

## **Networking Lab: Networking Assignment #2**

**Sreelakshmy R**

## Contents

<b>Problem 1</b>	<b>3</b>
<b>Problem 2</b>	<b>5</b>
<b>Problem 3</b>	<b>6</b>

## Problem 1

1. Ping another IP address

Answer:

```
list arp table           : arp -n
clear the arp table     : sudo ip -s -s neigh flush all
```

5 start wirshark and start capturing

```
Ping another IP address : ping 10.30.56.101
This will be captured by wireshark.
<screen shots>
```

Screenshot:

list arp table and clear the arp table :

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 88 used 2/2/2 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
sree@sree-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress          Flags Mask          Iface
10.30.56.1       (incomplete)
sree@sree-HP-Compaq-Pro-6300-MT:~$
```

Pinging another IP address:

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ ping 10.30.56.101
PING 10.30.56.101 (10.30.56.101) 56(84) bytes of data.
64 bytes from 10.30.56.101: icmp_req=1 ttl=64 time=1.32 ms
64 bytes from 10.30.56.101: icmp_req=2 ttl=64 time=0.667 ms
64 bytes from 10.30.56.101: icmp_req=3 ttl=64 time=0.652 ms
^Z
[17]+  Stopped                  ping 10.30.56.101
sree@sree-HP-Compaq-Pro-6300-MT:~$
```

lisitng the arp table :

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ arp -n
Address          HWtype  HWaddress          Flags Mask          Iface
10.30.56.1       ether   00:1f:9d:f2:bc:c9   C                   eth0
10.30.56.101     ether   88:51:fb:42:80:72   C                   eth0
```

wireshark:

53.103825	6c:3b:e5:31:2f:a5	Broadcast	ARP	42 Who has 10.30.56.101? Tell 10.30.56.123
63.104445	88:51:fb:42:80:72	6c:3b:e5:31:2f:a5	ARP	60 10.30.56.101 is at 88:51:fb:42:80:72
73.104457	10.30.56.123	10.30.56.101	ICMP	98 Echo (ping) request id=0x1455, seq=1/256, ttl=64
83.105165	10.30.56.101	10.30.56.123	ICMP	98 Echo (ping) reply id=0x1455, seq=1/256, ttl=64
93.227444	10.30.56.147	10.30.56.255	NBNS	92 Name query NB IMAGE.JPG<00>
103.460883	10.30.56.147	10.30.56.255	NBNS	92 Name query NB PIC.JPG<00>
113.836262	Hewlett- 98:d7:a6	Broadcast	ARP	60 Who has 10.30.56.1? Tell 10.30.56.147
123.978386	10.30.56.147	10.30.56.255	NBNS	92 Name query NB IMAGE.JPG<00>
134.831847	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x0f4d, seq=400/36865, ttl=1
144.105283	10.30.56.123	10.30.56.101	ICMP	98 Echo (ping) request id=0x1455, seq=2/512, ttl=64
154.105929	10.30.56.101	10.30.56.123	ICMP	98 Echo (ping) reply id=0x1455, seq=2/512, ttl=64
164.211552	10.30.56.147	10.30.56.255	NBNS	92 Name query NB PIC.JPG<00>
174.728965	10.30.56.147	10.30.56.255	NBNS	92 Name query NB IMAGE.JPG<00>
184.961926	10.30.56.147	10.30.56.255	NBNS	92 Name query NB PIC.JPG<00>
195.039852	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x0f4d, seq=401/37121, ttl=1
205.105901	10.30.56.123	10.30.56.101	ICMP	98 Echo (ping) request id=0x1455, seq=3/768, ttl=64
215.106521	10.30.56.101	10.30.56.123	ICMP	98 Echo (ping) reply id=0x1455, seq=3/768, ttl=64
226.047975	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x0f4d, seq=402/37377, ttl=1
236.185902	10.30.56.123	10.30.56.101	ICMP	98 Echo (ping) request id=0x1455, seq=4/1024, ttl=64
246.106530	10.30.56.101	10.30.56.123	ICMP	98 Echo (ping) reply id=0x1455, seq=4/1024, ttl=64

## Problem 2

### 2. Ping 4.2.2.1

Answer:

```
list arp table           : arp -n
clear the arp table     : sudo ip -s -s neigh flush all
```

start wirshark and start capturing

Ping another IP address : ping 4.2.2.1

This will be captured by wireshark.

<screen shots>

Screenshot:

Pinging 4.2.2.1

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ arp -n
Address      HWtype  HWaddress      Flags Mask    Iface
10.30.56.1   (incomplete)
10.30.56.101 (incomplete)
10.30.56.107 (incomplete)
sree@sree-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=186 ms
64 bytes from 4.2.2.1: icmp_req=2 ttl=55 time=189 ms
64 bytes from 4.2.2.1: icmp_req=3 ttl=55 time=189 ms
```

Wireshark:

12	9.072186	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3515/47885, ttl=1
13	10.088017	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3516/48141, ttl=1
14	10.409522	HewlettP f8:ca:b0	Broadcast	ARP	60 Who has 10.30.56.101?	Tell 10.30.56.112
15	10.742515	6c:3b:e5:31:2f:a5	Broadcast	ARP	42 Who has 10.30.56.17?	Tell 10.30.56.123
16	10.743478	Cisco f2:bc:c9	6c:3b:e5:31:2f:a5	ARP	60 10.30.56.1 is at 00:1f:9d:f2:bc:c9	
17	10.743490	10.30.56.123	4.2.2.1	ICMP	98 Echo (ping) request	id=0x1b10, seq=1/256, ttl=64
18	10.885903	74.125.236.117	10.30.56.123	TLSv1	467 Application Data	
19	10.885933	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=402 Win=580 Len=0	TSval=7511366 TSecr=134609503
20	10.886163	74.125.236.117	10.30.56.123	TLSv1	356 Application Data	
21	10.886177	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=692 Win=580 Len=0	TSval=7511366 TSecr=134609510
22	10.933983	4.2.2.1	10.30.56.123	ICMP	98 Echo (ping) reply	id=0x1b10, seq=1/256, ttl=55
23	11.088068	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3517/48397, ttl=1
24	11.743901	10.30.56.123	4.2.2.1	ICMP	98 Echo (ping) request	id=0x1b10, seq=2/512, ttl=64
25	11.952435	4.2.2.1	10.30.56.123	ICMP	98 Echo (ping) reply	id=0x1b10, seq=2/512, ttl=55
26	12.095985	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3518/48653, ttl=1
27	12.745337	10.30.56.123	4.2.2.1	ICMP	98 Echo (ping) request	id=0x1b10, seq=3/768, ttl=64
28	12.936929	4.2.2.1	10.30.56.123	ICMP	98 Echo (ping) reply	id=0x1b10, seq=3/768, ttl=55
29	13.104081	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3519/48909, ttl=1
30	13.630051	10.30.56.108	10.30.59.255	NBNS	92 Name query NB WORKGROUP<ld>	
31	13.678112	10.30.56.147	10.30.56.255	NBNS	92 Name query NB DEVICESTA.RU<00>	
32	14.024874	74.125.236.117	10.30.56.123	TLSv1	613 Application Data	
33	14.024897	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=1239 Win=580 Len=0	TSval=7512150 TSecr=134692649
34	14.024911	74.125.236.117	10.30.56.123	TLSv1	462 Application Data	
35	14.024921	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=1635 Win=580 Len=0	TSval=7512150 TSecr=134692650
36	14.025444	74.125.236.117	10.30.56.123	TLSv1	356 Application Data	
37	14.025458	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=1925 Win=580 Len=0	TSval=7512150 TSecr=134692654
38	14.112191	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3520/49165, ttl=1
39	14.428072	10.30.56.147	10.30.56.255	NBNS	92 Name query NB DEVICESTA.RU<00>	
40	15.120893	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=3521/49421, ttl=1

## Problem 3

### 2. Ping 4.2.2.1

Answer:

```
list arp table           : arp -n
clear the arp table     : sudo ip -s -s neigh flush all
```

5 start wirshark and start capturing

```
Ping another IP address : ping 224.0.0.1
```

This will be captured by wireshark.

<screen shots>

Screenshot:

Pinging multicast 224.0.0.1

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ arp -n
Address HWtype HWaddress Flags Mask Iface
10.30.56.1 (incomplete) eth0
sree@sree-HP-Compaq-Pro-6300-MT:~$ ping 224.0.0.1
PING 224.0.0.1 (224.0.0.1) 56(84) bytes of data.
^C
--- 224.0.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2016ms
sree@sree-HP-Compaq-Pro-6300-MT:~$
```

Wireshark:

16	8.215631	10.30.56.123	224.0.0.1	ICMP	98 Echo (ping) request id=0x1b36, seq=1/256, ttl=1
17	8.406087	74.125.236.117	10.30.56.123	TLSv1	229 Application Data
18	8.406117	6c:3b:e5:31:2f:a5	Broadcast	ARP	42 Who has 10.30.56.1? Tell 10.30.56.123
19	8.406131	74.125.236.117	10.30.56.123	TLSv1	357 Application Data
20	8.406138	74.125.236.117	10.30.56.123	TLSv1	117 Application Data
21	8.406999	Cisco f2:bc:c9	6c:3b:e5:31:2f:a5	ARP	60 10.30.56.1 is at 00:1f:9d:f2:bc:c9
22	8.407011	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=164 Win=580 Len=0 TSval=7618603 TSecr=135118468
23	8.407018	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=455 Win=580 Len=0 TSval=7618603 TSecr=135118468
24	8.407020	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=506 Win=580 Len=0 TSval=7618603 TSecr=135118468
25	8.411821	74.125.236.117	10.30.56.123	TLSv1	352 Application Data
26	8.411835	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=792 Win=580 Len=0 TSval=7618604 TSecr=135118474
27	9.071820	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request id=0x173f, seq=3943/26383, ttl=1
28	9.223574	10.30.56.123	224.0.0.1	ICMP	98 Echo (ping) request id=0x1b36, seq=2/512, ttl=1
29	9.458367	74.125.236.117	10.30.56.123	TLSv1	357 Application Data
30	9.458392	10.30.56.123	74.125.236.117	TCP	66 50563 > https [ACK] Seq=1 Ack=1083 Win=580 Len=0 TSval=7618666 TSecr=135119520