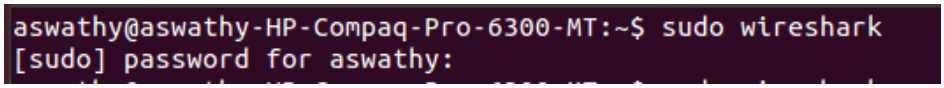
Networking Lab: Assignment #2

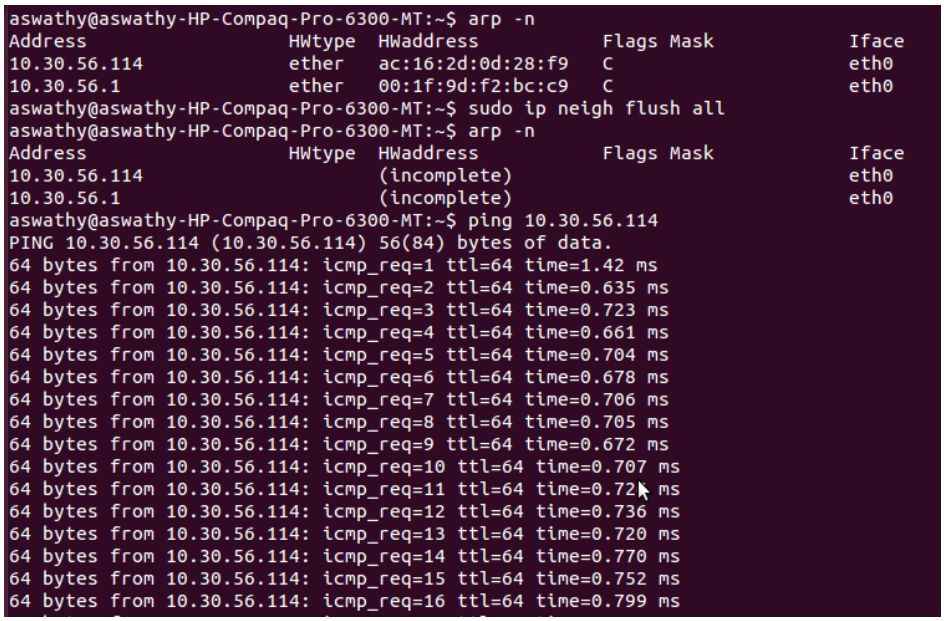
Aswathy Mohan S

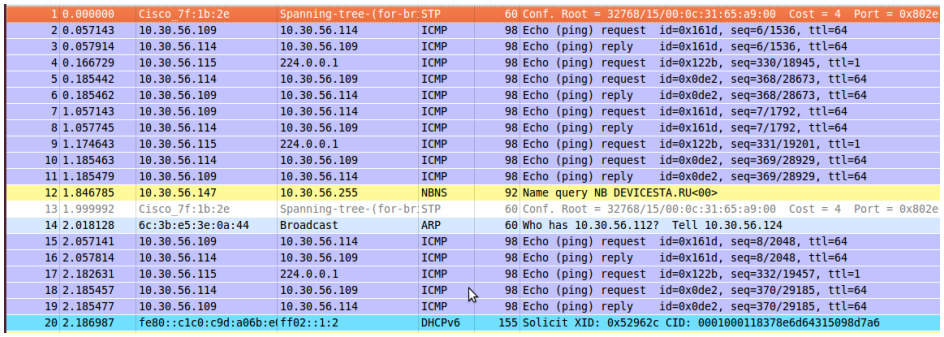
Contents

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





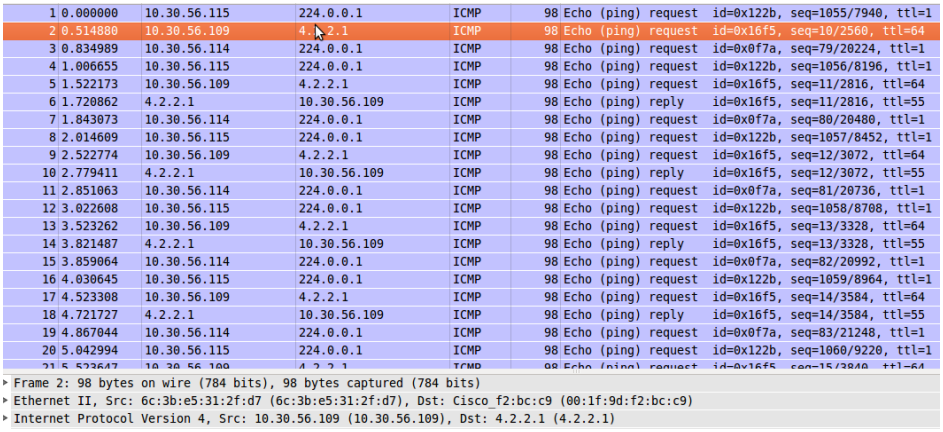


Problem 2

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)                              eth0
10.30.56.1                       (incomplete)                              eth0
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
```



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                     (incomplete)                              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)                              eth0
10.30.56.1                       (incomplete)                              eth0
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	1.008048	10.30.56.114	224.0.0.1	ICMP	98	Echo (ping) request id=0x0f7a, seq=323/17153, ttl=
5	1.050012	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