

# IP LAB ASSIGNMENT

The topology configured among the four PC's is :

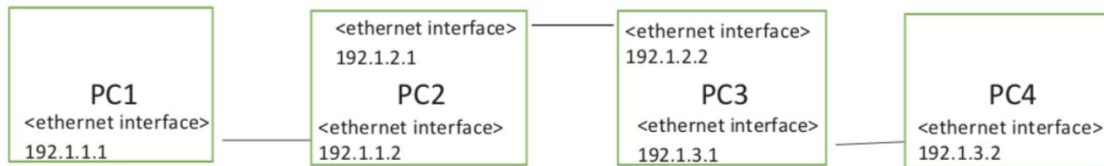


Figure 1: Network topology

1. Assign proper IP addresses to the interfaces of the PCs in the topology of Figure1.

The IP addresses are assigned as per figure1

For PC1:

```
root@PC1:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
14: eth2@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b6:90:4d:73:68:75 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 192.1.1.1/24 scope global eth2
        valid_lft forever preferred_lft forever
root@PC1:~#
```

For PC2:

```
root@PC2:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.3/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
13: eth1@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 1a:24:e8:71:92:b5 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 192.1.1.2/24 scope global eth1
        valid_lft forever preferred_lft forever
16: eth3@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 22:0b:98:b4:af:c7 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 192.1.2.1/24 scope global eth3
        valid_lft forever preferred_lft forever
root@PC2:~#
```

For PC3:

```
root@PC3:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.4/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
15: eth2@if16: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether ce:bc:ff:27:4a:d6 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 192.1.2.2/24 scope global eth2
        valid_lft forever preferred_lft forever
18: eth4@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether e6:8f:1f:92:19:06 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 192.1.3.1/24 scope global eth4
        valid_lft forever preferred_lft forever
root@PC3:~#
```

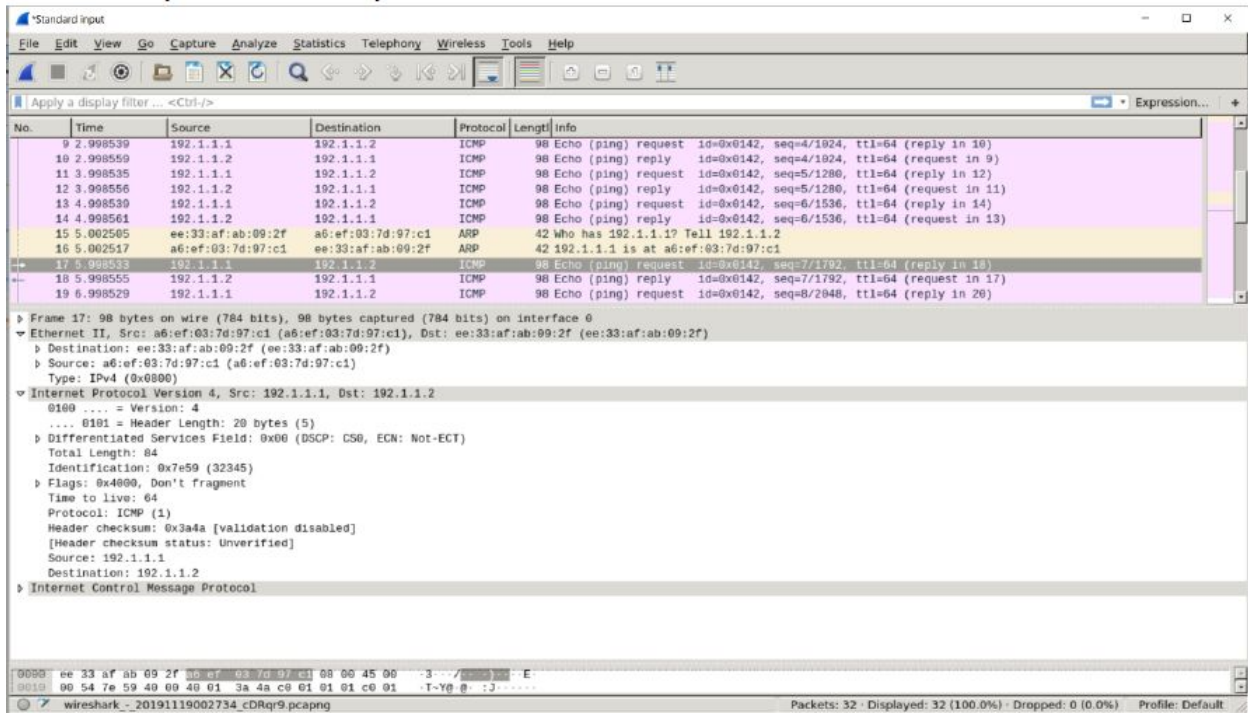
For PC4:

```
root@PC4:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
11: eth0@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.5/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
17: eth3@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 6a:a9:ca:ad:a8:8a brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 192.1.3.2/24 scope global eth3
        valid_lft forever preferred_lft forever
root@PC4:~#
```

2. Run Wireshark on each PC and make sure that it works properly; if there is a problem you may consult the setup document.

Ans: Wireshark is working properly on all the PC's.

## Wireshark capture of ICMP request on eth1 of PC2

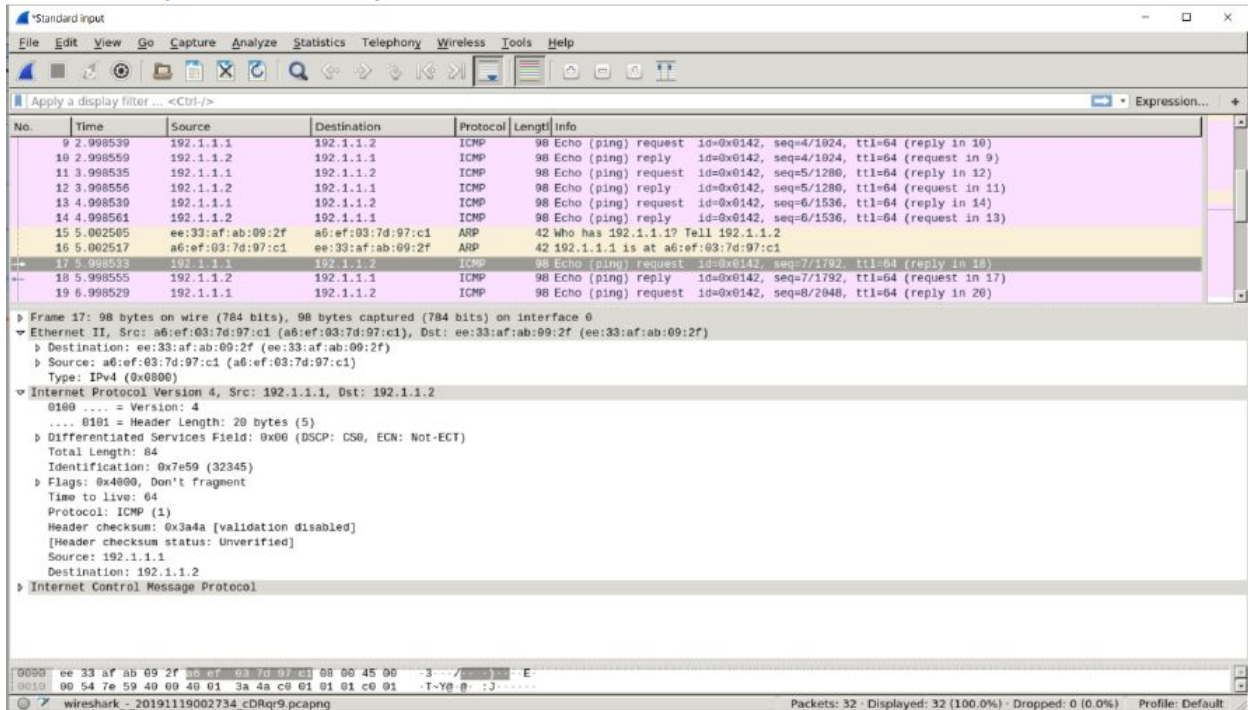


The screenshot shows a Wireshark capture on interface eth1. The packet list displays several ICMP Echo (ping) requests and replies between 192.1.1.1 and 192.1.1.2. Packet 17 is selected, showing an ICMP Echo (ping) request from 192.1.1.1 to 192.1.1.2. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) header. The ICMP header indicates a request with sequence number 4 and TTL 64. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=4/1024, ttl=64 (reply in 10)
10	2.998559	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=4/1024, ttl=64 (request in 9)
11	3.998535	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=5/1280, ttl=64 (reply in 12)
12	3.998556	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=5/1280, ttl=64 (request in 11)
13	4.998530	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=6/1536, ttl=64 (reply in 14)
14	4.998561	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=6/1536, ttl=64 (request in 13)
15	5.002505	ee:33:af:ab:09:2f	a6:ef:03:7d:97:c1	ARP	42	Who has 192.1.1.1? Tell 192.1.1.2
16	5.002517	a6:ef:03:7d:97:c1	ee:33:af:ab:09:2f	ARP	42	192.1.1.1 is at a6:ef:03:7d:97:c1
17	5.998533	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=7/1792, ttl=64 (reply in 18)
18	5.998555	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=7/1792, ttl=64 (request in 17)
19	6.998529	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=8/2048, ttl=64 (reply in 20)

Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1), Dst: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Destination: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Source: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.1.2  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x7e59 (32345)  
Flags: 0x4000, Don't Fragment  
Time to live: 64  
Protocol: ICMP (1)  
Header checksum: 0x3a4a [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.1.1.1  
Destination: 192.1.1.2  
Internet Control Message Protocol

## Wireshark capture of ARP packet on eth3 of PC2



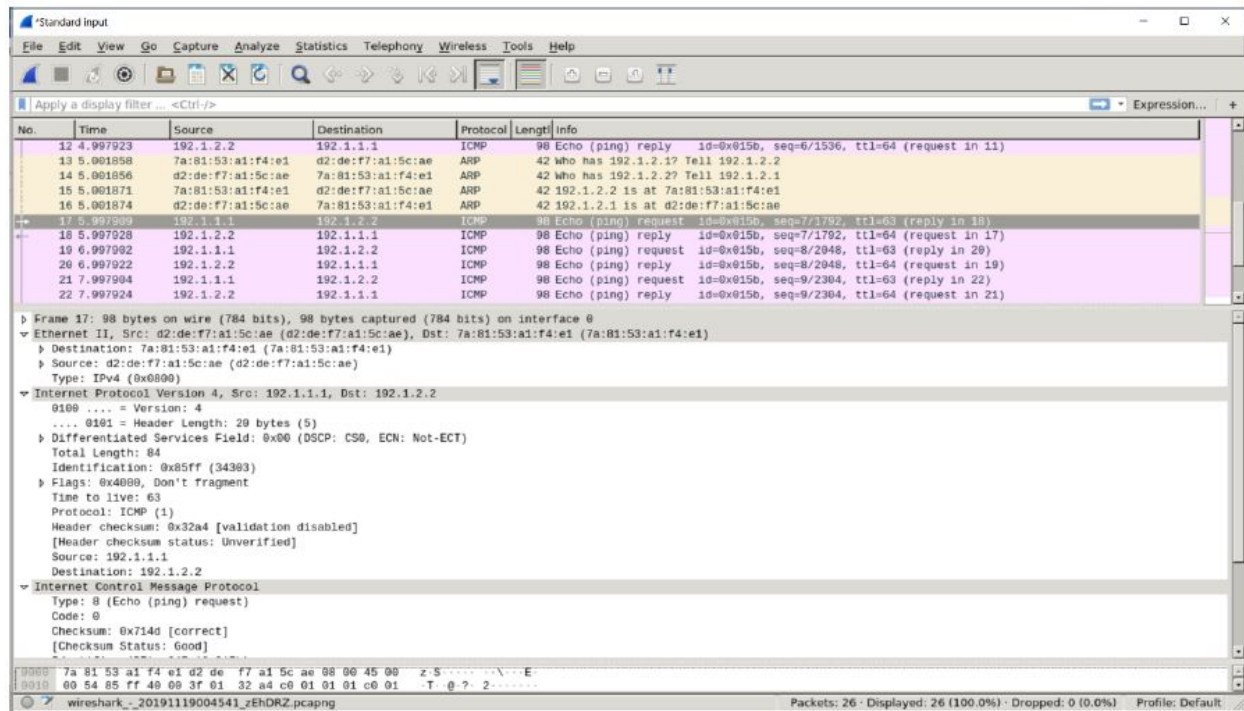
The screenshot shows a Wireshark capture on interface eth3. The packet list displays several ICMP Echo (ping) requests and replies between 192.1.1.1 and 192.1.1.2. Packet 17 is selected, showing an ARP request from 192.1.1.1 to 192.1.1.2. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) header. The ICMP header indicates a request with sequence number 4 and TTL 64. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=4/1024, ttl=64 (reply in 10)
10	2.998559	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=4/1024, ttl=64 (request in 9)
11	3.998535	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=5/1280, ttl=64 (reply in 12)
12	3.998556	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=5/1280, ttl=64 (request in 11)
13	4.998530	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=6/1536, ttl=64 (reply in 14)
14	4.998561	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=6/1536, ttl=64 (request in 13)
15	5.002505	ee:33:af:ab:09:2f	a6:ef:03:7d:97:c1	ARP	42	Who has 192.1.1.1? Tell 192.1.1.2
16	5.002517	a6:ef:03:7d:97:c1	ee:33:af:ab:09:2f	ARP	42	192.1.1.1 is at a6:ef:03:7d:97:c1
17	5.998533	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=7/1792, ttl=64 (reply in 18)
18	5.998555	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=7/1792, ttl=64 (request in 17)
19	6.998529	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=8/2048, ttl=64 (reply in 20)

Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1), Dst: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Destination: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Source: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.1.2  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x7e59 (32345)  
Flags: 0x4000, Don't Fragment  
Time to live: 64  
Protocol: ICMP (1)  
Header checksum: 0x3a4a [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.1.1.1  
Destination: 192.1.1.2  
Internet Control Message Protocol



## Wireshark capture of ICMP request packet on eth2 of PC3



The screenshot shows a Wireshark capture of network traffic on interface eth2. The packet list displays several ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) request from 192.1.1.1 to 192.1.2.2.

No.	Time	Source	Destination	Protocol	Length	Info
12	4.997923	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=6/1536, ttl=64 (request in 11)
13	5.001958	7a:81:53:a1:f4:e1	d2:de:f7:a1:5c:ae	ARP	42	Who has 192.1.2.1? Tell 192.1.2.2
14	5.001956	d2:de:f7:a1:5c:ae	7a:81:53:a1:f4:e1	ARP	42	Who has 192.1.2.2? Tell 192.1.2.1
15	5.001871	7a:81:53:a1:f4:e1	d2:de:f7:a1:5c:ae	ARP	42	192.1.2.2 is at 7a:81:53:a1:f4:e1
16	5.001874	d2:de:f7:a1:5c:ae	7a:81:53:a1:f4:e1	ARP	42	192.1.2.1 is at d2:de:f7:a1:5c:ae
17	5.997989	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=7/1792, ttl=63 (reply in 18)
18	5.997928	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=7/1792, ttl=64 (request in 17)
19	6.997992	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=8/2048, ttl=63 (reply in 20)
20	6.997922	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=8/2048, ttl=64 (request in 19)
21	7.997904	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=9/2304, ttl=63 (reply in 22)
22	7.997924	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=9/2304, ttl=64 (request in 21)

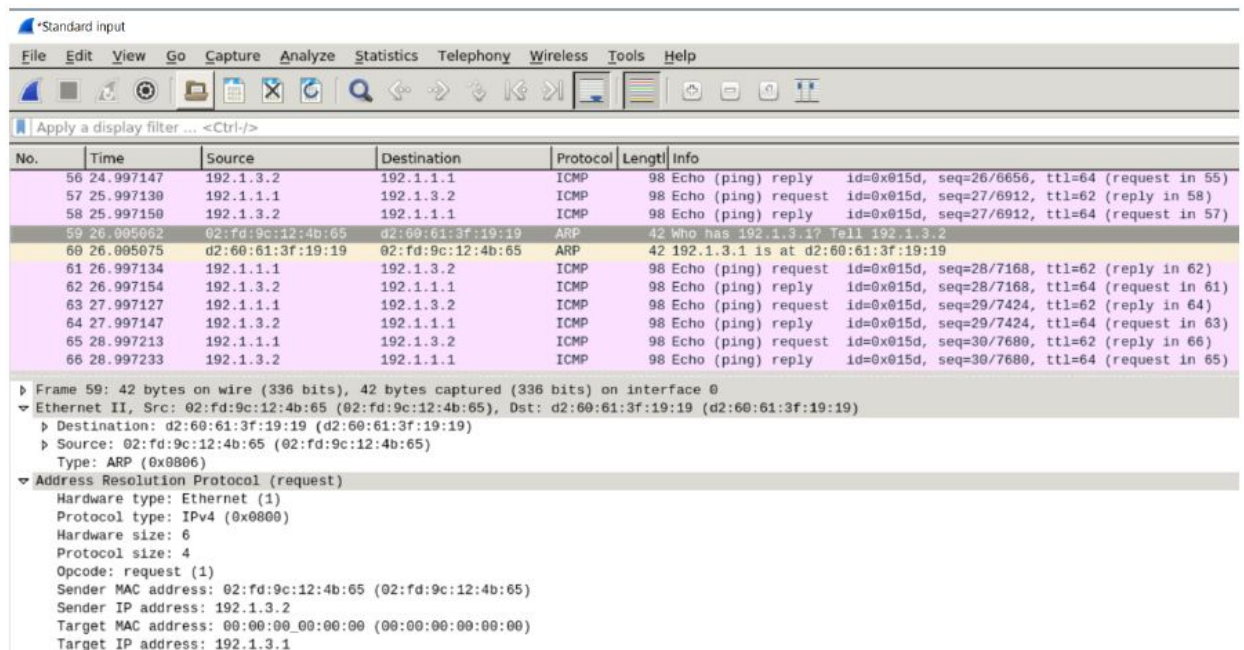
**Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0**

- Ethernet II, Src: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae), Dst: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)
  - Destination: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)
  - Source: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.2.2
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 84
  - Identification: 0x85ff (34383)
  - Flags: 0x4000, Don't fragment
  - Time to live: 63
  - Protocol: ICMP (1)
  - Header checksum: 0x32a4 [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 192.1.1.1
  - Destination: 192.1.2.2
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x714d [correct]
  - [Checksum Status: Good]

0000 7a 81 53 a1 f4 e1 d2 de f7 a1 5c ae 00 00 45 00 2 5 .....E  
0010 00 54 85 ff 40 09 3f 01 32 ad c0 01 01 01 c0 01 T . 0 2 .....

Wireshark\_20191119004541\_EhDRZ.pcapng Packets: 26 · Displayed: 26 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

## Wireshark capture of ARP packet on eth3 of PC4



The screenshot shows a Wireshark capture of network traffic on interface eth3. The packet list displays several ICMP Echo (ping) requests and replies. The selected packet is an ARP request from 02:fd:9c:12:4b:65 to d2:60:61:3f:19:19.

No.	Time	Source	Destination	Protocol	Length	Info
56	24.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=26/6656, ttl=64 (request in 55)
57	25.997130	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=27/6912, ttl=62 (reply in 58)
58	25.997150	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=27/6912, ttl=64 (request in 57)
59	26.005062	02:fd:9c:12:4b:65	d2:60:61:3f:19:19	ARP	42	Who has 192.1.3.1? Tell 192.1.3.2
60	26.005075	d2:60:61:3f:19:19	02:fd:9c:12:4b:65	ARP	42	192.1.3.1 is at d2:60:61:3f:19:19
61	26.997134	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=28/7168, ttl=62 (reply in 62)
62	26.997154	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=28/7168, ttl=64 (request in 61)
63	27.997127	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=29/7424, ttl=62 (reply in 64)
64	27.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=29/7424, ttl=64 (request in 63)
65	28.997213	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=30/7680, ttl=62 (reply in 66)
66	28.997233	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=30/7680, ttl=64 (request in 65)

**Frame 59: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0**

- Ethernet II, Src: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65), Dst: d2:60:61:3f:19:19 (d2:60:61:3f:19:19)
  - Destination: d2:60:61:3f:19:19 (d2:60:61:3f:19:19)
  - Source: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)
  - 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: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)
  - Sender IP address: 192.1.3.2
  - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  - Target IP address: 192.1.3.1

3. Examine the ARP table of each PC.

Ans:

For PC1:

```
root@PC1:~# arp -a  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC1:~#
```

For PC2:

```
root@PC2:~# arp -a  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC2:~#
```

For PC3:

```
root@PC3:~# arp -a  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC3:~#
```

For PC4;

```
root@PC4:~# arp -a  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC4:~#
```

4. Examine the routing table of each PC.

Ans:

For PC1:

```
root@PC1:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.2
192.1.1.0/24 dev eth2 proto kernel scope link src 192.1.1.1
root@PC1:~#
```

For PC2:

```
root@PC2:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.3
192.1.1.0/24 dev eth1 proto kernel scope link src 192.1.1.2
192.1.2.0/24 dev eth3 proto kernel scope link src 192.1.2.1
root@PC2:~#
```

For PC3:

```
root@PC3:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.4
192.1.2.0/24 dev eth2 proto kernel scope link src 192.1.2.2
192.1.3.0/24 dev eth4 proto kernel scope link src 192.1.3.1
root@PC3:~#
```

For PC4:

```
root@PC4:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.5
192.1.3.0/24 dev eth3 proto kernel scope link src 192.1.3.2
root@PC4:~#
```

5. Ping PC2, PC3 and PC4 from PC1

Ans:

Ping from PC1 to PC2

The Ping was successful.

```
root@PC1:~# ping 192.1.1.2
PING 192.1.1.2 (192.1.1.2) 56(84) bytes of data.
64 bytes from 192.1.1.2: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 192.1.1.2: icmp_seq=2 ttl=64 time=0.054 ms
^C
--- 192.1.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.054/0.090/0.126/0.036 ms
root@PC1:~#
```

Ping from PC1 to PC3

The destination host is unreachable

```
root@PC1:~#
root@PC1:~# ping 192.1.2.2
PING 192.1.2.2 (192.1.2.2) 56(84) bytes of data.
From 128.109.191.97 icmp_seq=2 Destination Net Unreachable
^C
--- 192.1.2.2 ping statistics ---
3 packets transmitted, 0 received, +1 errors, 100% packet loss, time 2008ms
root@PC1:~#
```

Ping from PC1 to PC4:

The ping is not successful

```
root@PC1:~# ping 192.1.3.3
PING 192.1.3.3 (192.1.3.3) 56(84) bytes of data.
^C
--- 192.1.3.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3023ms
root@PC1:~# █
```

6.Examine the ARP table of each PC

Ans:

In PC1

```
root@PC1:~# arp -a
? (192.1.1.2) at 1a:24:e8:71:92:b5 [ether] on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC1:~#
```

In PC2:

```
root@PC2:~# arp -a
? (192.1.1.1) at b6:90:4d:73:68:75 [ether] on eth1
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC2:~#
```

In PC3:

```
root@PC3:~# arp -a
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC3:~#
```

In PC4:

```
root@PC4:~# arp -a
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC4:~#
```



7. Add routes at PC2 and PC3 to allow packets to be forwarded along the path from PC1 to PC4.

Ans:

For PC1:

```
root@PC1:~# ip route add 192.1.3.0/24 via 192.1.1.2 dev eth2
root@PC1:~#
root@PC1:~# ip route add 192.1.2.0/24 via 192.1.1.2 dev eth2
root@PC1:~#
root@PC1:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.2
192.1.1.0/24 dev eth2 proto kernel scope link src 192.1.1.1
192.1.2.0/24 via 192.1.1.2 dev eth2
192.1.3.0/24 via 192.1.1.2 dev eth2
root@PC1:~#
```

For PC2:

```
root@PC2:~#
root@PC2:~# ip route add 192.1.3.0/24 via 192.1.2.2 dev eth3
root@PC2:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.3
192.1.1.0/24 dev eth1 proto kernel scope link src 192.1.1.2
192.1.2.0/24 dev eth3 proto kernel scope link src 192.1.2.1
192.1.3.0/24 via 192.1.2.2 dev eth3
root@PC2:~#
```

For PC3:

```
root@PC3:~#
root@PC3:~# ip route add 192.1.1.0/24 via 192.1.2.1 dev eth2
root@PC3:~#
root@PC3:~# ip route show
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.4
192.1.1.0/24 via 192.1.2.1 dev eth2
192.1.2.0/24 dev eth2 proto kernel scope link src 192.1.2.2
192.1.3.0/24 dev eth4 proto kernel scope link src 192.1.3.1
root@PC3:~#
```

For PC4:

```
root@PC4:~#  
root@PC4:~# ip route add 192.1.2.0/24 via 192.1.3.1 dev eth3  
root@PC4:~# ip route add 192.1.1.0/24 via 192.1.3.1 dev eth3  
root@PC4:~#  
root@PC4:~# ip route show  
default via 172.17.0.1 dev eth0  
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.5  
192.1.1.0/24 via 192.1.3.1 dev eth3  
192.1.2.0/24 via 192.1.3.1 dev eth3  
192.1.3.0/24 dev eth3 proto kernel scope link src 192.1.3.2  
root@PC4:~#
```

8. Make sure forwarding is turned “on” at each PC

Ans:

For PC1:

```
root@PC1:~# cat /proc/sys/net/ipv4/ip_forward  
1  
root@PC1:~#
```

For PC2:

```
root@PC2:~# cat /proc/sys/net/ipv4/ip_forward  
1  
root@PC2:~#
```

For PC3:

```
root@PC3:~# cat /proc/sys/net/ipv4/ip_forward  
1  
root@PC3:~#
```

For PC4:

```
root@PC4:~# cat /proc/sys/net/ipv4/ip_forward  
1  
root@PC4:~#
```

9. Ping PC2, PC3 and PC4 from PC1.

Ans:

When PC2 was pinged from PC1

```
root@PC1:~# ping 192.1.1.2
PING 192.1.1.2 (192.1.1.2) 56(84) bytes of data.
64 bytes from 192.1.1.2: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.1.1.2: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from 192.1.1.2: icmp_seq=3 ttl=64 time=0.059 ms
^C
--- 192.1.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.059/0.444/1.214/0.544 ms
root@PC1:~#
```

When PC3 was pinged from PC1

```
root@PC1:~# ping 192.1.2.2
PING 192.1.2.2 (192.1.2.2) 56(84) bytes of data.
64 bytes from 192.1.2.2: icmp_seq=1 ttl=63 time=0.159 ms
64 bytes from 192.1.2.2: icmp_seq=2 ttl=63 time=0.066 ms
64 bytes from 192.1.2.2: icmp_seq=3 ttl=63 time=0.070 ms
64 bytes from 192.1.2.2: icmp_seq=4 ttl=63 time=0.069 ms
^C
--- 192.1.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.066/0.091/0.159/0.039 ms
root@PC1:~#
```

When PC4 was pinged from PC1:

```
root@PC1:~# ping 192.1.3.2
PING 192.1.3.2 (192.1.3.2) 56(84) bytes of data.
64 bytes from 192.1.3.2: icmp_seq=1 ttl=62 time=2.09 ms
64 bytes from 192.1.3.2: icmp_seq=2 ttl=62 time=0.084 ms
64 bytes from 192.1.3.2: icmp_seq=3 ttl=62 time=0.084 ms
^C
--- 192.1.3.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.084/0.754/2.096/0.948 ms
root@PC1:~#
```

10. Examine the ARP table of each PC.

Ans:

For PC1:

```
root@PC1:~# arp -a
? (192.1.1.2) at 1a:24:e8:71:92:b5 [ether] on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC1:~#
```

For PC2:

```
root@PC2:~# arp -a
? (192.1.1.1) at b6:90:4d:73:68:75 [ether] on eth1
? (192.1.2.2) at ce:bc:ff:27:4a:d6 [ether] on eth3
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC2:~#
```

For PC3:

```
root@PC3:~# arp -a
? (192.1.3.2) at 6a:a9:ca:ad:a8:8a [ether] on eth4
? (192.1.2.1) at 22:0b:98:b4:af:c7 [ether] on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC3:~#
```

For PC4:

```
root@PC4:~# arp -a
? (192.1.3.1) at e6:8f:1f:92:19:06 [ether] on eth3
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC4:~#
```



11. Clear the ARP table on all PCs, run wireshark on each PC, and repeat Steps 3-6.

Ans:

For PC1

```
root@PC1:~# ip -s -s neigh flush all
192.1.1.2 dev eth2 lladdr 1a:24:e8:71:92:b5 used 660/657/641 probes 1 STALE
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 6/0/5 probes 0 REACHABLE

*** Round 1, deleting 2 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 2, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 3, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 4, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 5, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 6, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 7, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 8, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 9, deleting 1 entries ***
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 0/0/0 probes 4 REACHABLE

*** Round 10, deleting 1 entries ***
*** Flush not complete bailing out after 10 rounds
root@PC1:~# arp -a
? (192.1.1.2) at <incomplete> on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC1:~#
```

## For PC2

```
root@PC2:~#  
root@PC2:~# ip -s -s neigh flush all  
192.1.1.1 dev eth1 lladdr b6:90:4d:73:68:75 used 605/602/584 probes 1 STALE  
192.1.2.2 dev eth3 lladdr ce:bc:ff:27:4a:d6 used 605/602/574 probes 1 STALE  
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 13/3/12 probes 0 REACHABLE  
  
*** Round 1, deleting 3 entries ***  
*** Flush is complete after 1 round ***  
root@PC2:~#  
root@PC2:~# arp -a  
? (192.1.1.1) at <incomplete> on eth1  
? (192.1.2.2) at <incomplete> on eth3  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC2:~#
```

## For PC3

```
root@PC3:~# ip -s -s neigh flush all  
192.1.3.2 dev eth4 lladdr 6a:a9:ca:ad:a8:8a used 543/543/525 probes 4 STALE  
192.1.2.1 dev eth2 lladdr 22:0b:98:b4:af:c7 used 541/538/502 probes 1 STALE  
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 16/1/12 probes 1 REACHABLE  
  
*** Round 1, deleting 3 entries ***  
*** Flush is complete after 1 round ***  
root@PC3:~#  
root@PC3:~# arp -s  
-: Unknown host  
root@PC3:~# arp -a  
? (192.1.3.2) at <incomplete> on eth4  
? (192.1.2.1) at <incomplete> on eth2  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC3:~#
```

## For PC4

```
root@PC4:~#  
root@PC4:~# ip -s -s neigh flush all  
192.1.3.1 dev eth3 lladdr e6:8f:1f:92:19:06 used 463/460/428 probes 1 STALE  
172.17.0.1 dev eth0 lladdr 02:42:1e:0f:92:39 ref 1 used 7/1/7 probes 1 REACHABLE  
  
*** Round 1, deleting 2 entries ***  
*** Flush is complete after 1 round ***  
root@PC4:~# arp -a  
? (192.1.3.1) at <incomplete> on eth3  
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0  
root@PC4:~#
```

## Wireshark Capture of ARP packet at eth1 of PC2

The screenshot shows a Wireshark capture of network traffic on interface eth1 of PC2. The packet list shows a series of ICMP Echo (ping) requests and replies between 192.1.1.1 and 192.1.1.2. Packet 15 is an ARP request from 192.1.1.2 to 192.1.1.1. Packet 16 is the corresponding ARP reply from 192.1.1.1 to 192.1.1.2. The packet details pane for packet 16 shows the Ethernet II header, the ARP protocol type, and the specific MAC and IP addresses involved in the request and reply.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=4/1024, ttl=64 (reply in 10)
10	2.998559	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=4/1024, ttl=64 (request in 9)
11	3.998535	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=5/1280, ttl=64 (reply in 12)
12	3.998556	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=5/1280, ttl=64 (request in 11)
13	4.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=6/1536, ttl=64 (reply in 14)
14	4.998561	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=6/1536, ttl=64 (request in 13)
15	5.002505	ee:33:af:ab:09:2f	a6:ef:03:7d:97:c1	ARP	42	Who has 192.1.1.1? Tell 192.1.1.2
16	5.002517	a6:ef:03:7d:97:c1	ee:33:af:ab:09:2f	ARP	42	192.1.1.1 is at a6:ef:03:7d:97:c1
17	5.998533	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=7/1792, ttl=64 (reply in 18)
18	5.998555	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=7/1792, ttl=64 (request in 17)
19	6.998529	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=8/2048, ttl=64 (reply in 20)

Frame 16: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1), Dst: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Destination: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Source: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1)  
Type: ARP (0x0806)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1)  
Sender IP address: 192.1.1.1  
Target MAC address: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Target IP address: 192.1.1.2

## Wireshark capture of ICMP request on eth1 of PC2

The screenshot shows a Wireshark capture of network traffic on interface eth1 of PC2. The packet list shows a series of ICMP Echo (ping) requests and replies between 192.1.1.1 and 192.1.1.2. Packet 17 is an ICMP Echo (ping) request from 192.1.1.1 to 192.1.1.2. The packet details pane for packet 17 shows the Ethernet II header, the IPv4 header, and the ICMP Echo (ping) request details, including the sequence number and TTL.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=4/1024, ttl=64 (reply in 10)
10	2.998559	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=4/1024, ttl=64 (request in 9)
11	3.998535	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=5/1280, ttl=64 (reply in 12)
12	3.998556	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=5/1280, ttl=64 (request in 11)
13	4.998539	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=6/1536, ttl=64 (reply in 14)
14	4.998561	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=6/1536, ttl=64 (request in 13)
15	5.002505	ee:33:af:ab:09:2f	a6:ef:03:7d:97:c1	ARP	42	Who has 192.1.1.1? Tell 192.1.1.2
16	5.002517	a6:ef:03:7d:97:c1	ee:33:af:ab:09:2f	ARP	42	192.1.1.1 is at a6:ef:03:7d:97:c1
17	5.998533	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=7/1792, ttl=64 (reply in 18)
18	5.998555	192.1.1.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0142, seq=7/1792, ttl=64 (request in 17)
19	6.998529	192.1.1.1	192.1.1.2	ICMP	98	Echo (ping) request id=0x0142, seq=8/2048, ttl=64 (reply in 20)

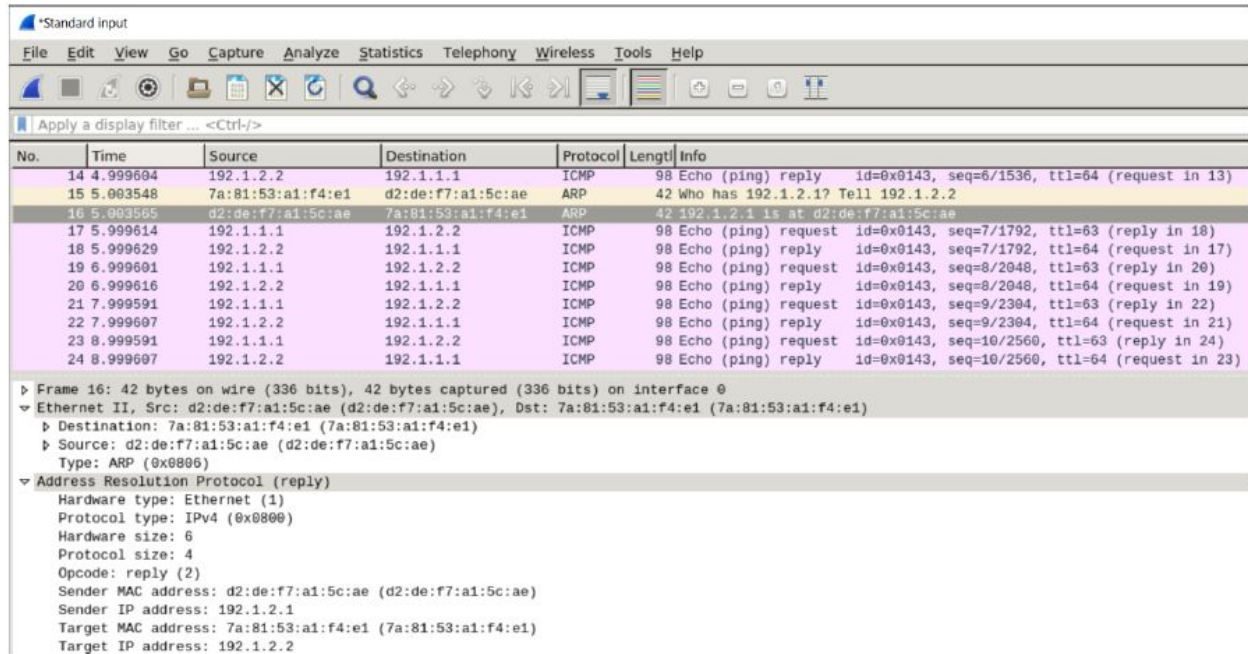
Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1), Dst: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Destination: ee:33:af:ab:09:2f (ee:33:af:ab:09:2f)  
Source: a6:ef:03:7d:97:c1 (a6:ef:03:7d:97:c1)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.1.2  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x7e59 (32345)  
Flags: 0x4000, Don't fragment  
Time to live: 64  
Protocol: ICMP (1)  
Header checksum: 0x3a4a [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.1.1.1  
Destination: 192.1.1.2  
Internet Control Message Protocol



When PC3 is pinged from PC1

```
root@PC1:~#
root@PC1:~# ping 192.1.2.2
PING 192.1.2.2 (192.1.2.2) 56(84) bytes of data.
64 bytes from 192.1.2.2: icmp_seq=1 ttl=63 time=0.231 ms
64 bytes from 192.1.2.2: icmp_seq=2 ttl=63 time=0.072 ms
64 bytes from 192.1.2.2: icmp_seq=3 ttl=63 time=0.068 ms
64 bytes from 192.1.2.2: icmp_seq=4 ttl=63 time=0.080 ms
^C
--- 192.1.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.068/0.112/0.231/0.069 ms
root@PC1:~#
```

Wireshark capture of ARP packet on eth3 of PC2

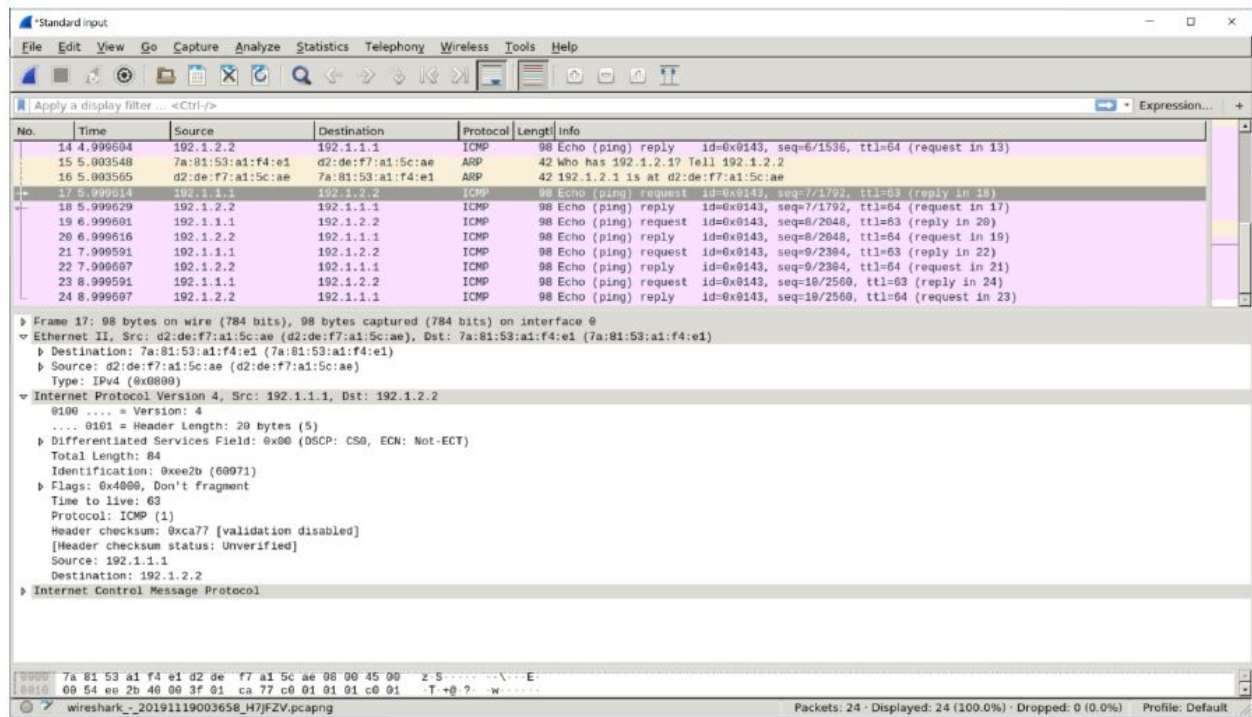


The image shows a Wireshark packet capture on interface eth3. The packet list shows several ICMP Echo (ping) requests and replies between 192.1.1.1 and 192.1.2.2. Packet 16 is an ARP request from 192.1.1.1 to 192.1.2.2. Packet 17 is an ARP reply from 192.1.2.2 to 192.1.1.1. The packet details pane for packet 17 shows the following information:

- Frame 16: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae), Dst: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)
  - Destination: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)
  - Source: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)
  - Type: ARP (0x0806)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)
  - Sender IP address: 192.1.2.1
  - Target MAC address: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)
  - Target IP address: 192.1.2.2



## Wireshark capture of ICMP request packet on eth3 of PC2



The screenshot shows a Wireshark capture of network traffic on interface eth3. The packet list displays several ICMP Echo (ping) requests and replies. The selected packet (No. 17) is an ICMP Echo (ping) request from 192.1.1.1 to 192.1.2.2. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

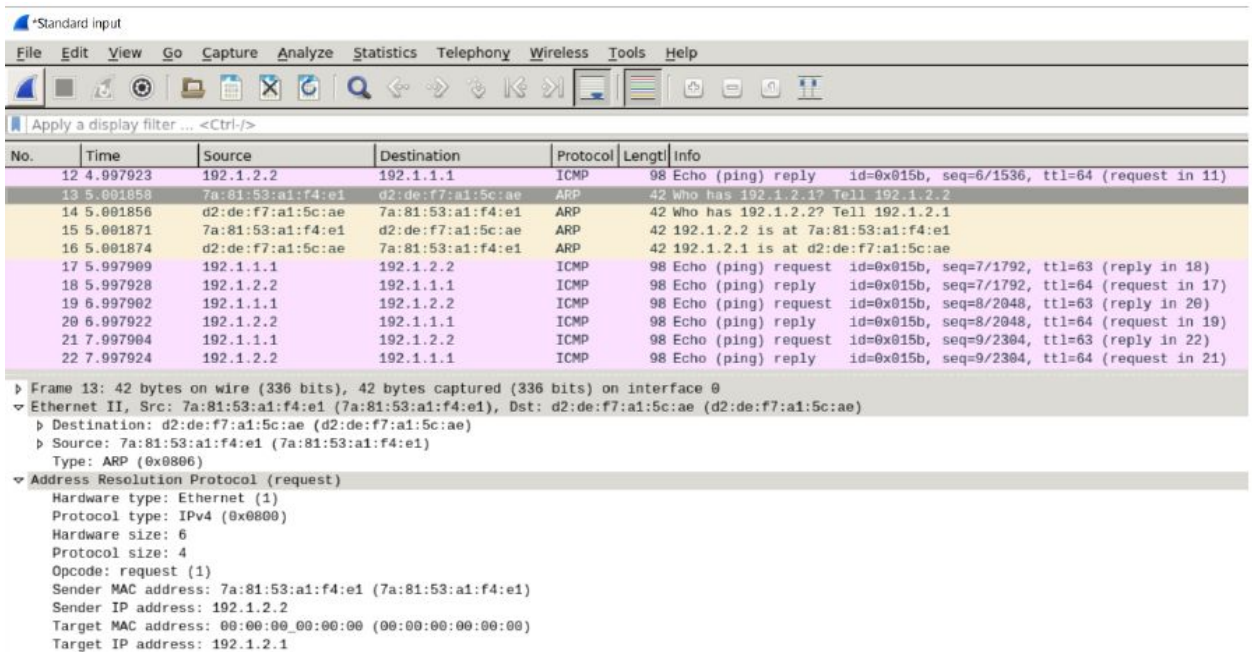
No.	Time	Source	Destination	Protocol	Length	Info
14	4.999604	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0143, seq=6/1536, ttl=64 (request in 13)
15	5.003548	7a:81:53:a1:f4:e1	d2:de:f7:a1:5c:ae	ARP	42	Who has 192.1.2.1? Tell 192.1.2.2
16	5.003565	d2:de:f7:a1:5c:ae	7a:81:53:a1:f4:e1	ARP	42	192.1.2.1 is at d2:de:f7:a1:5c:ae
17	5.999610	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x0143, seq=7/1792, ttl=63 (reply in 18)
18	5.999629	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0143, seq=7/1792, ttl=64 (request in 17)
19	6.999601	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x0143, seq=8/2048, ttl=63 (reply in 20)
20	6.999616	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0143, seq=8/2048, ttl=64 (request in 19)
21	7.999591	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x0143, seq=9/2384, ttl=63 (reply in 22)
22	7.999597	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0143, seq=9/2384, ttl=64 (request in 21)
23	8.999591	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x0143, seq=10/2560, ttl=63 (reply in 24)
24	8.999597	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x0143, seq=10/2560, ttl=64 (request in 23)

Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae), Dst: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)  
Destination: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)  
Source: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.2.2  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0xee2b (60971)  
Flags: 0x4000, Don't fragment  
Time to live: 63  
Protocol: ICMP (1)  
Header checksum: 0xca77 [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.1.1.1  
Destination: 192.1.2.2  
Internet Control Message Protocol

0000 7a 81 53 a1 f4 e1 d2 de f7 a1 5c ae 08 00 45 00 2 5 .....  
0010 00 54 ee 2b 46 00 3f 01 ca 77 c0 01 01 01 c0 01 T + @ ? w .....

Packets: 24 · Displayed: 24 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

## Wireshark capture of ARP packet on eth2 of PC3

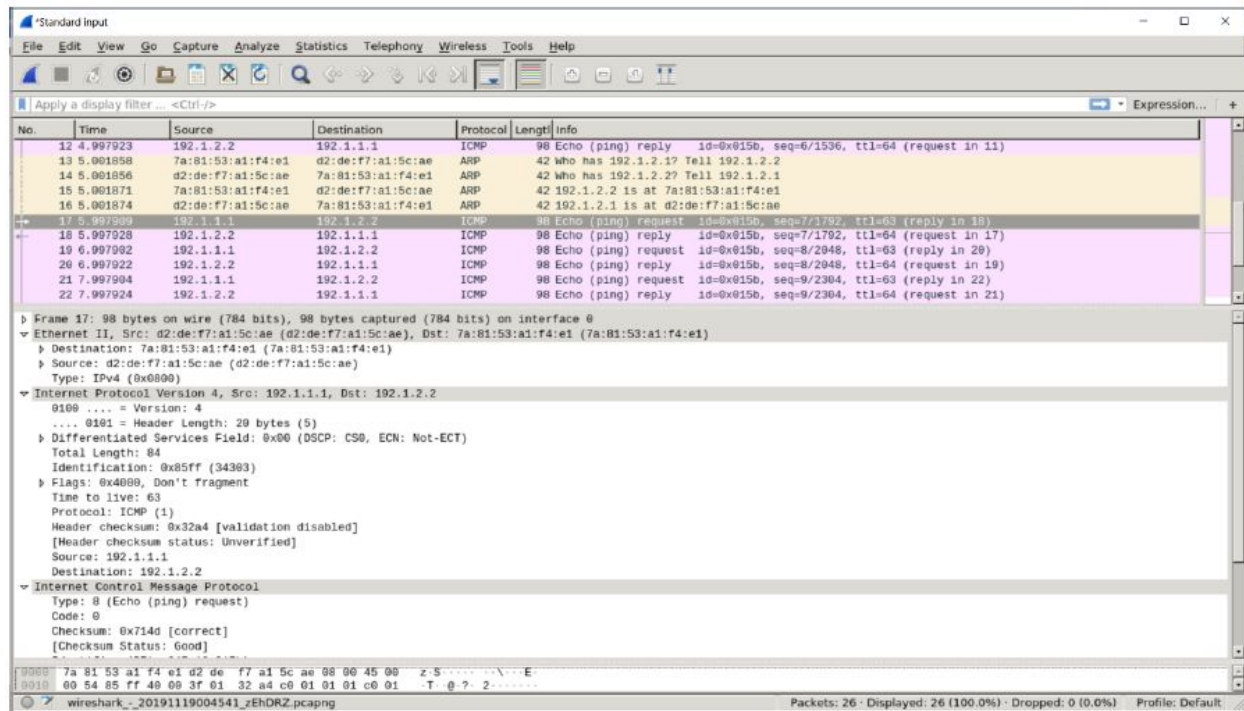


The screenshot shows a Wireshark capture of network traffic on interface eth2. The packet list displays several ICMP Echo (ping) requests and replies, and an ARP request. The selected packet (No. 13) is an ARP request from 192.1.2.2 to 192.1.1.1. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Address Resolution Protocol (ARP) header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
12	4.997923	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=6/1536, ttl=64 (request in 11)
13	5.001858	7a:81:53:a1:f4:e1	d2:de:f7:a1:5c:ae	ARP	42	Who has 192.1.2.1? Tell 192.1.2.2
14	5.001856	d2:de:f7:a1:5c:ae	7a:81:53:a1:f4:e1	ARP	42	Who has 192.1.2.2? Tell 192.1.2.1
15	5.001871	7a:81:53:a1:f4:e1	d2:de:f7:a1:5c:ae	ARP	42	192.1.2.2 is at 7a:81:53:a1:f4:e1
16	5.001874	d2:de:f7:a1:5c:ae	7a:81:53:a1:f4:e1	ARP	42	192.1.2.1 is at d2:de:f7:a1:5c:ae
17	5.997909	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=7/1792, ttl=63 (reply in 18)
18	5.997928	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=7/1792, ttl=64 (request in 17)
19	6.997902	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=8/2048, ttl=63 (reply in 20)
20	6.997922	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=8/2048, ttl=64 (request in 19)
21	7.997904	192.1.1.1	192.1.2.2	ICMP	98	Echo (ping) request id=0x015b, seq=9/2384, ttl=63 (reply in 22)
22	7.997924	192.1.2.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015b, seq=9/2384, ttl=64 (request in 21)

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1), Dst: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)  
Destination: d2:de:f7:a1:5c:ae (d2:de:f7:a1:5c:ae)  
Source: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)  
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: 7a:81:53:a1:f4:e1 (7a:81:53:a1:f4:e1)  
Sender IP address: 192.1.2.2  
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.1.2.1

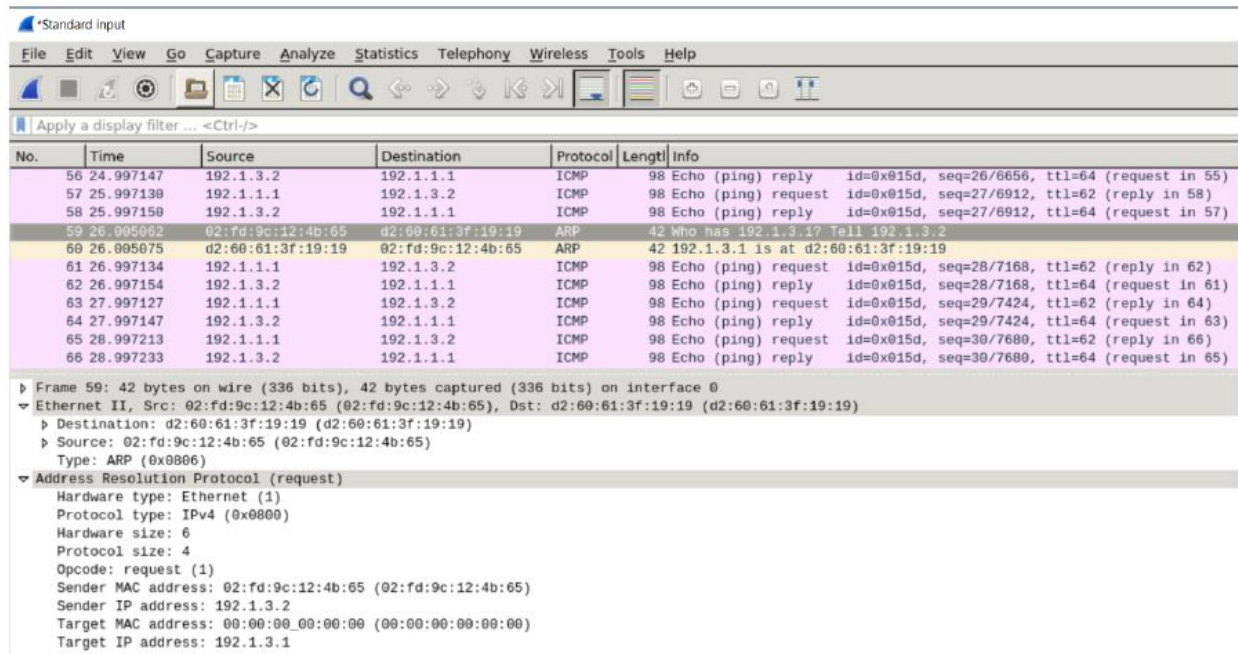
## Wireshark capture of ICMP request packet on eth2 of PC3



## When PC4 is pinged from PC1

```
root@PC1:~# ping 192.1.3.2
PING 192.1.3.2 (192.1.3.2) 56(84) bytes of data.
64 bytes from 192.1.3.2: icmp_seq=1 ttl=62 time=0.258 ms
64 bytes from 192.1.3.2: icmp_seq=2 ttl=62 time=0.086 ms
64 bytes from 192.1.3.2: icmp_seq=3 ttl=62 time=0.085 ms
64 bytes from 192.1.3.2: icmp_seq=4 ttl=62 time=0.116 ms
64 bytes from 192.1.3.2: icmp_seq=5 ttl=62 time=0.097 ms
^C
--- 192.1.3.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.085/0.128/0.258/0.066 ms
root@PC1:~#
```

## Wireshark capture of ARP packet on eth3 of PC4



Wireshark capture of ARP packet on eth3 of PC4. The packet list shows a series of ICMP Echo (ping) requests and replies, followed by an ARP request packet (Frame 59). The packet details pane shows the structure of the ARP request packet.

No.	Time	Source	Destination	Protocol	Length	Info
56	24.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=26/6656, ttl=64 (request in 55)
57	25.997130	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=27/6912, ttl=62 (reply in 58)
58	25.997150	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=27/6912, ttl=64 (request in 57)
59	26.005062	02:fd:9c:12:4b:65	d2:60:61:3f:19:19	ARP	42	Who has 192.1.3.1? Tell 192.1.3.2
60	26.005075	d2:60:61:3f:19:19	02:fd:9c:12:4b:65	ARP	42	192.1.3.1 is at d2:60:61:3f:19:19
61	26.997134	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=28/7168, ttl=62 (reply in 62)
62	26.997154	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=28/7168, ttl=64 (request in 61)
63	27.997127	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=29/7424, ttl=62 (reply in 64)
64	27.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=29/7424, ttl=64 (request in 63)
65	28.997213	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=30/7680, ttl=62 (reply in 66)
66	28.997233	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=30/7680, ttl=64 (request in 65)

Frame 59: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65), Dst: d2:60:61:3f:19:19 (d2:60:61:3f:19:19)

Destination: d2:60:61:3f:19:19 (d2:60:61:3f:19:19)

Source: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

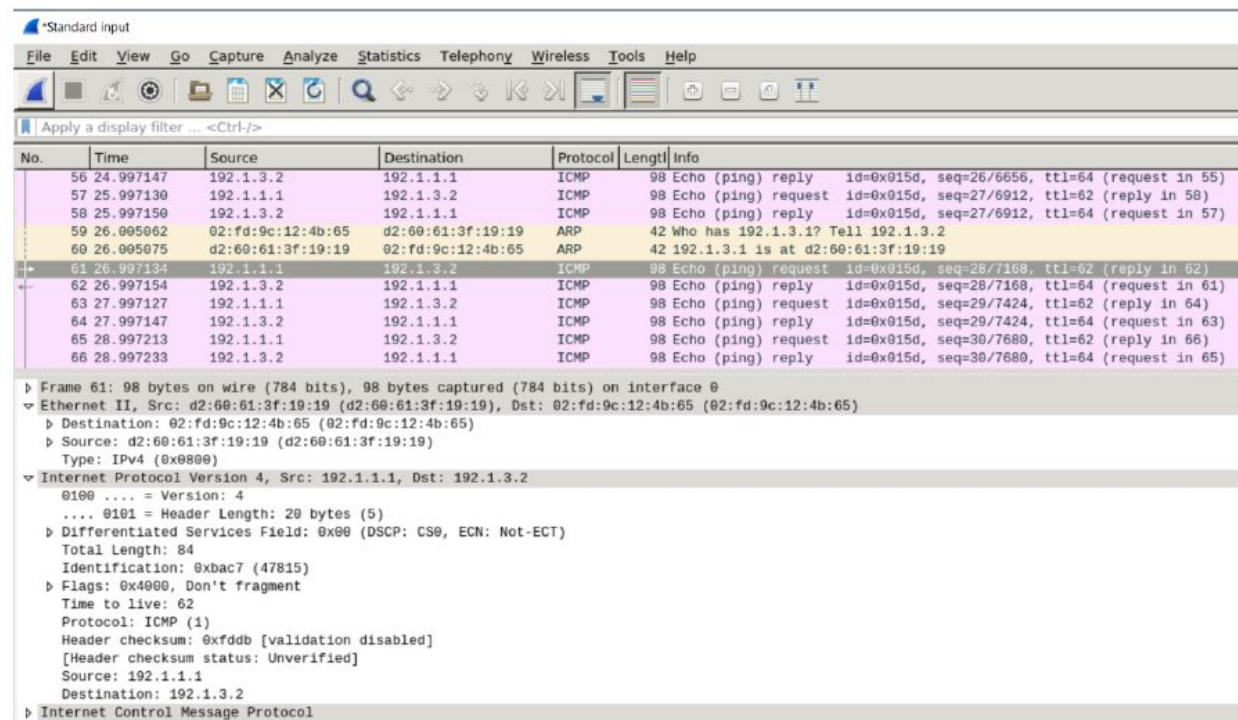
Sender MAC address: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)

Sender IP address: 192.1.3.2

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.1.3.1

## Wireshark capture of ICMP request packet on eth3 of PC4



Wireshark capture of ICMP request packet on eth3 of PC4. The packet list shows a series of ICMP Echo (ping) requests and replies, followed by an ICMP request packet (Frame 61). The packet details pane shows the structure of the ICMP request packet.

No.	Time	Source	Destination	Protocol	Length	Info
56	24.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=26/6656, ttl=64 (request in 55)
57	25.997130	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=27/6912, ttl=62 (reply in 58)
58	25.997150	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=27/6912, ttl=64 (request in 57)
59	26.005062	02:fd:9c:12:4b:65	d2:60:61:3f:19:19	ARP	42	Who has 192.1.3.1? Tell 192.1.3.2
60	26.005075	d2:60:61:3f:19:19	02:fd:9c:12:4b:65	ARP	42	192.1.3.1 is at d2:60:61:3f:19:19
61	26.997134	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=28/7168, ttl=62 (reply in 62)
62	26.997154	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=28/7168, ttl=64 (request in 61)
63	27.997127	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=29/7424, ttl=62 (reply in 64)
64	27.997147	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=29/7424, ttl=64 (request in 63)
65	28.997213	192.1.1.1	192.1.3.2	ICMP	98	Echo (ping) request id=0x015d, seq=30/7680, ttl=62 (reply in 66)
66	28.997233	192.1.3.2	192.1.1.1	ICMP	98	Echo (ping) reply id=0x015d, seq=30/7680, ttl=64 (request in 65)

Frame 61: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: d2:60:61:3f:19:19 (d2:60:61:3f:19:19), Dst: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)

Destination: 02:fd:9c:12:4b:65 (02:fd:9c:12:4b:65)

Source: d2:60:61:3f:19:19 (d2:60:61:3f:19:19)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.1.1.1, Dst: 192.1.3.2

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0xbac7 (47815)

Flags: 0x4000, Don't fragment

Time to live: 62

Protocol: ICMP (1)

Header checksum: 0xfddb [validation disabled]

[Header checksum status: Unverified]

Source: 192.1.1.1

Destination: 192.1.3.2

Internet Control Message Protocol



#### Arp table of PC1

```
root@PC1:~# arp -a
? (192.1.1.2) at 1a:24:e8:71:92:b5 [ether] on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC1:~#
```

#### Arp table of PC2

```
root@PC2:~# arp -a
? (192.1.1.1) at b6:90:4d:73:68:75 [ether] on eth1
? (192.1.2.2) at ce:bc:ff:27:4a:d6 [ether] on eth3
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC2:~#
```

#### Arp table of PC3

```
root@PC3:~# arp -a
? (192.1.3.2) at 6a:a9:ca:ad:a8:8a [ether] on eth4
? (192.1.2.1) at 22:0b:98:b4:af:c7 [ether] on eth2
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC3:~#
```

#### Arp table of PC4

```
root@PC4:~# arp -a
? (192.1.3.1) at e6:8f:1f:92:19:06 [ether] on eth3
? (172.17.0.1) at 02:42:1e:0f:92:39 [ether] on eth0
root@PC4:~#
```



12. From PC1, change its default gateway to 192.1.1.2 (PC2), run “curl www.ncsu.edu”, and observe the Wireshark output

Ans: The routes initially

```
root@PC1:~# ip r
default via 172.17.0.1 dev eth0
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.2
192.1.1.0/24 dev eth2 proto kernel scope link src 192.1.1.1
192.1.2.0/24 via 192.1.1.2 dev eth2
192.1.3.0/24 via 192.1.1.2 dev eth2
```

When curl [www.ncsu.edu](http://www.ncsu.edu) is run initially

```
root@PC1:~# curl www.ncsu.edu
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
root@PC1:~#
```

## Wireshark captures at eth0 of PC1

The screenshot shows a Wireshark capture on interface eth0. The packet list displays several packets, with packet 184 selected. The packet details pane shows the structure of the selected packet, which is a TCP segment. The packet is an ACK packet (Seq=0, Ack=1, Win=29184, Len=0) from the server (99.86.230.124) to the client (172.17.0.2). The packet length is 74 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
182	28.024824	128.109.249.27	172.17.0.2	DNS	492	Standard query response 6xdbd A www.ncsu.edu CNAME d300e56p1qpps.cloudfront.net A 99.86.230.124
183	28.024866	128.109.249.27	172.17.0.2	DNS	536	Standard query response 6xeffd AAAA www.ncsu.edu CNAME d300e56p1qpps.cloudfront.net AAAA 2608:1f5:100::1
184	28.060546	99.86.230.124	172.17.0.2	TCP	74	66 80 -> 35460 [ACK] Seq=1 Ack=77 Win=29184 Len=0 TSval=158318646 TSecr=3058179
185	28.060546	99.86.230.124	172.17.0.2	TCP	74	66 80 -> 35460 [ACK] Seq=1 Ack=77 Win=29184 Len=0 TSval=158318646 TSecr=3058179
186	28.060598	172.17.0.2	99.86.230.124	TCP	66	35460 -> 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3058179 TSecr=158318645
187	28.060686	172.17.0.2	99.86.230.124	HTTP	142	GET / HTTP/1.1
188	28.071088	99.86.230.124	172.17.0.2	TCP	66	80 -> 35460 [ACK] Seq=1 Ack=77 Win=29184 Len=0 TSval=158318646 TSecr=3058179
189	28.071335	99.86.230.124	172.17.0.2	HTTP	644	HTTP/1.1 301 Moved Permanently (text/html)
190	28.071344	172.17.0.2	99.86.230.124	TCP	66	35460 -> 80 [ACK] Seq=77 Ack=579 Win=30464 Len=0 TSval=3058182 TSecr=158318646
191	28.071504	172.17.0.2	172.17.0.1	SSH	110	Server: Encrypted packet (len=44)
192	28.071526	172.17.0.1	172.17.0.2	TCP	66	41646 -> 22 [ACK] Seq=125 Ack=241 Win=313 Len=0 TSval=3058182 TSecr=3058182

Frame 184: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: 02:42:ac:11:00:02 (02:42:ac:11:00:02), Dst: 02:42:44:d9:e9:7e (02:42:44:d9:e9:7e)  
Internet Protocol Version 4, Src: 172.17.0.2, Dst: 99.86.230.124  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 60  
Identification: 0x16ed (5869)  
Flags: 0x4000, Don't fragment  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0x2de9 [validation disabled]  
[Header checksum status: Unverified]  
Source: 172.17.0.2  
Destination: 99.86.230.124  
Transmission Control Protocol, Src Port: 35460, Dst Port: 80, Seq: 0, Len: 0  
Source Port: 35460  
Destination Port: 80  
[Stream index: 2]  
[TCP Segment Len: 0]  
Sequence number: 0 (relative sequence number)  
[Next sequence number: 0 (relative sequence number)]  
Acknowledgment number: 0

We can see the TCP SYN, SYN ACK and ACK packets for setting up the TCP connection between PC1 and the server of NCSU.

The screenshot shows a Wireshark capture on interface eth0. The packet list displays several packets, with packet 184 selected. The packet details pane shows the structure of the selected packet, which is a TCP segment. The packet is an ACK packet (Seq=0, Ack=1, Win=29184, Len=0) from the server (99.86.230.124) to the client (172.17.0.2). The packet length is 74 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
202	28.072784	172.17.0.1	172.17.0.2	TCP	66	41646 -> 22 [ACK] Seq=125 Ack=493 Win=313 Len=0 TSval=3058182 TSecr=3058182
203	28.073002	172.17.0.2	172.17.0.1	SSH	150	Server: Encrypted packet (len=84)
204	28.073038	172.17.0.1	172.17.0.2	TCP	66	41646 -> 22 [ACK] Seq=125 Ack=577 Win=313 Len=0 TSval=3058183 TSecr=3058182
205	28.073291	172.17.0.2	99.86.230.124	TCP	66	35460 -> 80 [FIN, ACK] Seq=77 Ack=579 Win=30464 Len=0 TSval=3058183 TSecr=158318646
206	28.074622	172.17.0.2	172.17.0.1	SSH	190	Server: Encrypted packet (len=124)
207	28.074643	172.17.0.1	172.17.0.2	TCP	66	41646 -> 22 [ACK] Seq=125 Ack=791 Win=313 Len=0 TSval=3058183 TSecr=3058183
208	28.083704	99.86.230.124	172.17.0.2	TCP	66	80 -> 35460 [FIN, ACK] Seq=579 Ack=78 Win=29184 Len=0 TSval=158318647 TSecr=3058183
209	28.083717	172.17.0.2	99.86.230.124	TCP	66	35460 -> 80 [ACK] Seq=78 Ack=589 Win=30464 Len=0 TSval=3058185 TSecr=158318647
210	28.097419	172.17.0.2	172.17.0.1	SSH	7396	Server: Encrypted packet (len=7240)
211	28.097451	172.17.0.1	172.17.0.2	TCP	66	41688 -> 22 [ACK] Seq=433 Ack=264613 Win=1424 Len=0 TSval=3058414 TSecr=3058414

Frame 184: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: 02:42:ac:11:00:02 (02:42:ac:11:00:02), Dst: 02:42:44:d9:e9:7e (02:42:44:d9:e9:7e)  
Internet Protocol Version 4, Src: 172.17.0.2, Dst: 99.86.230.124  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 60  
Identification: 0x16ed (5869)  
Flags: 0x4000, Don't fragment  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0x2de9 [validation disabled]  
[Header checksum status: Unverified]  
Source: 172.17.0.2  
Destination: 99.86.230.124  
Transmission Control Protocol, Src Port: 35460, Dst Port: 80, Seq: 0, Len: 0  
Source Port: 35460  
Destination Port: 80  
[Stream index: 2]  
[TCP Segment Len: 0]  
Sequence number: 0 (relative sequence number)  
[Next sequence number: 0 (relative sequence number)]  
Acknowledgment number: 0

We can see the TCP FIN, FIN ACK and ACK packets for closing the TCP connection between PC1 and NCSU server.

The routes after deleting the default gateway

```
root@PC1:~# ip r
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.2
192.1.1.0/24 dev eth2 proto kernel scope link src 192.1.1.1
192.1.2.0/24 via 192.1.1.2 dev eth2
192.1.3.0/24 via 192.1.1.2 dev eth2
root@PC1:~#
```

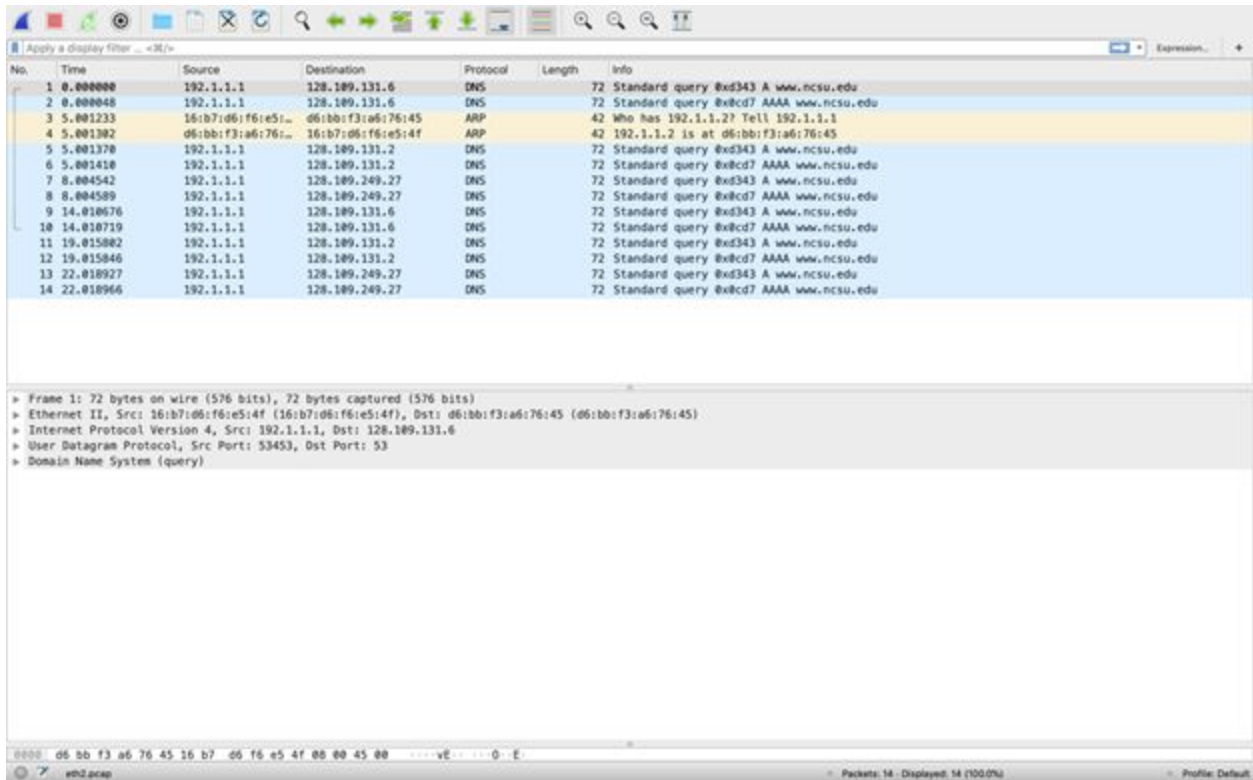
After adding the gateway via 192.1.1.2

```
root@PC1:~# ip route add default via 192.1.1.2
root@PC1:~#
root@PC1:~#
root@PC1:~# ip route show
default via 192.1.1.2 dev eth2
172.17.0.0/16 dev eth0 proto kernel scope link src 172.17.0.2
192.1.1.0/24 dev eth2 proto kernel scope link src 192.1.1.1
192.1.2.0/24 via 192.1.1.2 dev eth2
192.1.3.0/24 via 192.1.1.2 dev eth2
root@PC1:~#
```

When curl [www.ncsu.edu](http://www.ncsu.edu) is run later

```
root@PC1:~# curl www.ncsu.edu
curl: (6) Could not resolve host: www.ncsu.edu
root@PC1:~#
```

## Caputre at eth2 of PC1



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.1.1.1	128.109.131.6	DNS	72	Standard query 0x343 A www.ncsu.edu
2	0.000048	192.1.1.1	128.109.131.6	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu
3	5.001233	16:b7:d6:f6:e5:4f	06:bb:f3:a6:76:45	ARP	42	Who has 192.1.1.2? Tell 192.1.1.1
4	5.001302	06:bb:f3:a6:76:45	16:b7:d6:f6:e5:4f	ARP	42	192.1.1.2 is at 06:bb:f3:a6:76:45
5	5.001370	192.1.1.1	128.109.131.2	DNS	72	Standard query 0x343 A www.ncsu.edu
6	5.001410	192.1.1.1	128.109.131.2	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu
7	8.004542	192.1.1.1	128.109.249.27	DNS	72	Standard query 0x343 A www.ncsu.edu
8	8.004589	192.1.1.1	128.109.249.27	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu
9	14.010676	192.1.1.1	128.109.131.6	DNS	72	Standard query 0x343 A www.ncsu.edu
10	14.010719	192.1.1.1	128.109.131.6	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu
11	19.015082	192.1.1.1	128.109.131.2	DNS	72	Standard query 0x343 A www.ncsu.edu
12	19.015046	192.1.1.1	128.109.131.2	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu
13	22.010927	192.1.1.1	128.109.249.27	DNS	72	Standard query 0x343 A www.ncsu.edu
14	22.010966	192.1.1.1	128.109.249.27	DNS	72	Standard query 0x3cd7 AAAA www.ncsu.edu

Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)  
Ethernet II, Src: 16:b7:d6:f6:e5:4f (16:b7:d6:f6:e5:4f), Dst: 06:bb:f3:a6:76:45 (06:bb:f3:a6:76:45)  
Internet Protocol Version 4, Src: 192.1.1.1, Dst: 128.109.131.6  
User Datagram Protocol, Src Port: 53453, Dst Port: 53  
Domain Name System (query)

0000 06 bb f3 a6 76 45 16 b7 d6 f6 e5 4f 06 00 45 00 ...vE...0.E

eth2.pcap Packets: 14 - Displayed: 14 (100.0%) Profile: Default

Wireshark Capture at eth2 of the interface shows the DNS Query and Arp Request being sent but is unsuccessful in setting up a TCP connection between PC1 and NCSU server