# ADVANCED NETWORK: Assignment #2

**Amaljith K.R.**

29-8-2013

# Contents

# Problem 1

Install wireshark and analyze the packet while pinging an ip adress within the same network.Please make sure that arp table is empty before pinging.

```
amaljith@system-of-a-down:~$ sudo arp -a -d 10.30.56.122
amaljith@system-of-a-down:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.122                     (incomplete)                              eth0
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
amaljith@system-of-a-down:~$ sudo wireshark
```

```
amaljith@system-of-a-down:~$ ping 10.30.56.122
PING 10.30.56.122 (10.30.56.122) 56(84) bytes of data.
64 bytes from 10.30.56.122: icmp_req=1 ttl=64 time=1.37 ms
64 bytes from 10.30.56.122: icmp_req=2 ttl=64 time=0.676 ms
64 bytes from 10.30.56.122: icmp_req=3 ttl=64 time=0.648 ms
64 bytes from 10.30.56.122: icmp_req=4 ttl=64 time=0.746 ms
64 bytes from 10.30.56.122: icmp_req=5 ttl=64 time=0.642 ms
64 bytes from 10.30.56.122: icmp_req=6 ttl=64 time=0.607 ms
^C
--- 10.30.56.122 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.607/0.783/1.379/0.269 ms
amaljith@system-of-a-down:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.122             ether   6c:3b:e5:3d:90:08   C                     eth0
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
amaljith@system-of-a-down:~$
```

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | 0.063807 | Cisco_f2:bc:c9 | 88:51:fb:42:80:87 | ARP | 60 | 10.30.56.1 is at 00:1f:9d:f2:bc:c9 |
| 4 | 1.025152 | 88:51:fb:42:80:87 | Broadcast | ARP | 42 | Who has 10.30.56.122? Tell 10.30.56.102 |
| 5 | 1.025799 | 6c:3b:e5:3d:90:08 | 88:51:fb:42:80:87 | ARP | 60 | 10.30.56.122 is at 6c:3b:e5:3d:90:08 |
| 25 | 6.037660 | 6c:3b:e5:3d:90:08 | 88:51:fb:42:80:87 | ARP | 60 | Who has 10.30.56.102? Tell 10.30.56.122 |
| 26 | 6.037672 | 88:51:fb:42:80:87 | 6c:3b:e5:3d:90:08 | ARP | 42 | 10.30.56.102 is at 88:51:fb:42:80:87 |

# Problem 2

Analyze the packets while pinging to google.

```
amaljith@system-of-a-down:~$ ping google.com
PING google.com (74.125.236.96) 56(84) bytes of data.
64 bytes from bom03s01-in-f0.1e100.net (74.125.236.96): icmp_req=1 ttl=56 time=67.3
 ms
64 bytes from bom03s01-in-f0.1e100.net (74.125.236.96): icmp_req=2 ttl=56 time=68.7
 ms
64 bytes from bom03s01-in-f0.1e100.net (74.125.236.96): icmp_req=3 ttl=56 time=106
ms
64 bytes from bom03s01-in-f0.1e100.net (74.125.236.96): icmp_req=4 ttl=56 time=63.8
 ms
^C
--- google.com ping statistics ---
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 8 | 3.340302 | 10.30.56.102 | 8.8.8.8 | DNS | 70 | Standard query A google.com |
| 9 | 3.445239 | 8.8.8.8 | 10.30.56.102 | DNS | 246 | Standard query response A 74.125.236.96 A 74.125.236.99 A 74.125.236.105 A 74.125.236.103 |
| 12 | 3.513248 | 10.30.56.102 | 8.8.8.8 | DNS | 86 | Standard query PTR 96.236.125.74.in-addr.arpa |
| 13 | 3.608117 | 8.8.8.8 | 10.30.56.102 | DNS | 124 | Standard query response PTR bom03s01-in-f0.1e100.net |