

## Networking Lab: Assignment #2

Aswathy Mohan S

## Contents

<b>Problem 1</b>	<b>3</b>
<b>Problem 2</b>	<b>3</b>
<b>Problem 3</b>	<b>4</b>
<b>Problem 4</b>	<b>5</b>

## Problem 1

Ping another local IP address and do sniffer capture using wireshark

Answer: Wireshark is a free and opensource packet analyzer. Cleared ARP table using "sudo ip neigh flush all" command and then listed the details in the arp table using arp -n. The capturing is done in non-promiscuous mode.

```
sudo wireshark
```

```
arp -n
```

```
sudo ip neigh flush all
```

```
arp -n
```

```
ping 10.30.56.114
```

```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo wireshark
[sudo] password for aswathy:
```

```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress      Flags Mask    Iface
10.30.56.114     ether   ac:16:2d:0d:28:f9  C           eth0
10.30.56.1       ether   00:1f:9d:f2:bc:c9  C           eth0
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo ip neigh flush all
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress      Flags Mask    Iface
10.30.56.114     (incomplete)
10.30.56.1       (incomplete)
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping 10.30.56.114
PING 10.30.56.114 (10.30.56.114) 56(84) bytes of data:
64 bytes from 10.30.56.114: icmp_req=1 ttl=64 time=1.42 ms
64 bytes from 10.30.56.114: icmp_req=2 ttl=64 time=0.635 ms
64 bytes from 10.30.56.114: icmp_req=3 ttl=64 time=0.723 ms
64 bytes from 10.30.56.114: icmp_req=4 ttl=64 time=0.661 ms
64 bytes from 10.30.56.114: icmp_req=5 ttl=64 time=0.704 ms
64 bytes from 10.30.56.114: icmp_req=6 ttl=64 time=0.678 ms
64 bytes from 10.30.56.114: icmp_req=7 ttl=64 time=0.706 ms
64 bytes from 10.30.56.114: icmp_req=8 ttl=64 time=0.705 ms
64 bytes from 10.30.56.114: icmp_req=9 ttl=64 time=0.672 ms
64 bytes from 10.30.56.114: icmp_req=10 ttl=64 time=0.707 ms
64 bytes from 10.30.56.114: icmp_req=11 ttl=64 time=0.72 ms
64 bytes from 10.30.56.114: icmp_req=12 ttl=64 time=0.736 ms
64 bytes from 10.30.56.114: icmp_req=13 ttl=64 time=0.720 ms
64 bytes from 10.30.56.114: icmp_req=14 ttl=64 time=0.770 ms
64 bytes from 10.30.56.114: icmp_req=15 ttl=64 time=0.752 ms
64 bytes from 10.30.56.114: icmp_req=16 ttl=64 time=0.799 ms
```

1	0.000000	Cisco 7f:1b:2e	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
2	0.057143	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) request id=0x161d, seq=6/1536, ttl=64
3	0.057914	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) reply id=0x161d, seq=6/1536, ttl=64
4	0.166729	10.30.56.115	224.0.0.1	ICMP 98 Echo (ping) request id=0x122b, seq=330/18945, ttl=1
5	0.185442	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) request id=0x0de2, seq=368/28673, ttl=64
6	0.185462	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) reply id=0x0de2, seq=368/28673, ttl=64
7	1.057143	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) request id=0x161d, seq=7/1792, ttl=64
8	1.057745	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) reply id=0x161d, seq=7/1792, ttl=64
9	1.174643	10.30.56.115	224.0.0.1	ICMP 98 Echo (ping) request id=0x122b, seq=331/19201, ttl=1
10	1.185463	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) request id=0x0de2, seq=369/28929, ttl=64
11	1.185479	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) reply id=0x0de2, seq=369/28929, ttl=64
12	1.846785	10.30.56.147	10.30.56.255	NBNS 92 Name query NB DEVICESTA.RU<00>
13	1.999992	Cisco 7f:1b:2e	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
14	2.018128	6c:3b:e5:3e:0a:44	Broadcast	ARP 60 Who has 10.30.56.112? Tell 10.30.56.124
15	2.057141	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) request id=0x161d, seq=8/2048, ttl=64
16	2.057814	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) reply id=0x161d, seq=8/2048, ttl=64
17	2.182631	10.30.56.115	224.0.0.1	ICMP 98 Echo (ping) request id=0x122b, seq=332/19457, ttl=1
18	2.185457	10.30.56.114	10.30.56.109	ICMP 98 Echo (ping) request id=0x0de2, seq=370/29185, ttl=64
19	2.185477	10.30.56.109	10.30.56.114	ICMP 98 Echo (ping) reply id=0x0de2, seq=370/29185, ttl=64
20	2.186987	fe80::c1c0:c9d:a06b:eff02::1:2	DHCPv6	155 Solicit XID: 0x52962c CID: 0001000118378e6d64315098d7a6

## Problem 2

ping 4.2.2.1 and do sniffer capture using wireshark

Answer:

Done ARP flush before starting a new capture. The capturing is done in non-promiscuous mode.

```
sudo ip neigh flush all
```

ping 4.2.2.1

```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress           Flags Mask          Iface
10.30.56.114     ether   ac:16:2d:0d:28:f9   C                   eth0
10.30.56.1       ether   00:1f:9d:f2:bc:c9   C                   eth0
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo ip neigh flush all
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress           Flags Mask          Iface
10.30.56.114     (incomplete)
10.30.56.1       (incomplete)
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1) 56(84) bytes of data.
64 bytes from 4.2.2.1: icmp_req=1 ttl=55 time=233 ms
64 bytes from 4.2.2.1: icmp_req=2 ttl=55 time=270 ms
64 bytes from 4.2.2.1: icmp_req=3 ttl=55 time=194 ms
64 bytes from 4.2.2.1: icmp_req=4 ttl=55 time=310 ms
64 bytes from 4.2.2.1: icmp_req=5 ttl=55 time=285 ms
64 bytes from 4.2.2.1: icmp_req=6 ttl=55 time=282 ms
64 bytes from 4.2.2.1: icmp_req=7 ttl=55 time=312 ms
64 bytes from 4.2.2.1: icmp_req=8 ttl=55 time=201 ms
64 bytes from 4.2.2.1: icmp_req=9 ttl=55 time=236 ms
64 bytes from 4.2.2.1: icmp_req=11 ttl=55 time=198 ms
64 bytes from 4.2.2.1: icmp_req=12 ttl=55 time=256 ms
64 bytes from 4.2.2.1: icmp_req=13 ttl=55 time=298 ms
64 bytes from 4.2.2.1: icmp_req=14 ttl=55 time=198 ms
64 bytes from 4.2.2.1: icmp_req=15 ttl=55 time=205 ms
```

1	0.000000	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1055/7940, ttl=1
2	0.514880	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=10/2560, ttl=64
3	0.834989	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=79/20224, ttl=1
4	1.006655	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1056/8196, ttl=1
5	1.522173	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=11/2816, ttl=64
6	1.720862	4.2.2.1	10.30.56.109	ICMP	98 Echo (ping) reply	id=0x16f5, seq=11/2816, ttl=55
7	1.843073	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=80/20480, ttl=1
8	2.014609	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1057/8452, ttl=1
9	2.522774	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=12/3072, ttl=64
10	2.779411	4.2.2.1	10.30.56.109	ICMP	98 Echo (ping) reply	id=0x16f5, seq=12/3072, ttl=55
11	2.851063	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=81/20736, ttl=1
12	3.022608	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1058/8708, ttl=1
13	3.523262	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=13/3328, ttl=64
14	3.821487	4.2.2.1	10.30.56.109	ICMP	98 Echo (ping) reply	id=0x16f5, seq=13/3328, ttl=55
15	3.859064	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=82/20992, ttl=1
16	4.030645	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1059/8964, ttl=1
17	4.523308	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=14/3584, ttl=64
18	4.721727	4.2.2.1	10.30.56.109	ICMP	98 Echo (ping) reply	id=0x16f5, seq=14/3584, ttl=55
19	4.867044	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=83/21248, ttl=1
20	5.042994	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1060/9220, ttl=1
21	5.532647	10.30.56.109	4.2.2.1	ICMP	98 Echo (ping) request	id=0x16f5, seq=15/3840, ttl=64

▶ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)  
 ▶ Ethernet II, Src: 6c:3b:e5:31:2f:d7 (6c:3b:e5:31:2f:d7), Dst: Cisco f2:bc:c9 (00:1f:9d:f2:bc:c9)  
 ▶ Internet Protocol Version 4, Src: 10.30.56.109 (10.30.56.109), Dst: 4.2.2.1 (4.2.2.1)

## Problem 3

Multicast

Answer:

Done ARP flush before starting a new capture. The capturing is done in non-promiscuous mode.

MAC Address: 01:00:5e:00:00:01

sudo ip neigh flush all

ping 224.0.0.1

```

aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address            HWtype  HWaddress           Flags Mask            Iface
10.30.56.114       ether    (incomplete)
10.30.56.1          ether    00:1f:9d:f2:bc:c9   C                     eth0
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo ip neigh flush all
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address            HWtype  HWaddress           Flags Mask            Iface
10.30.56.114       ether    (incomplete)
10.30.56.1          ether    (incomplete)
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping 224.0.0.1
PING 224.0.0.1 (224.0.0.1) 56(84) bytes of data.
^Z
[1]+  Stopped                  ping 224.0.0.1
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping 224.0.0.1
PING 224.0.0.1 (224.0.0.1) 56(84) bytes of data.

```

2	0.042012	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=21/5376, ttl=1
3	0.169533	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1299/4869, ttl=
4	1.088048	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=323/17153, ttl=
5	1.050912	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=22/5632, ttl=1
6	1.177636	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1300/5125, ttl=
7	2.016053	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=324/17409, ttl=
8	2.057991	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=23/5888, ttl=1
9	2.185613	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1301/5381, ttl=
10	3.024053	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=325/17665, ttl=
11	3.066018	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=24/6144, ttl=1
12	3.193518	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1302/5637, ttl=
13	4.032063	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=326/17921, ttl=
14	4.074006	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=25/6400, ttl=1
15	4.201486	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1303/5893, ttl=
16	5.040092	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=327/18177, ttl=
17	5.082013	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=26/6656, ttl=1
18	5.209532	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1304/6149, ttl=
19	6.048316	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=328/18433, ttl=
20	6.090011	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x1719, seq=27/6912, ttl=1
21	6.217481	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1305/6405, ttl=
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)						
▶ Ethernet II, Src: HewlettP_0d:28:f9 (ac:16:2d:0d:28:f9), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)						
▶ Internet Protocol Version 4, Src: 10.30.56.114 (10.30.56.114), Dst: 224.0.0.1 (224.0.0.1)						
▶ Internet Control Message Protocol						

## Problem 4

Broadcast

Answer:

MAC Address: ff:ff:ff:ff:ff:ff