

## Networking Lab: Networking Assignment #2

Sreelakshmy R

## **Contents**

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

start wirshark and start capturing

Ping another IP address : ping 10.30.56.107

This will be captured by wireshark.

<screen shots>

Screenshot:

list arp table and clear 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
sree@sree-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
[sudo] password for sree:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 35 used 27/27/27 probes 1 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)                   eth0
sree@sree-HP-Compaq-Pro-6300-MT:~$
```

Pinging another IP address:

```
sree@sree-HP-Compaq-Pro-6300-MT:~$ ping 10.30.56.107
PING 10.30.56.107 (10.30.56.107) 56(84) bytes of data.
 64 bytes from 10.30.56.107: icmp_req=1 ttl=64 time=1.47 ms
 64 bytes from 10.30.56.107: icmp_req=2 ttl=64 time=0.636 ms
 64 bytes from 10.30.56.107: icmp_req=3 ttl=64 time=0.741 ms
 64 bytes from 10.30.56.107: icmp_req=4 ttl=64 time=0.639 ms
 64 bytes from 10.30.56.107: icmp_req=5 ttl=64 time=0.763 ms
 64 bytes from 10.30.56.107: icmp_req=6 ttl=64 time=0.629 ms
 64 bytes from 10.30.56.107: icmp_req=7 ttl=64 time=0.791 ms
 64 bytes from 10.30.56.107: icmp_req=8 ttl=64 time=0.644 ms
 64 bytes from 10.30.56.107: icmp_req=9 ttl=64 time=0.784 ms
 64 bytes from 10.30.56.107: icmp_req=10 ttl=64 time=0.635 ms
 64 bytes from 10.30.56.107: icmp_req=11 ttl=64 time=0.770 ms
 64 bytes from 10.30.56.107: icmp_req=12 ttl=64 time=0.594 ms
 64 bytes from 10.30.56.107: icmp_req=13 ttl=64 time=0.772 ms
 64 bytes from 10.30.56.107: icmp_req=14 ttl=64 time=0.578 ms
 64 bytes from 10.30.56.107: icmp_req=15 ttl=64 time=0.784 ms
 64 bytes from 10.30.56.107: icmp_req=16 ttl=64 time=0.589 ms
 64 bytes from 10.30.56.107: icmp_req=17 ttl=64 time=0.768 ms
 64 bytes from 10.30.56.107: icmp_req=18 ttl=64 time=0.581 ms
```

listing 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
10.30.56.107 ether   6c:3b:e5:31:2f:a8   C                   eth0
```

wireshark:

20	6.870482	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=1/256, ttl=64
21	6.871183	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=1/256, ttl=64
22	7.871305	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=2/512, ttl=64
23	7.871923	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=2/512, ttl=64
24	7.998865	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
25	8.058311	8.8.8.8	10.30.56.123	DNS	108 Standard query response A 91.189.95.54 A 91.189.95.55
26	8.058323	10.30.56.123	8.8.8.8	ICMP	130 Destination unreachable (Port unreachable)
27	8.692280	74.125.236.125	10.30.56.123	TLSv1	103 Application Data
28	8.692302	10.30.56.123	74.125.236.125	TCP	54 41040 > https [RST] Seq=1 Win=0 Len=0
29	8.870416	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=3/768, ttl=64
30	8.871143	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=3/768, ttl=64
31	8.954610	74.125.236.112	10.30.56.123	TCP	60 https > 43662 [RST] Seq=1 Win=0 Len=0
32	9.870421	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=4/1024, ttl=64
33	9.871041	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=4/1024, ttl=64
34	9.999966	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
35	10.870418	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=5/1280, ttl=64
36	10.871163	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=5/1280, ttl=64
37	11.534549	74.125.236.125	10.30.56.123	TCP	60 https > 41040 [RST] Seq=1 Win=0 Len=0
38	11.675153	74.125.236.112	10.30.56.123	TCP	60 https > 43662 [RST] Seq=1 Win=0 Len=0
39	11.870422	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=6/1536, ttl=64
40	11.871033	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=6/1536, ttl=64
41	11.878471	6c:3b:e5:31:2f:a8	6c:3b:e5:31:2f:a5	ARP	60 Who has 10.30.56.123? Tell 10.30.56.107
42	11.878486	6c:3b:e5:31:2f:a5	6c:3b:e5:31:2f:a8	ARP	42 10.30.56.123 is at 6c:3b:e5:31:2f:a5
43	11.998879	Cisco 7f:1b:2e	Spanning-tree-(for-br)	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
44	12.870419	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=7/1792, ttl=64
45	12.871192	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=7/1792, ttl=64
46	13.870461	10.30.56.123	10.30.56.107	ICMP	98 Echo (ping) request id=0x16e5, seq=8/2048, ttl=64
47	13.871101	10.30.56.107	10.30.56.123	ICMP	98 Echo (ping) reply id=0x16e5, seq=8/2048, ttl=64

## Problem 2

### 2. Ping google.com

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 google.com

This will be captured by wireshark.

<screen shots>

Screenshot:

Pinging google.com

```
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
sree@sree-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
[sudo] password for sree:
Sorry, try again.
[sudo] password for sree:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 22 used 70/70/54 probes 1 STALE

*** 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) eth0
sree@sree-HP-Compaq-Pro-6300-MT:~$ ping google.com
PING google.com (74.125.236.99) 56(84) bytes of data:
64 bytes from bom03s01-in-f3.1e100.net (74.125.236.99): icmp_req=1 ttl=56 time=9
1.1 ms
64 bytes from bom03s01-in-f3.1e100.net (74.125.236.99): icmp_req=2 ttl=56 time=8
8.6 ms
64 bytes from bom03s01-in-f3.1e100.net (74.125.236.99): icmp_req=3 ttl=56 time=9
2.9 ms
64 bytes from bom03s01-in-f3.1e100.net (74.125.236.99): icmp_req=4 ttl=56 time=8
9.3 ms
64 bytes from bom03s01-in-f3.1e100.net (74.125.236.99): icmp_req=5 ttl=56 time=9
1.7 ms
^Z
[2]+  Stopped                  ping google.com
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
```

Wireshark:

1	0.000000	10.30.56.108	10.30.59.255	BROWSER	291 Host Announcement ARCHANA-HP-COMPA, Workstation, Server, Print Queue Server, Xenix
2	0.788293	Cisco 7f:1b:2e	Spanning-tree (for-br):STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
3	1.433557	10.30.56.123	74.125.236.112	TLSv1	93 Encrypted Alert
4	2.794333	Cisco 7f:1b:2e	Spanning-tree (for-br):STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
5	4.789765	fe80::6e3b:e5ff:fe3d::ff02::fb	MONS	149 Standard query SRV analjith@system-of-a-down.presence.tcp.local, "QM" question A	
6	4.790889	fe80::8a51:fbff:fe42::ff02::fb	MONS	185 Standard query response AAAA, cache flush fe80::8a51:fbff:fe42:8887 SRV, cache flush	
7	4.791812	Cisco 7f:1b:2e	Spanning-tree (for-br):STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
8	4.825556	10.30.56.123	23.50.20.61	TCP	66 50496 > http [FIN, ACK] Seq=1 Ack=1 Win=331 Len=0 TSval=1115872 TSecr=608359319
9	5.274182	10.30.56.102	224.0.0.251	MONS	151 Standard query A VEJESH-HP-Compaq-Pro-6300-MT.local, "QM" question SRV vejesh@VEJESH
10	5.274464	10.30.56.125	224.0.0.251	MONS	203 Standard query response SRV, cache flush 0 0 5298 VEJESH-HP-Compaq-Pro-6300-MT.local
11	5.791523	10.30.56.123	8.8.8.8	DNS	76 Standard query A daisy.ubuntu.com
12	6.382253	10.30.56.123	8.8.8.8	DNS	70 Standard query A google.com
13	6.495365	8.8.8.8	10.30.56.123	DNS	246 Standard query response A 74.125.236.98 A 74.125.236.105 A 74.125.236.102 A 74.125.
14	6.495638	10.30.56.123	74.125.236.98	ICMP	98 Echo (ping) request id=0x1633, seq=1/256, ttl=64
15	6.791582	Cisco 7f:1b:2e	Spanning-tree (for-br):STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
16	6.873555	10.30.56.123	23.50.20.61	TCP	66 50503 > http [FIN, ACK] Seq=1 Ack=1 Win=453 Len=0 TSval=1116384 TSecr=608359317
17	6.873573	10.30.56.123	23.50.20.61	TCP	78 50502 > http [FIN, ACK] Seq=1 Ack=1 Win=160 Len=0 TSval=1116384 TSecr=801747603 SLI
18	7.065546	10.30.56.123	74.125.236.111	TLSv1	146 Application Data, Encrypted Alert
19	7.503671	10.30.56.123	74.125.236.98	ICMP	98 Echo (ping) request id=0x1633, seq=2/512, ttl=64
20	7.503947	74.125.236.98	10.30.56.123	ICMP	98 Echo (ping) reply id=0x1633, seq=2/512, ttl=56
21	7.594188	10.30.56.123	8.8.8.8	DNS	86 Standard query PTR 98.236.125.74.in-addr.arpa
22	8.791625	Cisco 7f:1b:2e	Spanning-tree (for-br):STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
23	9.104957	fe80::6e3b:e5ff:fe3d::ff02::fb	MONS	171 Standard query AAAA VEJESH-HP-Compaq-Pro-6300-MT.local, "QM" question SRV vejesh@VEJESH	
24	9.105577	fe80::8a51:fbff:fe42::ff02::fb	MONS	207 Standard query response SRV, cache flush 0 0 5298 VEJESH-HP-Compaq-Pro-6300-MT.local	
25	9.833546	6c:3b:e5:31:2f:a5	Cisco f2:bc:c9	ARP	42 Who has 10.30.56.1? Tell 10.30.56.123
26	9.835931	Cisco f2:bc:c9	6c:3b:e5:31:2f:a5	ARP	60 10.30.56.1 is at 00:1f:9d:f2:bc:c9