Sr. No.	Objective of assignment	Date	Sign
1.	Basic Network Utilities and commands	21/02/22	
2.	Simulation of star topologies using a Switch/hub using cisco packet tracer.	28/02/22	
3.	Simulation of Tree and Ring Topologies Using ICMP and ARP.	21/03/22	
4.	Using Wireshark as a sniffing tool for protocol analysis (Live HTTP packet capturing)	28/03/22	
5.	Using Wireshark to analyze the captured PING(ICMP) request and response packets.	11/04/22	
6.	Simulation of two-star networks using ICMP request/response packets. Capturing and analyzing ethernet frames of trace file. Run ARP commands to analyze ARP cache	18/04/22	
7.	Analyzing a trace of IP Datagrams sent and received by an execution of traceroute program, investigating IP Protocol.	08/05/22	
8.	Using cisco packet tracer to perform subnetting of given address space, construct routing tables of each router and test for end-to-end connectivity.	15/05/22	

Network Commands

`ipconfig`

`ipconfig` is a utility that communicates with the IPConfiguration agent to retrieve and set IP configuration parameters. The IPConfiguration agent is responsible for configuring and managing the IPv4 and IPv6 addresses on direct, connectionless interfaces such as ethernet and Wi-Fi.

```
gaurav — -zsh — 100×30
gaurav@MacBookAir ~ % ipconfig getsummary en0
<dictionary> {
  BSSID : 46:39:cd:bb:47:e5
  IPv4 : <array> {
    0 : <dictionary> {
      Addresses : <array> {
        0 : 172.20.10.2
      }
      ChildServiceID : LINKLOCAL-en0
      ConfigMethod : DHCP
      DHCP : <dictionary> {
        LeaseExpirationTime : 05/27/2022 21:52:00
        LeaseStartTime : 05/26/2022 21:52:00
        Packet : op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0x5e276694
secs = 0
ciaddr = 0.0.0.0
yiaddr = 172.20.10.2
siaddr = 172.20.10.1
giaddr = 0.0.0.0
chaddr = d4:57:63:df:0:49
sname = Gauravs-iPhone
file =
options:
Options count is 7
dhcp_message_type (uint8): ACK 0x5
```

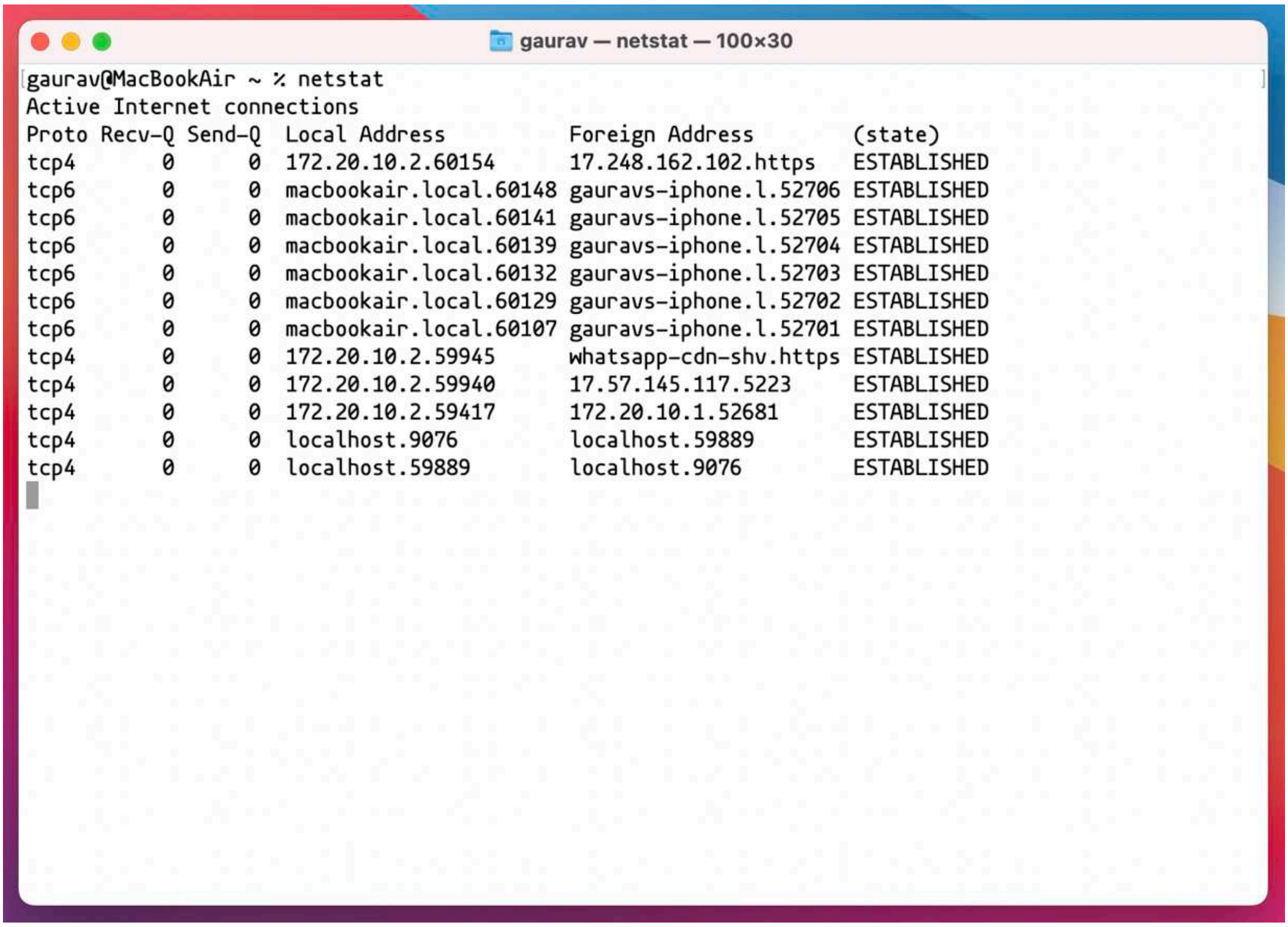
`traceroute`

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. traceroute utilizes the IP protocol 'time to live' field and attempts to elicit an ICMP `TIME_EXCEEDED` response from each gateway along the path to some host.

```
gaurav — traceroute www.google.com — 100×30
gaurav@MacBookAir ~ % traceroute www.google.com
traceroute to www.google.com (142.250.199.132), 64 hops max, 52 byte packets
 1  172.20.10.1 (172.20.10.1)  5.033 ms  4.659 ms  4.394 ms
 2  * * *
 3  10.72.221.39 (10.72.221.39)  79.174 ms
    10.72.220.199 (10.72.220.199)  57.031 ms
    10.72.221.39 (10.72.221.39)  44.294 ms
 4  192.168.30.47 (192.168.30.47)  52.749 ms
    192.168.30.53 (192.168.30.53)  52.093 ms  59.577 ms
 5  192.168.30.48 (192.168.30.48)  38.888 ms
    192.168.30.46 (192.168.30.46)  38.451 ms
    192.168.30.52 (192.168.30.52)  38.390 ms
 6  172.26.101.134 (172.26.101.134)  78.145 ms  63.430 ms  39.880 ms
 7  172.26.101.146 (172.26.101.146)  40.241 ms
    172.26.101.147 (172.26.101.147)  77.694 ms  38.307 ms
 8  192.168.30.58 (192.168.30.58)  68.103 ms
    192.168.30.54 (192.168.30.54)  38.793 ms
    192.168.30.56 (192.168.30.56)  79.204 ms
 9  192.168.30.61 (192.168.30.61)  43.179 ms
    192.168.30.55 (192.168.30.55)  96.755 ms
    192.168.30.61 (192.168.30.61)  45.008 ms
10  172.16.4.49 (172.16.4.49)  48.906 ms
    172.16.4.47 (172.16.4.47)  81.213 ms
    172.16.4.45 (172.16.4.45)  72.616 ms
11  172.16.4.53 (172.16.4.53)  127.789 ms  48.776 ms
    172.16.18.33 (172.16.18.33)  59.820 ms
```

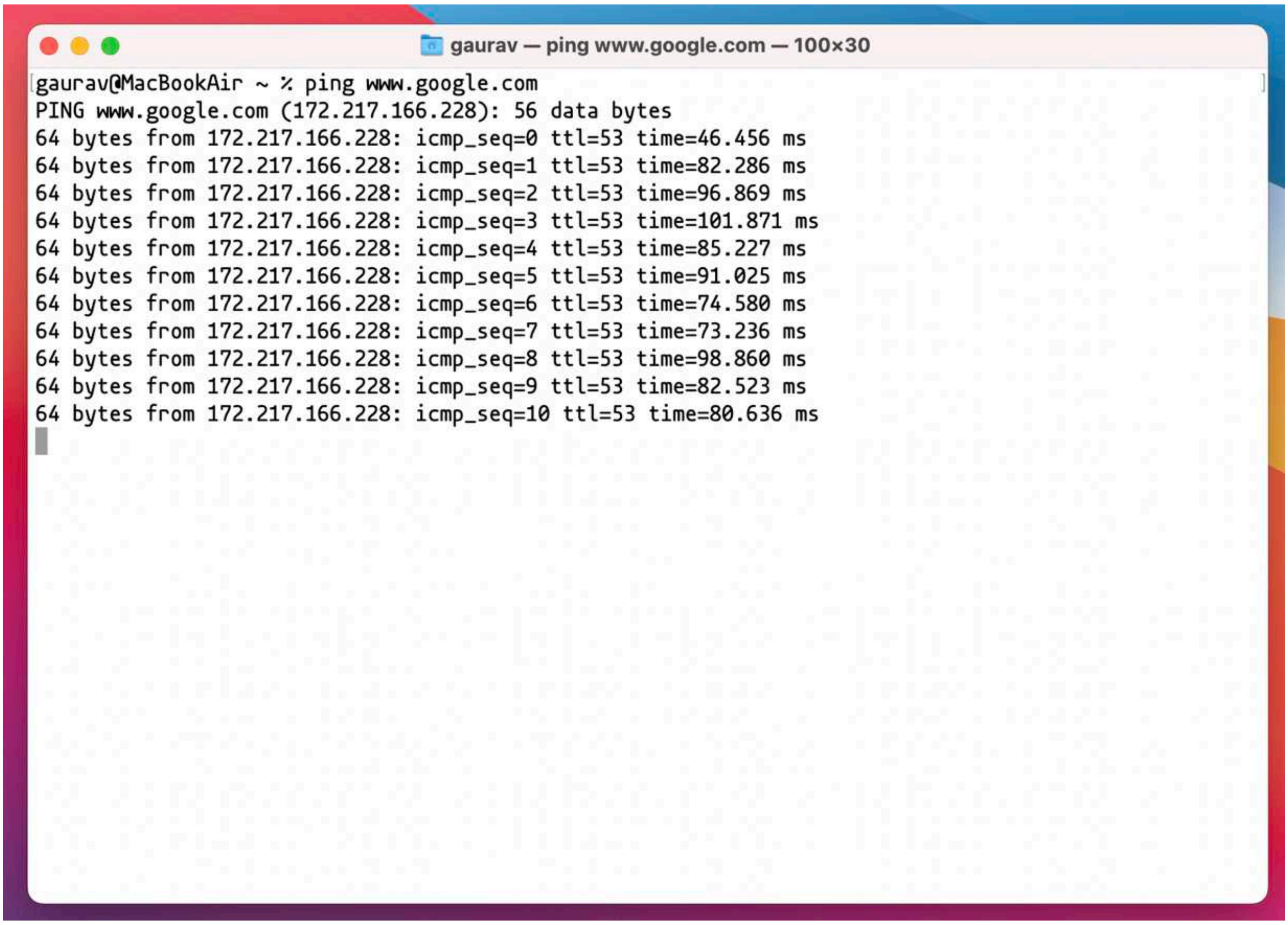
netstat

The netstat command symbolically displays the contents of various network-related data structures. There are a number of output formats, depending on the options for the information presented. The first form of the command displays a list of active sockets for each protocol. The second form presents the contents of one of the other network data structures according to the option selected. Using the third form, with a wait interval specified, netstat will continuously display the information regarding packet traffic on the configured network interfaces. The fourth form displays statistics for the specified protocol or address family. If a wait interval is specified, the protocol information over the last interval seconds will be displayed. The fifth form displays per-interface statistics for the specified protocol or address family. The sixth form displays mbuf(9) statistics. The seventh form displays routing table for the specified address family. The eighth form displays routing statistics.



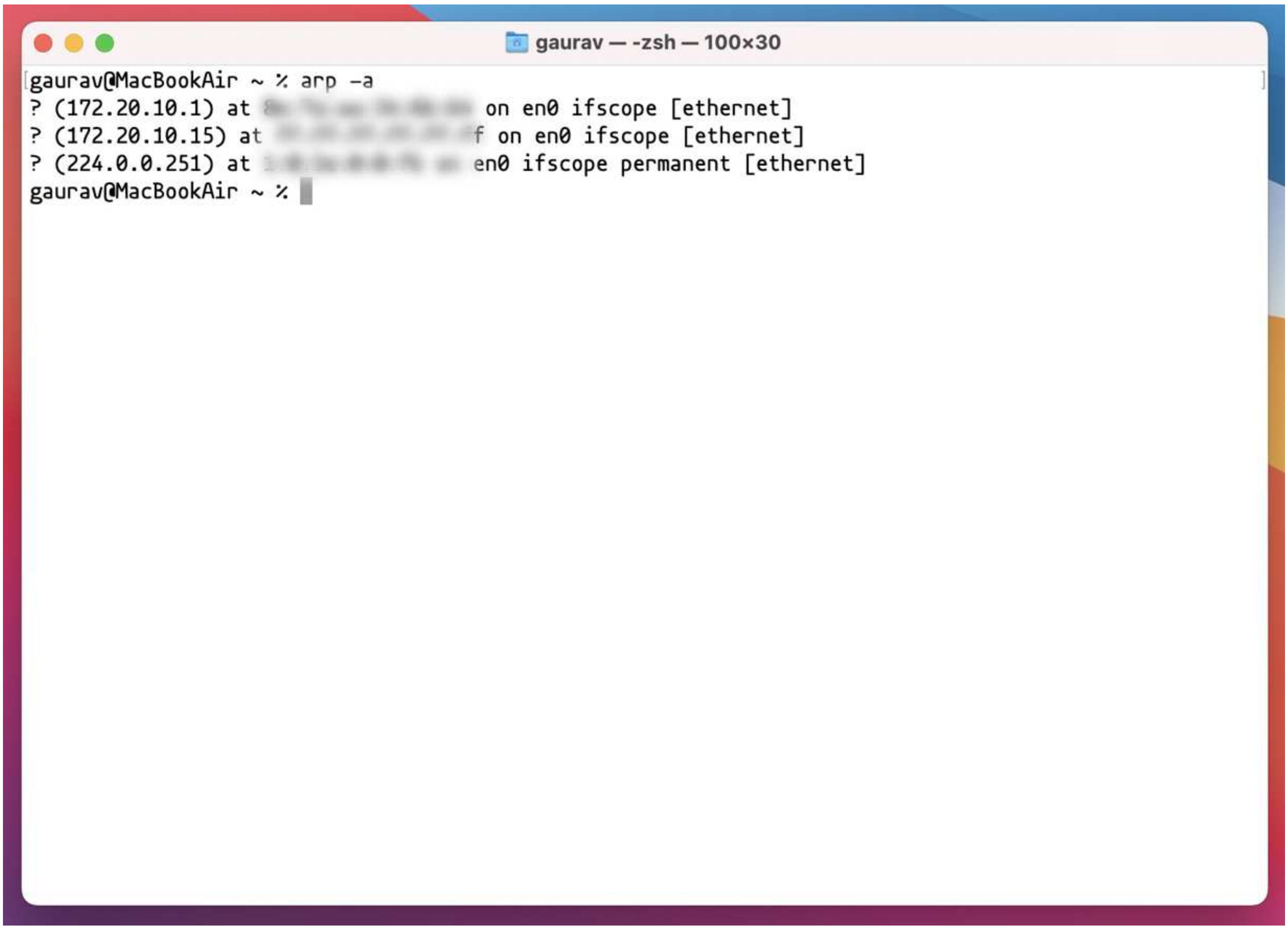
ping

The `ping` utility uses the ICMP protocol's mandatory `ECHO_REQUEST` datagram to elicit an ICMP `ECHO_RESPONSE` from a host or gateway. `ECHO_REQUEST` datagrams have an IP and ICMP header, followed by a "struct timeval" and then an arbitrary number of "pad" bytes used to fill out the packet



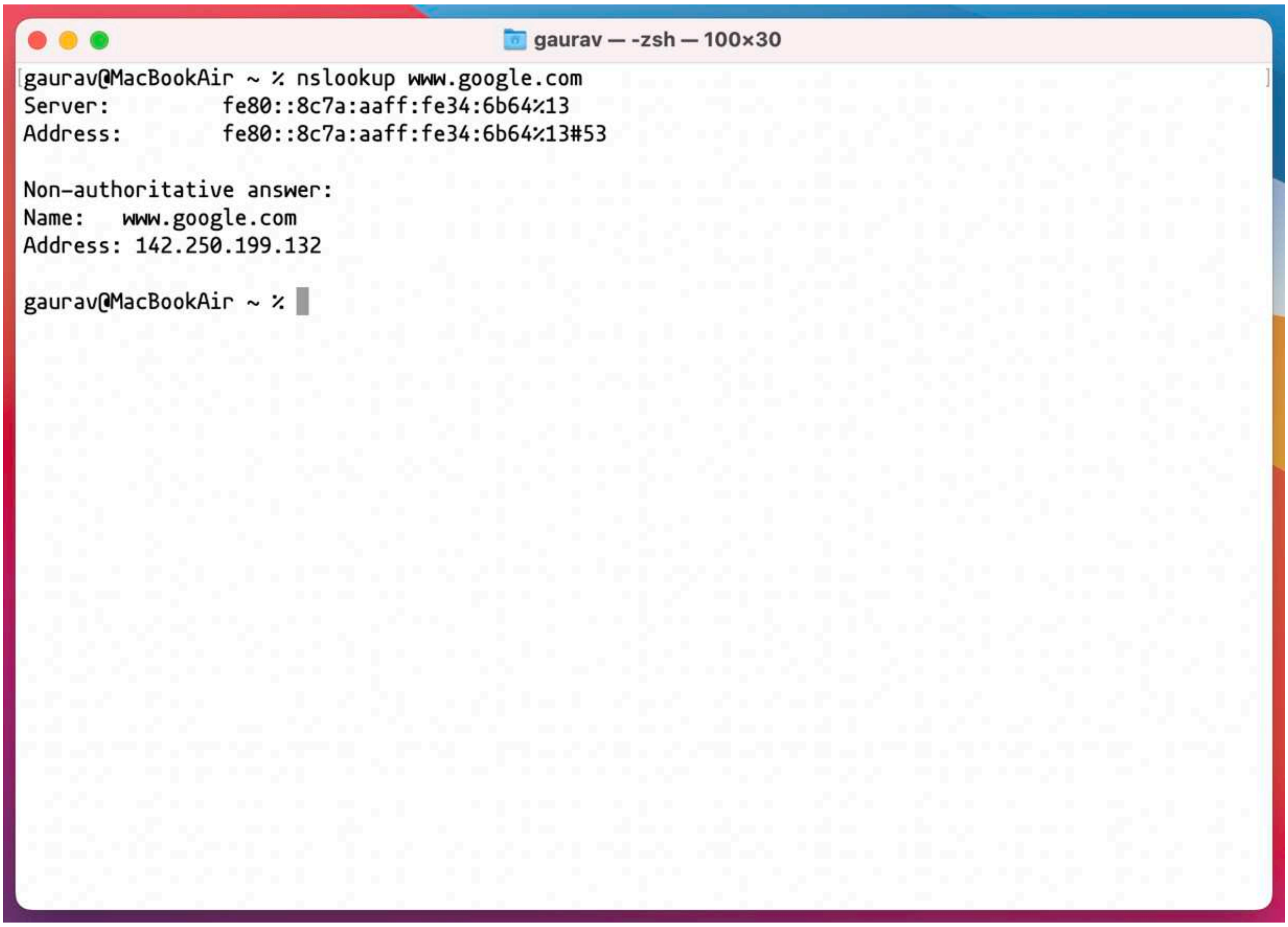
`arp`

The `arp` utility displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol. With no flags, the program displays the current ARP entry for the specified hostname. The host may be specified by name or by number, using Internet dot notation



`nslookup`

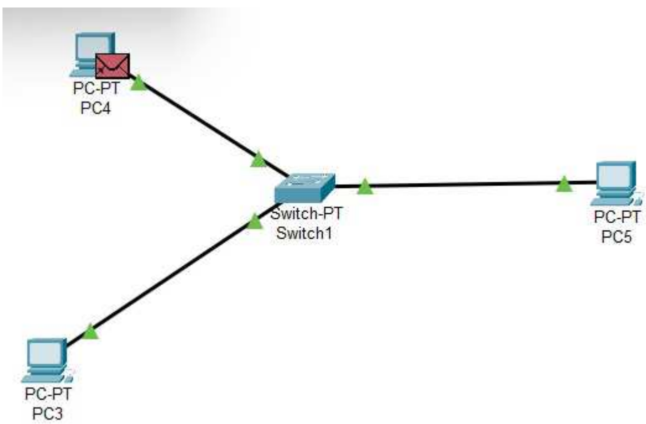
`nslookup` is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

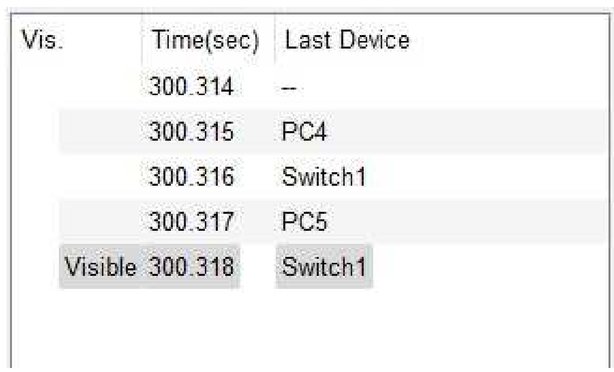


Assignment #1

Topology 1:

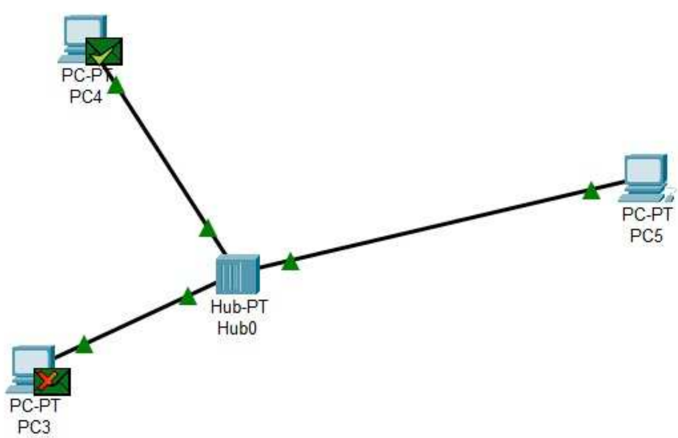
Use the Cisco Packet Tracer Simulation Tool to design the following network topologies in real-time mode. Use the Simulation mode to test the ICMP Ping service (using a Simple PDU) on both the networks

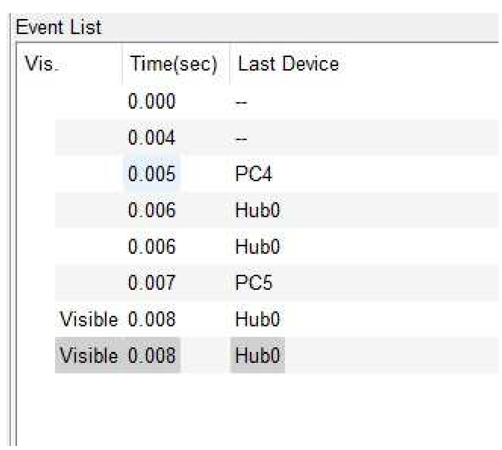




Vis.	Time(sec)	Last Device
	300.314	--
	300.315	PC4
	300.316	Switch1
	300.317	PC5
Visible	300.318	Switch1

In the above topology, replace the switch with a hub and compare the behavior.

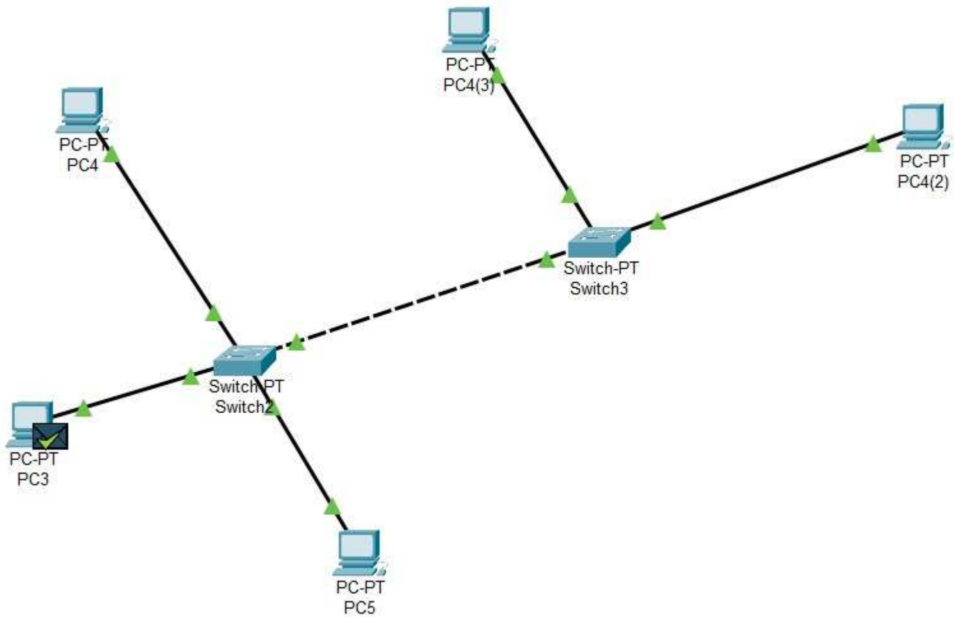




Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.004	--
	0.005	PC4
	0.006	Hub0
	0.006	Hub0
	0.007	PC5
Visible	0.008	Hub0
Visible	0.008	Hub0

Topology 2:

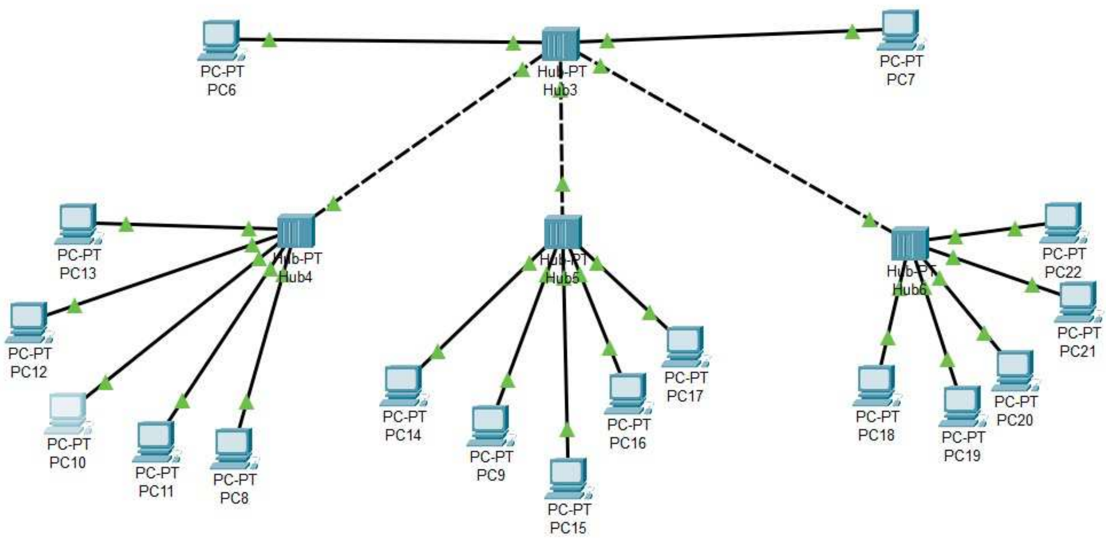


Event List

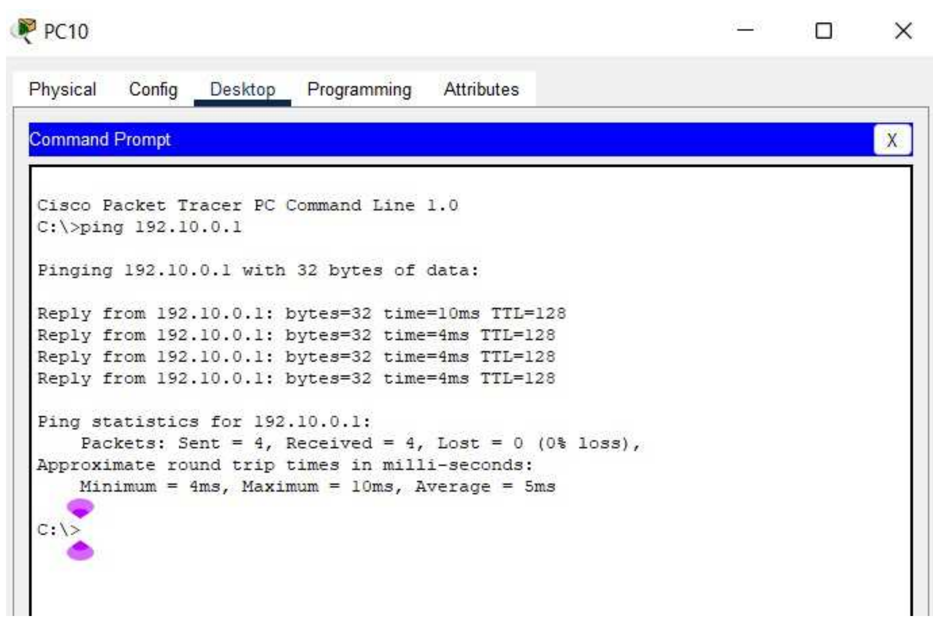
Vis.	Time(sec)	Last Device
	0.000	--
	0.006	--
	0.007	PC3
	0.008	Switch2
	0.009	Switch3
	0.010	PC4(3)
	0.011	Switch3
Visible	0.012	Switch2

Assignment #2

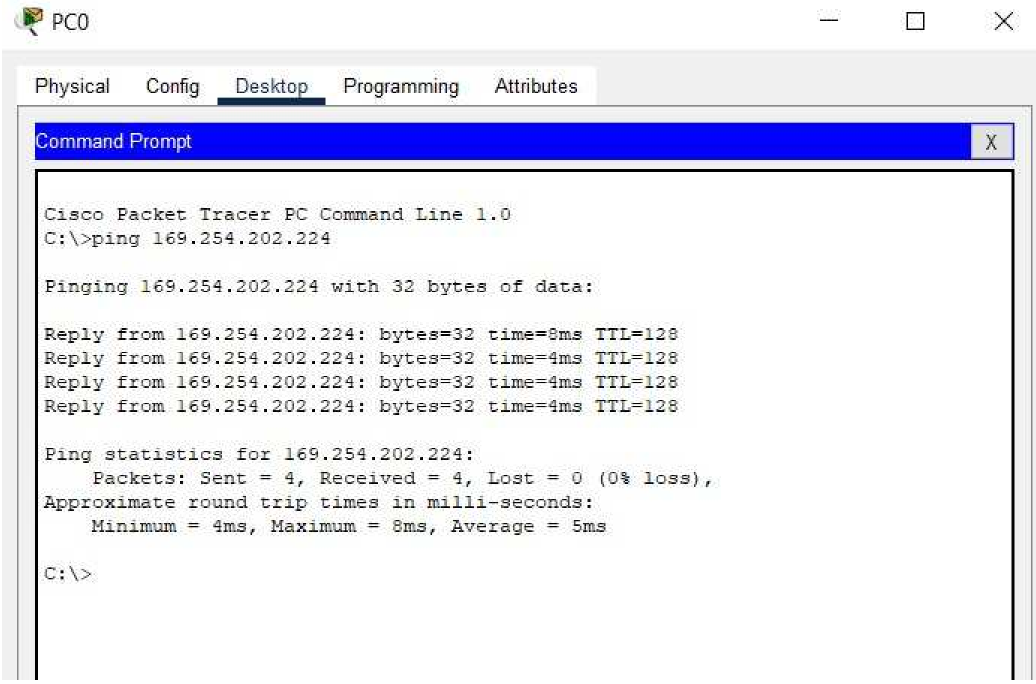
1. Construct a tree topology that uses a primary hub to connect three secondary hubs. The primary hub has two hosts connected directly to it, whereas each of the three secondary hubs have five directly connected hosts. Simulate the above constructed tree network using ICMP request/response packets to perform the following:



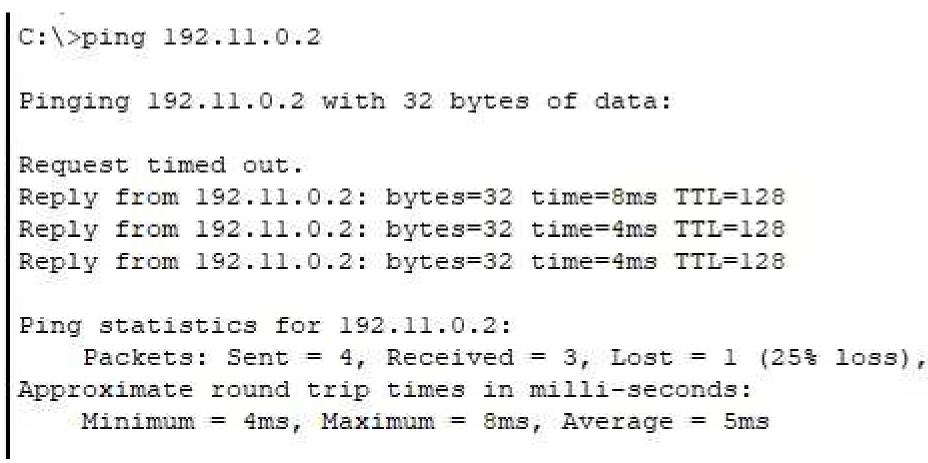
a) Check connectivity between any two hosts directly connected to the same secondary hub (Do it for all the three secondary hubs).



b) Check connectivity between two hosts directly connected to the primary hub.



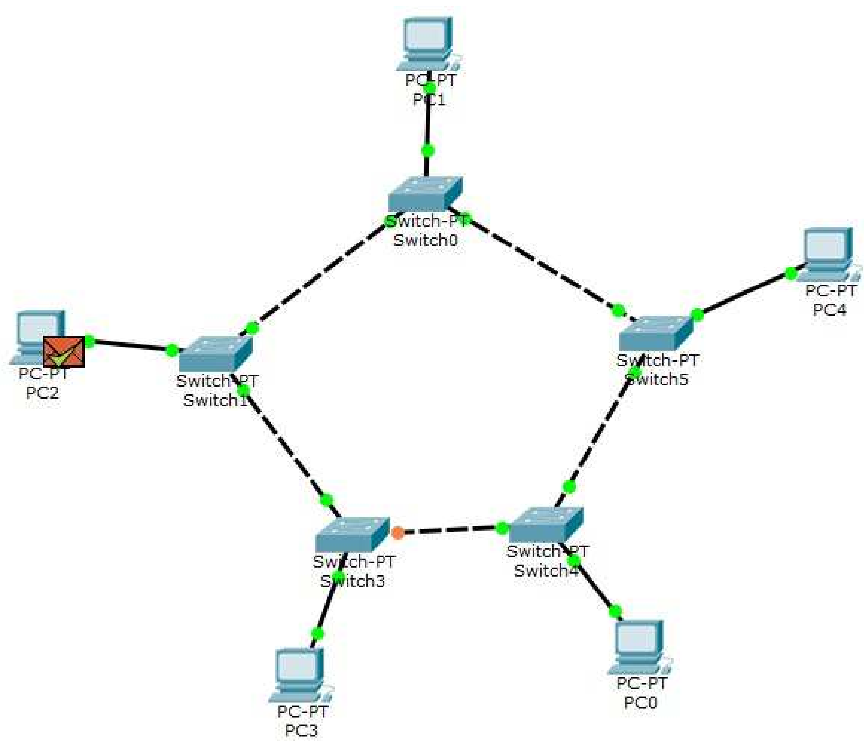
c) Check connectivity between a host connected to the primary hub and a host connected to any of the three secondary hubs

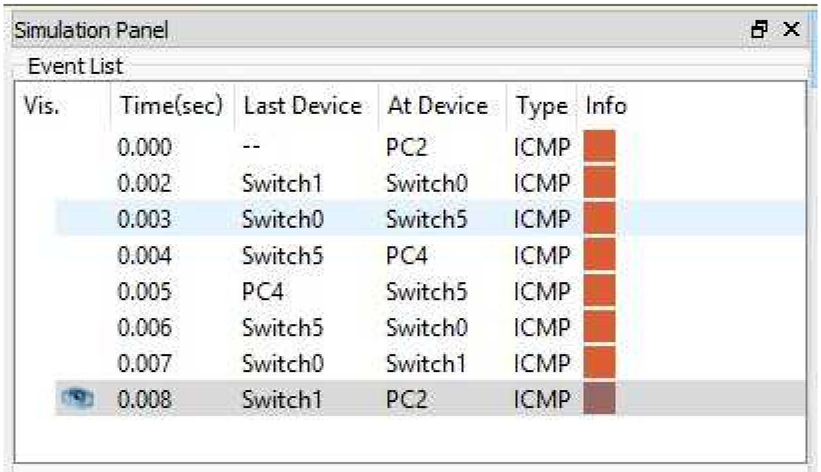


d) Check connectivity between a host connected directly to a secondary hub and another host connected directly to some other secondary hub.

```
C:\>ping 169.254.74.16

Pinging 169.254.74.16 with 32 bytes of data:

Reply from 169.254.74.16: bytes=32 time=8ms TTL=128
Reply from 169.254.74.16: bytes=32 time=8ms TTL=128
Reply from 169.254.74.16: bytes=32 time=8ms TTL=128
Reply from 169.254.74.16: bytes=32 time=8ms TTL=128

Ping statistics for 169.254.74.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms

C:\>
```

2. Construct a LAN of five hosts arranged in a ring topology and check connectivity between the hosts by sending ICMP request/response pack



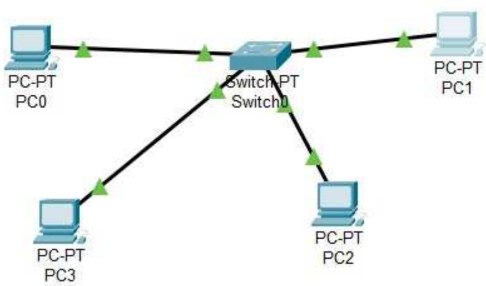


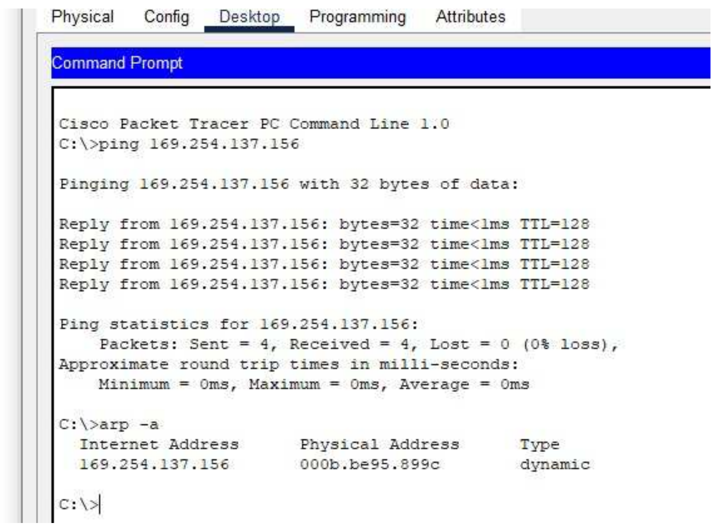
Simulation Panel

Event List

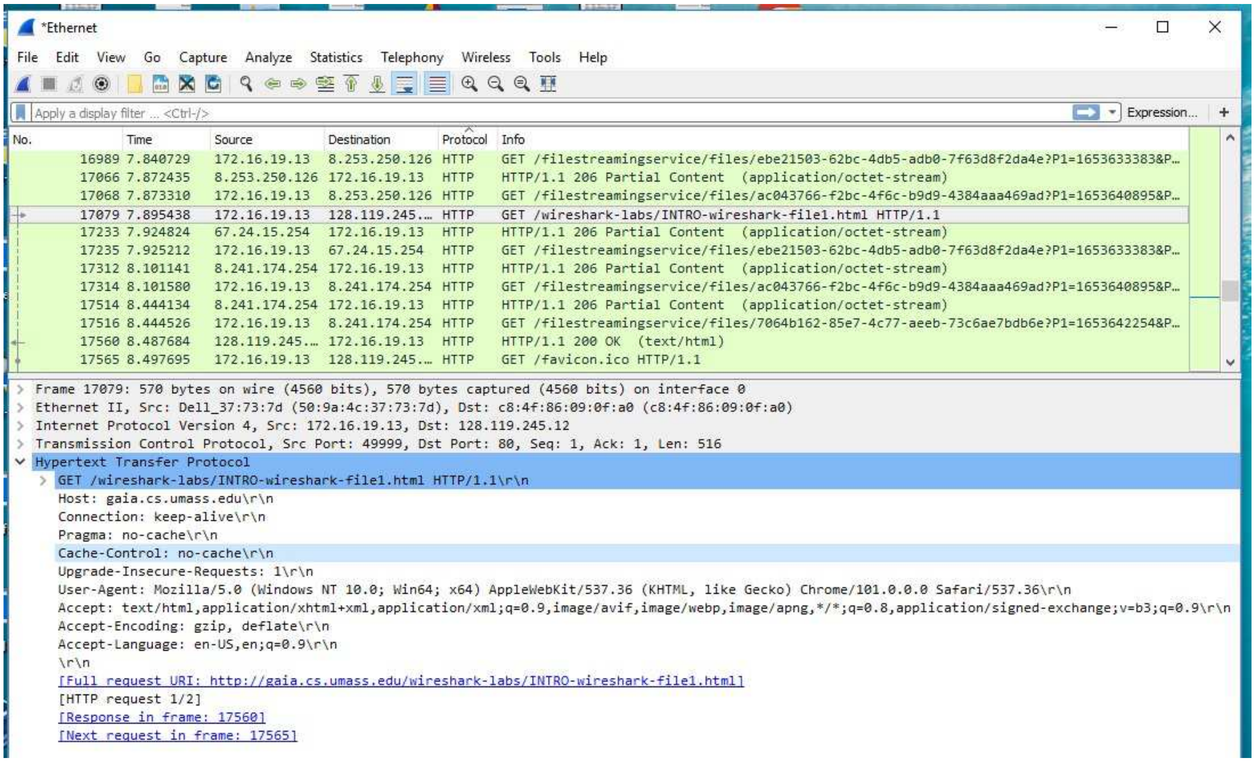
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC2	ICMP	
	0.002	Switch1	Switch0	ICMP	
	0.003	Switch0	Switch5	ICMP	
	0.004	Switch5	PC4	ICMP	
	0.005	PC4	Switch5	ICMP	
	0.006	Switch5	Switch0	ICMP	
	0.007	Switch0	Switch1	ICMP	
	0.008	Switch1	PC2	ICMP	

3. Use Command Line prompt to PING hosts in a network and check their ARP Tables.





Assignment #3



1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer: TCP, UDP & HTTP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.

Answer: 0.592246 seconds

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Answer: Address for gaia.cs.umass.edu is 128.119.245.12 and that of my computer is 172.16.19.13

4. Print the two HTTP messages (GET and OK) referred to in question 2 above.

Answer:

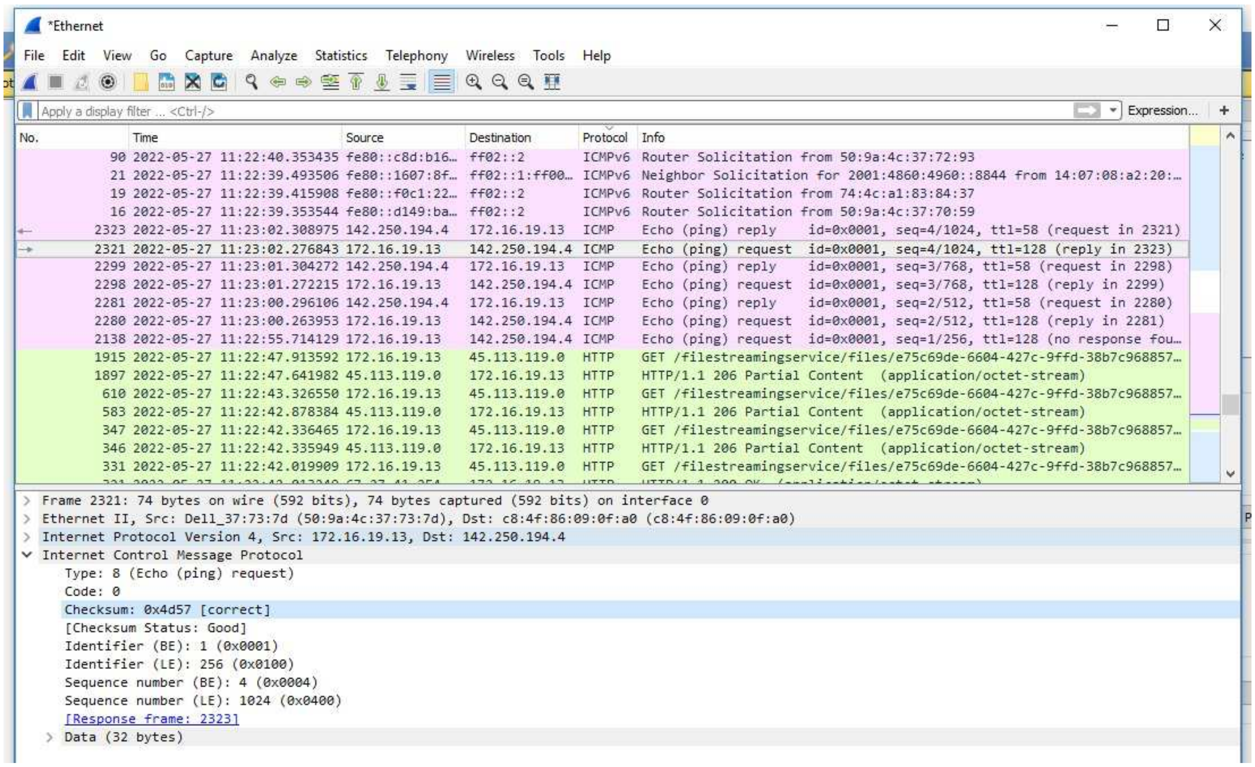
```
  17079 2022-05-27 10:58:50.107170    172.16.19.13          128.119.245.12        HTTP      GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 17079: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface 0
Ethernet II, Src: Dell_37:73:7d (50:9a:4c:37:73:7d), Dst: c8:4f:86:09:0f:a0 (c8:4f:86:09:0f:a0)
Internet Protocol Version 4, Src: 172.16.19.13, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49999, Dst Port: 80, Seq: 1, Ack: 1, Len: 516
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 17560]
    [Next request in frame: 17565]
```

```
  17560 2022-05-27 10:58:50.699416    128.119.245.12        172.16.19.13          HTTP      HTTP/1.1 200 OK  (text/html)
Frame 17560: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
Ethernet II, Src: c8:4f:86:09:0f:a0 (c8:4f:86:09:0f:a0), Dst: Dell_37:73:7d (50:9a:4c:37:73:7d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.19.13
Transmission Control Protocol, Src Port: 80, Dst Port: 49999, Seq: 1, Ack: 517, Len: 476
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 27 May 2022 05:29:04 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 27 May 2022 05:29:01 GMT\r\n
    ETag: "51-5dff7957bfc7a"\r\n
    Accept-Ranges: none\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Content-Length: 81\r\n
    Via: HTTP/1.1 forward.http.proxy:3128\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.592246000 seconds]
    [Request in frame: 17079]
    [Next request in frame: 17565]
    [Next response in frame: 18015]
    File Data: 81 bytes
Line-based text data: text/html
```

Assignment #4

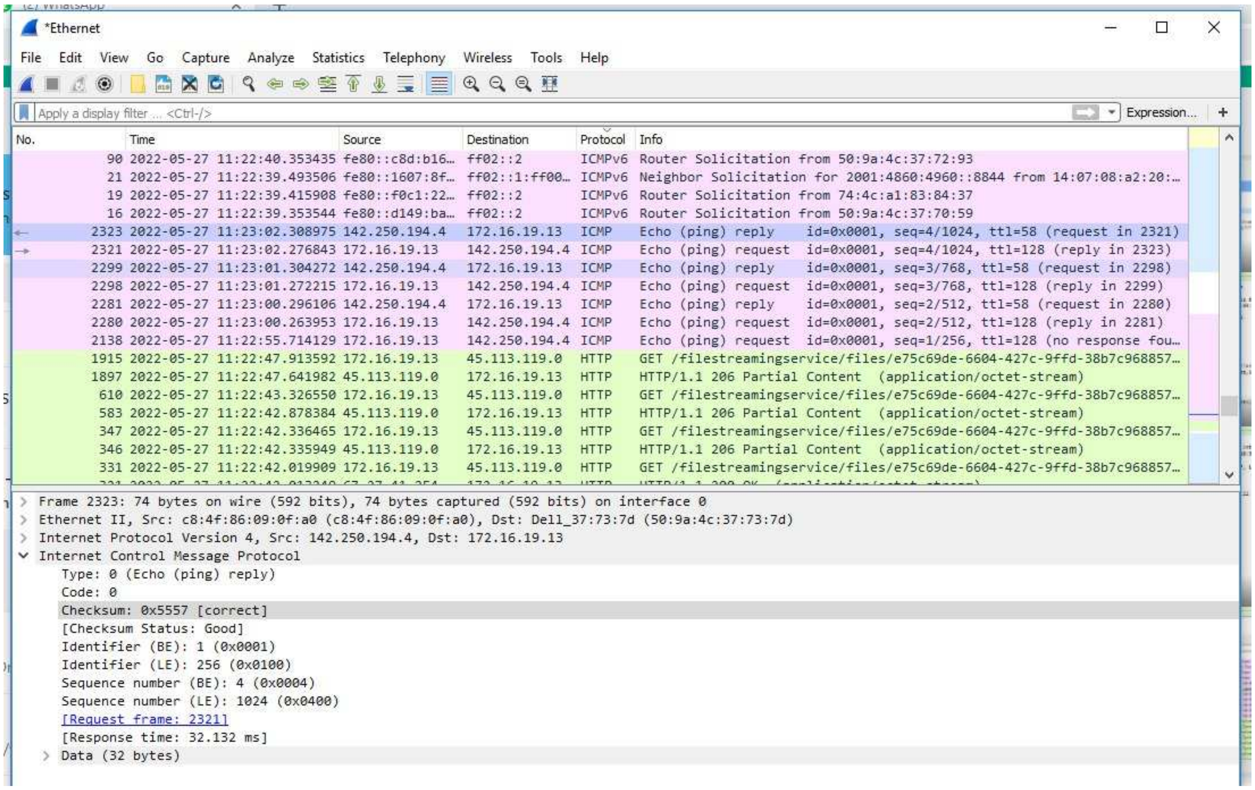
1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Answer: ICMP type is “8 (Echo (ping) request)”, code is 0. Other fields are Checksum, Identifier, Sequence number, Response time and Data.



2. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Answer: ICMP type is “0 (Echo (ping) reply)”, code is 0. Other fields are Checksum, Identifier, Sequence number, Response time and Data.



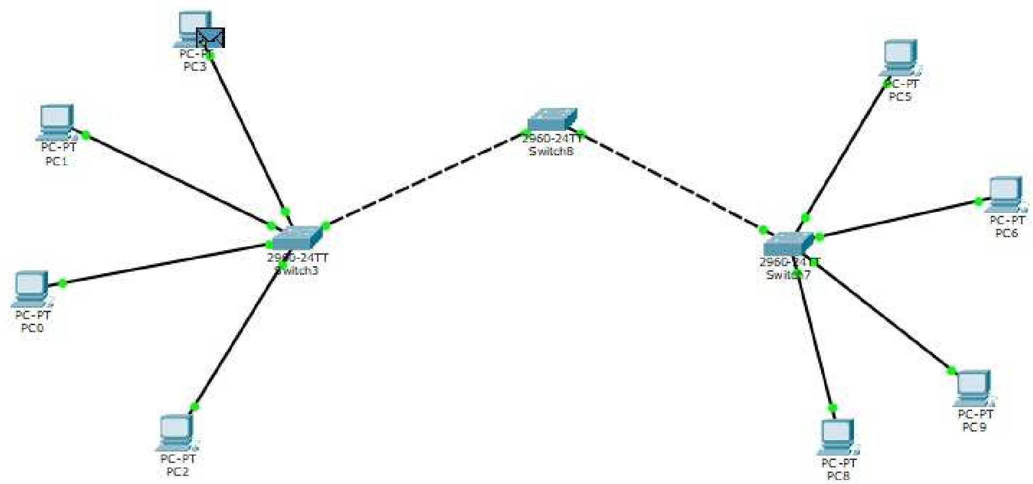
3. What is the IP address of your host? What is the IP address of the target destination host?

Answer: IP address of my machine is 172.16.19.13 and that of destination is 142.250.194.4 (www.google.com)

Assignment #5

Q.1. Cisco Packet Tracer

Use Cisco Packet Tracer to construct two separate star networks comprising four hosts each (Use hubs to create both the star networks). Now use a layer-2 switch to provide connectivity between both the star networks. Simulate the above network using ICMP request/response packets to perform the following:



a) Assign Static IP addresses (manual configuration) to the host devices. Apply ARP and ICMP filters before starting the simulation.
b) Check connectivity using ICMP/PING between any two hosts in the same star network (Do it for both star networks).

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=13ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 13ms, Average = 6ms
```

c) Check connectivity using ICMP/PING between a host of one star network and a host of the other star network.

```
Packet Tracer PC Command Line 1.0
C:\>ping 169.254.134.201

Pinging 169.254.134.201 with 32 bytes of data:

Reply from 169.254.134.201: bytes=32 time<1ms TTL=128
Reply from 169.254.134.201: bytes=32 time<1ms TTL=128
Reply from 169.254.134.201: bytes=32 time<1ms TTL=128
Reply from 169.254.134.201: bytes=32 time=4ms TTL=128

Ping statistics for 169.254.134.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

d) Will there be any change in the nature of communication, if the layer-2 switch is replaced by a simple hub?

Answer: No, there'd be none.

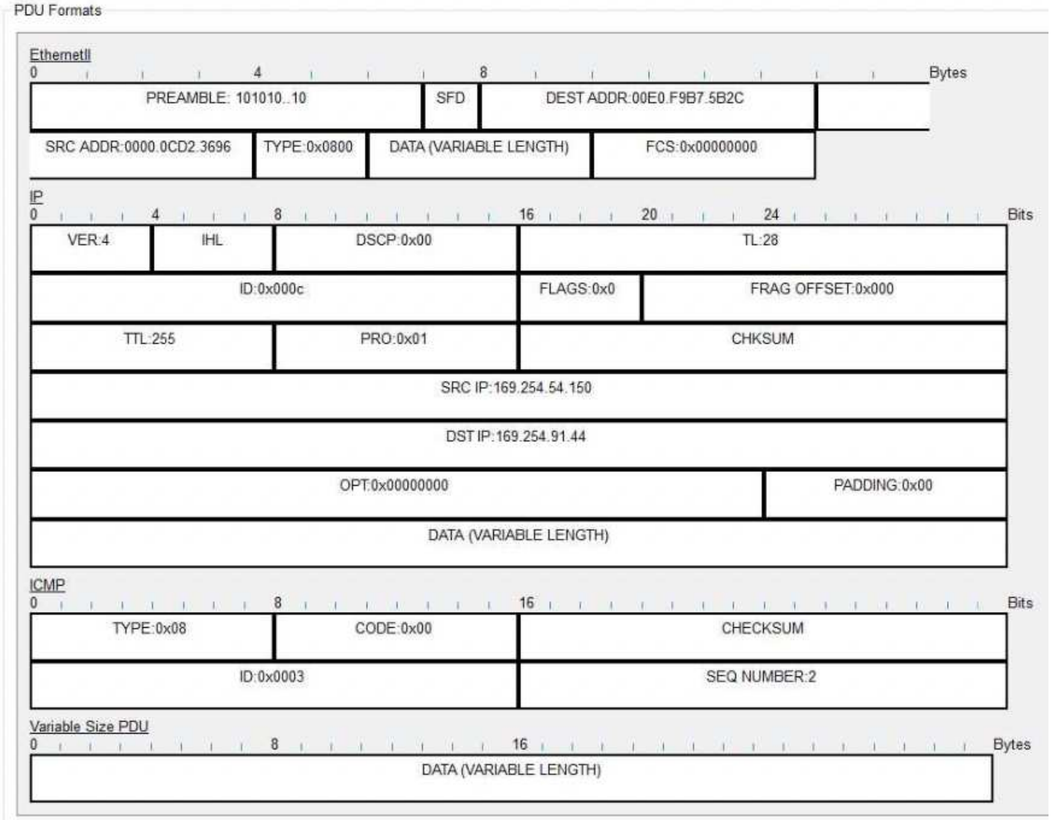
e) Check/Print ARP tables of all communicating hosts before and after sending of the ARP packets.

IP Address	Hardware Address	Interface
169.254.91.44	00E0.F9B7.5B2C	FastEthernet0

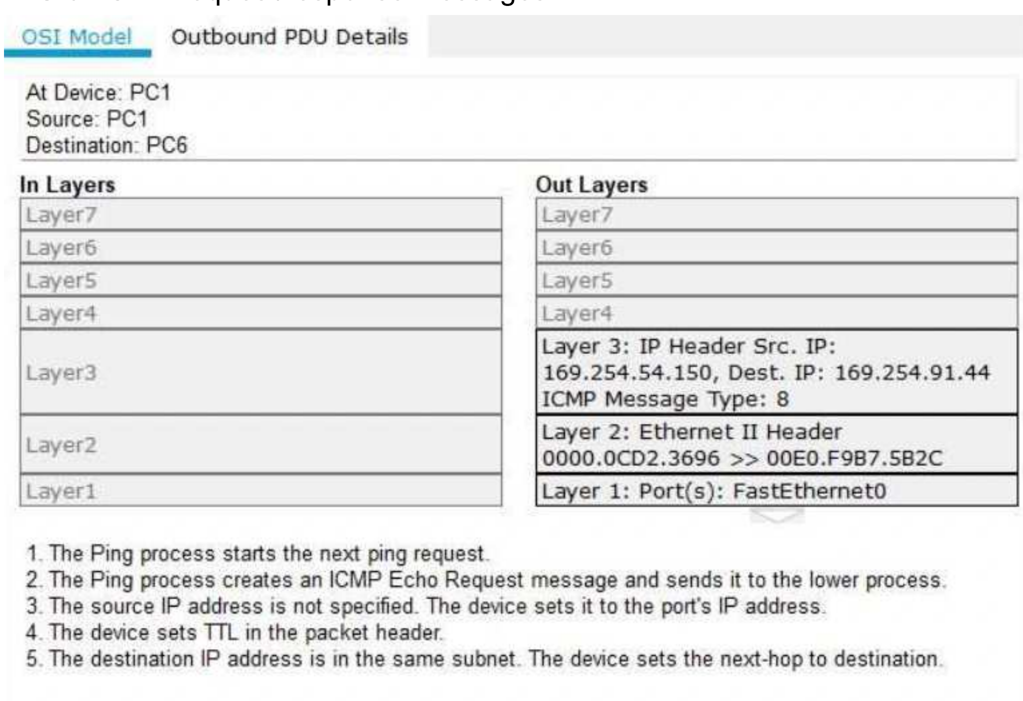
f) Check/Print MAC tables of all the switches before and after sending the ICMP request packet.

VLAN	Mac Address	Port
1	0000.0CD2.3696	FastEthernet0/1
1	0001.426C.86C9	FastEthernet0/1
1	0004.9A75.058B	FastEthernet0/1
1	0060.2F16.EC4B	FastEthernet0/1
1	0090.0C76.E79C	FastEthernet0/2
1	0090.0C7E.5D5C	FastEthernet0/2
1	00D0.FF9A.A153	FastEthernet0/2
1	00E0.F9B7.5B2C	FastEthernet0/2

g) Print Ethernet Header and PDU of ARP request/response messages.

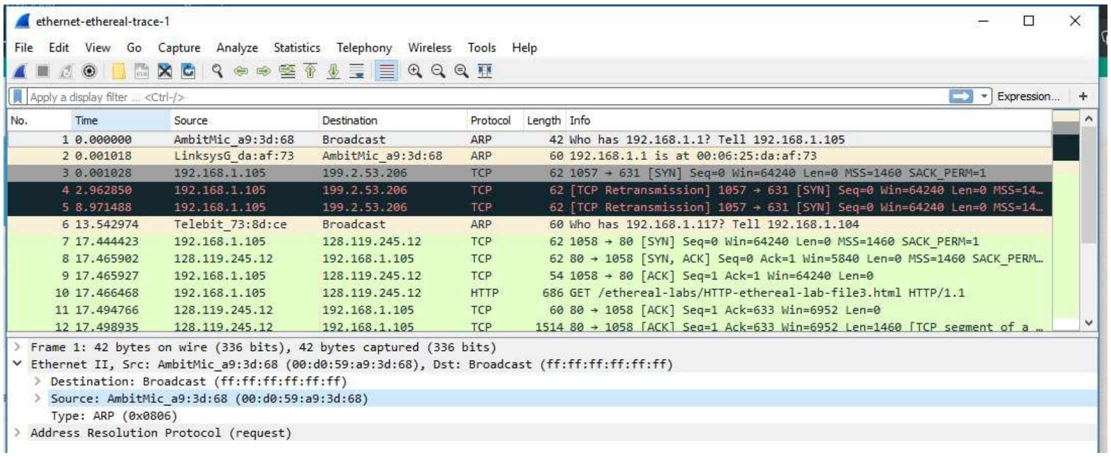


h) Print PDU of ICMP request/response messages.



Q.2. Wireshark

Capturing and analyzing Ethernet frames



1. What is the 48-bit Ethernet address of your computer?
Answer: The ethernet address is 00:d0:59:a9:3d:68

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?
Answer: The destination address is 00:06:25:da:af:73. This is the intermediary device's (router) ethernet address.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
Answer: The value for frame type is 0x800. It corresponds to the Internet Protocol.

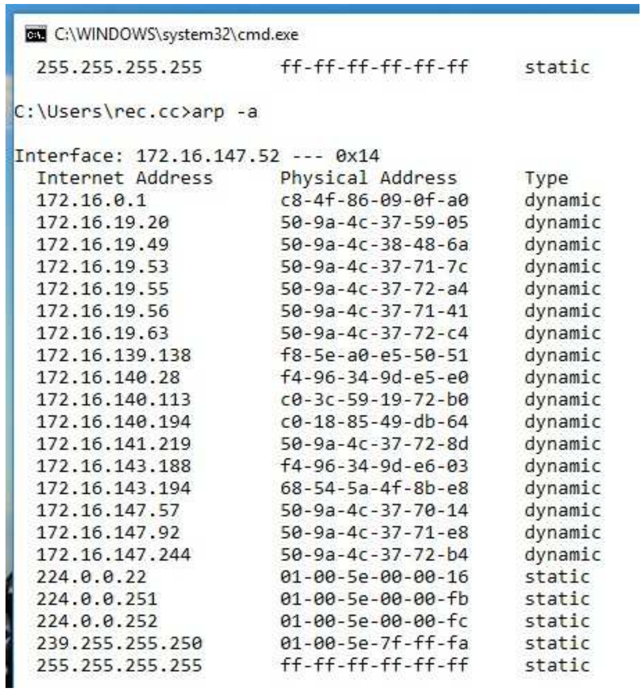
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
Answer: It appears at an offset of 52 bytes from the start.

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
Answer: The source address is 00:06:25:da:af:73 and it's the router's address

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
Answer: The destination address is my machine's address, i.e 00:d0:59:a9:3d:68

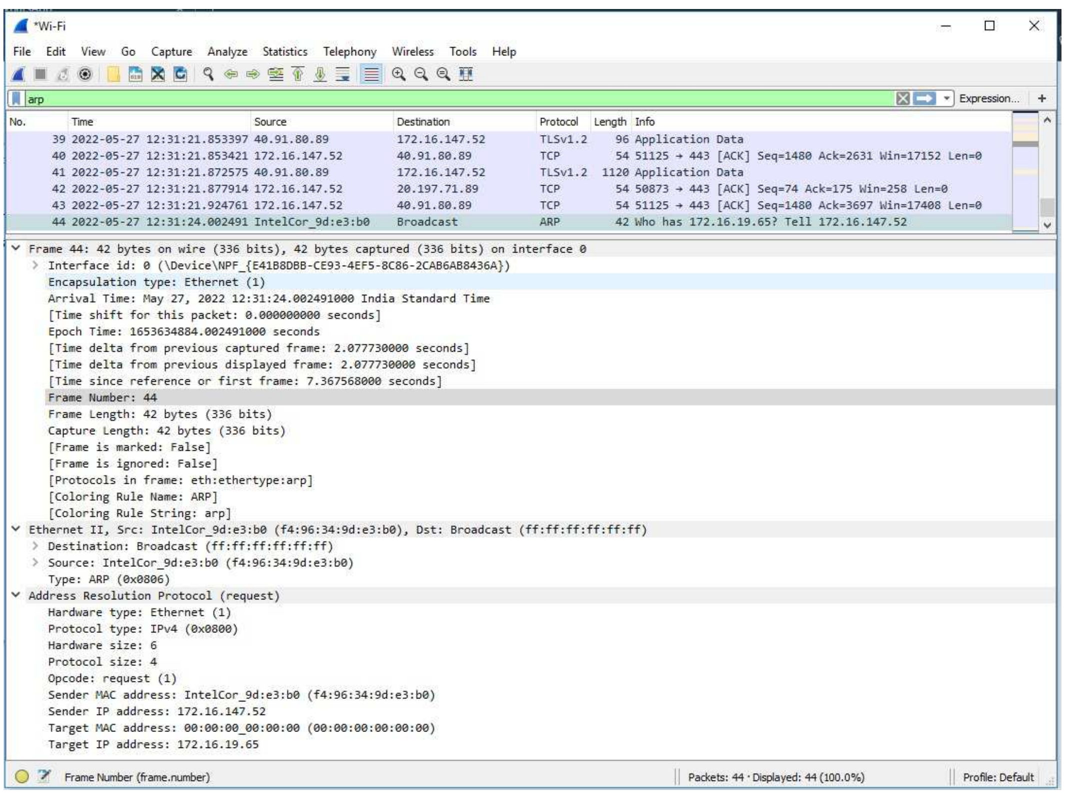
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appears in the Ethernet frame?
Answer: It appears at an offset of 52 bytes from the start.

ARP (Address resolution protocol)



C:\WINDOWS\system32\cmd.exe

```
 255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\rec.cc>arp -a

Interface: 172.16.147.52 --- 0x14
  Internet Address      Physical Address      Type
  172.16.0.1            c8-4f-86-09-0f-a0     dynamic
  172.16.19.20          50-9a-4c-37-59-05     dynamic
  172.16.19.49          50-9a-4c-38-48-6a     dynamic
  172.16.19.53          50-9a-4c-37-71-7c     dynamic
  172.16.19.55          50-9a-4c-37-72-a4     dynamic
  172.16.19.56          50-9a-4c-37-71-41     dynamic
  172.16.19.63          50-9a-4c-37-72-c4     dynamic
  172.16.139.138        f8-5e-a0-e5-50-51     dynamic
  172.16.140.28         f4-96-34-9d-e5-e0     dynamic
  172.16.140.113        c0-3c-59-19-72-b0     dynamic
  172.16.140.194        c0-18-85-49-db-64     dynamic
  172.16.141.219        50-9a-4c-37-72-8d     dynamic
  172.16.143.188        f4-96-34-9d-e6-03     dynamic
  172.16.143.194        68-54-5a-4f-8b-e8     dynamic
  172.16.147.57         50-9a-4c-37-70-14     dynamic
  172.16.147.92         50-9a-4c-37-71-e8     dynamic
  172.16.147.244        50-9a-4c-37-72-b4     dynamic
  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
```



No.	Time	Source	Destination	Protocol	Length	Info
39	2022-05-27 12:31:21.853397	40.91.80.89	172.16.147.52	TLSv1.2	96	Application Data
40	2022-05-27 12:31:21.853421	172.16.147.52	40.91.80.89	TCP	54	51125 → 443 [ACK] Seq=1480 Ack=2631 Win=17152 Len=0
41	2022-05-27 12:31:21.872575	40.91.80.89	172.16.147.52	TLSv1.2	1120	Application Data
42	2022-05-27 12:31:21.877914	172.16.147.52	20.197.71.89	TCP	54	50873 → 443 [ACK] Seq=74 Ack=175 Win=258 Len=0
43	2022-05-27 12:31:21.924761	172.16.147.52	40.91.80.89	TCP	54	51125 → 443 [ACK] Seq=1480 Ack=3697 Win=17408 Len=0
44	2022-05-27 12:31:24.002491	IntelCor_9d:e3:b0	Broadcast	ARP	42	Who has 172.16.19.65? Tell 172.16.147.52

```
Frame 44: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  Interface id: 0 (\Device\NPF_{E41B8DBB-CE93-4EF5-8C86-2CAB6AB8436A})
  Encapsulation type: Ethernet (1)
  Arrival Time: May 27, 2022 12:31:24.002491000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1653634884.002491000 seconds
  [Time delta from previous captured frame: 2.077730000 seconds]
  [Time delta from previous displayed frame: 2.077730000 seconds]
  [Time since reference or first frame: 7.367568000 seconds]
  Frame Number: 44
  Frame Length: 42 bytes (336 bits)
  Capture Length: 42 bytes (336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
Ethernet II, Src: IntelCor_9d:e3:b0 (f4:96:34:9d:e3:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: IntelCor_9d:e3:b0 (f4:96:34:9d:e3:b0)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: IntelCor_9d:e3:b0 (f4:96:34:9d:e3:b0)
  Sender IP address: 172.16.147.52
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.16.19.65
```

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?
Answer: The first column is the IP address, second is the MAC/physical address and the last is the type.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
Answer: The source is fa:96:34:9d:e3:b0 and the destination is ff:ff:ff:ff:ff:ff

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
Answer: The value for Ethernet frame type is 0x806

12. A readable, detailed discussion of ARP is available at
http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
Answer: It begins at 20 bytes from the start

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
Answer: The value of the opcode field is "request (1)"

c) Does the ARP message contain the IP address of the sender?
Answer: Yes, it does and it is 172.16.147.52

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
Answer: The owner of the IP 172.16.19.65 is being queried

13. Now find the ARP reply that was sent in response to the ARP request.
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
Answer: It begins at 20 bytes from the start

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is
made?
Answer: The value for Opcode is 0x0002

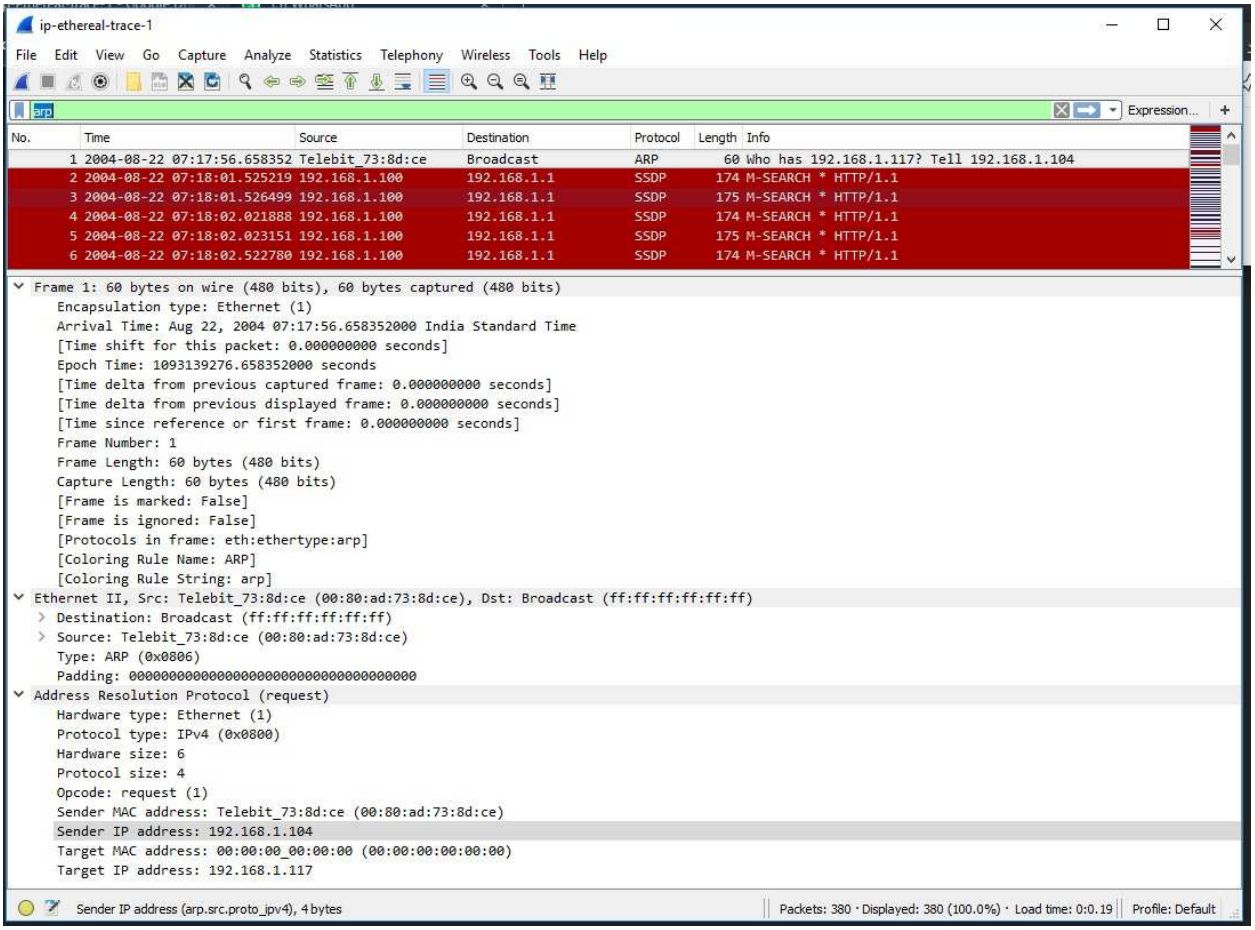
c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
Answer: The answer appears in the Sender's MAC Address field.

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
Answer: The source is fa:96:34:9d:e3:b0 and the destination is 00:00:00:00:00:00

15. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
Answer: There’s no reply available.

Assignment #6

1. A look at the trace



1. What is the IP address of your computer?
Answer: It is 192.168.1.04

2. Within the IP packet header, what is the value in the upper layer protocol field?
Answer: Within the header, the value in the upper layer protocol field is ICMP (0x01).

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
Answer: There are 20 bytes in the IP header, and 56 bytes total length, this gives 36 bytes in the payload of the IP datagram.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
Answer: The more fragments bit = 0, so the data is not fragmented.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
Answer: Identification, Time to live and Header checksum always change.

6. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
Answer:
The fields that stay constant across the IP datagrams are:
- Version (since we are using IPv4 for all packets)
- header length (since these are ICMP packets)
- source IP (since we are sending from the same source)
- destination IP (since we are sending to the same dest)
- Differentiated Services (since all packets are ICMP they use the same Type of Service class)
- Upper Layer Protocol (since these are ICMP packets)

The fields that must stay constant are:
- Version (since we are using IPv4 for all packets) • header length (since these are ICMP packets)
- source IP (since we are sending from the same source) • destination IP (since we are sending to the same dest)
- Differentiated Services (since all packets are ICMP they use the same Type of Service class)
- Upper Layer Protocol (since these are ICMP packets)

The fields that must change are:
- Identification(IP packets must have different ids)
- Time to live (traceroute increments each subsequent packet)
- Header checksum (since header changes, so must checksum)

7. Describe the pattern you see in the values in the Identification field of the IP datagram.
Answer: The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request. Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

8.What is the value in the Identification field and the TTL field?
Answer: The nearest hop is 192.168.1.102.

Fragmentation

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?
Answer: Yes, it has.

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?
Answer: The Flags bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header.

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?
Answer: We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.

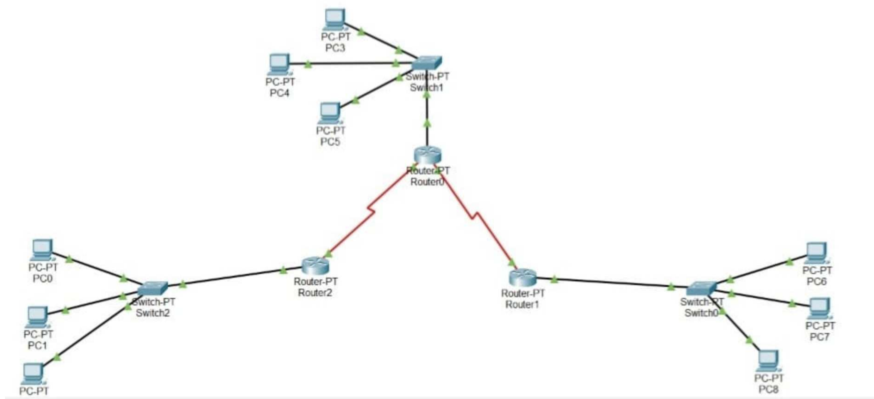
13. What fields change in the IP header between the first and second fragment?
Answer: The IP header fields that changed between the fragments are: total length, flags, fragment offset, and checksum. Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

14. How many fragments were created from the original datagram?
Answer: After switching to 3500, there are 3 packets created from the original datagram.

16. What fields change in the IP header among the fragments?
Answer: The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0.

Assignment #7

1. **Design and document an addressing scheme based on requirements.**



Subnet 1:
Subnet Address = 192.168.1.0/25
Broadcast Address = 192.168.1.127/25
Host ID = 192.168.1.1/25 – 192.168.1.126/25
Subnet 2:
Subnet Address = 192.168.1.128/26
Broadcast Address = 192.168.1.191/26
Host ID = 192.168.1.129/26 – 192.168.1.190/26
Subnet 3:
Subnet Address = 192.168.1.192/27
Broadcast Address = 192.168.1.223/27
Host ID = 192.168.1.193/27 – 192.168.1.222/27

2. **Test End to End Connectivity**

Router (host 80) :

```
     192.168.1.0/24 is variably subnetted, 4 subnets, 4 masks
C       192.168.1.0/25 is directly connected, FastEthernet0/0
S       192.168.1.128/26 [1/0] via 192.168.1.226
S       192.168.1.192/27 [1/0] via 192.168.1.226
C       192.168.1.224/30 is directly connected, Serial2/0
Router>
```

Router (host 40) :

```
     192.168.1.0/24 is variably subnetted, 4 subnets, 4 masks
S       192.168.1.0/25 [1/0] via 192.168.1.229
C       192.168.1.128/26 is directly connected, FastEthernet0/0
S       192.168.1.192/27 [1/0] via 192.168.1.229
C       192.168.1.228/30 is directly connected, Serial2/0
Router>
```

Router(host 20):

```
     192.168.1.0/24 is variably subnetted, 5 subnets, 4 masks
S       192.168.1.0/25 [1/0] via 192.168.1.225
S       192.168.1.128/26 [1/0] via 192.168.1.230
C       192.168.1.192/27 is directly connected, FastEthernet0/0
C       192.168.1.224/30 is directly connected, Serial2/0
C       192.168.1.228/30 is directly connected, Serial3/0
Router>
```