Practical no:-03

Aim:-Using linux-terminal or Windows-cmd,execute following networking commands and note the output:ping,traceroute,netstat,arp,ipconfig.

1)arp

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

Syntax

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

Parameters

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.

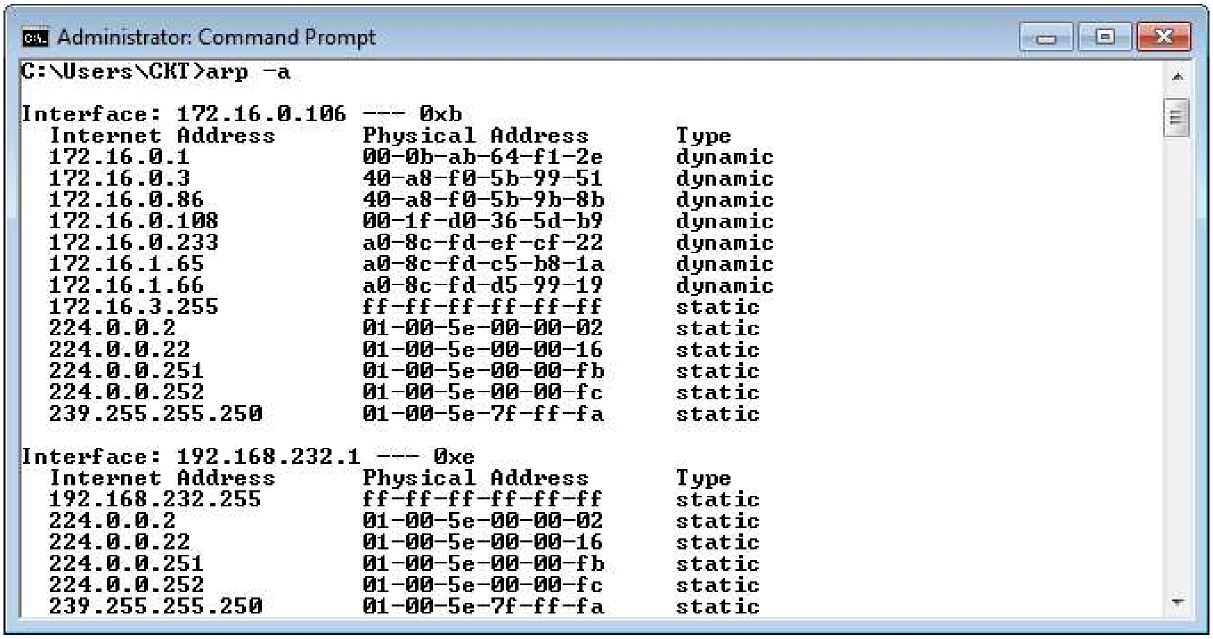
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

```
 > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
 > arp -a                                    .... Displays the arp table.
```



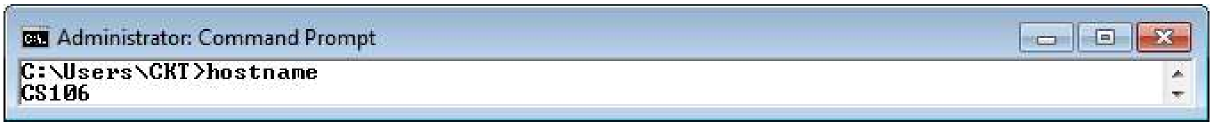
```
C:\Users\CKT>arp -a

Interface: 172.16.0.106 --- 0xb
  Internet Address      Physical Address      Type
  172.16.0.1            00-0b-ab-64-f1-2e     dynamic
  172.16.0.3            40-a8-f0-5b-99-51     dynamic
  172.16.0.86           40-a8-f0-5b-9b-8b     dynamic
  172.16.0.108          00-1f-d0-36-5d-b9     dynamic
  172.16.0.233          a0-8c-fd-ef-cf-22     dynamic
  172.16.1.65           a0-8c-fd-c5-b8-1a     dynamic
  172.16.1.66           a0-8c-fd-d5-99-19     dynamic
  172.16.3.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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

Interface: 192.168.232.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.232.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
```

2. Hostname:

The hostname command displays the hostname of the machine that is running it.

Syntax: Hostname

Parameters: No Parameter



```
C:\Users\CKT>hostname
CS106
```

3) ipconfig:

This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only ipconfig without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask, and default gateway.

Syntax :

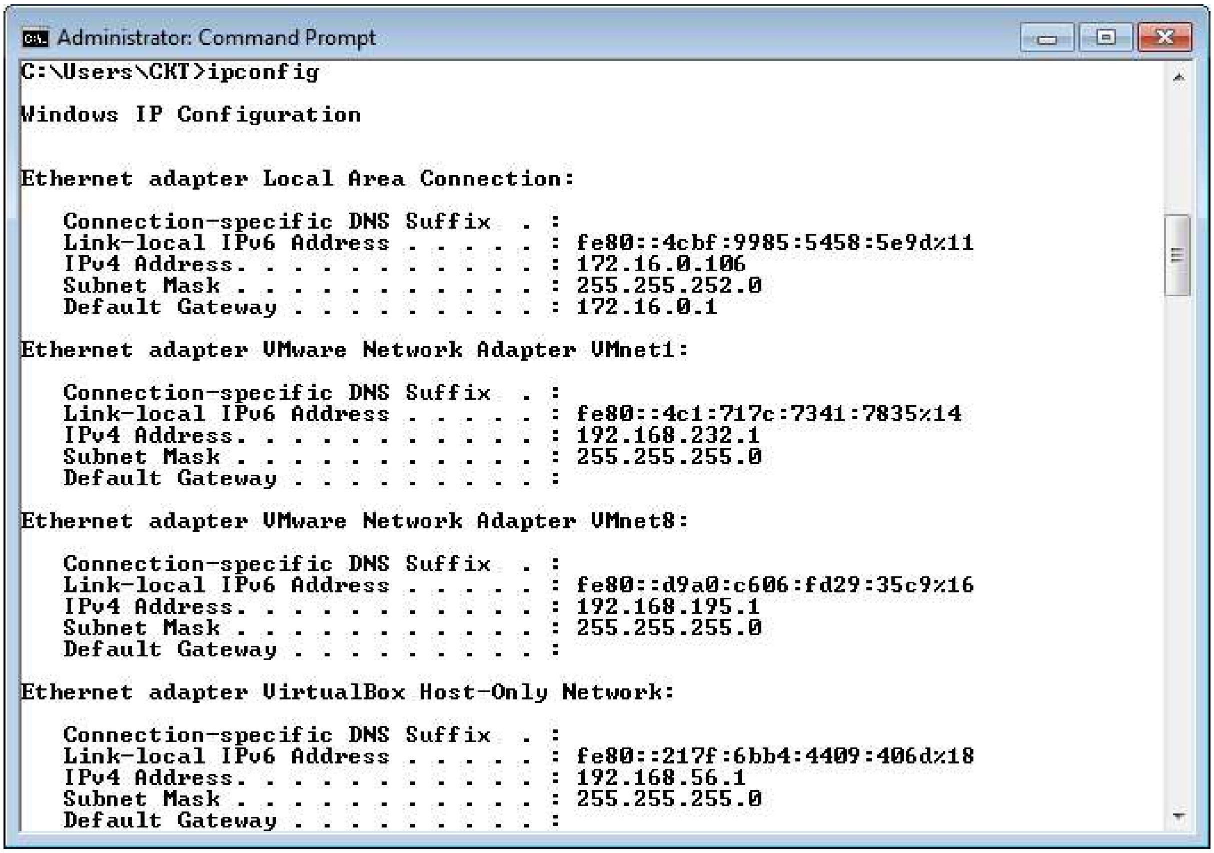
ipconfig [/all/renew (adapter)|/release (adapter)]

Parameters :

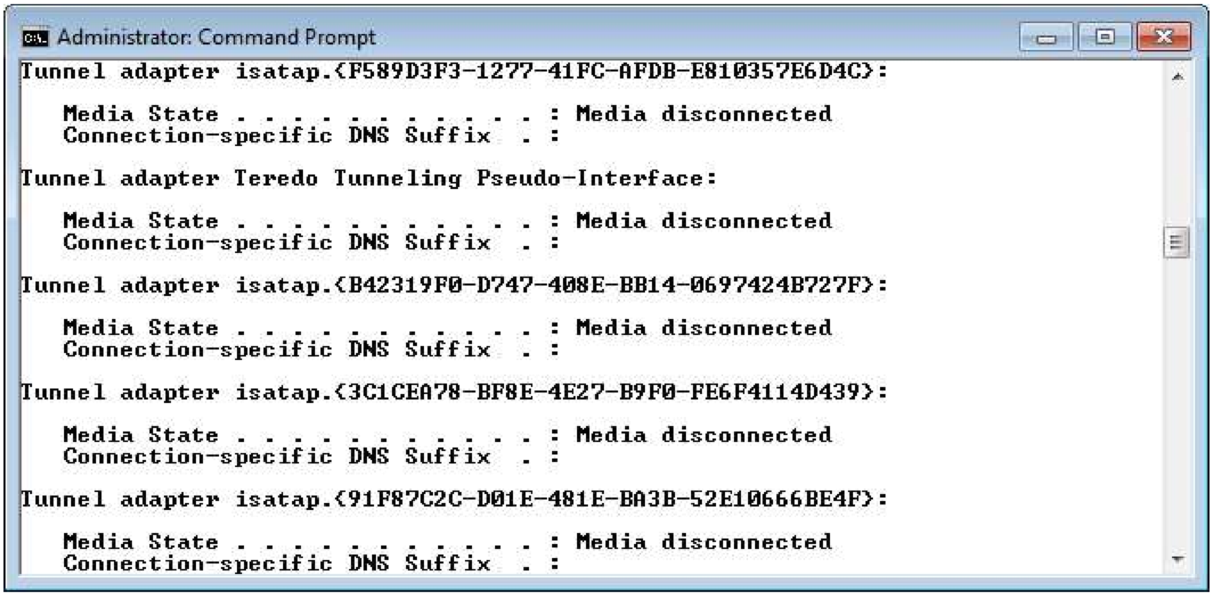
all Produces a full display. Without this switch, ipconfig displays only the IP address, subnet mask, and default gateway values for each network card.

renew [adapter] Renews DHCP configuration parameters. This option is available only on computers running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

release [adapter] Releases the current DHCP configuration. This option disables TCP/IP on the local computer and is available only on DHCP clients. To specify an adapter name,type the adapter name that appears when you use ipconfig without parameters.



```
C:\Users\CKT>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4cbf:9985:5458:5e9d%11
   IPv4 Address. . . . . . . . . . . : 172.16.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 172.16.0.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4c1:717c:7341:7835%14
   IPv4 Address. . . . . . . . . . . : 192.168.232.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d9a0:c606:fd29:35c9%16
   IPv4 Address. . . . . . . . . . . : 192.168.195.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::217f:6bb4:4409:406d%18
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```



```
Tunnel adapter isatap.{F589D3F3-1277-41FC-AFDB-E810357E6D4C}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Tunnel adapter isatap.{B42319F0-D747-408E-BB14-0697424B727F}:

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

Tunnel adapter isatap.{3C1CEA78-BF8E-4E27-B9F0-FE6F4114D439}:

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

Tunnel adapter isatap.{91F87C2C-D01E-481E-BA3B-52E10666BE4F}:

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

4) Netstat:

Displays protocol statistics and current TCP/IP network connections.

Syntax:

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

Parameters:

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.

-e Displays Ethernet statistics. This may be combined with the -s option.

-f Displays Fully Qualified Domain Names (FQDN) for foreign addresses.

-n Displays addresses and port numbers in numerical form.

-o Displays the owning process ID associated with each connection.

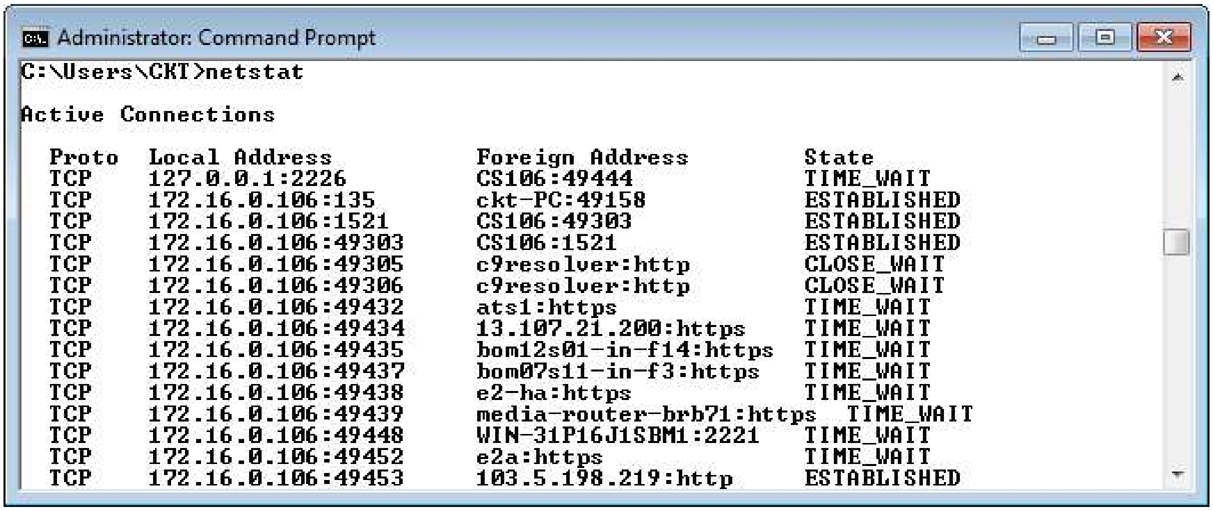
-p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are
shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
the -p option may be used to specify a subset of the default.

-t Displays the current connection offload state.

interval Redisplays selected statistics, pausing interval seconds
between each display. Press CTRL+C to stop redisplaying
statistics. If omitted, netstat will print the current
configuration information once.



```
C:\Users\CKT>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:2226         CS106:49444            TIME_WAIT
  TCP    172.16.0.106:135       ckt-PC:49158           ESTABLISHED
  TCP    172.16.0.106:1521      CS106:49303            ESTABLISHED
  TCP    172.16.0.106:49303     CS106:1521             ESTABLISHED
  TCP    172.16.0.106:49305     c9resolver:http        CLOSE_WAIT
  TCP    172.16.0.106:49306     c9resolver:http        CLOSE_WAIT
  TCP    172.16.0.106:49432     ats1:https             TIME_WAIT
  TCP    172.16.0.106:49434     13.107.21.200:https    TIME_WAIT
  TCP    172.16.0.106:49435     bom12s01-in-f14:https  TIME_WAIT
  TCP    172.16.0.106:49437     bom07s11-in-f3:https   TIME_WAIT
  TCP    172.16.0.106:49438     e2-ha:https            TIME_WAIT
  TCP    172.16.0.106:49439     media-router-brb71:https  TIME_WAIT
  TCP    172.16.0.106:49448     WIN-31P16J1SBM1:2221   TIME_WAIT
  TCP    172.16.0.106:49452     e2a:https              TIME_WAIT
  TCP    172.16.0.106:49453     103.5.198.219:http     ESTABLISHED
```

5)Ping:

This diagnostic command verifies connections to one or more remote computers.

Syntax:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Parameters:

-t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.

-a Resolve addresses to hostnames.

-n count Number of echo requests to send.

-l size Send buffer size.

-f Set Don't Fragment flag in packet (IPv4-only).

-i TTL Time To Live.

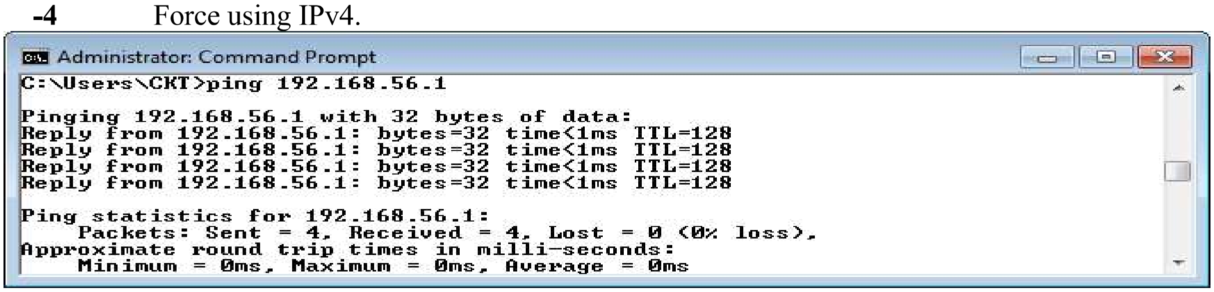
-v TOS Type Of Service (IPv4-only. This setting has been deprecated
and has no effect on the type of service field in the IP Head
er).

-r count Record route for count hops (IPv4-only).

-s count Timestamp for count hops (IPv4-only).

-j host-list Loose source route along host-list (IPv4-only).

-k host-list   Strict source route along host-list (IPv4-only).
-w timeout   Timeout in milliseconds to wait for each reply.
-R   Use routing header to test reverse route also (IPv6-only).
-S srcaddr   Source address to use.
-4   Force using IPv4.



```
C:\Users\CKT>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6)Tracert:

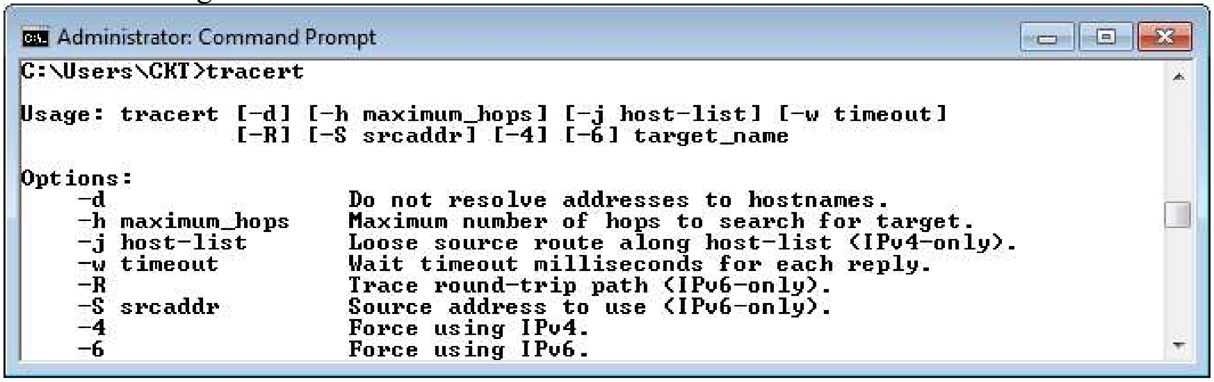
This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0. the router is supposed to send back an ICMP Time Exceeded message to the source computer. Tracert determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired TTLs and will be invisible to tracert.

Syntax:

tracert -d] [-h maximum_hops] [-j host-list] [-w timeout] target name

Parameters :

-d Specifies not to resolve addressss to host names.
-h Maximum_hops Specifies maximum number of hops to search for target.
-j host-list Specifies loose source route along host-list.
-w timeout Waits the number of milliseconds specified by timeout for each reply.target_name name of the target host.

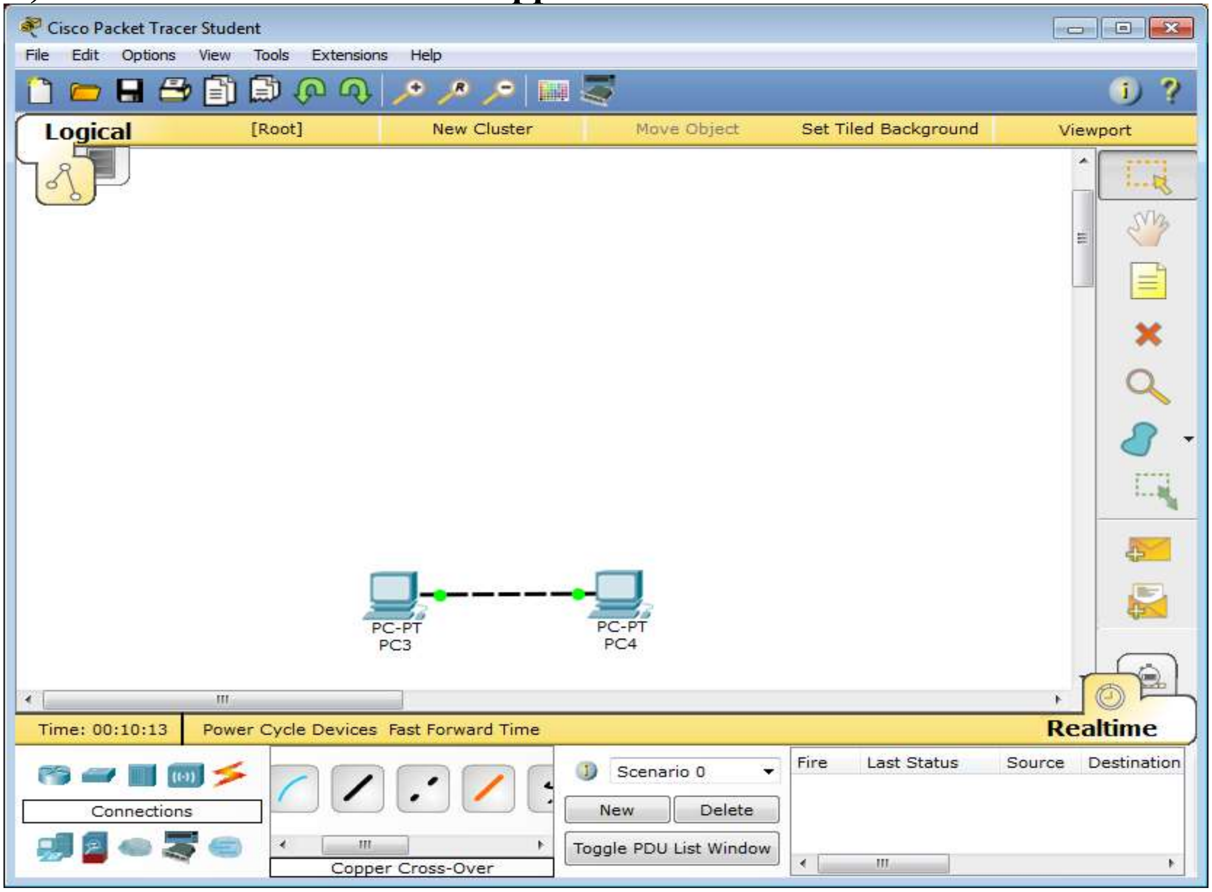


```
C:\Users\CKT>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

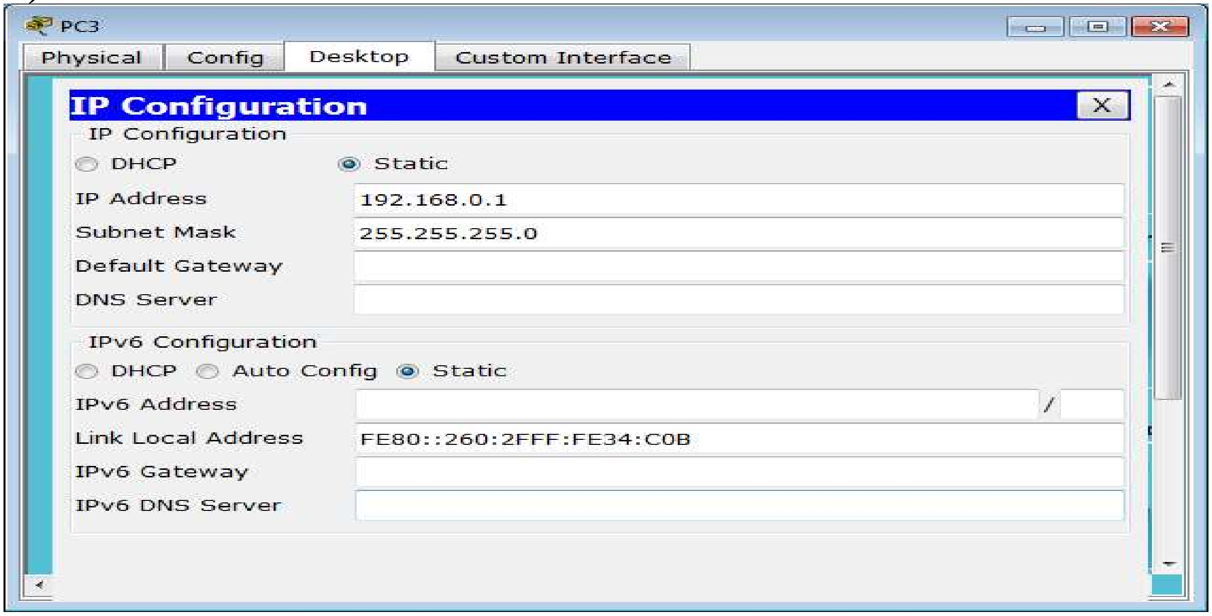
Practical No:-04

i)Aim:- Using packet tracer,create a basic network of two computers using appropriate network wire.

A)Connect both the PC with Copper Cross-Over wire.



B) Set the IP and Subnet Mask for PC-PT PC0



IP Configuration

○ DHCP ● Static

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

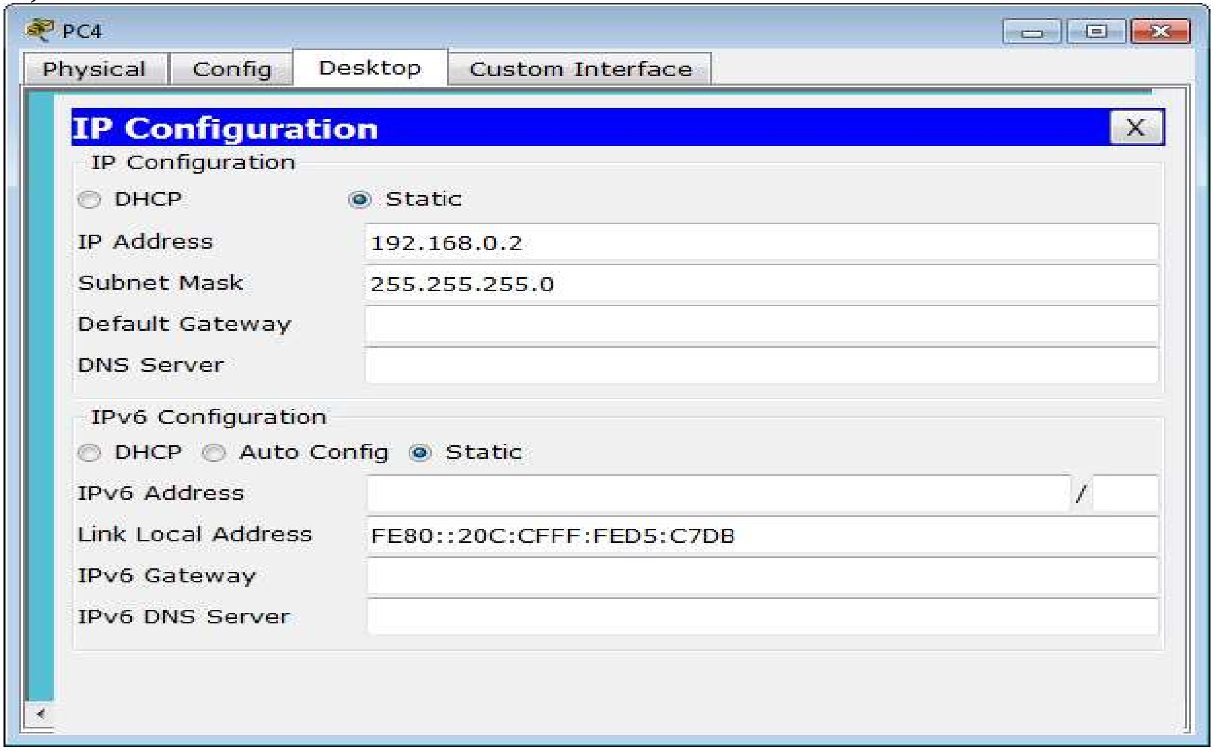
IPv6 Address: /

Link Local Address: FE80::260:2FFF:FE34:C0B

IPv6 Gateway:

IPv6 DNS Server:

C) Set the IP and Subnet Mask for PC-PT PC2



IP Configuration

○ DHCP ● Static

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

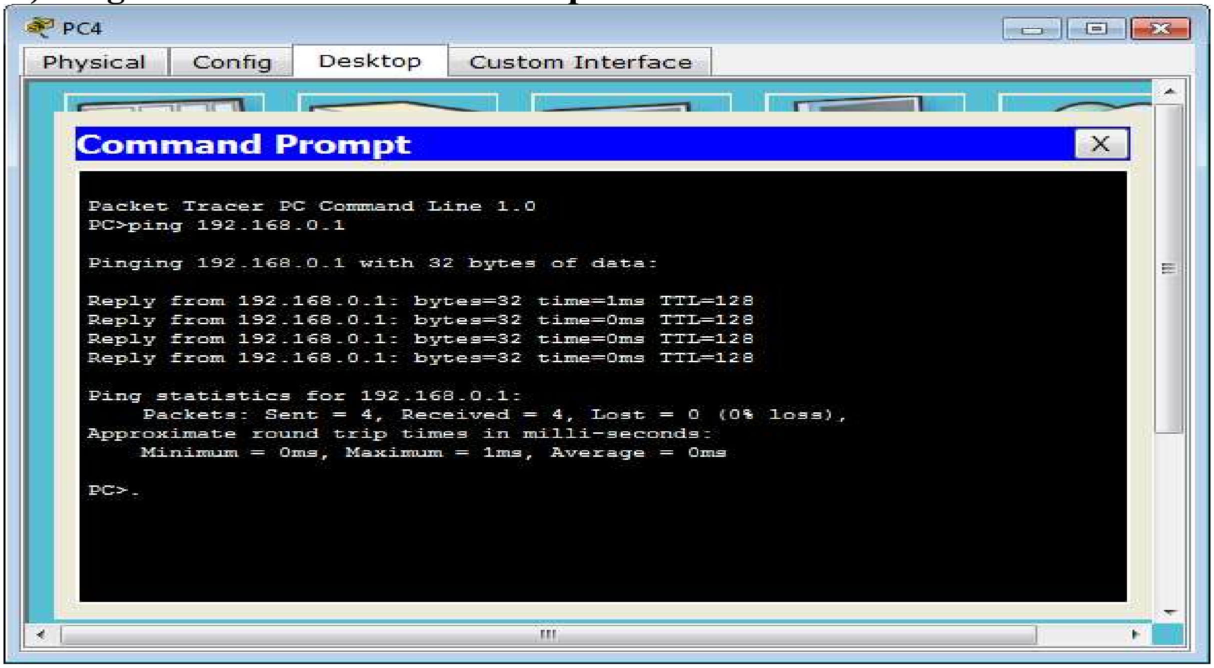
IPv6 Address: /

Link Local Address: FE80::20C:CFFF:FED5:C7DB

IPv6 Gateway:

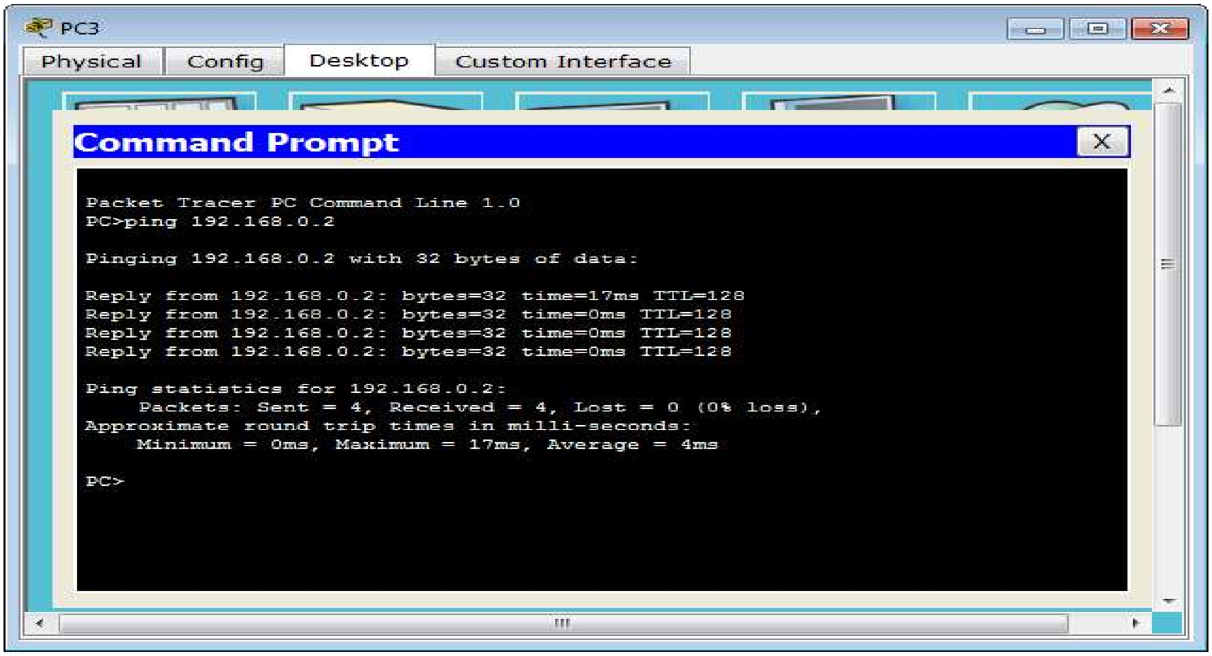
IPv6 DNS Server:

D) Ping PC2 from Command Prompt of PC0



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>_
```

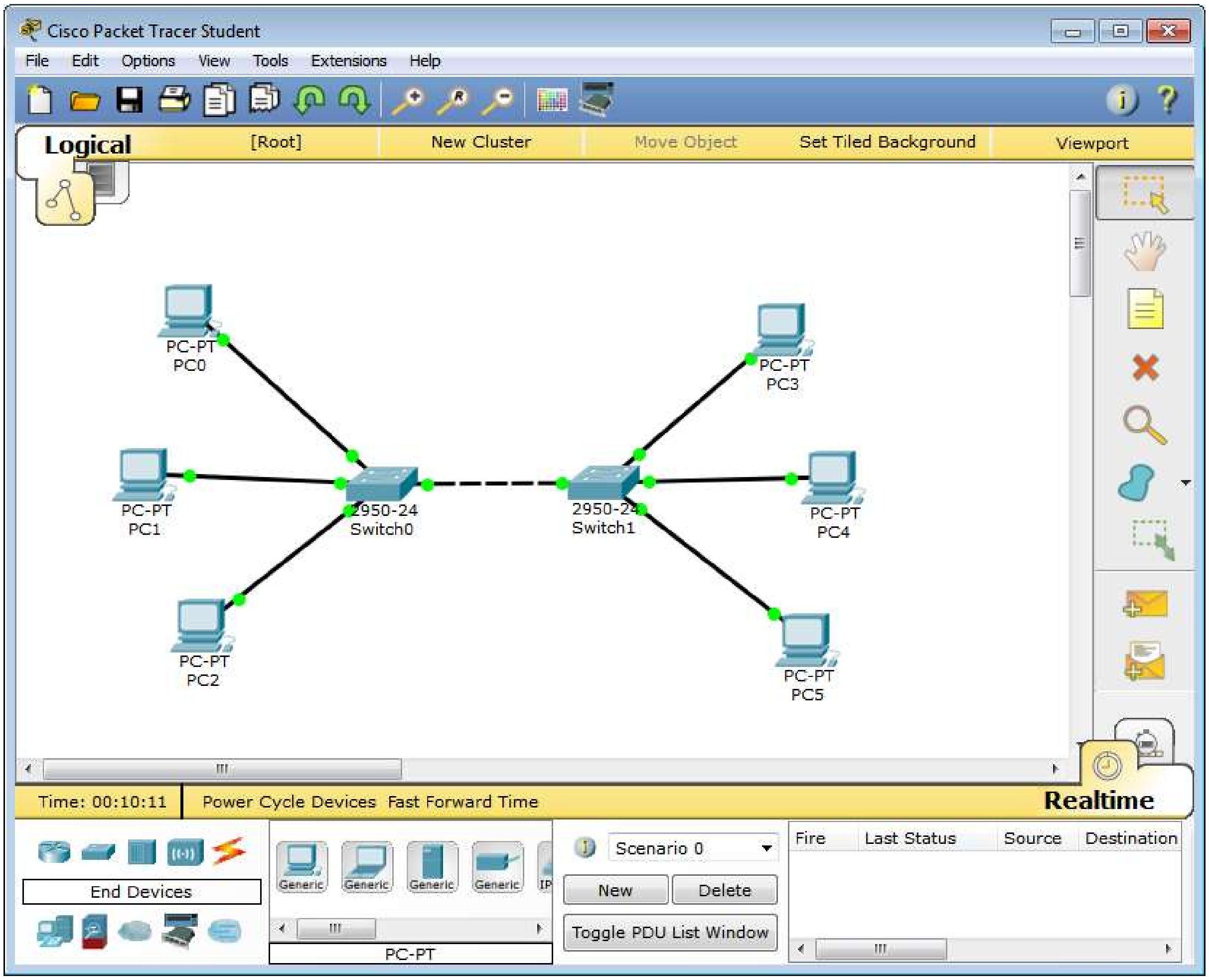
E) Ping PC0 from Command Prompt of PC2



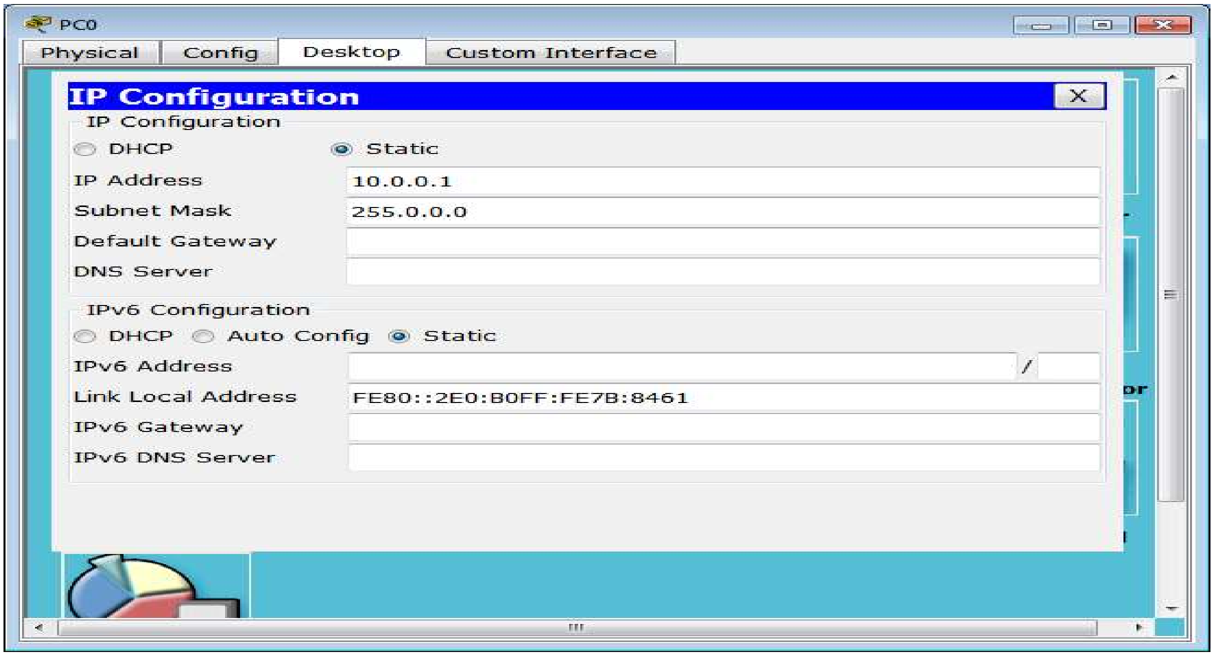
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=17ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 4ms

PC>
```

Practical No:-04

ii)Aim:-Using packet tracer create multiple (minimum 6) computer using layer 2 switches.



Open PC0 and give the IP address



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

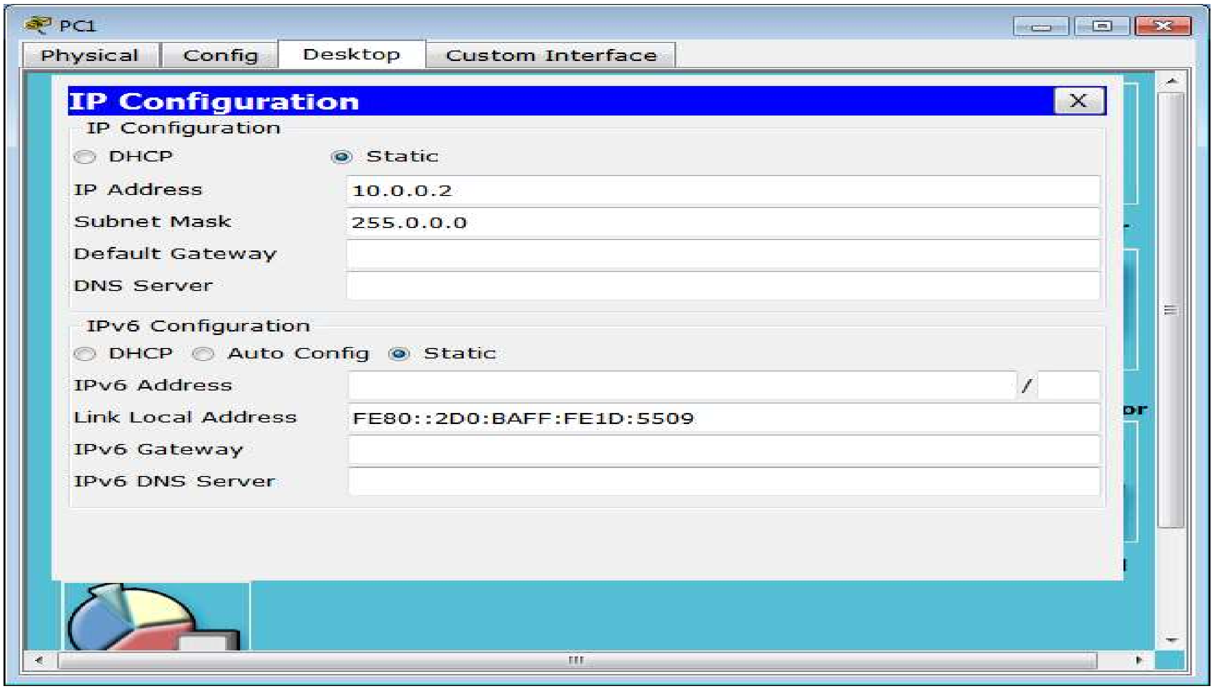
IPv6 Address /

Link Local Address FE80::2E0:B0FF:FE7B:8461

IPv6 Gateway

IPv6 DNS Server

Open PC1 and give the IP address



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

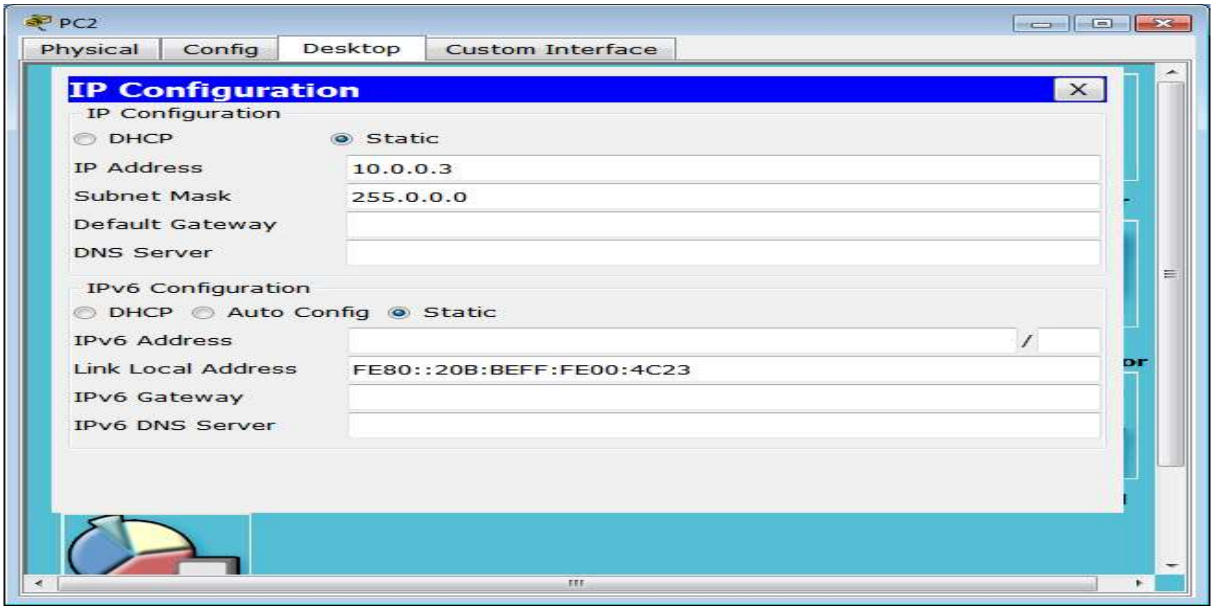
IPv6 Address /

Link Local Address FE80::2D0:BAFF:FE1D:5509

IPv6 Gateway

IPv6 DNS Server

Open PC2 and give the IP address



IP Configuration

○ DHCP ● Static

IP Address: 10.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

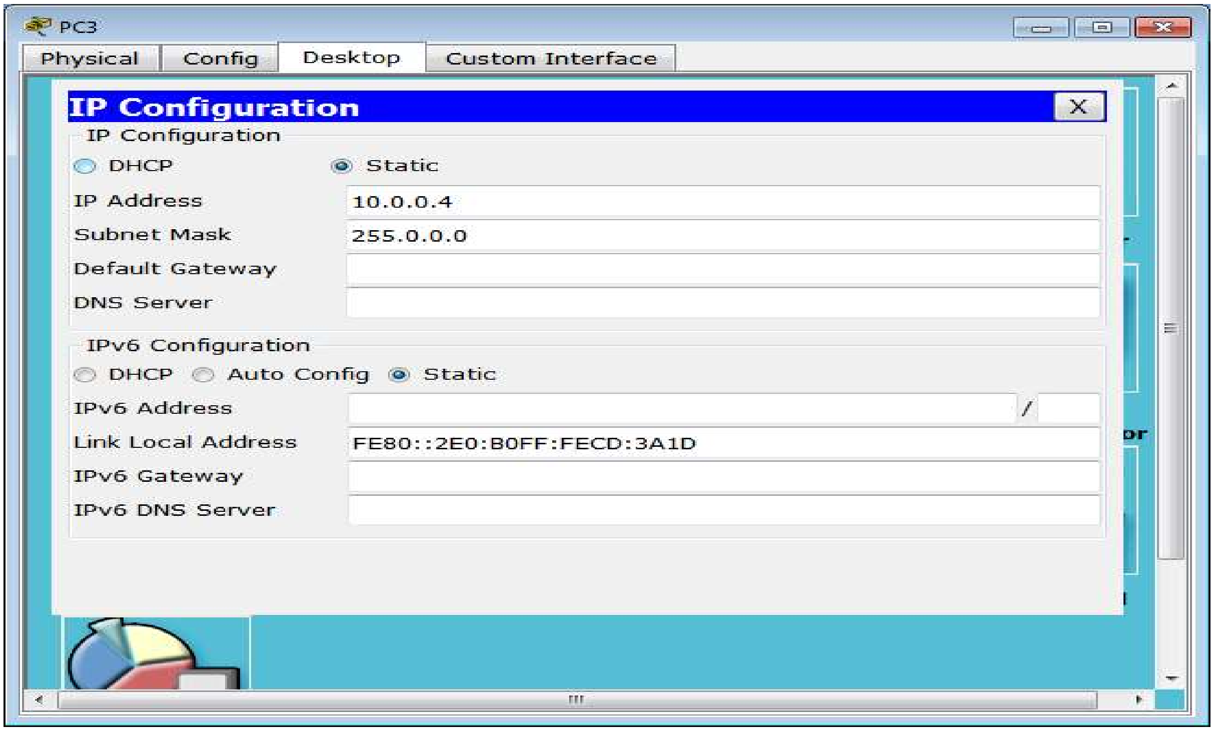
IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FE00:4C23

IPv6 Gateway:

IPv6 DNS Server:

Open PC3 and give the IP address



IP Configuration

○ DHCP ● Static

IP Address: 10.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

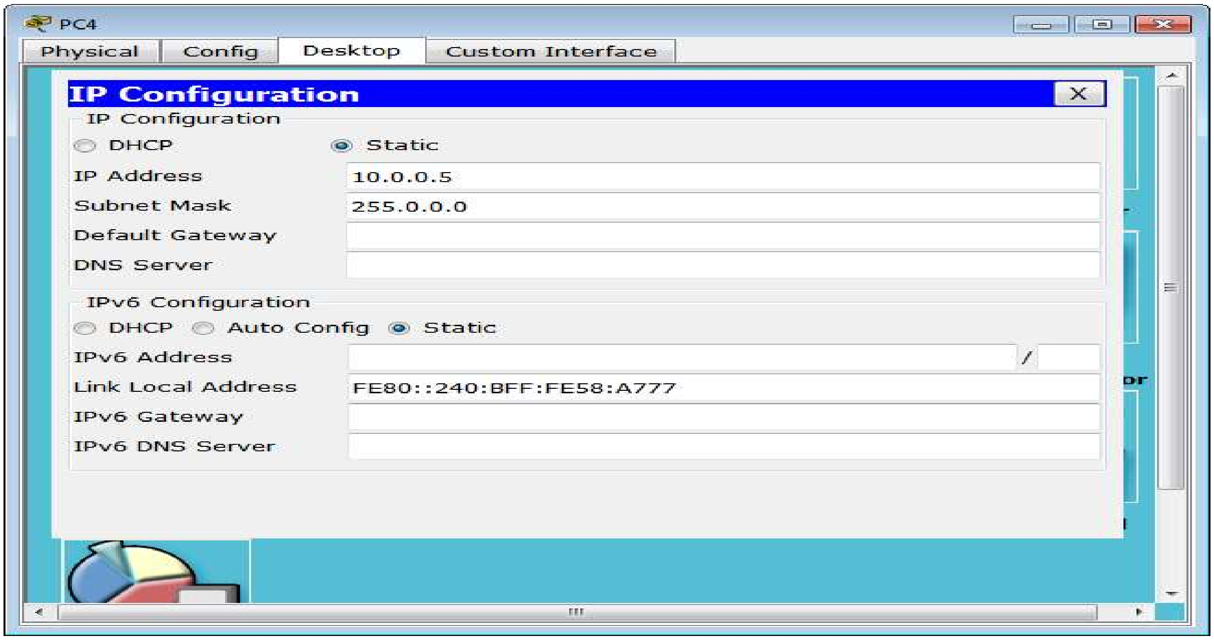
IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FECD:3A1D

IPv6 Gateway:

IPv6 DNS Server:

Open PC4 and give the IP address



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.5

Subnet Mask 255.0.0.0

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

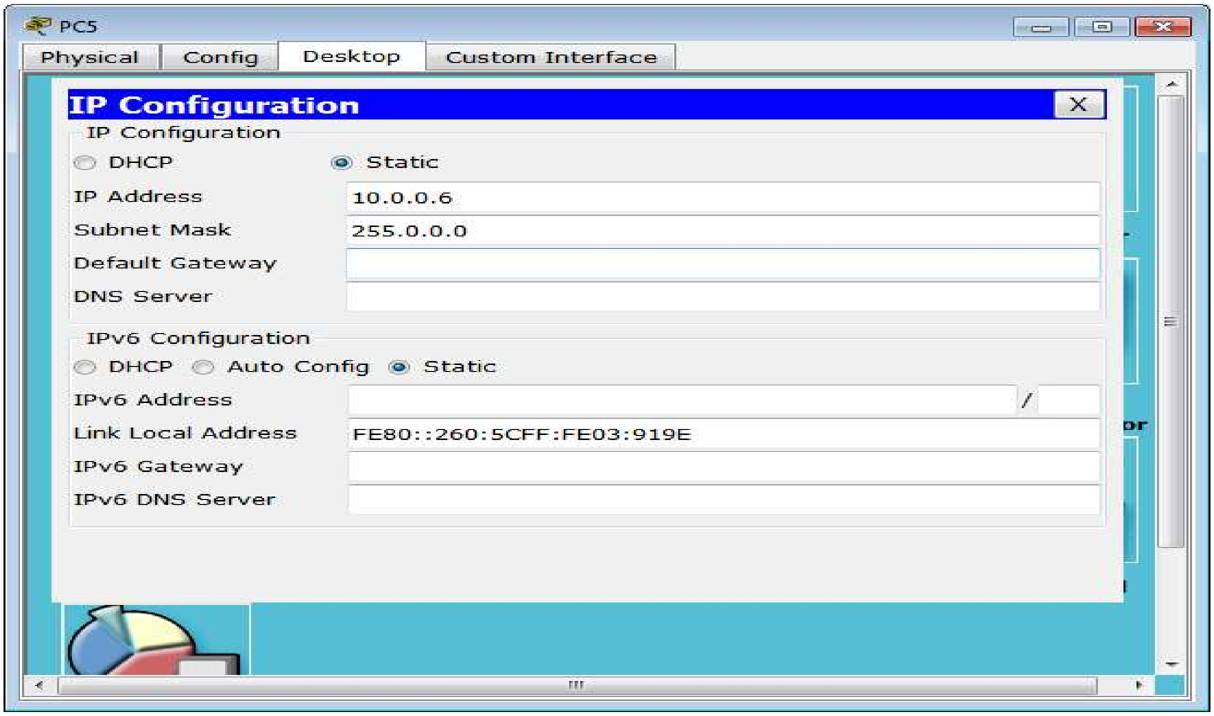
IPv6 Address /

Link Local Address FE80::240:BFF:FE58:A777

IPv6 Gateway

IPv6 DNS Server

Open PC5 and give the IP address



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.6

Subnet Mask 255.0.0.0

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

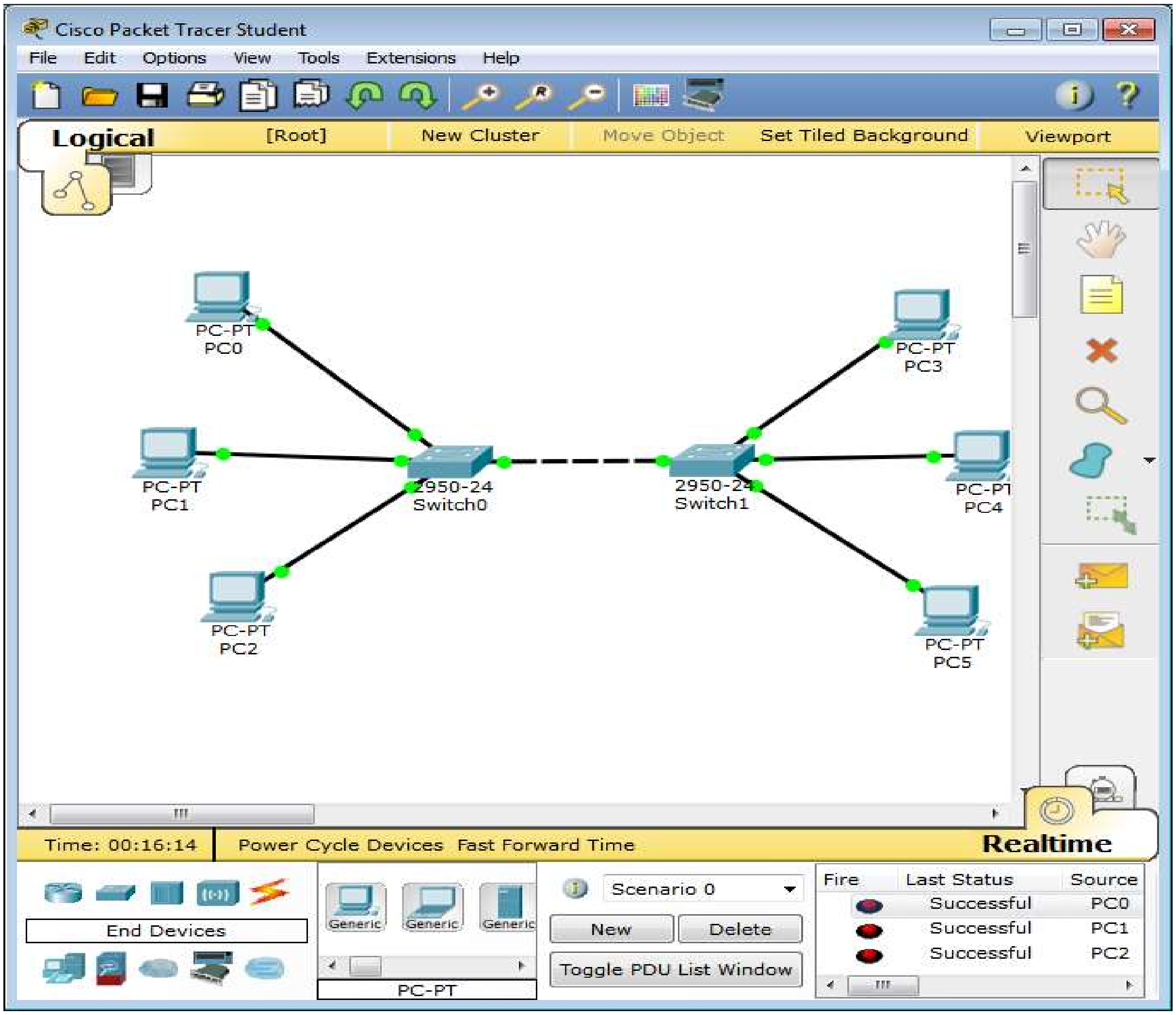
Link Local Address FE80::260:5CFF:FE03:919E

IPv6 Gateway

IPv6 DNS Server

Sending packets to one switch to another:

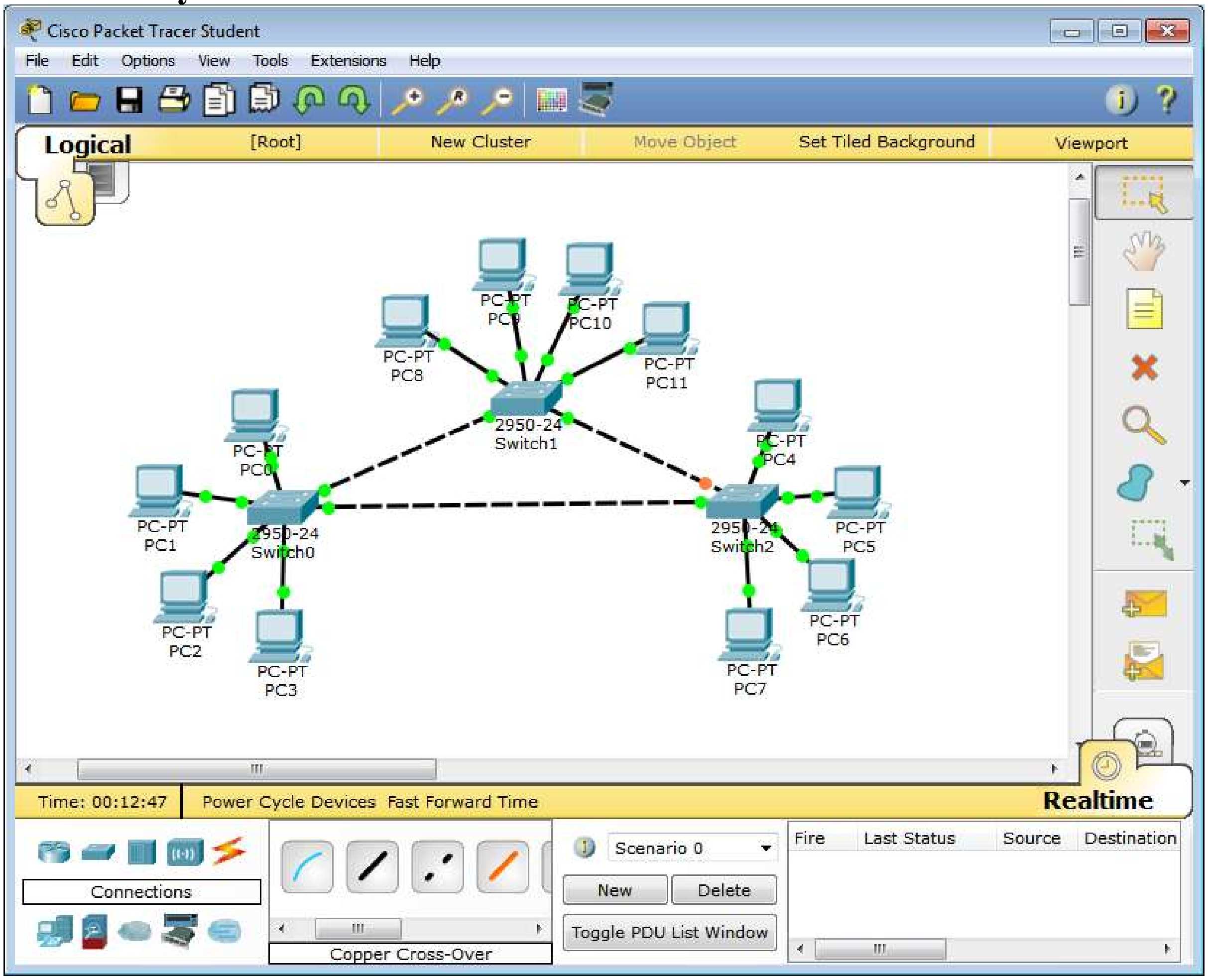
Sending packet PC0 to PC3:
Sending packet PC1 to PC4:
Sending packet PC2 to PC5:



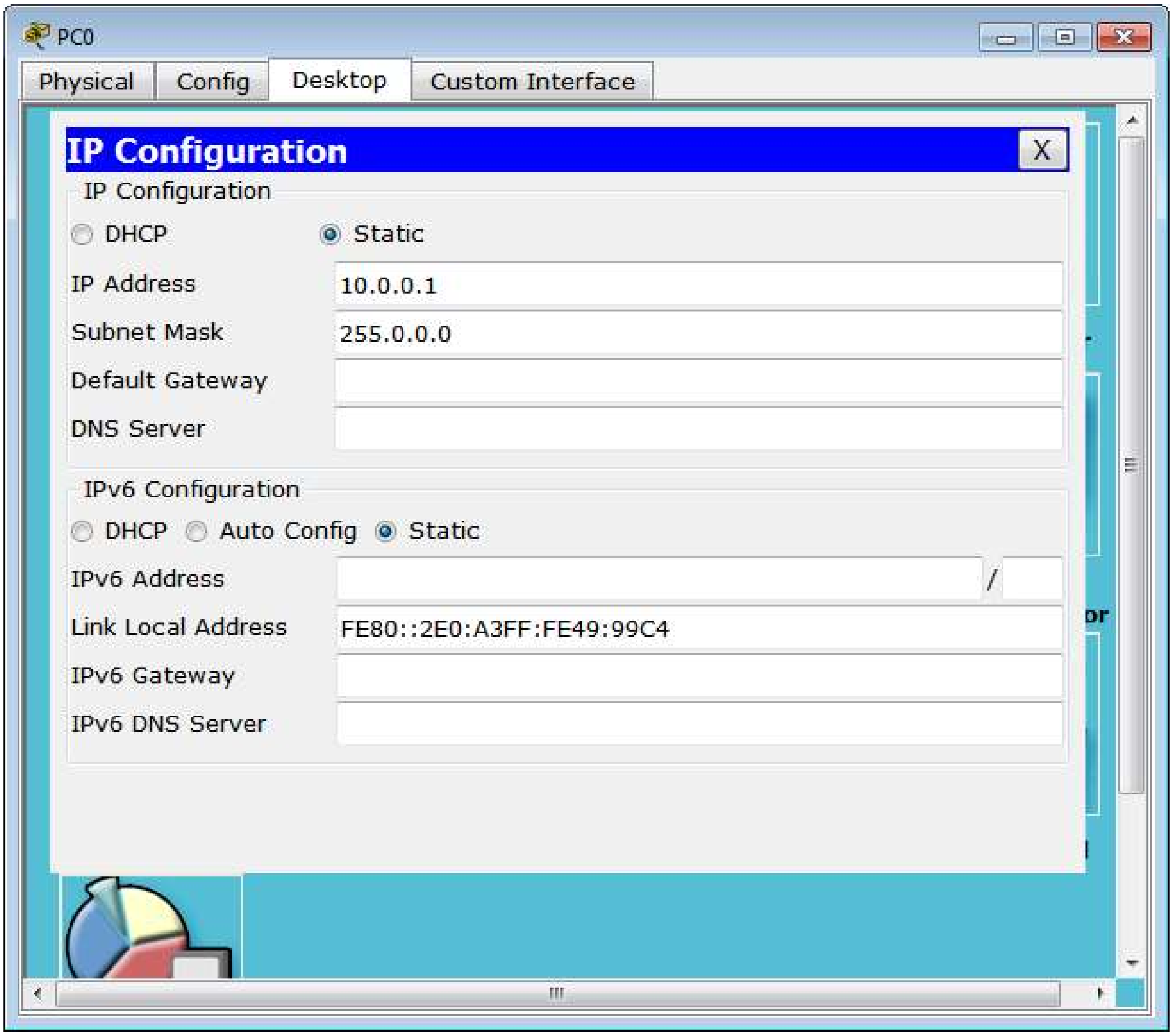
Fire	Last Status	Source
●	Successful	PC0
●	Successful	PC1
●	Successful	PC2

Practical No:-04

iii)Aim:- Connect a network in triangular shape with three layer two switches and every switch will have four computer. Verify their connectivity with each other



Open PC0 and give the IP address:



IP Configuration

○ DHCP ● Static

IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Default Gateway	
DNS Server	

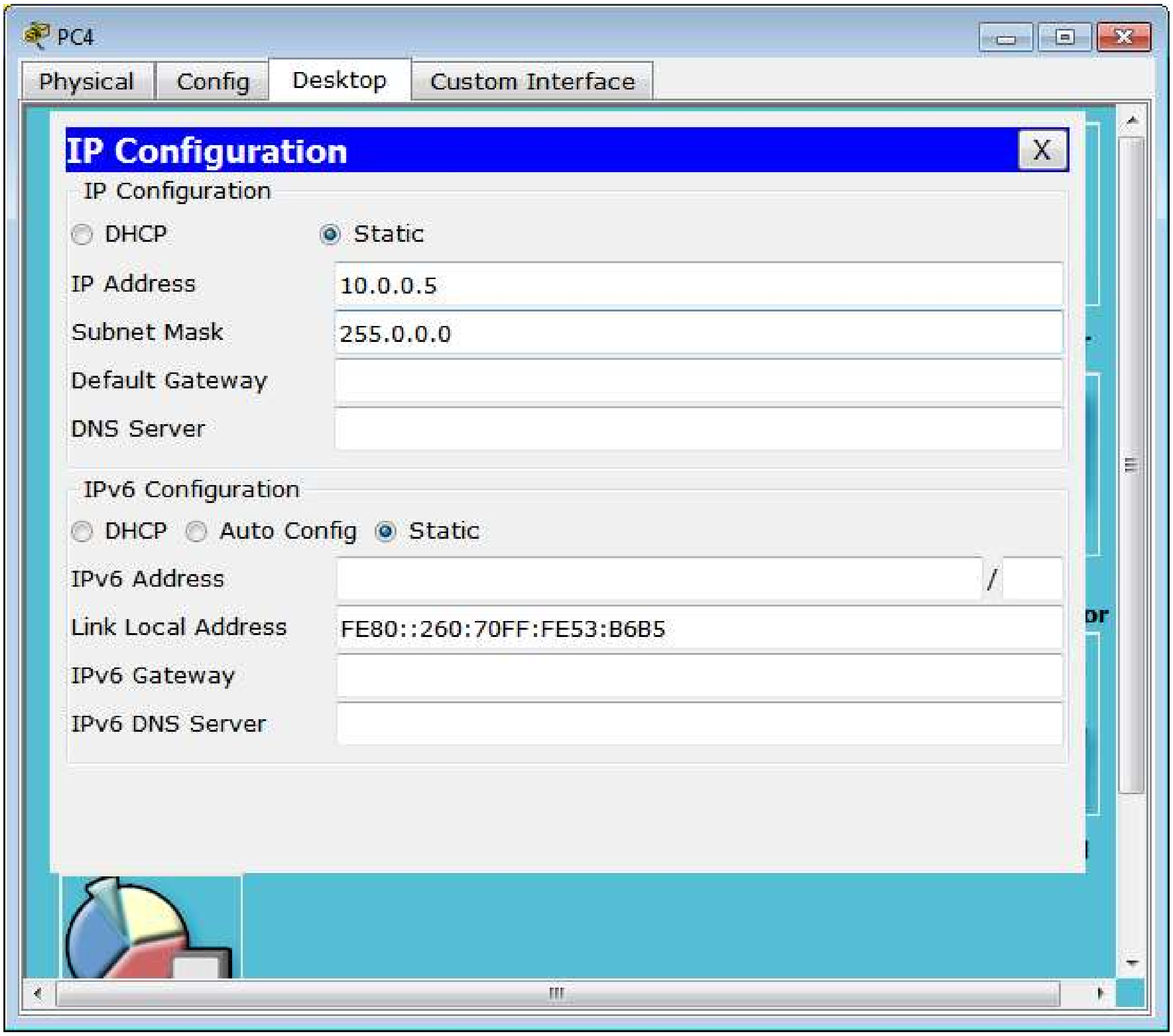
IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address	/
Link Local Address	FE80::2E0:A3FF:FE49:99C4
IPv6 Gateway	
IPv6 DNS Server	

Similarly assign to the PC1, PC2, PC3

Open PC4 and give the IP address:



IP Configuration

○ DHCP ● Static

IP Address: 10.0.0.5

Subnet Mask: 255.0.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

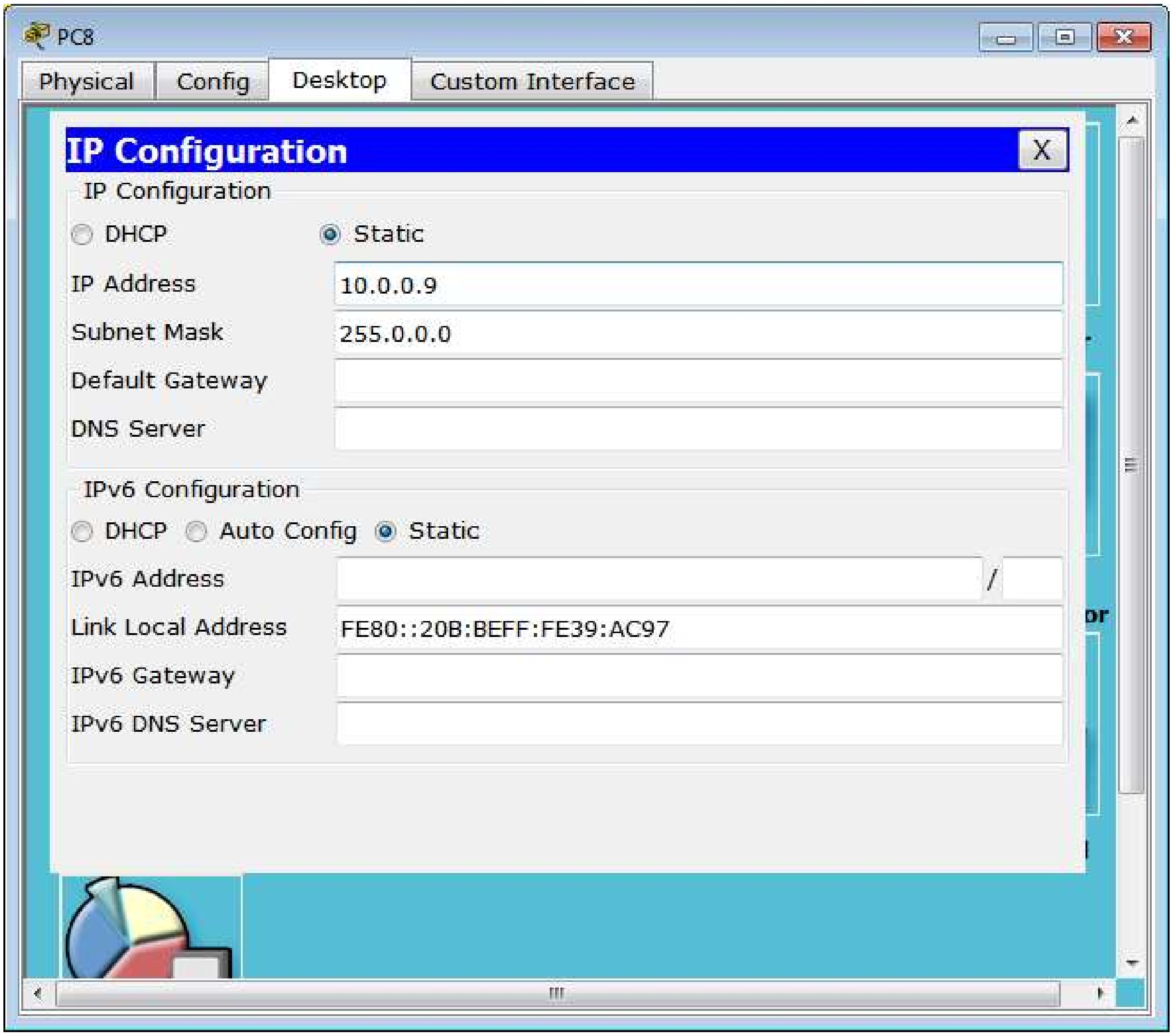
Link Local Address: FE80::260:70FF:FE53:B6B5

IPv6 Gateway:

IPv6 DNS Server:

Similarly assign to the PC5, PC6, PC7

Open PC8 and give the IP address:



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 10.0.0.9

Subnet Mask: 255.0.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FE39:AC97

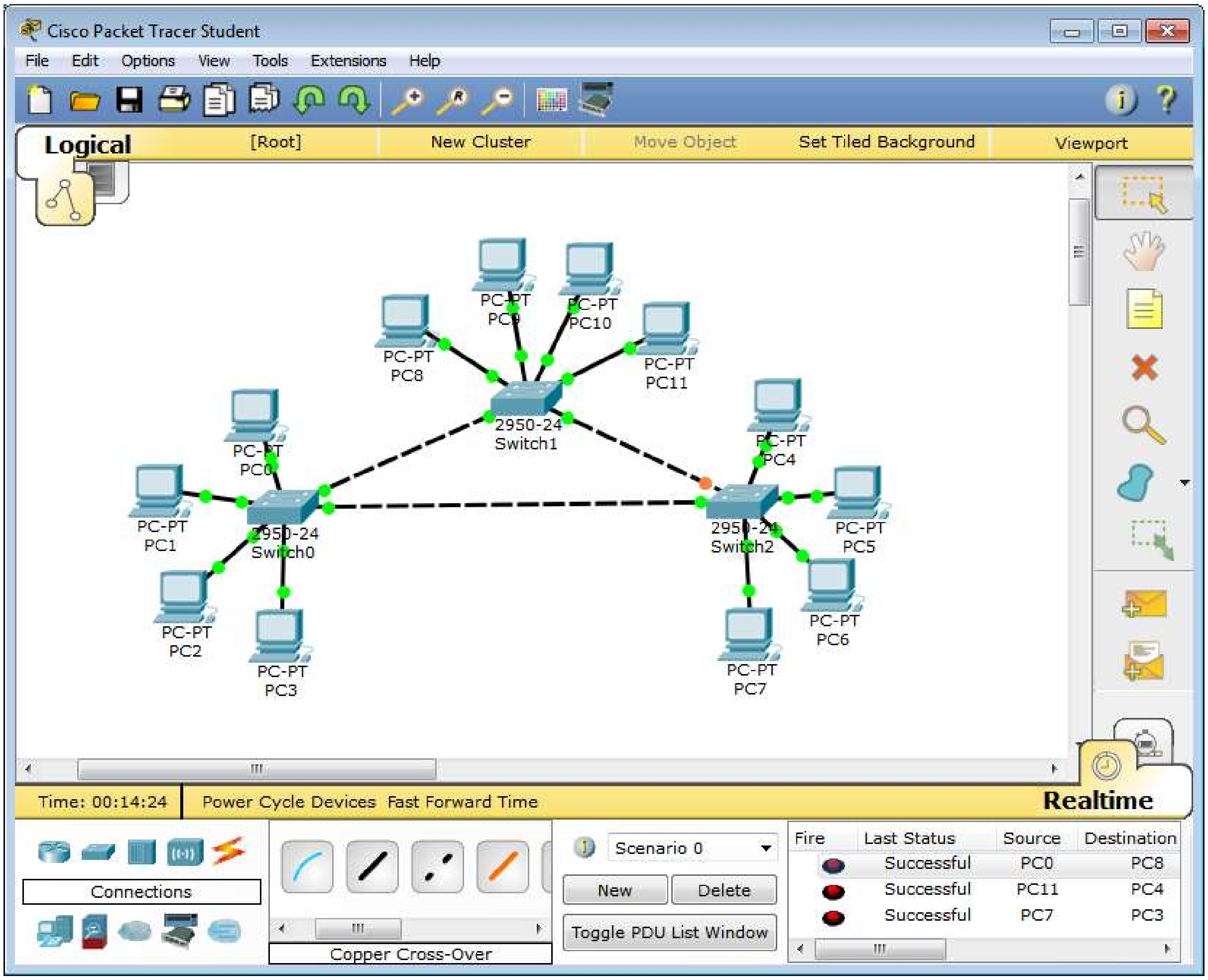
IPv6 Gateway:

IPv6 DNS Server:

Similarly assign to the PC9, PC10, PC11

Sending packets to one switch to another:

Sending packet PC0 to PC8:
Sending packet PC11 to PC4:
Sending packet PC7 to PC3:

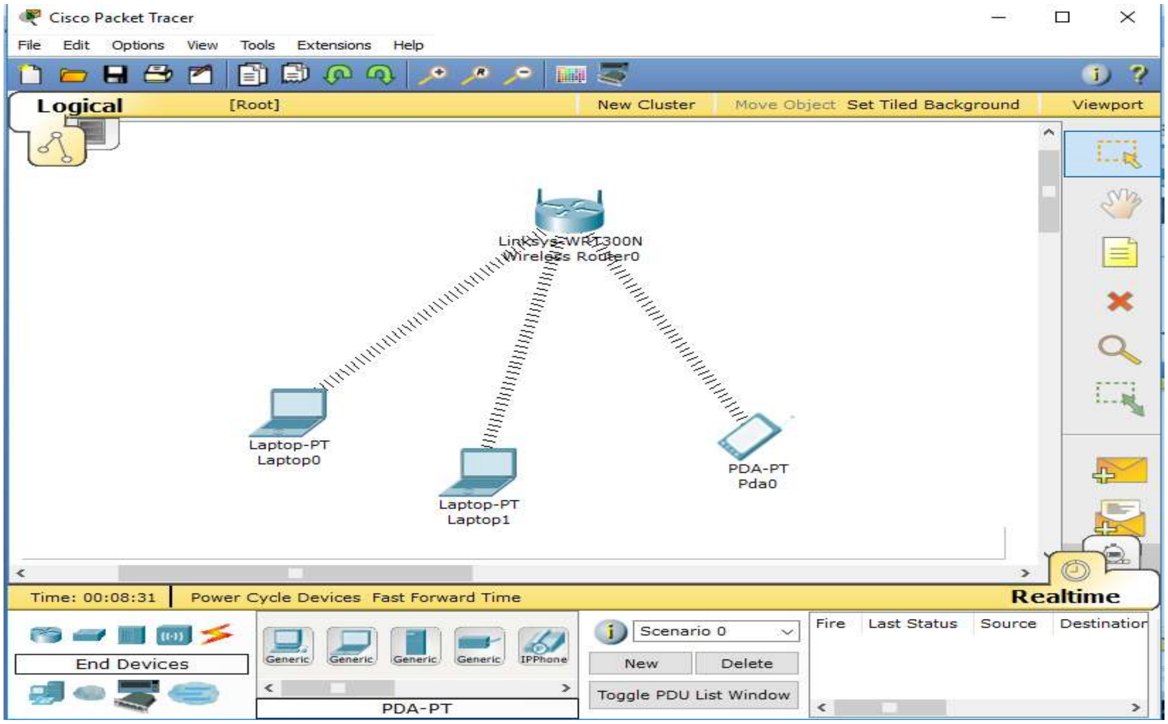


Fire	Last Status	Source	Destination
●	Successful	PC0	PC8
●	Successful	PC11	PC4
●	Successful	PC7	PC3

Practical No 5

Aim: Using Packet Tracer, create a wireless network of multiple PCs using appropriate access point.

Topology:

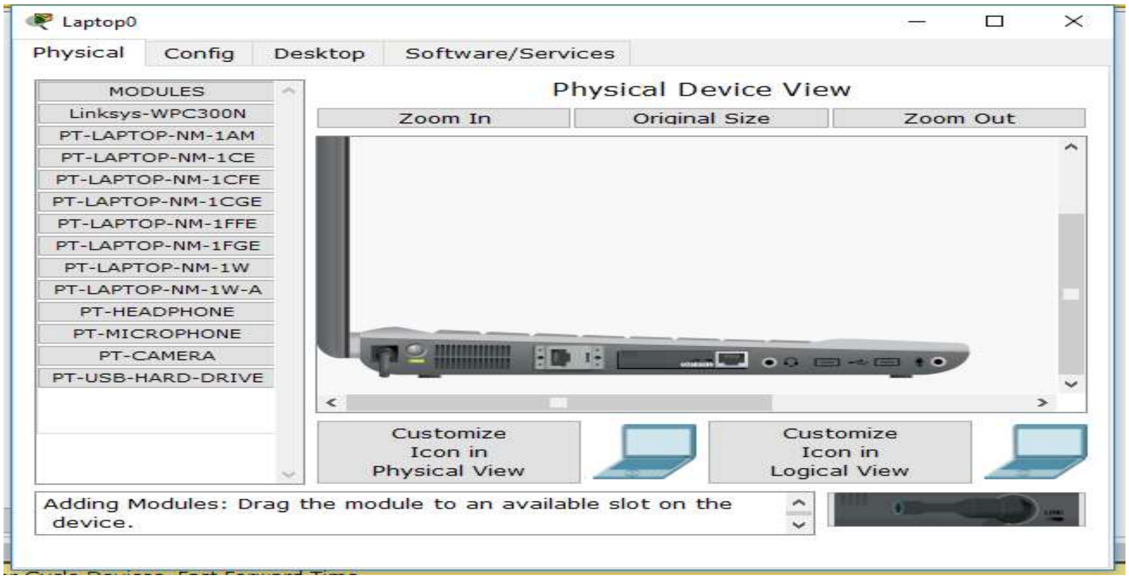


Steps:

i)Drag and drop wireless router from wireless devices

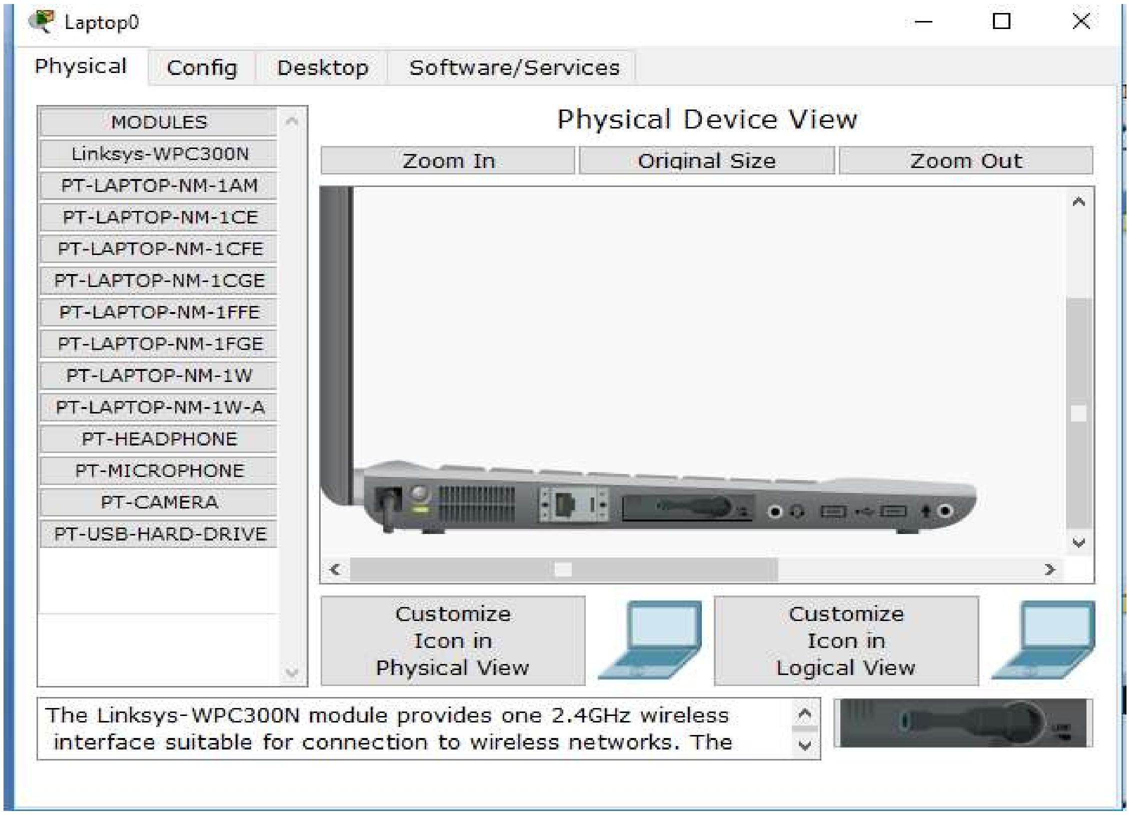
ii) Drag and drop two laptops and one smart device from end devices

iii) Open the laptop setting in order to add the module for wireless connectivity



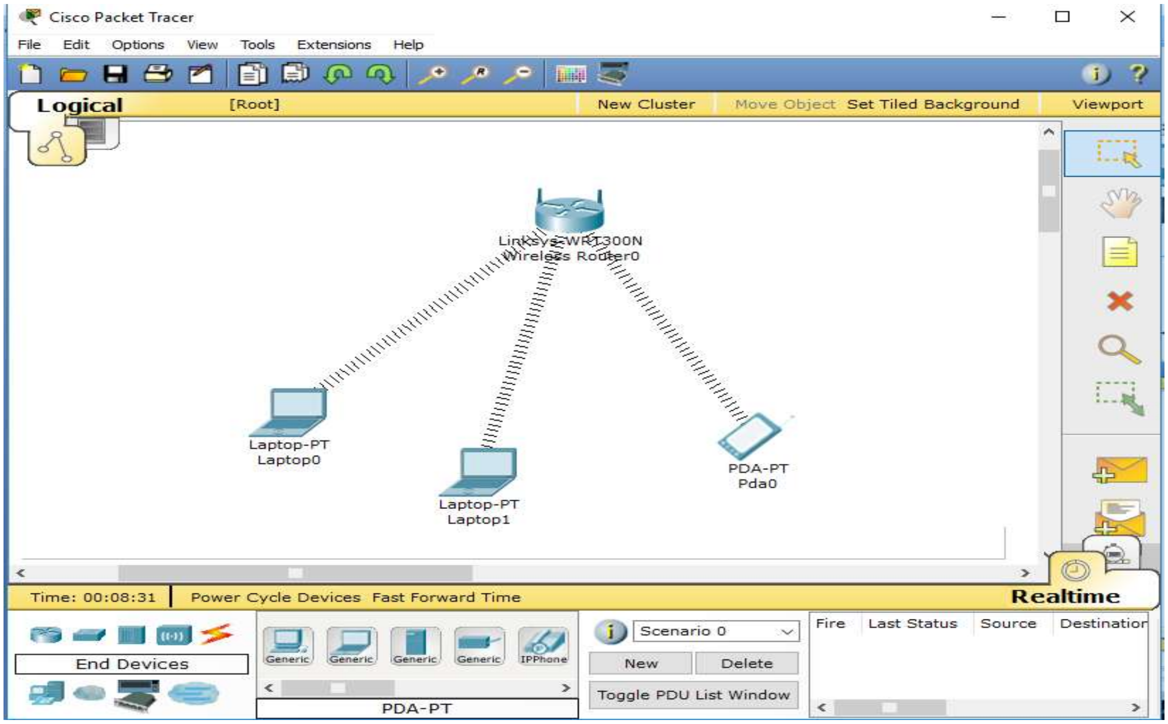
Adding Modules: Drag the module to an available slot on the device.

iv) Off the port then add the Linksys-WPC300N module which provides one 2.4GHz wireless interface suitable for connection to wireless network then on the port again do the same for another laptop

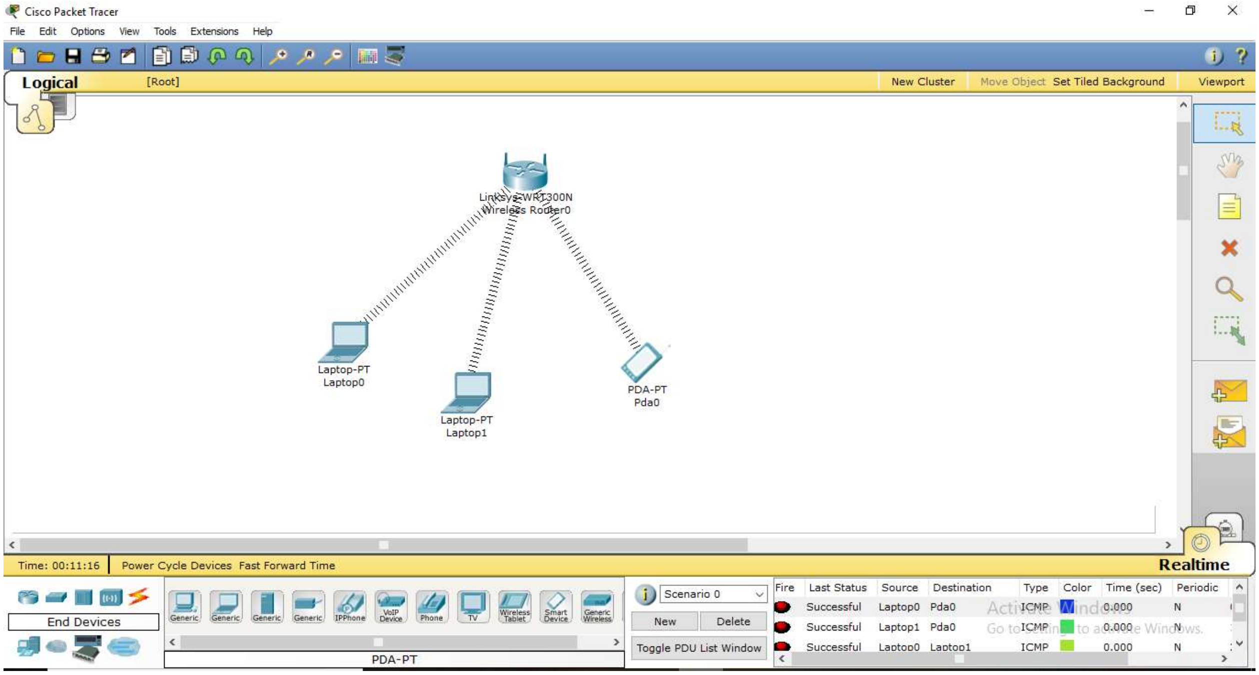


The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The

v) Once done you can see laptops are connected to wireless router



vi) Now check the connectivity by sending packet

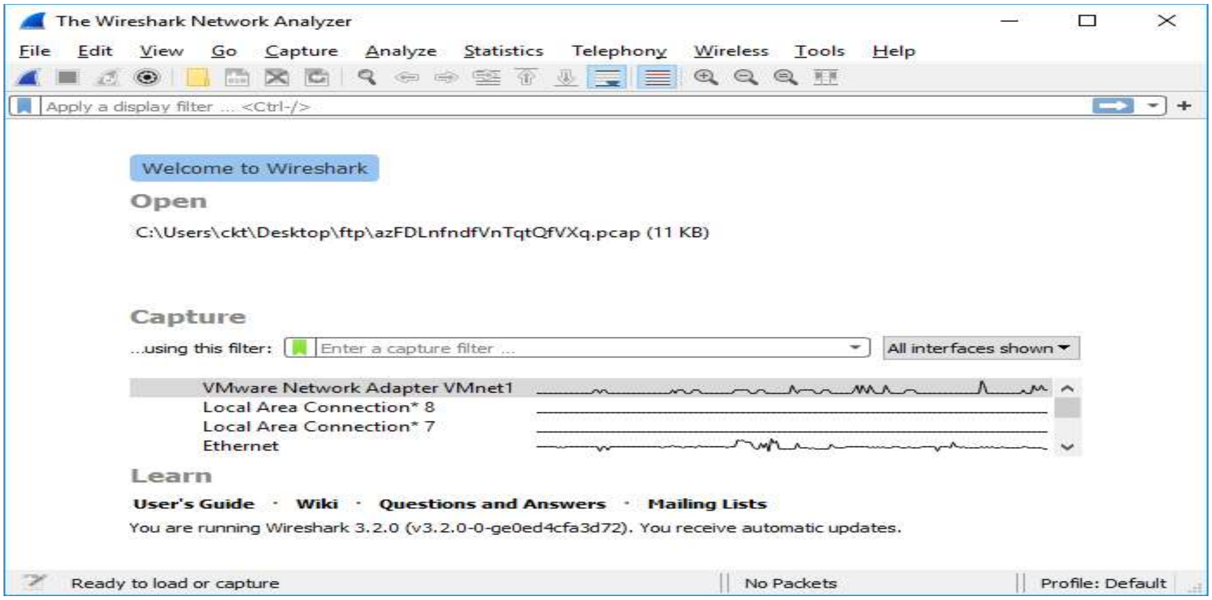


Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	Laptop0	Pda0	ICMP	🟦	0.000	N
●	Successful	Laptop1	Pda0	ICMP	🟩	0.000	N
●	Successful	Laptop0	Laptop1	ICMP	🟩	0.000	N

Practical-06

Aim: Using Wireshark network analyser set the filter for ICMP, TCP, HTTP, UDP, FTP and perform respective protocols transaction to show that network analyser is working.

1. **Wireshark network analyser**


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

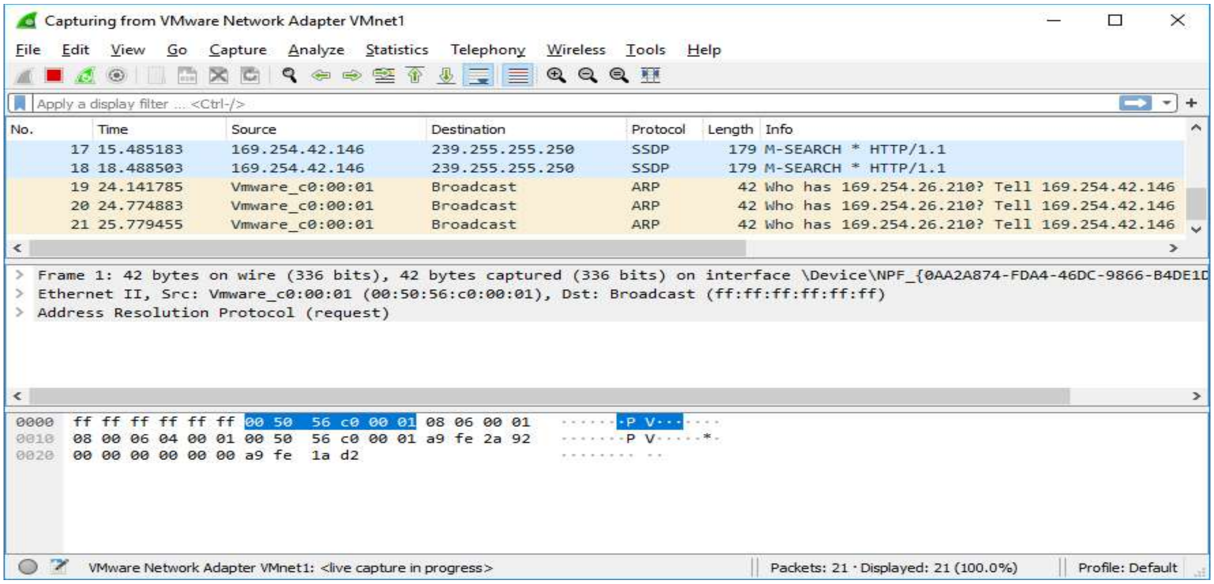
C:\Users\ckt\Desktop\ftp\azFDLnfndfVnTqtQfVXq.pcap (11 KB)

VMware Network Adapter VMnet1
Local Area Connection* 8
Local Area Connection* 7
Ethernet

You are running Wireshark 3.2.0 (v3.2.0-0-ge0ed4cfa3d72). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

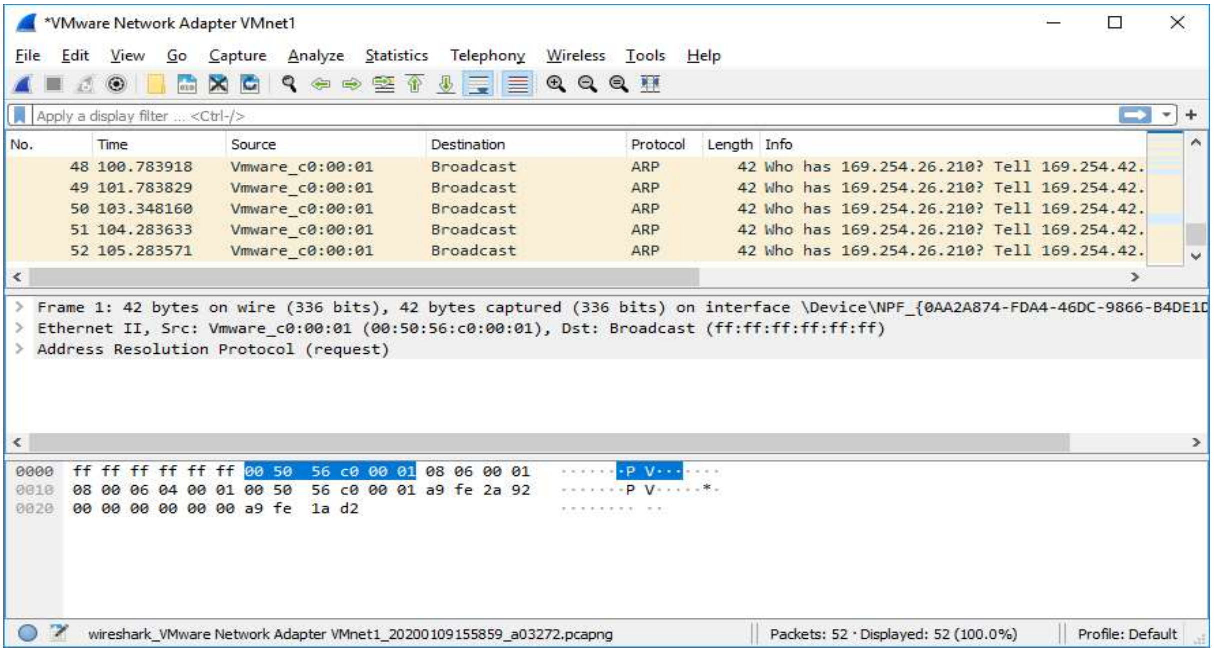
2. **Then click on start capturing packet present in the leftmost corner with blue icon colour.**


Capturing from VMware Network Adapter VMnet1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source           Destination       Protocol  Length Info
   17 15.485183   169.254.42.146   239.255.255.250   SSDP       179 M-SEARCH * HTTP/1.1
   18 18.488503   169.254.42.146   239.255.255.250   SSDP       179 M-SEARCH * HTTP/1.1
   19 24.141785   Vmware_c0:00:01  Broadcast         ARP         42 Who has 169.254.26.210? Tell 169.254.42.146
   20 24.774883   Vmware_c0:00:01  Broadcast         ARP         42 Who has 169.254.26.210? Tell 169.254.42.146
   21 25.779455   Vmware_c0:00:01  Broadcast         ARP         42 Who has 169.254.26.210? Tell 169.254.42.146

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{0AA2A874-FDA4-46DC-9866-B4DE1D
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 50  56 c0 00 01 08 06 00 01   ······-P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 01 a9 fe 2a 92   ·······P V·····*·
0020  00 00 00 00 00 00 a9 fe  1a d2                     ········ ··
```

VMware Network Adapter VMnet1: <live capture in progress>
Packets: 21 · Displayed: 21 (100.0%)
Profile: Default

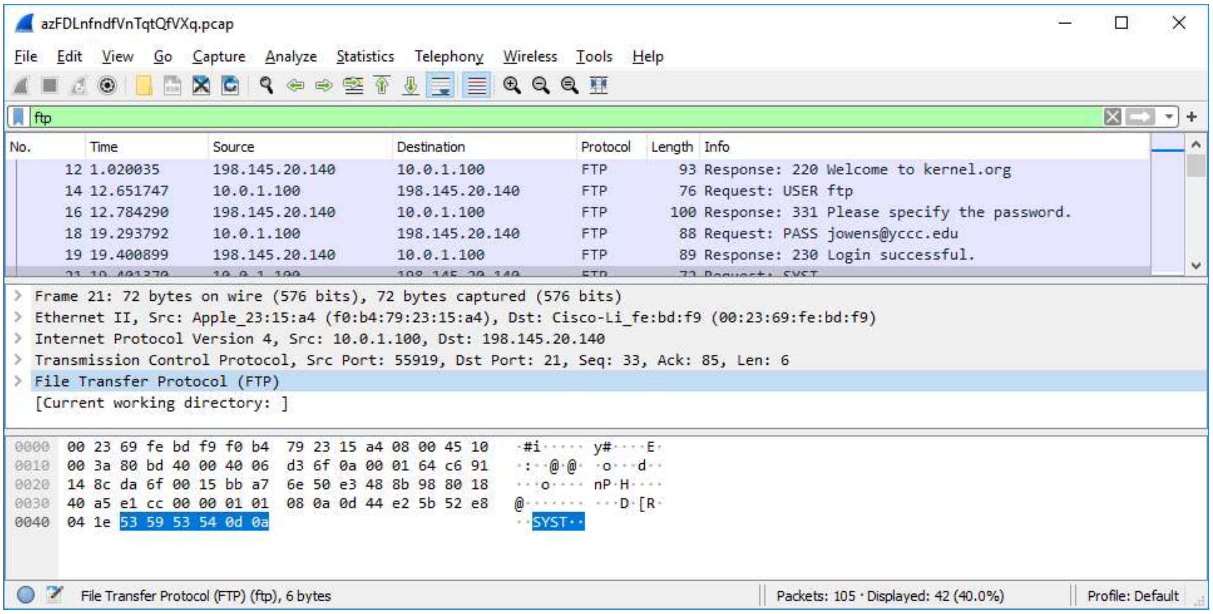
3. **Do some activity in your web browser and come back to wireshark and click on stop button.**


*VMware Network Adapter VMnet1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time         Source           Destination  Protocol  Length Info
   48 100.783918   Vmware_c0:00:01  Broadcast    ARP         42 Who has 169.254.26.210? Tell 169.254.42.
   49 101.783829   Vmware_c0:00:01  Broadcast    ARP         42 Who has 169.254.26.210? Tell 169.254.42.
   50 103.348160   Vmware_c0:00:01  Broadcast    ARP         42 Who has 169.254.26.210? Tell 169.254.42.
   51 104.283633   Vmware_c0:00:01  Broadcast    ARP         42 Who has 169.254.26.210? Tell 169.254.42.
   52 105.283571   Vmware_c0:00:01  Broadcast    ARP         42 Who has 169.254.26.210? Tell 169.254.42.

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{0AA2A874-FDA4-46DC-9866-B4DE1D
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 50  56 c0 00 01 08 06 00 01   ······-P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 01 a9 fe 2a 92   ·······P V·····*·
0020  00 00 00 00 00 00 a9 fe  1a d2                     ········ ··
```

wireshark_VMware Network Adapter VMnet1_20200109155859_a03272.pcapng
Packets: 52 · Displayed: 52 (100.0%)
Profile: Default

4. **Into a apply filter display (search option) enter specific protocols and check related with that protocol activities.**
   - **ftp:**



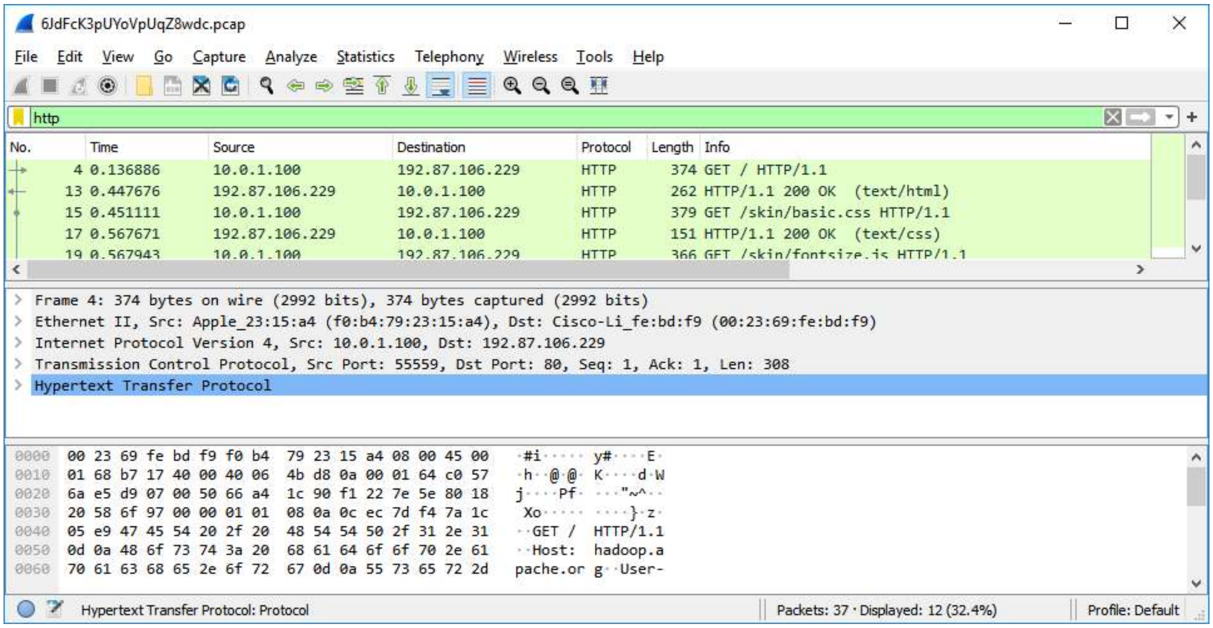
```
No.   Time        Source          Destination     Protocol Length Info
   12 1.020035    198.145.20.140  10.0.1.100      FTP         93 Response: 220 Welcome to kernel.org
   14 12.651747   10.0.1.100      198.145.20.140  FTP         76 Request: USER ftp
   16 12.784290   198.145.20.140  10.0.1.100      FTP        100 Response: 331 Please specify the password.
   18 19.293792   10.0.1.100      198.145.20.140  FTP         88 Request: PASS jowens@yccc.edu
   19 19.400899   198.145.20.140  10.0.1.100      FTP         89 Response: 230 Login successful.
   21 19.401370   10.0.1.100      198.145.20.140  FTP         72 Request: SYST
```

```
> Frame 21: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: Apple_23:15:a4 (f0:b4:79:23:15:a4), Dst: Cisco-Li_fe:bd:f9 (00:23:69:fe:bd:f9)
> Internet Protocol Version 4, Src: 10.0.1.100, Dst: 198.145.20.140
> Transmission Control Protocol, Src Port: 55919, Dst Port: 21, Seq: 33, Ack: 85, Len: 6
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 23 69 fe bd f9 f0 b4  79 23 15 a4 08 00 45 10   ·#i····· y#····E·
0010  00 3a 80 bd 40 00 40 06  d3 6f 0a 00 01 64 c6 91   ·:··@·@· ·o···d··
0020  14 8c da 6f 00 15 bb a7  6e 50 e3 48 8b 98 80 18   ···o···· nP·H····
0030  40 a5 e1 cc 00 00 01 01  08 0a 0d 44 e2 5b 52 e8   @······· ···D·[R·
0040  04 1e 53 59 53 54 0d 0a                            ··SYST··
```

File Transfer Protocol (FTP) (ftp), 6 bytes | Packets: 105 · Displayed: 42 (40.0%) | Profile: Default

- **http:**



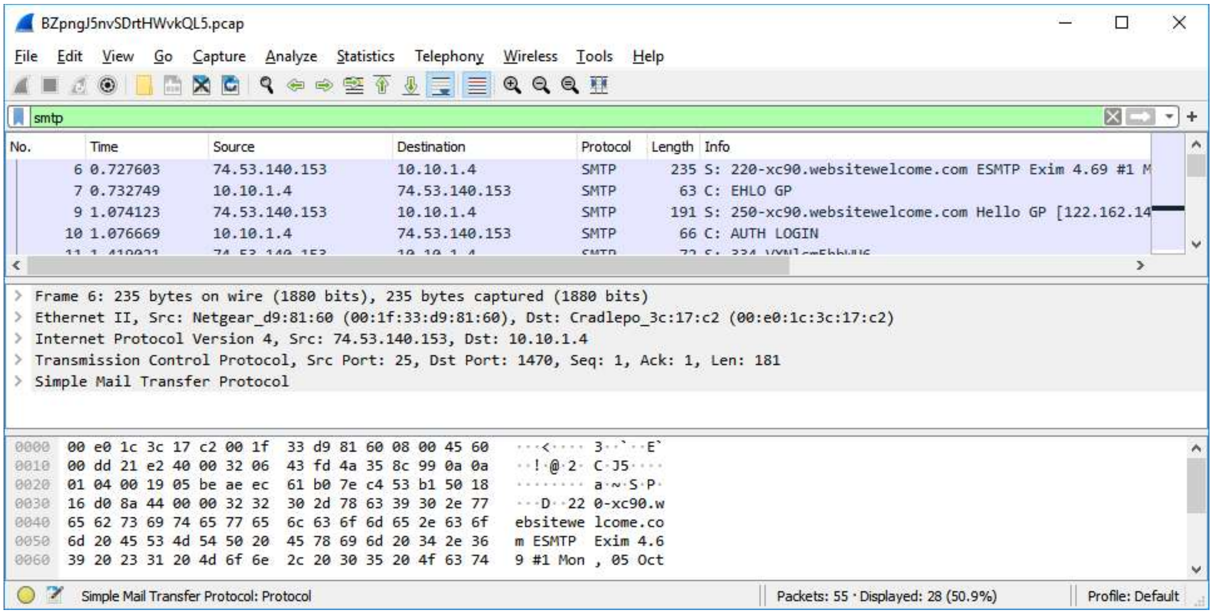
```
No.   Time        Source          Destination     Protocol Length Info
    4 0.136886    10.0.1.100      192.87.106.229  HTTP       374 GET / HTTP/1.1
   13 0.447676    192.87.106.229  10.0.1.100      HTTP       262 HTTP/1.1 200 OK  (text/html)
   15 0.451111    10.0.1.100      192.87.106.229  HTTP       379 GET /skin/basic.css HTTP/1.1
   17 0.567671    192.87.106.229  10.0.1.100      HTTP       151 HTTP/1.1 200 OK  (text/css)
   19 0.567943    10.0.1.100      192.87.106.229  HTTP       366 GET /skin/fontsize.js HTTP/1.1
```

```
> Frame 4: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits)
> Ethernet II, Src: Apple_23:15:a4 (f0:b4:79:23:15:a4), Dst: Cisco-Li_fe:bd:f9 (00:23:69:fe:bd:f9)
> Internet Protocol Version 4, Src: 10.0.1.100, Dst: 192.87.106.229
> Transmission Control Protocol, Src Port: 55559, Dst Port: 80, Seq: 1, Ack: 1, Len: 308
> Hypertext Transfer Protocol
```

```
0000  00 23 69 fe bd f9 f0 b4  79 23 15 a4 08 00 45 00   ·#i····· y#····E·
0010  01 68 b7 17 40 00 40 06  4b d8 0a 00 01 64 c0 57   ·h··@·@· K····d·W
0020  6a e5 d9 07 00 50 66 a4  1c 90 f1 22 7e 5e 80 18   j····Pf· ···"~^··
0030  20 58 6f 97 00 00 01 01  08 0a 0c ec 7d f4 7a 1c    Xo····· ····}·z·
0040  05 e9 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  68 61 64 6f 6f 70 2e 61   ··Host:  hadoop.a
0060  70 61 63 68 65 2e 6f 72  67 0d 0a 55 73 65 72 2d   pache.or g··User-
```

Hypertext Transfer Protocol: Protocol | Packets: 37 · Displayed: 12 (32.4%) | Profile: Default

- **smtp:**


BZpngJ5nvSDrtHWvkQL5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp

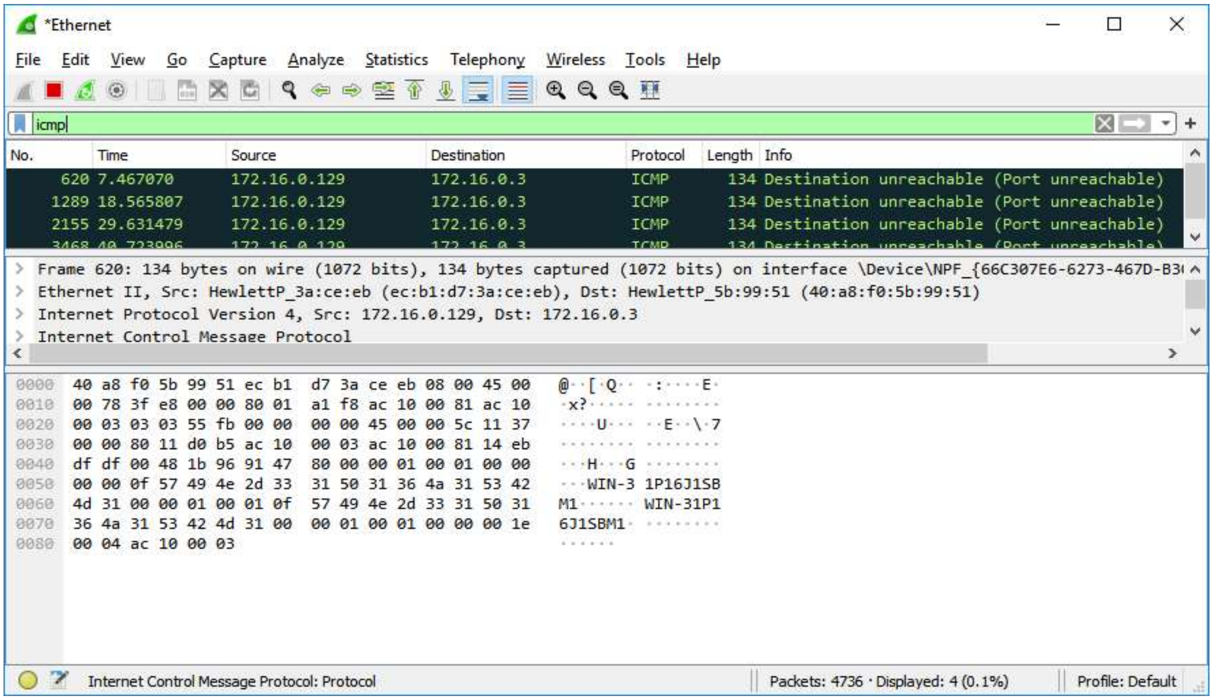
```
No.   Time        Source          Destination     Protocol  Length Info
    6 0.727603    74.53.140.153   10.10.1.4       SMTP         235 S: 220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 M
    7 0.732749    10.10.1.4       74.53.140.153   SMTP          63 C: EHLO GP
    9 1.074123    74.53.140.153   10.10.1.4       SMTP         191 S: 250-xc90.websitewelcome.com Hello GP [122.162.14
   10 1.076669    10.10.1.4       74.53.140.153   SMTP          66 C: AUTH LOGIN
```

```
> Frame 6: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
> Ethernet II, Src: Netgear_d9:81:60 (00:1f:33:d9:81:60), Dst: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2)
> Internet Protocol Version 4, Src: 74.53.140.153, Dst: 10.10.1.4
> Transmission Control Protocol, Src Port: 25, Dst Port: 1470, Seq: 1, Ack: 1, Len: 181
> Simple Mail Transfer Protocol
```

```
0000  00 e0 1c 3c 17 c2 00 1f  33 d9 81 60 08 00 45 60   ···<···· 3··`··E`
0010  00 dd 21 e2 40 00 32 06  43 fd 4a 35 8c 99 0a 0a   ··!·@·2· C·J5····
0020  01 04 00 19 05 be ae ec  61 b0 7e c4 53 b1 50 18   ········ a·~·S·P·
0030  16 d0 8a 44 00 00 32 32  30 2d 78 63 39 30 2e 77   ···D··22 0-xc90.w
0040  65 62 73 69 74 65 77 65  6c 63 6f 6d 65 2e 63 6f   ebsitewe lcome.co
0050  6d 20 45 53 4d 54 50 20  45 78 69 6d 20 34 2e 36   m ESMTP  Exim 4.6
0060  39 20 23 31 20 4d 6f 6e  2c 20 30 35 20 4f 63 74   9 #1 Mon , 05 Oct
```

Simple Mail Transfer Protocol: Protocol | Packets: 55 · Displayed: 28 (50.9%) | Profile: Default

- **icmp:**


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

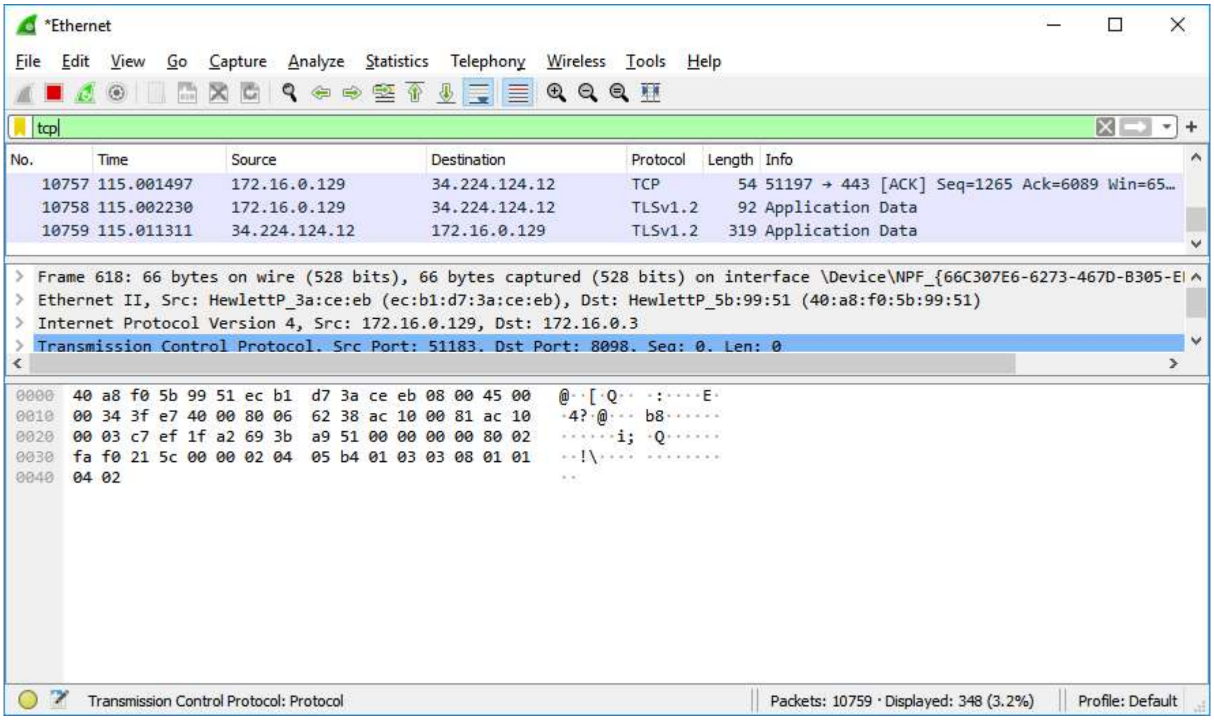
```
No.   Time         Source          Destination     Protocol  Length Info
  620 7.467070     172.16.0.129    172.16.0.3      ICMP         134 Destination unreachable (Port unreachable)
 1289 18.565807    172.16.0.129    172.16.0.3      ICMP         134 Destination unreachable (Port unreachable)
 2155 29.631479    172.16.0.129    172.16.0.3      ICMP         134 Destination unreachable (Port unreachable)
```

```
> Frame 620: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{66C307E6-6273-467D-B3
> Ethernet II, Src: HewlettP_3a:ce:eb (ec:b1:d7:3a:ce:eb), Dst: HewlettP_5b:99:51 (40:a8:f0:5b:99:51)
> Internet Protocol Version 4, Src: 172.16.0.129, Dst: 172.16.0.3
> Internet Control Message Protocol
```

```
0000  40 a8 f0 5b 99 51 ec b1  d7 3a ce eb 08 00 45 00   @··[·Q·· ·:····E·
0010  00 78 3f e8 00 00 80 01  a1 f8 ac 10 00 81 ac 10   ·x?····· ········
0020  00 03 03 03 55 fb 00 00  00 00 45 00 00 5c 11 37   ····U··· ··E··\·7
0030  00 00 80 11 d0 b5 ac 10  00 03 ac 10 00 81 14 eb   ········ ········
0040  df df 00 48 1b 96 91 47  80 00 00 01 00 01 00 00   ···H···G ········
0050  00 00 0f 57 49 4e 2d 33  31 50 31 36 4a 31 53 42   ···WIN-3 1P16J1SB
0060  4d 31 00 00 01 00 01 0f  57 49 4e 2d 33 31 50 31   M1······ WIN-31P1
0070  36 4a 31 53 42 4d 31 00  00 01 00 01 00 00 00 1e   6J1SBM1· ········
0080  00 04 ac 10 00 03                                  ······
```

Internet Control Message Protocol: Protocol | Packets: 4736 · Displayed: 4 (0.1%) | Profile: Default

- **tcp:**


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

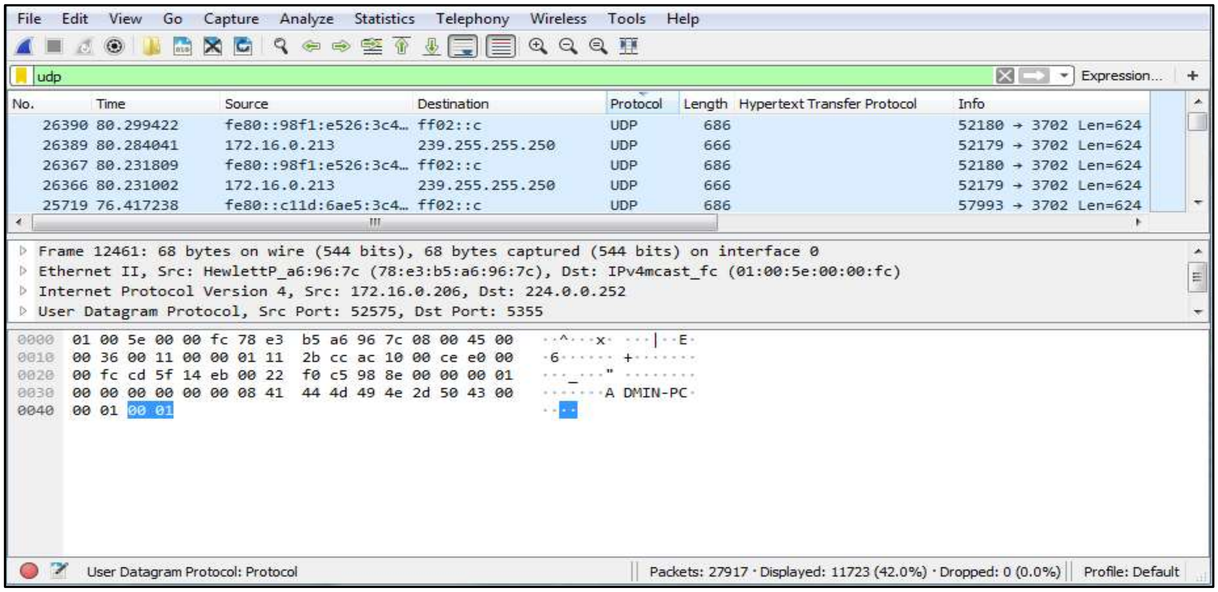
```
No.     Time        Source          Destination     Protocol  Length Info
  10757 115.001497  172.16.0.129    34.224.124.12   TCP           54 51197 → 443 [ACK] Seq=1265 Ack=6089 Win=65…
  10758 115.002230  172.16.0.129    34.224.124.12   TLSv1.2       92 Application Data
  10759 115.011311  34.224.124.12   172.16.0.129    TLSv1.2      319 Application Data
```

```
> Frame 618: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{66C307E6-6273-467D-B305-E
> Ethernet II, Src: HewlettP_3a:ce:eb (ec:b1:d7:3a:ce:eb), Dst: HewlettP_5b:99:51 (40:a8:f0:5b:99:51)
> Internet Protocol Version 4, Src: 172.16.0.129, Dst: 172.16.0.3
> Transmission Control Protocol, Src Port: 51183, Dst Port: 8098, Seq: 0, Len: 0
```

```
0000  40 a8 f0 5b 99 51 ec b1  d7 3a ce eb 08 00 45 00   @··[·Q·· ·:····E·
0010  00 34 3f e7 40 00 80 06  62 38 ac 10 00 81 ac 10   ·4?·@··· b8······
0020  00 03 c7 ef 1f a2 69 3b  a9 51 00 00 00 00 80 02   ······i; ·Q······
0030  fa f0 21 5c 00 00 02 04  05 b4 01 03 03 08 01 01   ··!\···· ········
0040  04 02                                              ··
```

Transmission Control Protocol: Protocol | Packets: 10759 · Displayed: 348 (3.2%) | Profile: Default

- **udp:**


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp

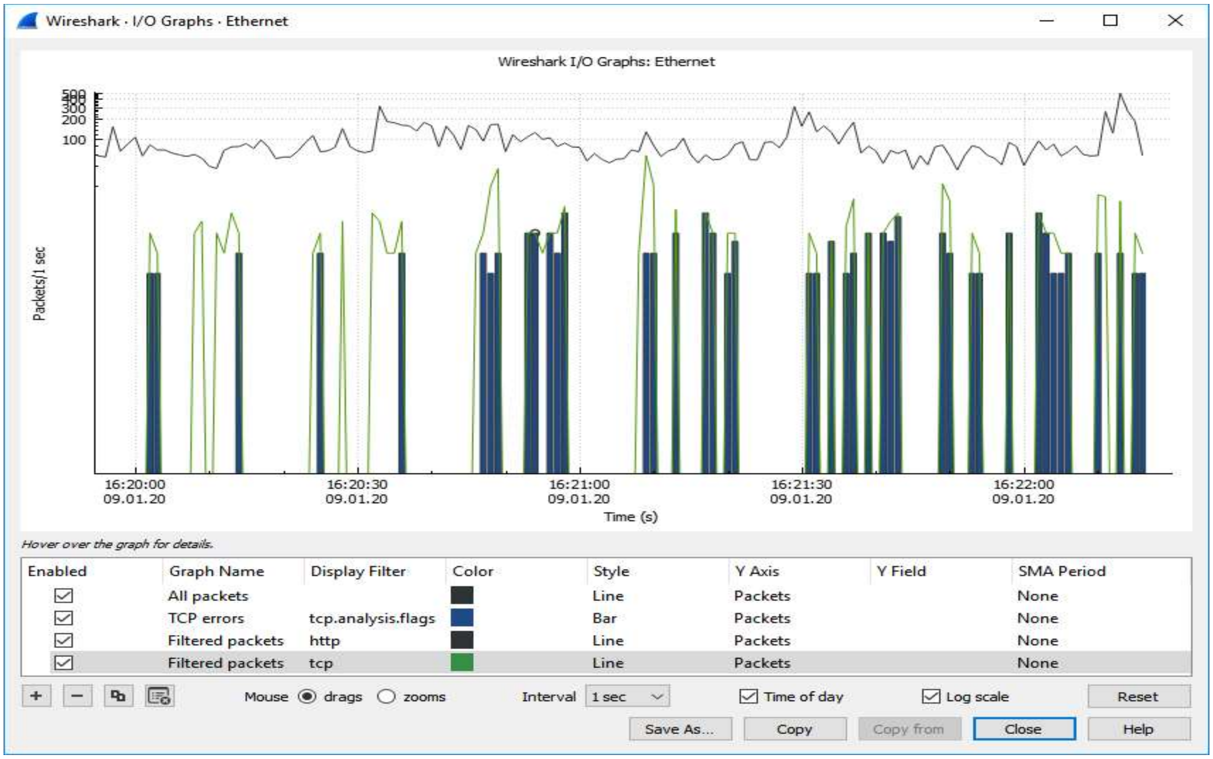
```
No.     Time       Source                  Destination       Protocol  Length Hypertext Transfer Protocol  Info
  26390 80.299422  fe80::98f1:e526:3c4…    ff02::c           UDP       686                                52180 → 3702 Len=624
  26389 80.284041  172.16.0.213            239.255.255.250   UDP       666                                52179 → 3702 Len=624
  26367 80.231809  fe80::98f1:e526:3c4…    ff02::c           UDP       686                                52180 → 3702 Len=624
  26366 80.231002  172.16.0.213            239.255.255.250   UDP       666                                52179 → 3702 Len=624
  25719 76.417238  fe80::c11d:6ae5:3c4…    ff02::c           UDP       686                                57993 → 3702 Len=624
```

```
▷ Frame 12461: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▷ Ethernet II, Src: HewlettP_a6:96:7c (78:e3:b5:a6:96:7c), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
▷ Internet Protocol Version 4, Src: 172.16.0.206, Dst: 224.0.0.252
▷ User Datagram Protocol, Src Port: 52575, Dst Port: 5355
```

```
0000  01 00 5e 00 00 fc 78 e3  b5 a6 96 7c 08 00 45 00   ··^···x· ···|··E·
0010  00 36 00 11 00 00 01 11  2b cc ac 10 00 ce e0 00   ·6······ +·······
0020  00 fc cd 5f 14 eb 00 22  f0 c5 98 8e 00 00 00 01   ···_···" ········
0030  00 00 00 00 00 00 08 41  44 4d 49 4e 2d 50 43 00   ·······A DMIN-PC·
0040  00 01 00 01                                        ····
```

User Datagram Protocol: Protocol | Packets: 27917 · Displayed: 11723 (42.0%) · Dropped: 0 (0.0%) | Profile: Default

5. **Then go to the statistic and select option I/O graph. Then you will come into the Wireshark I/O graph.**



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All packets		⬛	Line	Packets		None
☑	TCP errors	tcp.analysis.flags	🟦	Bar	Packets		None
☑	Filtered packets	http	⬛	Line	Packets		None
☑	Filtered packets	tcp	🟩	Line	Packets		None

Mouse ● drags ○ zooms

Interval 1 sec

☑ Time of day

☑ Log scale