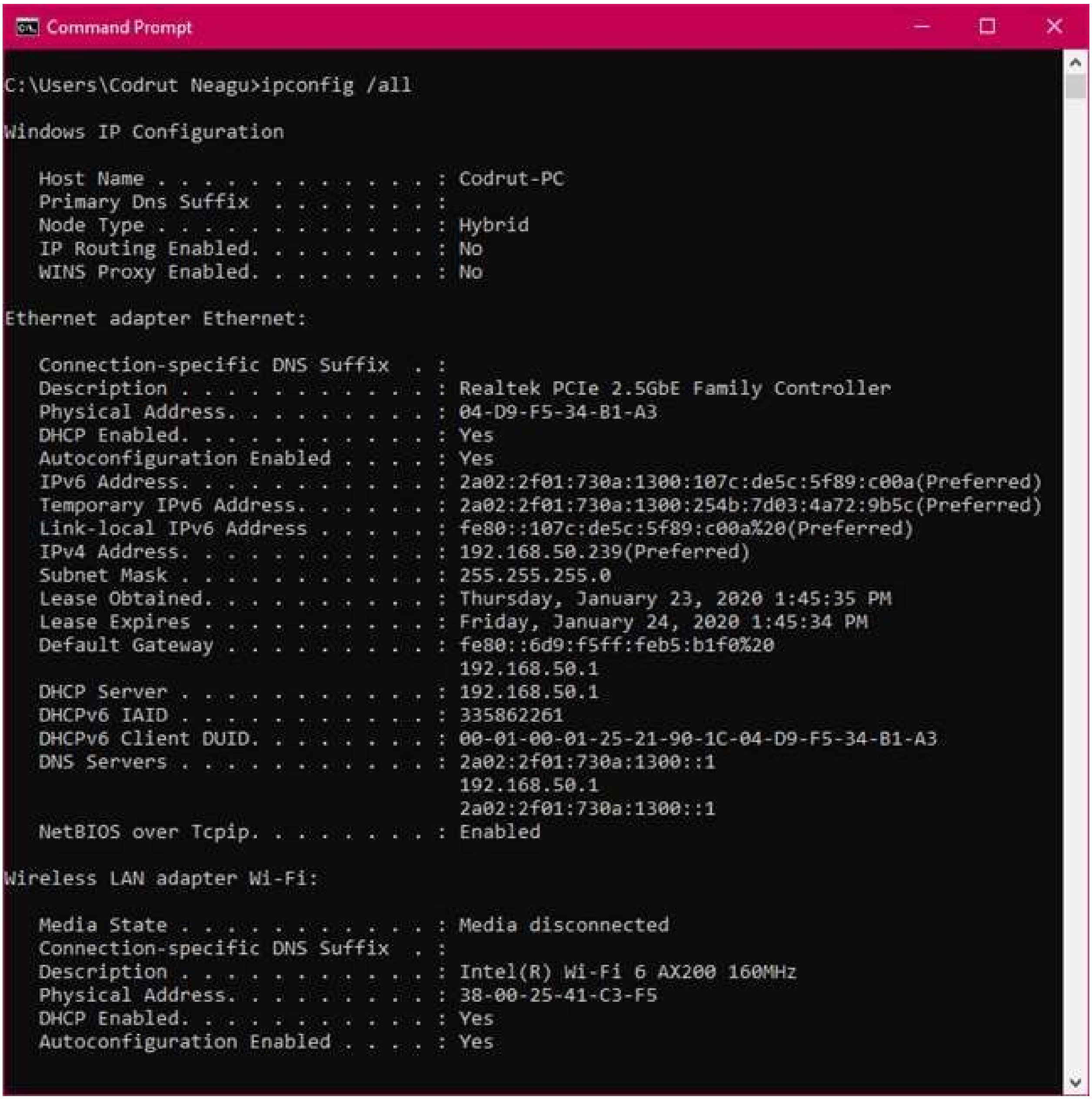
C:\ipconfig



```
C:\>ipconfig

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
```

Now type

If you ad evel of detail: DN s field), and other inf o see a sample of what you get from the "ipconfig /all" command.



```
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
   DHCPv6 IAID . . . . . . . . . . . : 335862261
   DHCPv6 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

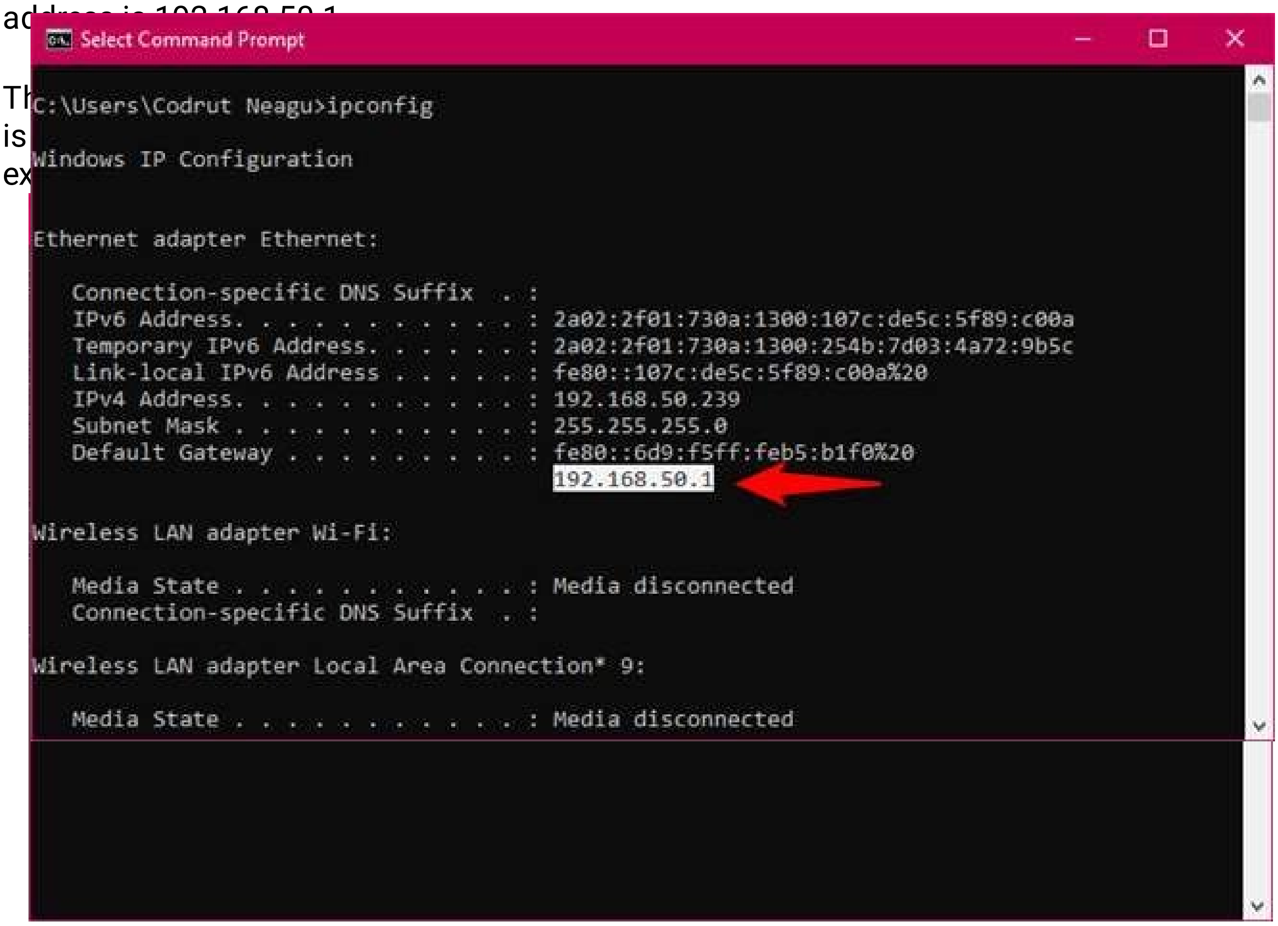
How to check your network connection in CMD

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

Th

is

ex



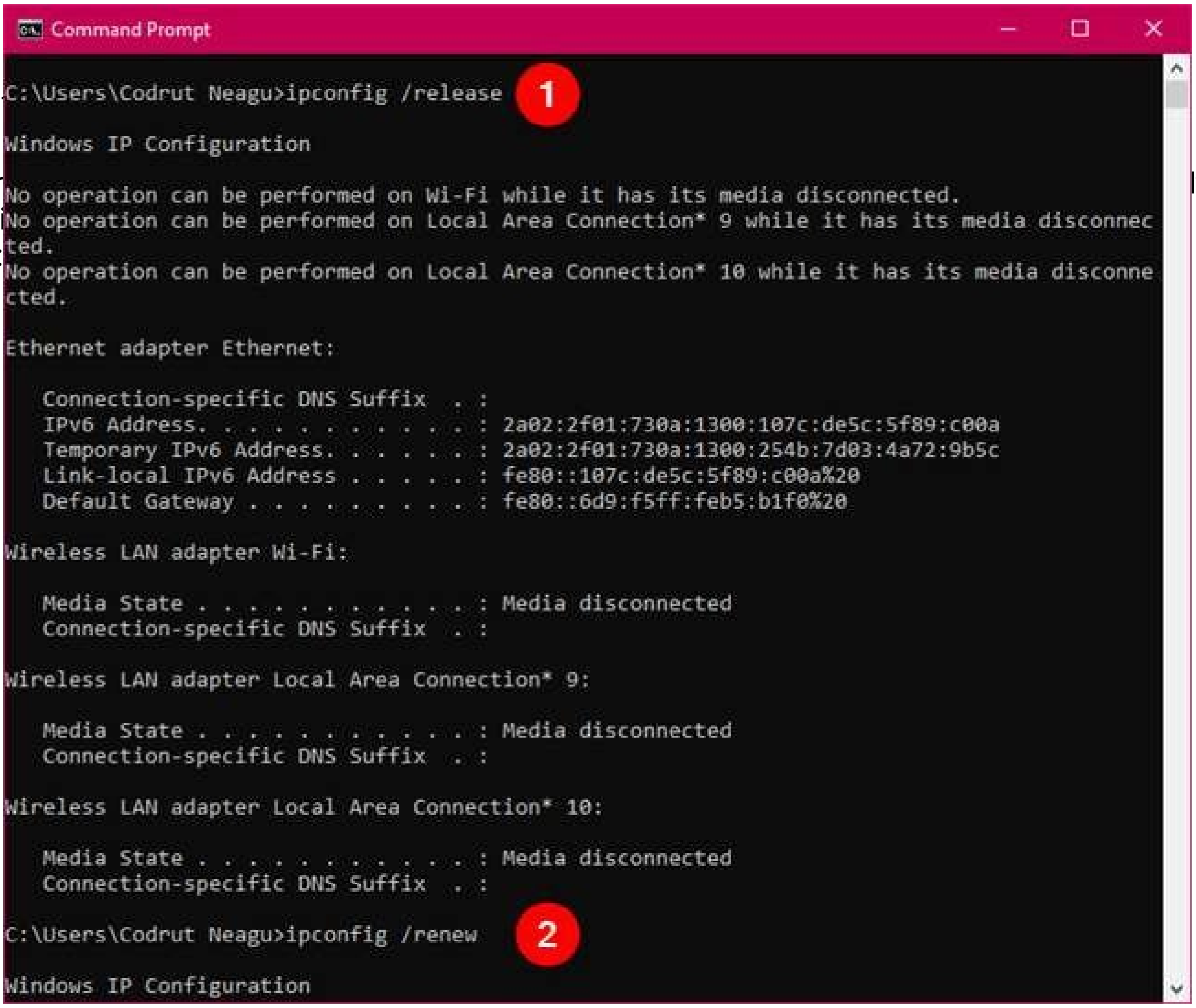
```
C:\Users\Codrut Neagu>ipconfig

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: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

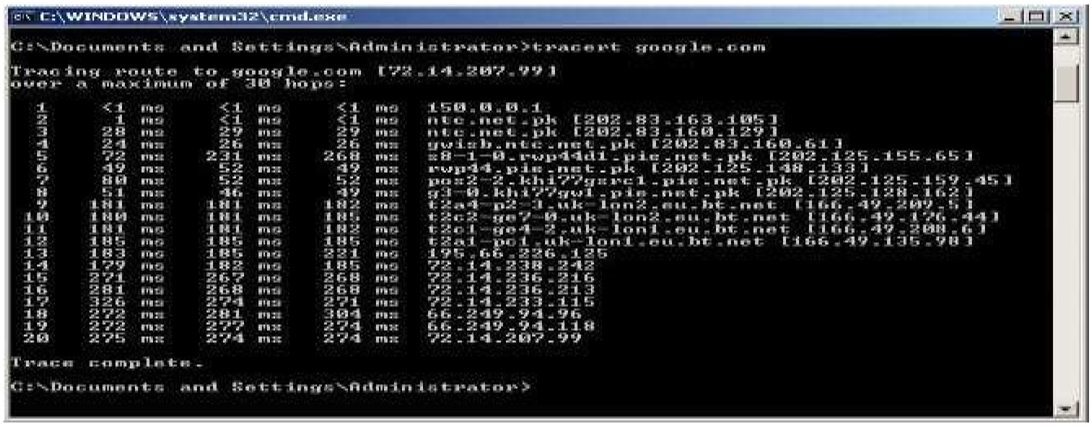
When your network connection doesn't work as it should, your network adapter might not have the right IP address assigned. A quick way of trying to solve this issue is to renew its IP address and, fortunately, you can do that quickly, straight from the Command Prompt. Open CMD and run the following commands: 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.



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

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 disconnec
ted.
No operation can be performed on Local Area Connection* 10 while it has its media disconne
cted.

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

Windows IP Configuration
```

3

Tr It
wi
C:



```
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 [202.83.163.105]
  3    28 ms    29 ms    29 ms  ntc.net.pk [202.83.160.129]
  4    24 ms    26 ms    26 ms  gwisb.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    52 ms  pos2-2.khi77gsrc1.pie.net.pk [202.125.159.45]
  8    51 ms    46 ms    49 ms  g3-0.khi77gw1.pie.net.pk [202.125.128.162]
  9   181 ms   181 ms   182 ms  t2a4-p2-3.uk-lon2.eu.bt.net [166.49.209.5]
 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   274 ms   271 ms  72.14.233.115
 18   272 ms   281 ms   304 ms  66.249.94.96
 19   272 ms   277 ms   274 ms  66.249.94.118
 20   275 ms   274 ms   274 ms  72.14.207.99

Trace complete.

C:\Documents and Settings\Administrator>
```

4. NSLOOKUP Command

Displays the default DNS server information.

Type the following command

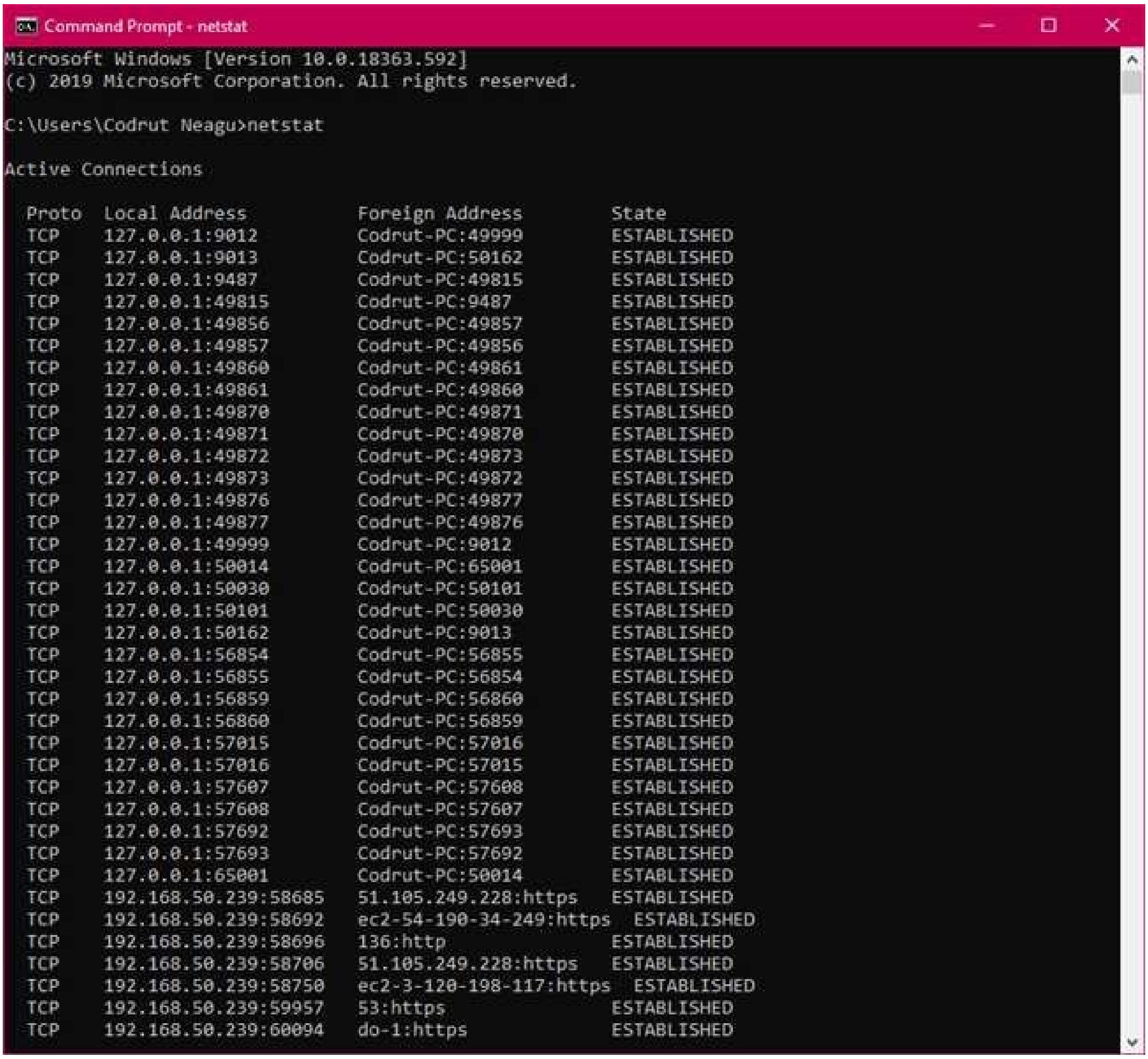
C:\>nslookup

What is your default DNS server's IP address?

5. NETSTAT Command

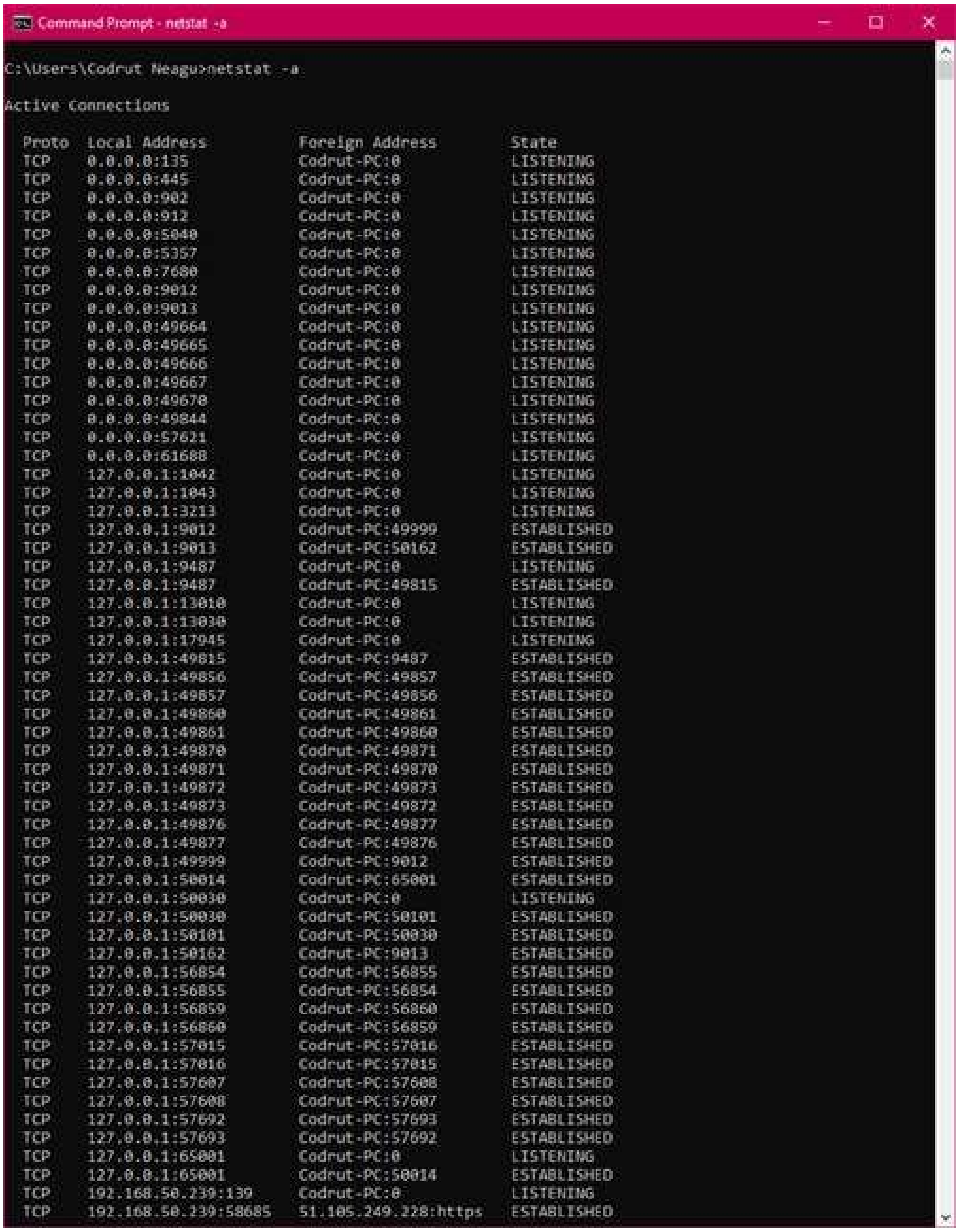
You can get other useful cmd nic info from the netstat command, which lets you see the network connections that are active between your system and any other systems on your network or the internet.

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



```
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:9012         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: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: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.



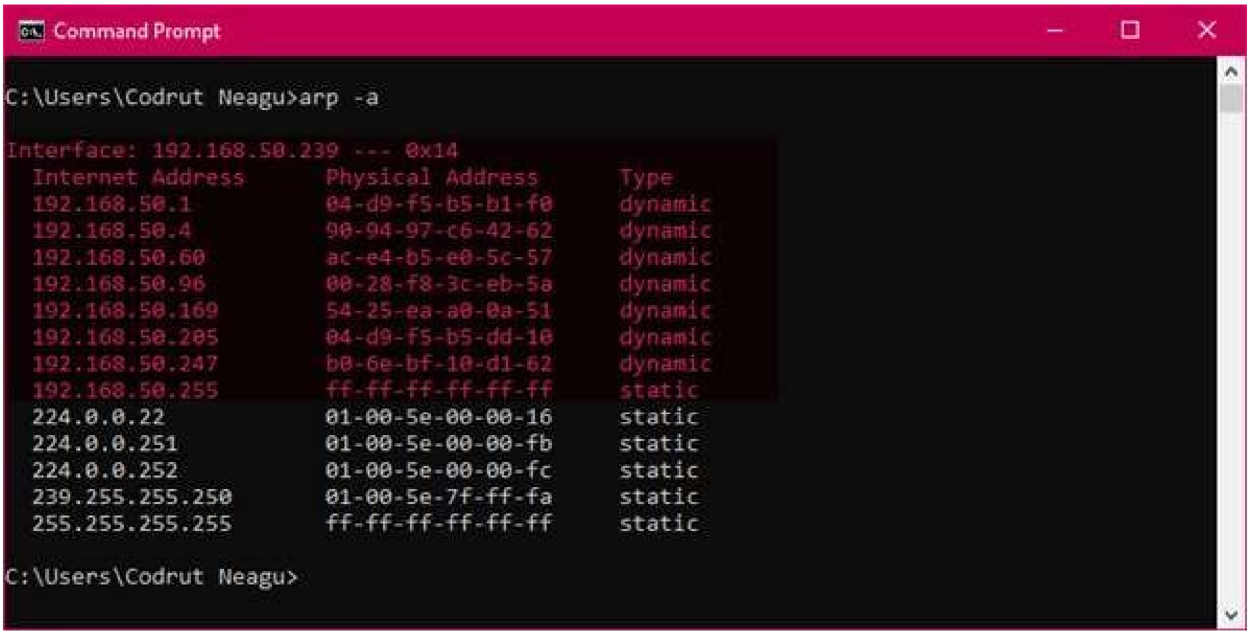
```
C:\Users\Codrut Neagu>netstat -a

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    0.0.0.0:9013           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: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:0            LISTENING
  TCP    127.0.0.1:65001        Codrut-PC:50014        ESTABLISHED
  TCP    192.168.50.239:139     Codrut-PC:0            LISTENING
  TCP    192.168.50.239:58685   51.105.249.228:https   ESTABLISHED
```

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

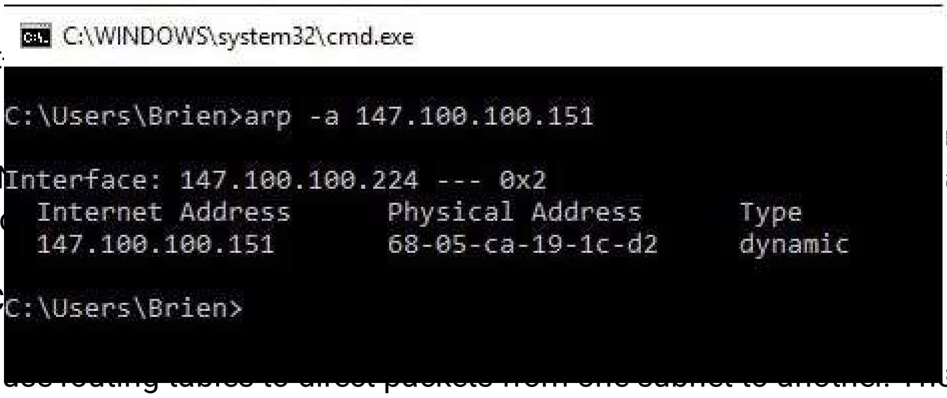
6. ARP Command

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.



```
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>
```



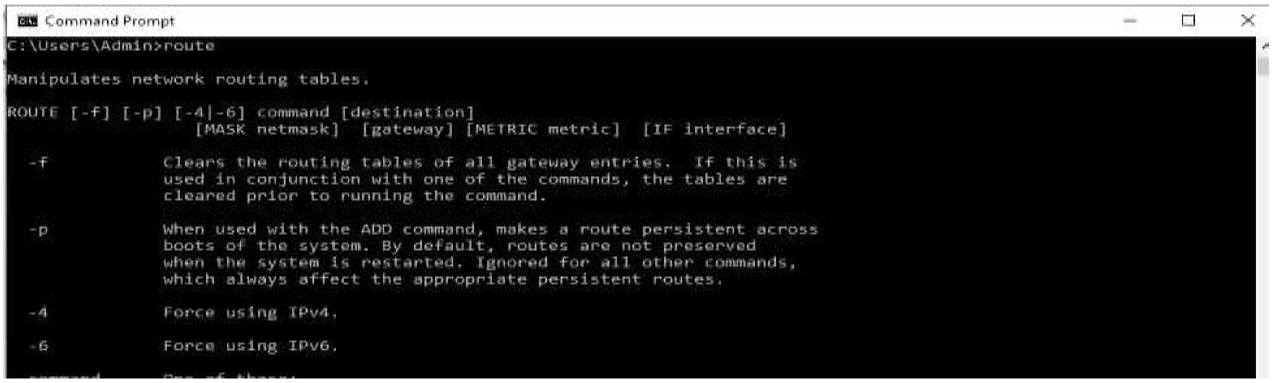
```
C:\Users\Brien>arp -a 147.100.100.151

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

The NbtStat e by a device. The N as been able to resolve re

8. Route C

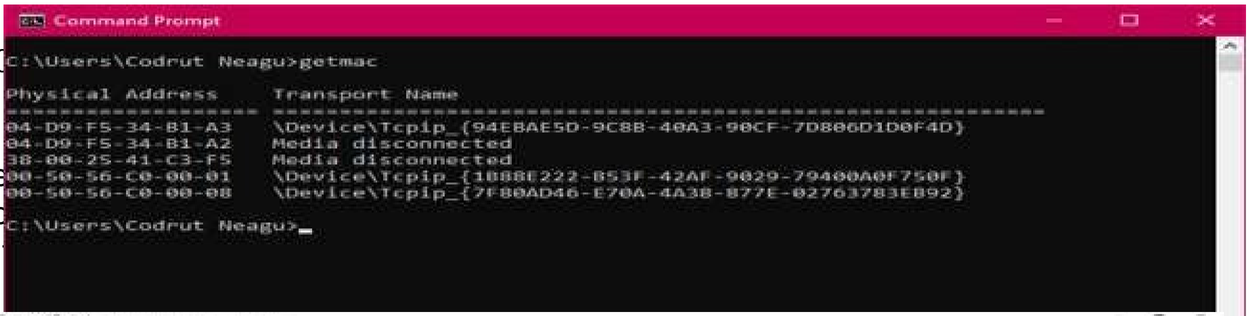
IP networks use routing tables to direct packets from one subnet to another. The Windows Route utility allows you to view the device's routing tables. The Route command is that it not only shows you the routing table, it lets you make changes. Commands such as Route Add, Route Delete, and Route Change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



```
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.



```
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_{1888E222-B53F-42AF-9029-79400A0F750F}
00-50-56-C0-00-08   \Device\Tcpip_{7F80AD46-E70A-4A38-877E-02763783EB92}

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

10

If

ve

yo

in

```
[illegible]
```

CISCO PACKET TRACER TOOL

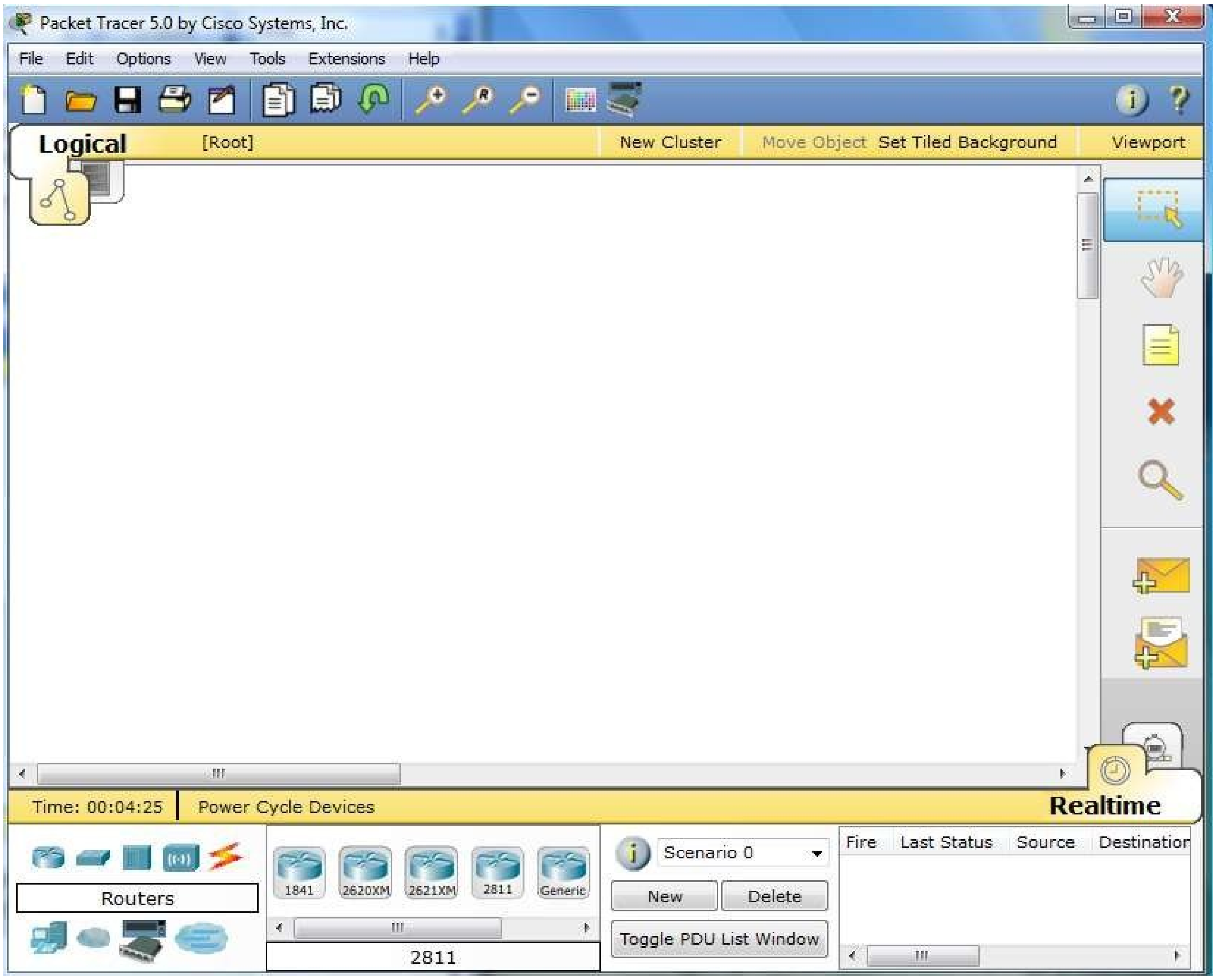
Packet Tracer – Creating a New Topology

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

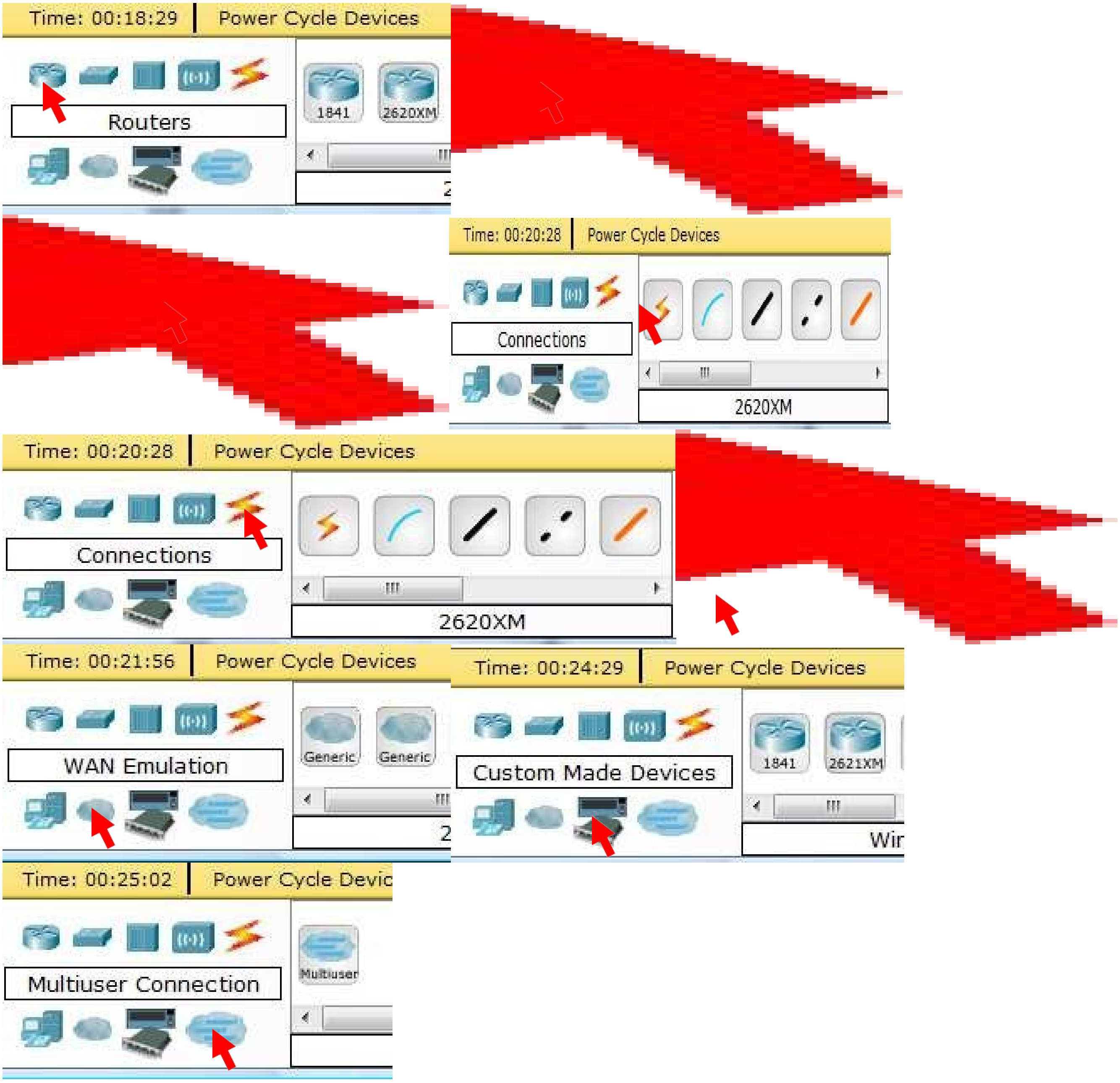
Step 1: Start Packet Tracer



Step 2: Choosing Devices and Connections

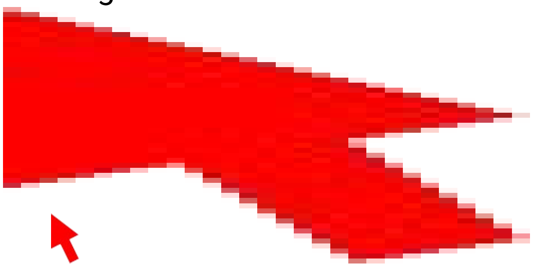
We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, Hubs, and Connections.

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

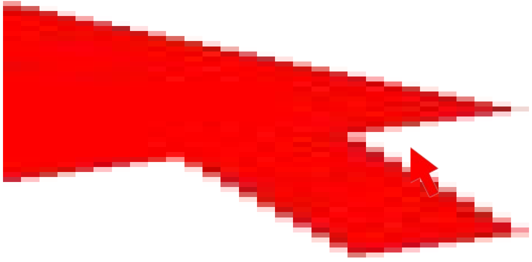


Step 3: Building the Topology – Adding Hosts

Single click on the End Devices.



Single click on the Generic host.

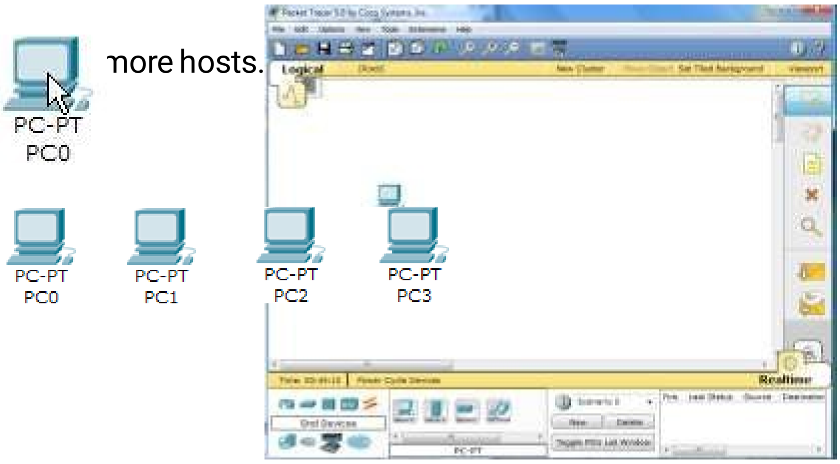


Move the cursor into topology area. You will notice it turns into a plus “+” sign.

+

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

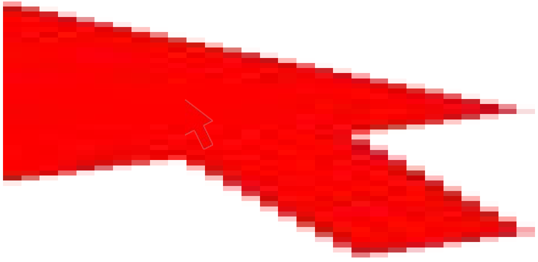
Ad more hosts.

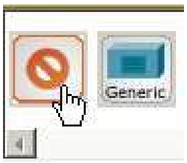


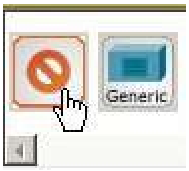
Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

Adding a Hub

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

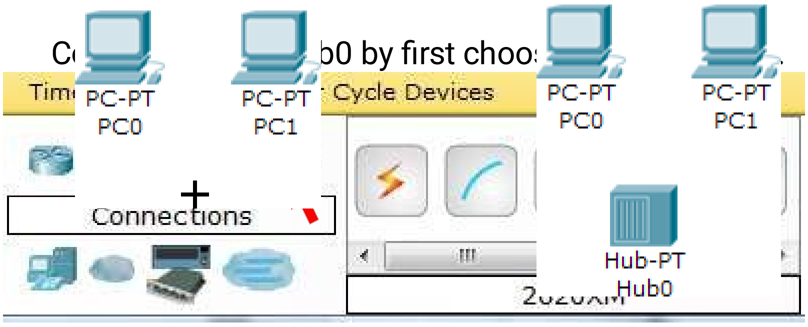




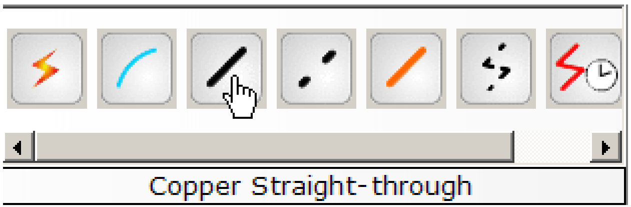


Add the hub by moving the plus sign "+" below PC0 and PC1 and click once.

C b0 by first choo



Click once on the Copper Straight-through cable.



o Hub0:

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.

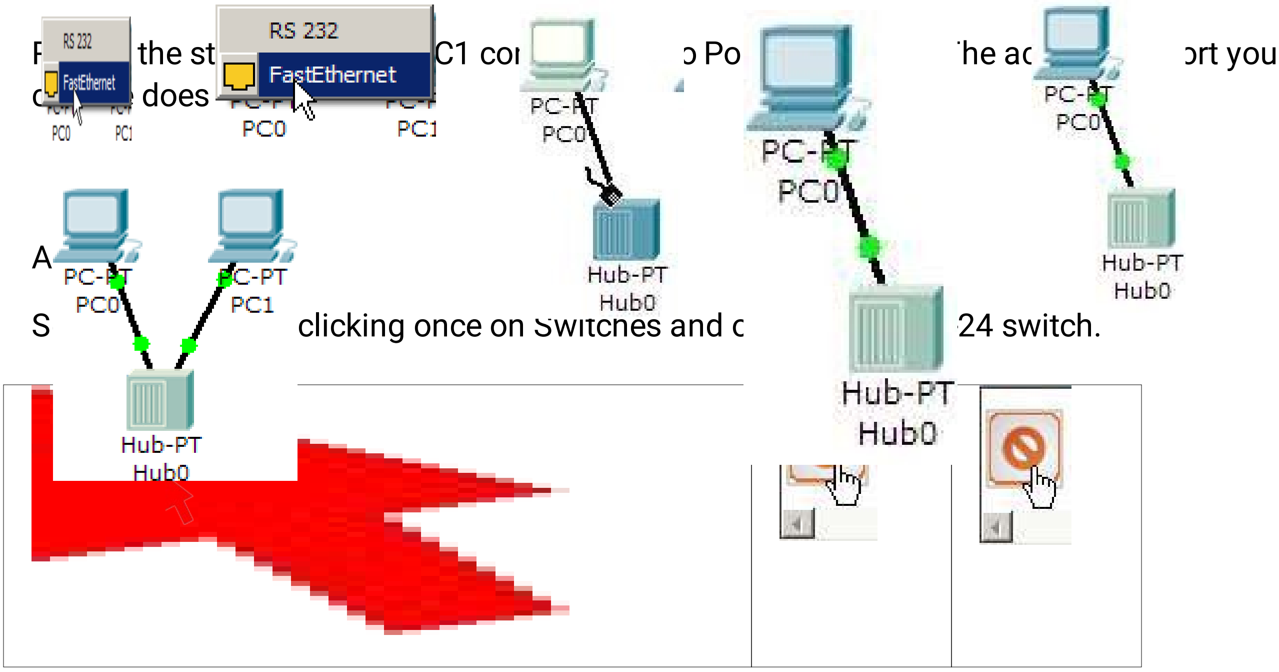
12345

F the st C1 co Po he ac ort you

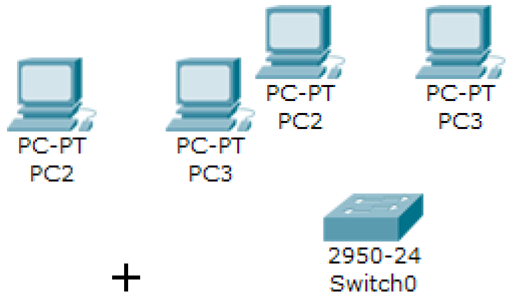
c does

A

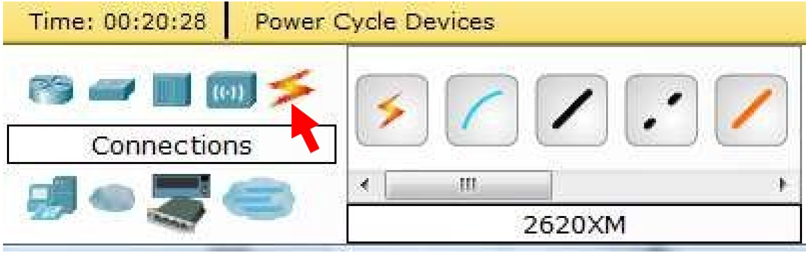
S clicking once on Switches and c 24 switch.



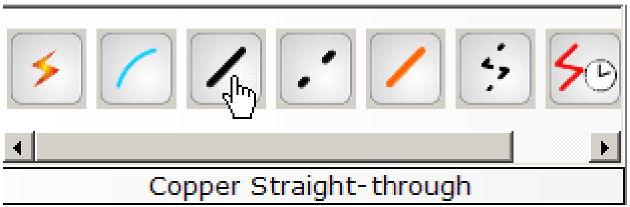
Add the switch by moving the plus sign “+” below PC2 and PC3 and click once.



Connect PC2 to Hub0 by first choosing Connections.



Click once on the Copper Straight-through cable.

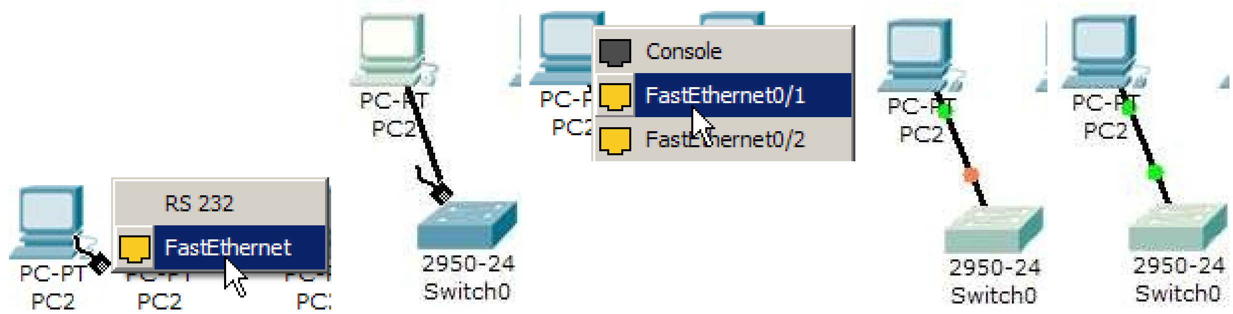


o Switch0:

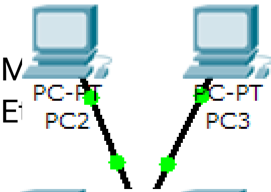
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0 FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP)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

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

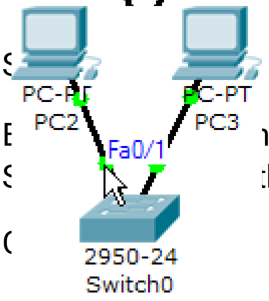
123456



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



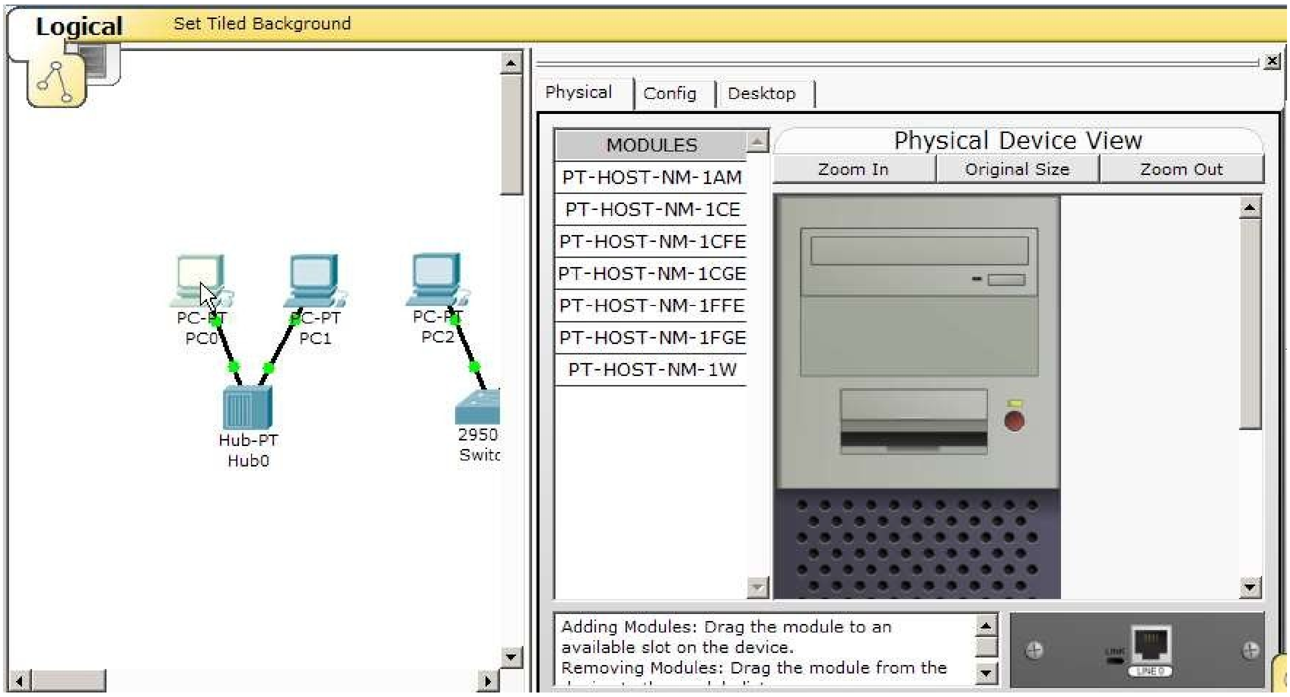
M er the link light to view the port number. Fa means FastEthernet, 100 Mbps E



S IP Addresses and Subnet Masks on the Hosts

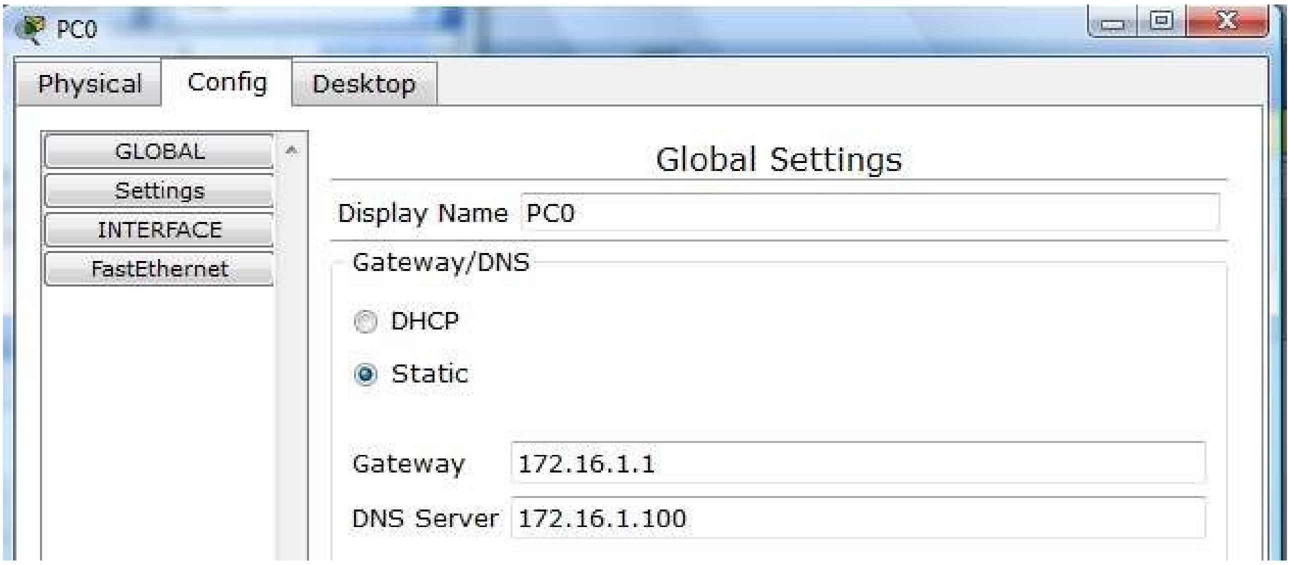
E ımunicate between the hosts we need to configure IP Addresses and S :he devices.

(



Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the

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.



Global Settings

Display Name PC0

Gateway/DNS

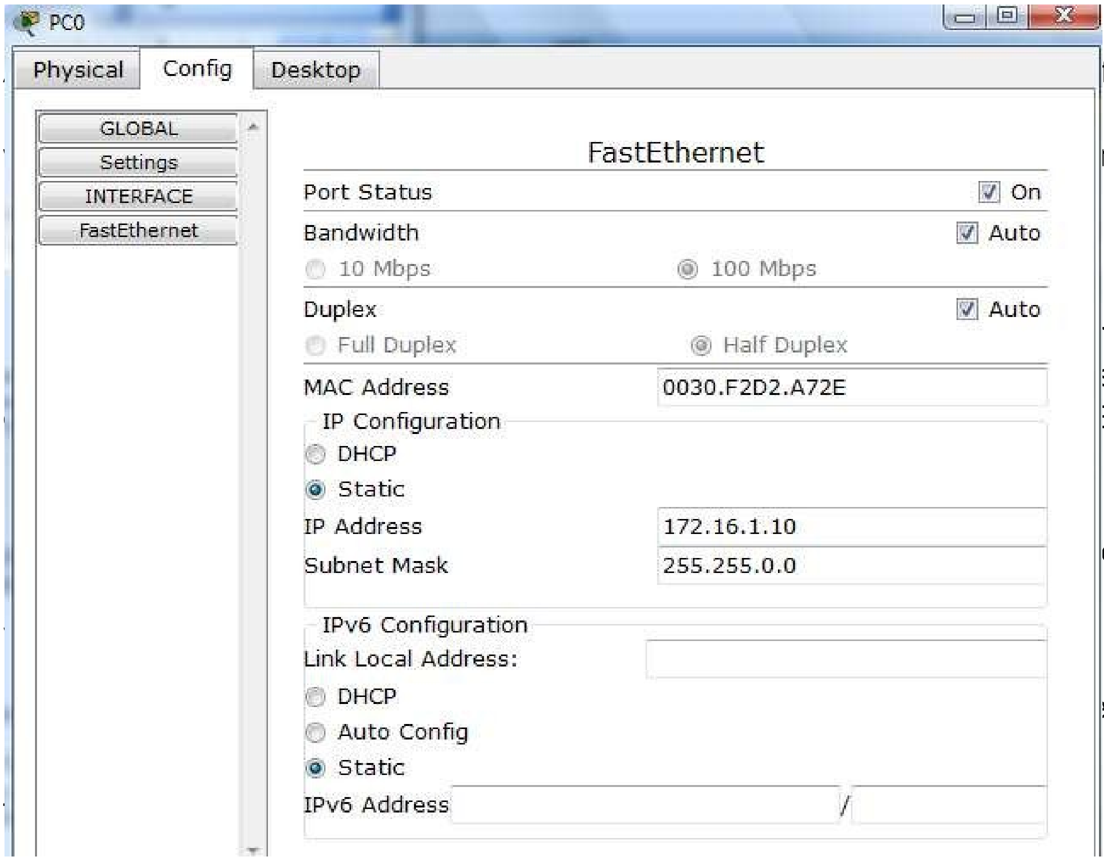
○ DHCP

● Static

Gateway 172.16.1.1

DNS Server 172.16.1.100

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.



FastEthernet

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

○ Full Duplex ● Half Duplex

MAC Address 0030.F2D2.A72E

IP Configuration

○ DHCP

● Static

IP Address 172.16.1.10

Subnet Mask 255.255.0.0

IPv6 Configuration

Link Local Address:

○ DHCP

○ Auto Config

● Static

IPv6 Address /

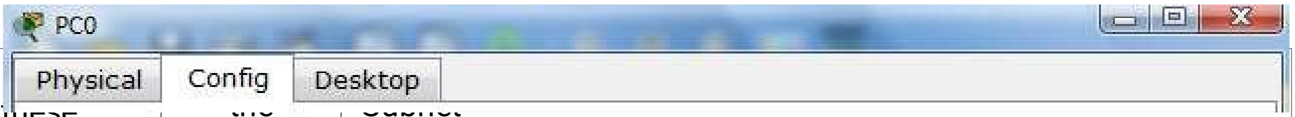
f the Ethernet
ns the NIC
nually set by

e Ethernet
switch port
thernet).

oose Half Duplex.

s Full Duplex
If the switch
Half Duplex.

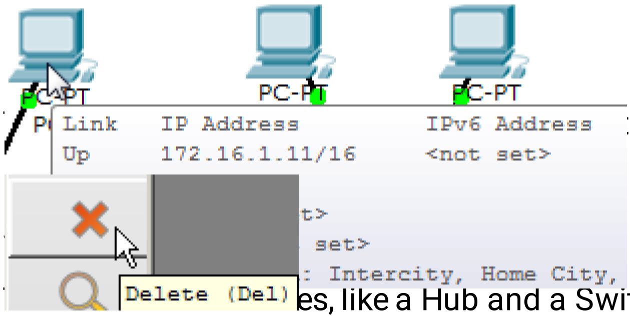
To close this dialog box, click the “X” in the upper right.



these Masks.	the	Subnet
Host	IP Address	Subnet Mask
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

Verify the information

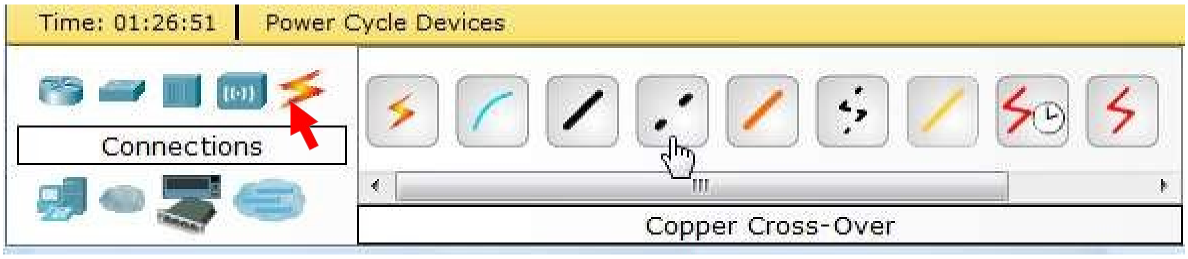
To verify the information that you entered, move the Select tool (arrow) over each host.



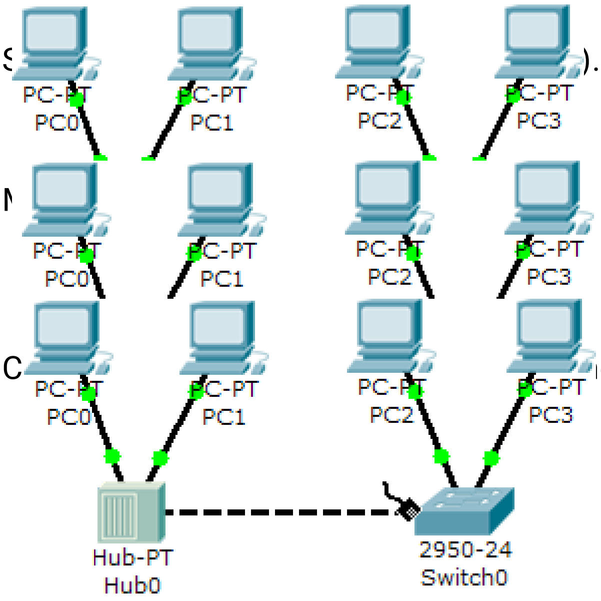
```
Link    IP Address          IPv6 Address
Up      172.16.1.11/16      <not set>
t>
set>
: Intercity, Home City,
```

tool and click on the item you wish to delete.

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



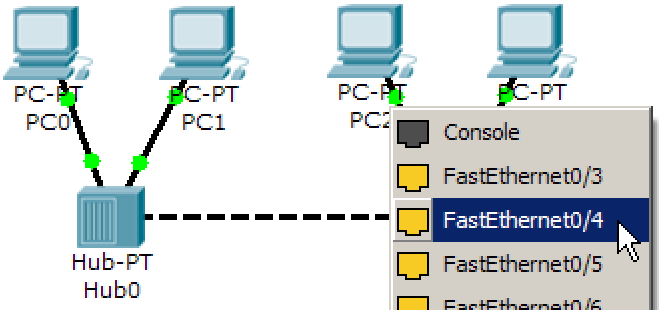
Move the Connections cursor over Hub0 and click once.



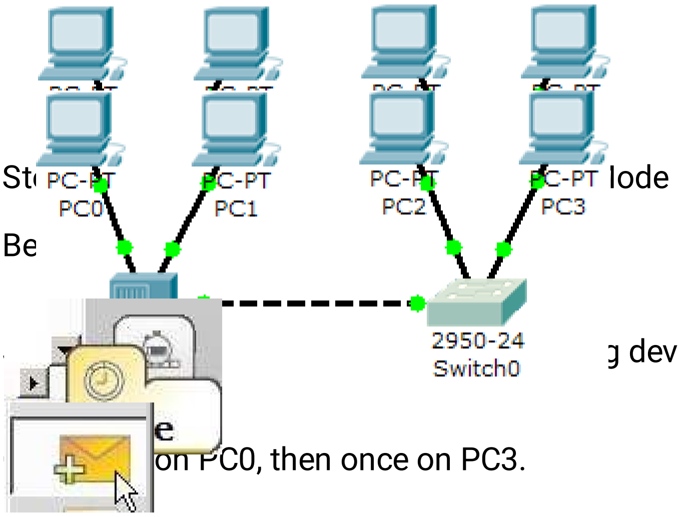
S).

N

C ernet0/4 (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.

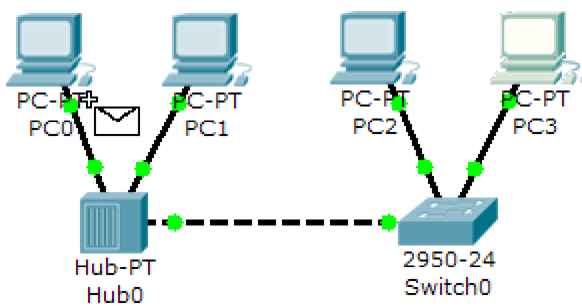


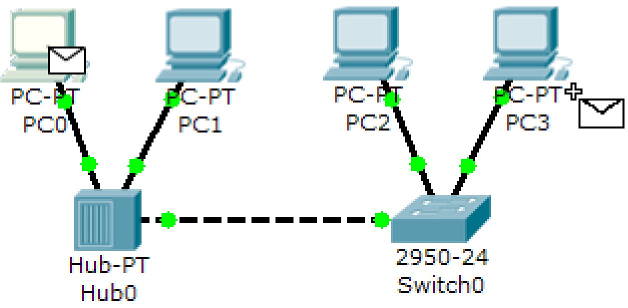
St lode

Be

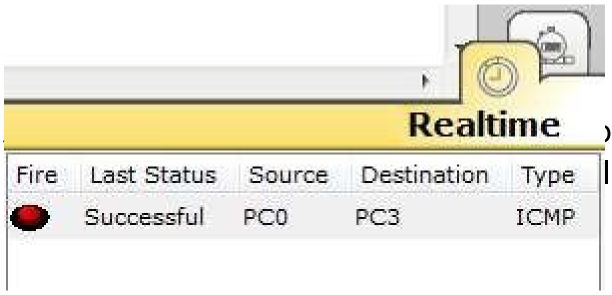
g devices..

on PC0, then once on PC3.



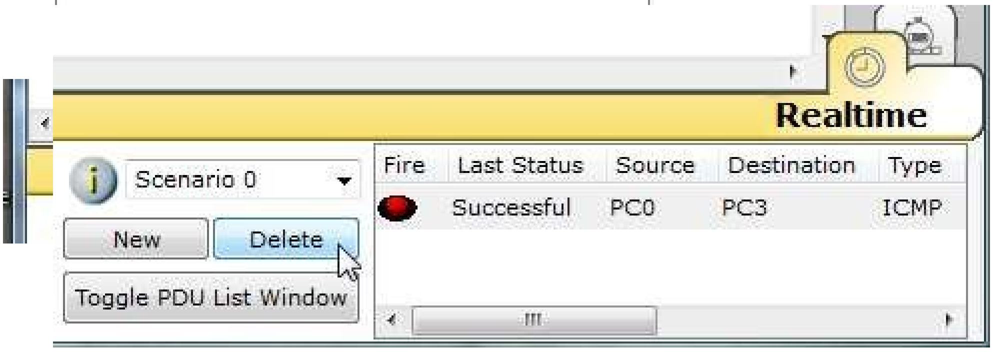


The PDU Last Status should show as Successful.

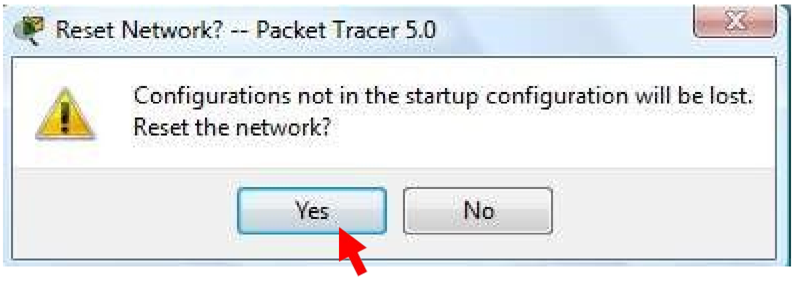


Fire	Last Status	Source	Destination	Type
●	Successful	PC0	PC3	ICMP

rk, Whenever you want to reset the network and lowing tasks:



Fire	Last Status	Source	Destination	Type
●	Successful	PC0	PC3	ICMP

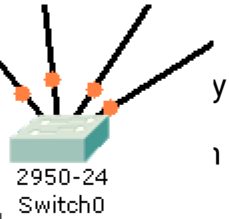


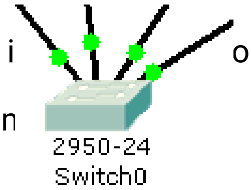
Reset Network? -- Packet Tracer 5.0

Configurations not in the startup configuration will be lost. Reset the network?

Waiting for Spanning Tree Protocol (STP)

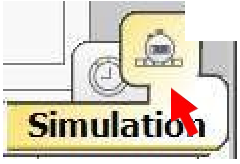
Note: Because Packet Tracer also simulates the Spanning Tree Protocol (later), at times the switch may show amber lights on its interfaces. You will need to wait for the lights to turn green on the switches before they will forward any Ethernet frames.



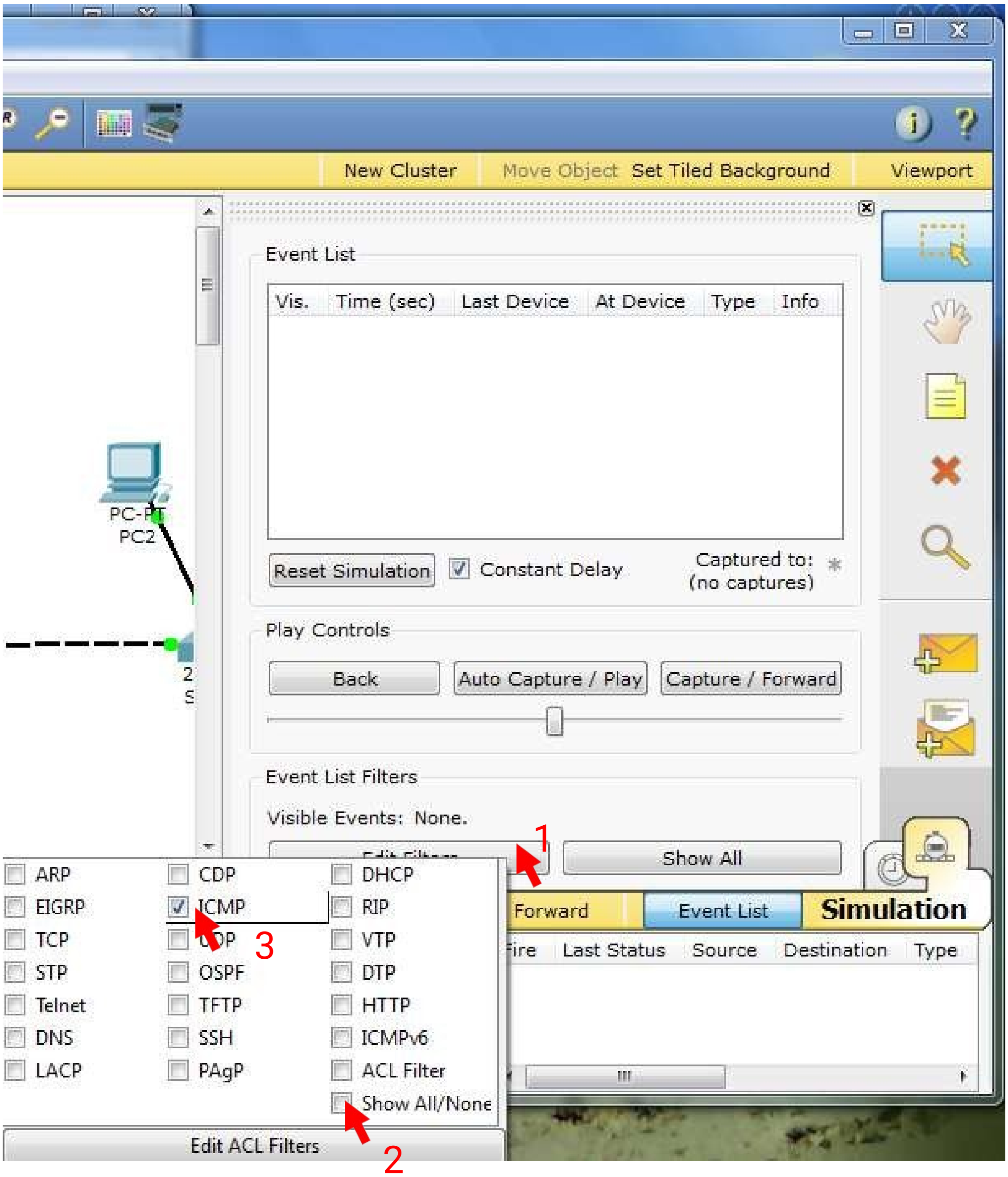


Step 8: Ve y i ode

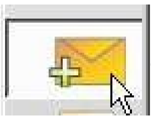
Be sure yo ı n

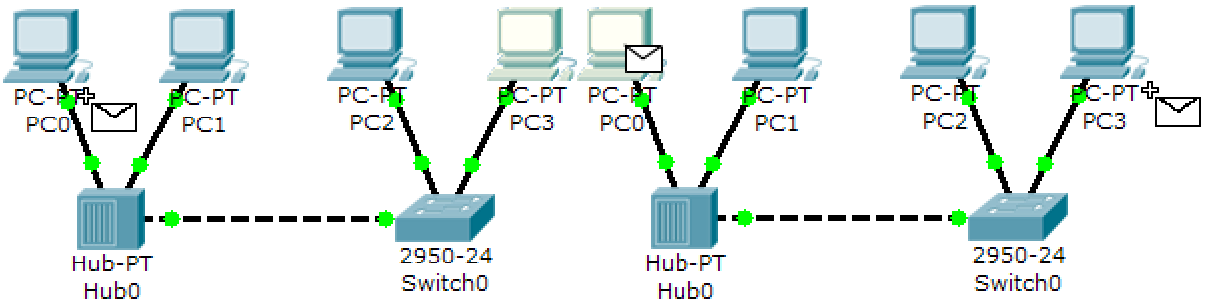


Deselect all filters (All/None) and select only ICMP.

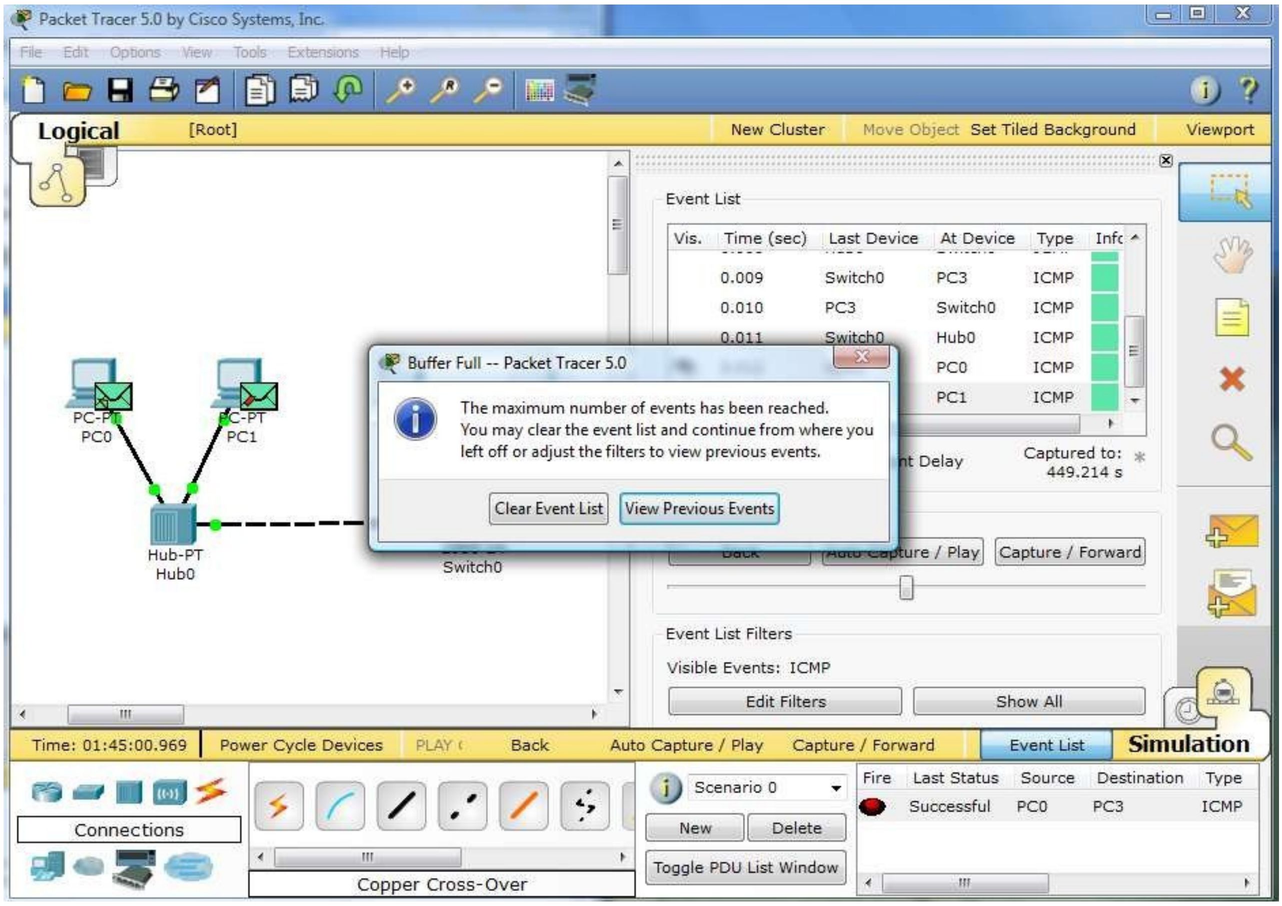


Select the Add Simple PDU tool used to ping devices..

 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.



Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.009	Switch0	PC3	ICMP	🟩
	0.010	PC3	Switch0	ICMP	🟩
	0.011	Switch0	Hub0	ICMP	🟩
			PC0	ICMP	🟩
			PC1	ICMP	🟩

Buffer Full -- Packet Tracer 5.0

The maximum number of events has been reached.
You may clear the event list and continue from where you left off or adjust the filters to view previous events.

...t Delay

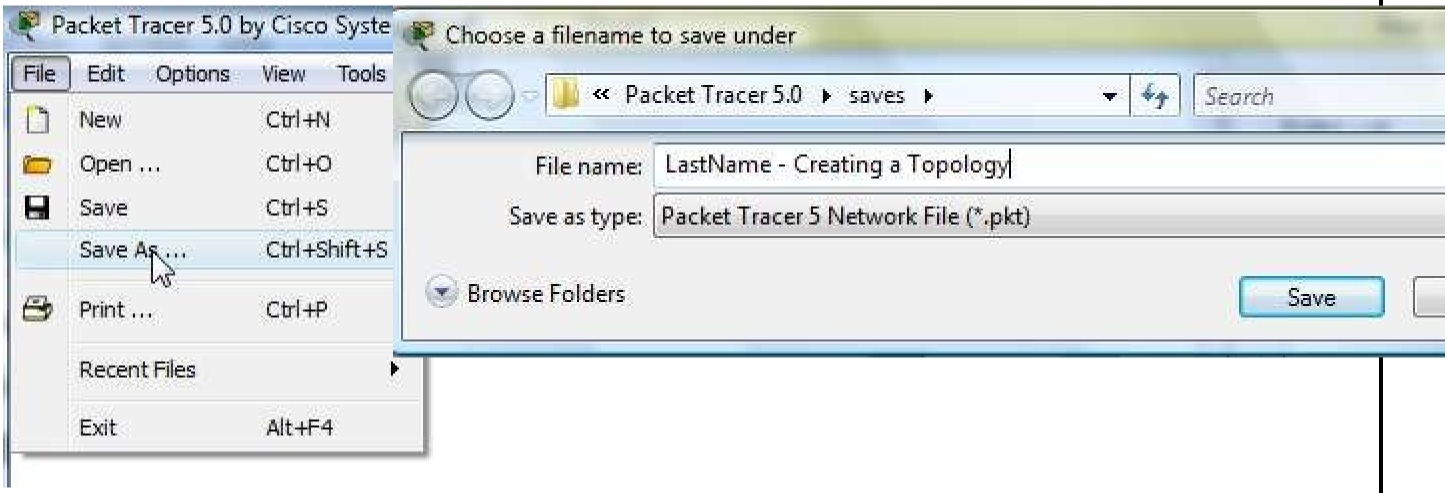
Captured to:
449.214 s

Visible Events: ICMP

Time: 01:45:00.969

Scenario 0

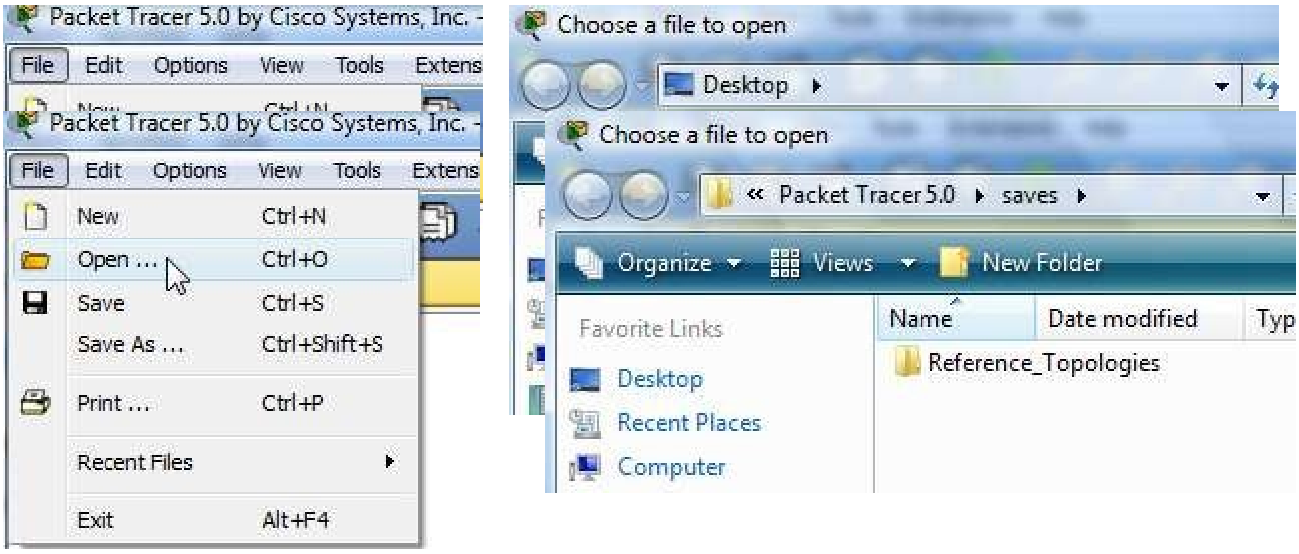
Fire	Last Status	Source	Destination	Type
●	Successful	PC0	PC3	ICMP

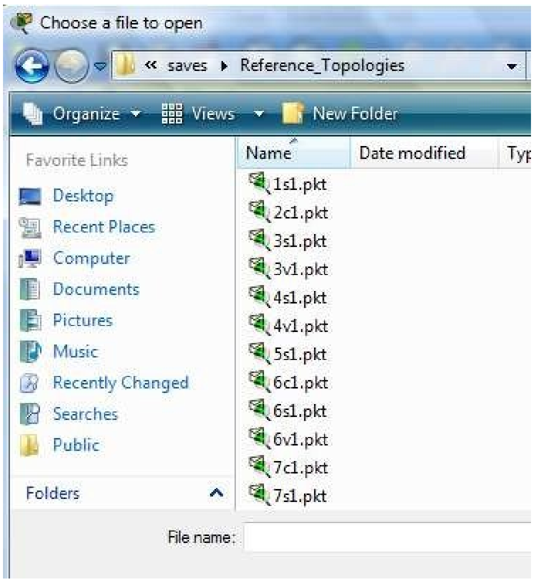


File name: LastName - Creating a Topology

Save as type: Packet Tracer 5 Network File (*.pkt)

Opening Existing Topologies




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