

CS 620 ADVANCED COMPUTER NETWORKS:
Assignment #2

Anand Raj Essar Vaishakh

AM.EN.P2CSN13004

Contents

Problem 1	3
Problem 2	5

Problem 1

Task 1 :

Install Wireshark

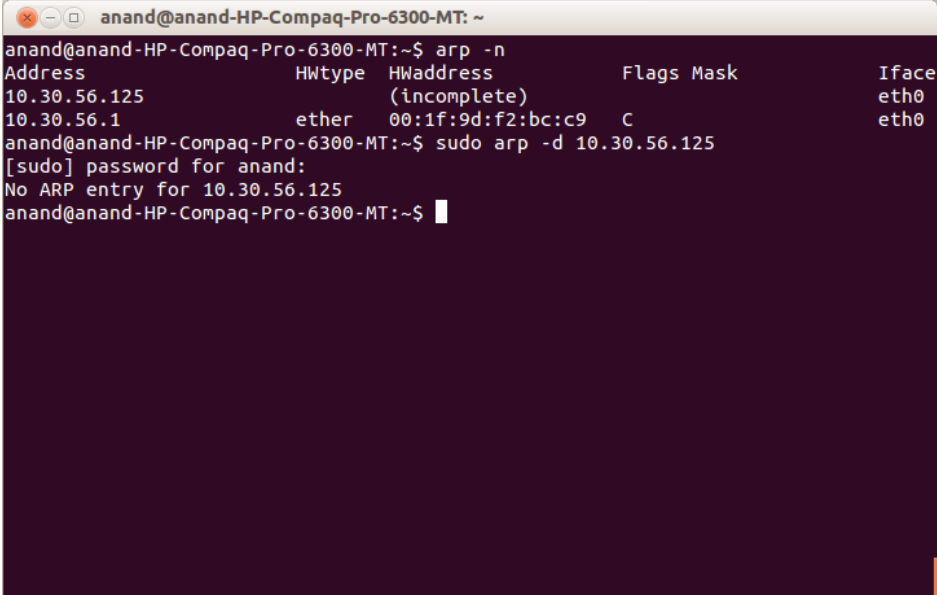
Start sniffing packets

Ping an IP continuously and capture the packets

Analyse and save the file

Installed wireshark from Ubuntu repository. Before starting the capture, our ARP table needs to be cleared.

ARP Table cleared :

A terminal window titled 'anand@anand-HP-Compaq-Pro-6300-MT: ~' showing the execution of the 'arp -n' command. The output displays the ARP table with columns: Address, HWtype, HWaddress, Flags, Mask, and Iface. The first entry is for 10.30.56.125 with an incomplete HWaddress. The second entry is for 10.30.56.1 with HWaddress 00:1f:9d:f2:bc:c9 and flag C. Then, the 'sudo arp -d 10.30.56.125' command is executed, and the output shows 'No ARP entry for 10.30.56.125'.

```
anand@anand-HP-Compaq-Pro-6300-MT:~$ arp -n
Address      HWtype  HWaddress      Flags Mask    Iface
10.30.56.125      (incomplete)
10.30.56.1      ether   00:1f:9d:f2:bc:c9  C        eth0
anand@anand-HP-Compaq-Pro-6300-MT:~$ sudo arp -d 10.30.56.125
[sudo] password for anand:
No ARP entry for 10.30.56.125
anand@anand-HP-Compaq-Pro-6300-MT:~$
```

Now , open the Wireshark tool with root permission. Choose an interface from the list. Start ping to an IP in your local network. In my case, it is 10.30.56.125. Observe the packets captured. There is a 'filter' option for better analysis. Save the capture file.

ARP is used for IP to MAC mapping, which means we use it for getting the MAC ID of an unknown host(means no entry in ARP Table) in our local network.

Now clear the ARP table

`sudo arp -d 10.30.56.125`

ARP Table with entries:

```
anand@anand-HP-Compaq-Pro-6300-MT: ~  
anand@anand-HP-Compaq-Pro-6300-MT:~$ arp -n  
Address          HWtype  HWaddress      Flags Mask    Iface  
10.30.56.125     ether   88:51:fb:42:80:89 C           eth0  
10.30.56.1       ether   00:1f:9d:f2:bc:c9 C           eth0  
10.30.56.119     ether   6c:3b:e5:3d:90:60 C           eth0  
anand@anand-HP-Compaq-Pro-6300-MT:~$
```

```
eth0 [Wireshark 1.6.7]  
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help  
Filter: Expression... Clear Apply  
No. Time Source Destination Protocol Length Info  
23 8.140925 10.30.56.125 10.30.56.104 ICMP 98 Echo (ping) reply id=0x0d55, seq=5/1280, t  
24 8.962381 Cisco 7f:1b:2e Spanning-tree-(for-br:STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost  
25 9.140116 10.30.56.104 10.30.56.125 ICMP 98 Echo (ping) request id=0x0d55, seq=6/1536, t  
26 9.140624 10.30.56.125 10.30.56.104 ICMP 98 Echo (ping) reply id=0x0d55, seq=6/1536, t  
27 9.144614 88:51:fb:42:80:89 88:51:fb:42:80:7e ARP 60 Who has 10.30.56.104? Tell 10.30.56.125  
28 9.144628 88:51:fb:42:80:7e 88:51:fb:42:80:89 ARP 42 10.30.56.104 is at 88:51:fb:42:80:7e  
29 10.140116 10.30.56.104 10.30.56.125 ICMP 98 Echo (ping) request id=0x0d55, seq=7/1792, t  
30 10.140879 10.30.56.125 10.30.56.104 ICMP 98 Echo (ping) reply id=0x0d55, seq=7/1792, t  
31 10.963828 Cisco 7f:1b:2e Spanning-tree-(for-br:STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost  
32 11.052857 10.30.56.103 224.0.0.251 MDNS 204 Standard query response PTR udisks-ssh. tcp.  
33 11.059204 10.30.56.103 224.0.0.251 MDNS 303 Standard query ANY ameyavp. udisks-ssh. tcp.  
34 11.140115 10.30.56.104 10.30.56.125 ICMP 98 Echo (ping) request id=0x0d55, seq=8/2048, t  
35 11.140776 10.30.56.125 10.30.56.104 ICMP 98 Echo (ping) reply id=0x0d55, seq=8/2048, t  
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)  
Ethernet II, Src: 88:51:fb:42:80:7e (88:51:fb:42:80:7e), Dst: Cisco f2:bc:c9 (00:1f:9d:f2:bc:c9)  
Internet Protocol Version 4, Src: 10.30.56.104 (10.30.56.104), Dst: 8.8.8.8 (8.8.8.8)  
User Datagram Protocol, Src Port: 59390 (59390), Dst Port: domain (53)  
Domain Name System (query)  
0000 00 1f 9d f2 bc c9 88 51 fb 42 80 7e 00 00 45 00 .....Q.B...E.  
0010 00 3e 00 00 40 00 11 e8 19 0a 1e 38 68 08 08 .>.@. ....8h..  
0020 08 08 e7 fe 00 35 00 2a 52 d1 6f 60 01 00 00 01 .....5.*R.o'....  
0030 00 00 00 00 00 05 64 61 69 73 79 06 75 62 75 .....d aisy.ubu  
Ethernet (eth), 14 bytes Packets: 74 Displayed: 74 Marked: 0 Dropped: 0 Profile: Default
```

Problem 2

Task 2:

Open sniffer capture again and ping google.com

Analyse and save file

Open Wireshark again and also ping to google.com

You will get response from Google

You can see the DNS message

