Advanced Computer Network Lab Assignment: Assignment #2

G.Reshma Nayar

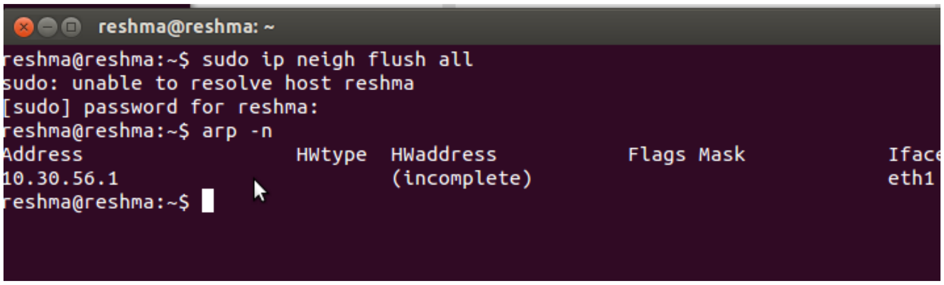
AM.EN.P2CSN13010

Contents

Problem 1

Question 1

a)ARP flush before each capture

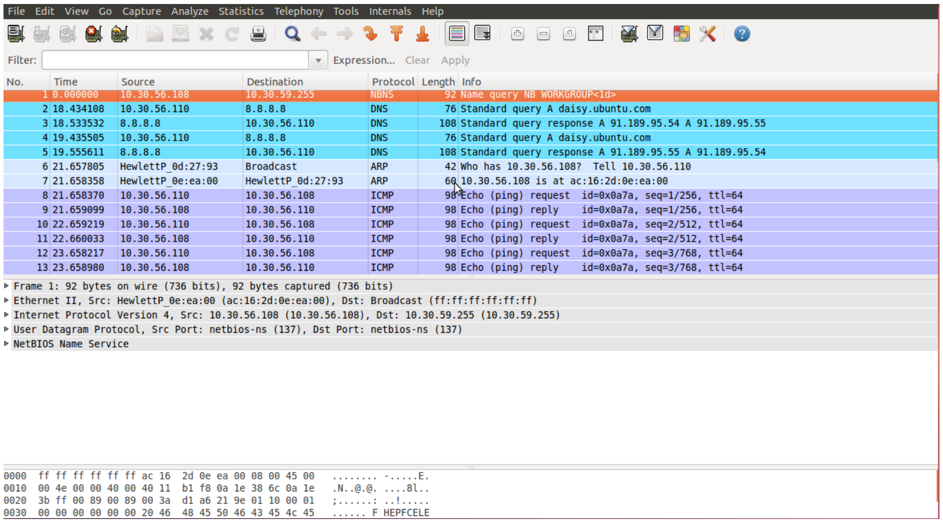


```
reshma@reshma:~$ sudo ip neigh flush all
sudo: unable to resolve host reshma
[sudo] password for reshma:
reshma@reshma:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1                       (incomplete)                              eth1
reshma@reshma:~$
```

b)Non-promiscuous mode capture

Steps:
a)Open wireshark
b)Select the "Capture" option and uncheck the promiscuous mode
c)Then click "Start" button.

c)Ping a local machine
ping 10.30.56.108

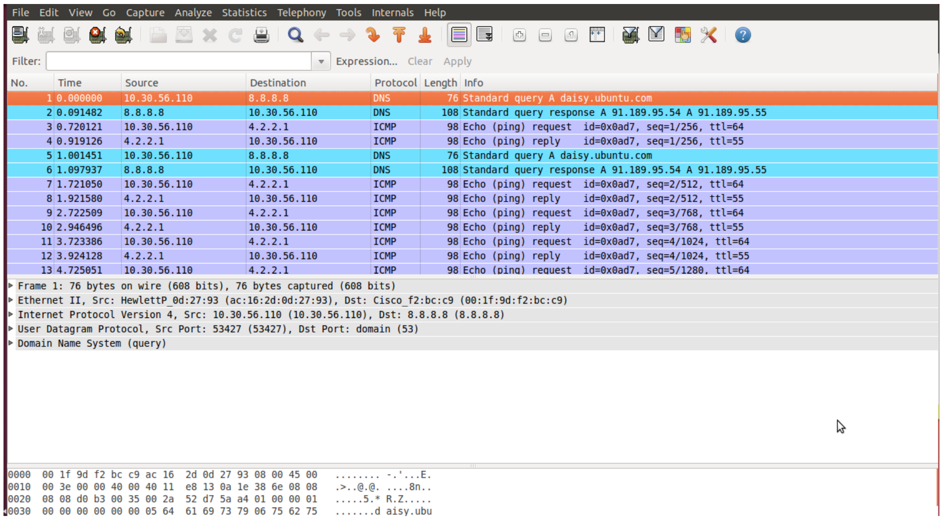

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.30.56.108	10.30.59.255	NBNS	92	Name query NB WORKGROUP<1d>
2	18.434108	10.30.56.110	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
3	18.533532	8.8.8.8	10.30.56.110	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
4	19.435505	10.30.56.110	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
5	19.555611	8.8.8.8	10.30.56.110	DNS	108	Standard query response A 91.189.95.55 A 91.189.95.54
6	21.657805	HewlettP_0d:27:93	Broadcast	ARP	42	Who has 10.30.56.108? Tell 10.30.56.110
7	21.658358	HewlettP_0e:ea:00	HewlettP_0d:27:93	ARP	60	10.30.56.108 is at ac:16:2d:0e:ea:00
8	21.658370	10.30.56.110	10.30.56.108	ICMP	98	Echo (ping) request id=0x0a7a, seq=1/256, ttl=64
9	21.659099	10.30.56.108	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0a7a, seq=1/256, ttl=64
10	22.659219	10.30.56.110	10.30.56.108	ICMP	98	Echo (ping) request id=0x0a7a, seq=2/512, ttl=64
11	22.660033	10.30.56.108	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0a7a, seq=2/512, ttl=64
12	23.658217	10.30.56.110	10.30.56.108	ICMP	98	Echo (ping) request id=0x0a7a, seq=3/768, ttl=64
13	23.658980	10.30.56.108	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0a7a, seq=3/768, ttl=64

```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: HewlettP_0e:ea:00 (ac:16:2d:0e:ea:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.30.56.108 (10.30.56.108), Dst: 10.30.59.255 (10.30.59.255)
▸ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
▸ NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff ac 16  2d 0e ea 00 08 00 45 00   ........ -.....E.
0010  00 4e 00 00 40 00 40 11  b1 f8 0a 1e 38 6c 0a 1e   .N..@.@. ....8l..
0020  3b ff 00 89 00 89 00 3a  d1 a6 21 9e 01 10 00 01   ;......: ..!.....
0030  00 00 00 00 00 00 20 46  48 45 50 46 43 45 4c 45   ...... F HEPFCELE
```

d)Ping 4.2.2.1
ping 4.2.2.1


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.30.56.110	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
2	0.091482	8.8.8.8	10.30.56.110	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
3	0.720121	10.30.56.110	4.2.2.1	ICMP	98	Echo (ping) request id=0x0ad7, seq=1/256, ttl=64
4	0.919126	4.2.2.1	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0ad7, seq=1/256, ttl=55
5	1.001451	10.30.56.110	8.8.8.8	DNS	76	Standard query A daisy.ubuntu.com
6	1.097937	8.8.8.8	10.30.56.110	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
7	1.721050	10.30.56.110	4.2.2.1	ICMP	98	Echo (ping) request id=0x0ad7, seq=2/512, ttl=64
8	1.921580	4.2.2.1	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0ad7, seq=2/512, ttl=55
9	2.722509	10.30.56.110	4.2.2.1	ICMP	98	Echo (ping) request id=0x0ad7, seq=3/768, ttl=64
10	2.946496	4.2.2.1	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0ad7, seq=3/768, ttl=55
11	3.723386	10.30.56.110	4.2.2.1	ICMP	98	Echo (ping) request id=0x0ad7, seq=4/1024, ttl=64
12	3.924128	4.2.2.1	10.30.56.110	ICMP	98	Echo (ping) reply id=0x0ad7, seq=4/1024, ttl=55
13	4.725051	10.30.56.110	4.2.2.1	ICMP	98	Echo (ping) request id=0x0ad7, seq=5/1280, ttl=64

```
▸ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▸ Ethernet II, Src: HewlettP_0d:27:93 (ac:16:2d:0d:27:93), Dst: Cisco_f2:bc:c9 (00:1f:9d:f2:bc:c9)
▸ Internet Protocol Version 4, Src: 10.30.56.110 (10.30.56.110), Dst: 8.8.8.8 (8.8.8.8)
▸ User Datagram Protocol, Src Port: 53427 (53427), Dst Port: domain (53)
▸ Domain Name System (query)
```

```
0000  00 1f 9d f2 bc c9 ac 16  2d 0d 27 93 08 00 45 00   ........ -.'...E.
0010  00 3e 00 00 40 00 40 11  e8 13 0a 1e 38 6e 08 08   .>..@.@. ....8n..
0020  08 08 d0 b3 00 35 00 2a  52 d7 5a a4 01 00 00 01   .....5.* R.Z.....
0030  00 00 00 00 00 00 05 64  61 69 73 79 06 75 62 75   .......d aisy.ubu
```

e) Determine MAC address values while:
i)broadcast
ii)multicast

i) MAC address of broadcast is ff:ff:ff:ff:ff:ff
ii) MAC address of multicast is 01:00:5e:00:00:01