

Networks Lab: Assignment #2

Vejesh V

Contents

Problem 1	3
Problem 2	5

Problem 1

Install sniffer capture tool(eg: Wireshark) and sniff packets when pinging a pingable IP address. Ensure that the ARP table is empty before pinging. Analyse the output and save the file.

Ans: **Terminal command:** \$ arp -n /* To list the contents of ARP table */

Terminal command: \$ sudo arp -d (ip in the table) /* To remove the specified IP from ARP table */

```
vejesh@VEJESH-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                    eth2
10.30.56.115              (incomplete)
10.30.56.122              (incomplete)
vejesh@VEJESH-HP-Compaq-Pro-6300-MT:~$
```

Terminal command: \$ sudo wireshark /* To launch wireshark with SuperUser permissions */

Start capturing the packets in wireshark using the system's ethernet interface, eth2 in my case.

Terminal command: \$ ping 10.30.56.122

```
vejesh@VEJESH-HP-Compaq-Pro-6300-MT:~$ 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=1.43 ms
64 bytes from 10.30.56.122: icmp_req=2 ttl=64 time=0.610 ms
^C
--- 10.30.56.122 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.610/1.021/1.433/0.412 ms
vejesh@VEJESH-HP-Compaq-Pro-6300-MT:~$
```

Stop capturing the packets in wireshark and save the output file.

No.	Time	Source	Destination	Protocol	Length	Info
136	8.569531	10.30.8.176	10.30.56.125	HTTP	259	HTTP/1.1 304 Not Modified
137	8.569964	10.30.56.125	10.30.8.176	HTTP	351	GET /apt-cacher/in.archive.ubuntu.com/ubuntu/dists/precise/universe/i18n/Index HTTP/1.1
138	8.571030	10.30.8.176	10.30.56.125	TCP	66	http -> 44244 [ACK] Seq=53278 Ack=7229 Win=41056 Len=0 TSval=215253171 TSecr=426781
139	8.791167	88:51:fb:42:80:89	Broadcast	ARP	42	Who has 10.30.56.122? Tell 10.30.56.125
140	8.791862	6c:3b:e5:3d:90:08	88:51:fb:42:80:89	ARP	60	10.30.56.122 is at 6c:3b:e5:3d:90:08
141	8.791874	10.30.56.125	10.30.56.122	ICMP	98	Echo (ping) request id=0x0d5a, seq=1/256, ttl=64
142	8.792579	10.30.56.122	10.30.56.125	ICMP	98	Echo (ping) reply id=0x0d5a, seq=1/256, ttl=64
143	9.042546	10.30.8.176	10.30.56.125	HTTP	261	HTTP/1.1 304 Not Modified
144	9.042945	10.30.56.125	10.30.8.176	HTTP	347	GET /apt-cacher/in.archive.ubuntu.com/ubuntu/dists/precise-updates/main/source/Sources.bz2
145	9.044161	10.30.8.176	10.30.56.125	TCP	66	http -> 44244 [ACK] Seq=53473 Ack=7510 Win=42272 Len=0 TSval=215253289 TSecr=426899
146	9.475496	10.30.8.176	10.30.56.125	HTTP	260	HTTP/1.1 304 Not Modified
147	9.475919	10.30.56.125	10.30.8.176	HTTP	353	GET /apt-cacher/in.archive.ubuntu.com/ubuntu/dists/precise-updates/restricted/source/Sources

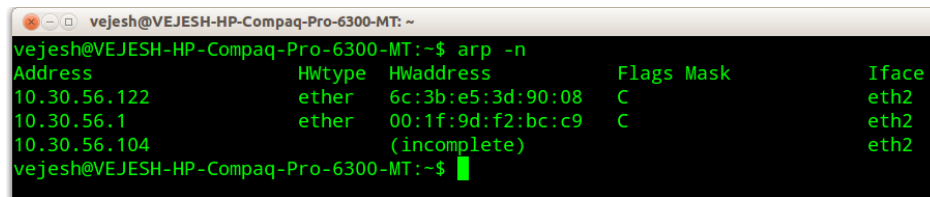
Line No.139 shows a ARP broadcast message being transmitted asking for Who has 10.30.56.122 and Tell 10.30.56.125 ie, System with MAC:88:51:fb:42:80:89 and IP 10.30.56.122 should reply to the system with IP 10.30.56.125 informing about its 48-Bit MAC address.

Line No.140 shows the reply to the ARP broadcast message telling that the system with IP 10.30.56.122 is having its MAC as 6c:3b:e5:3d:90:08

Line No.141 shows that the system is sending a ping request

Line No.142 shows that the system received a ping reply.

ARP table after pinging.

A terminal window titled 'vejesh@VEJESH-HP-Compaq-Pro-6300-MT: ~' showing the output of the 'arp -n' command. The output is a table with columns: Address, Hwtype, Hwaddress, Flags, Mask, and Iface. The table lists three entries: 10.30.56.122 with hwaddress 6c:3b:e5:3d:90:08, 10.30.56.1 with hwaddress 00:1f:9d:f2:bc:c9, and 10.30.56.104 with hwaddress (incomplete). All entries have 'C' in the Flags column and 'eth2' in the Iface column.

```
vejesh@VEJESH-HP-Compaq-Pro-6300-MT:~$ arp -n
Address      Hwtype  Hwaddress    Flags Mask    Iface
10.30.56.122  ether   6c:3b:e5:3d:90:08 C          eth2
10.30.56.1    ether   00:1f:9d:f2:bc:c9 C          eth2
10.30.56.104      (incomplete)          eth2
vejesh@VEJESH-HP-Compaq-Pro-6300-MT:~$
```

Problem 2

Using sniffer capture tool analyse the output and save the file when ping google.com

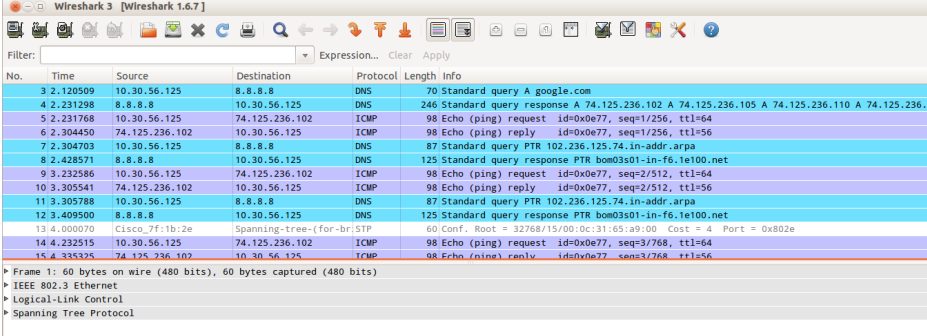
Ans: **Terminal command:** \$ sudo wireshark /* To open wireshark with root privilege. */

Start capturing packets using wireshark.

Terminal command: \$ ping google.com

Stop capturing packets in wireshark.

Save the output file.



The screenshot shows the Wireshark 1.6.7 interface with a packet capture of a ping to google.com. The packet list on the left shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
3	2.120509	10.30.56.125	8.8.8.8	DNS	70	Standard query A google.com
4	2.231298	8.8.8.8	10.30.56.125	DNS	246	Standard query response A 74.125.236.102 A 74.125.236.105 A 74.125.236.110 A 74.125.236.97
5	2.231768	10.30.56.125	74.125.236.102	ICMP	98	Echo (ping) request id=0x0e77, seq=1/256, ttl=64
6	2.304450	74.125.236.102	10.30.56.125	ICMP	98	Echo (ping) reply id=0x0e77, seq=1/256, ttl=56
7	2.304703	10.30.56.125	8.8.8.8	DNS	87	Standard query PTR 102.236.125.74.in-addr.arpa
8	2.428571	8.8.8.8	10.30.56.125	DNS	125	Standard query response PTR bom03s01-in-f6.1e100.net
9	2.232586	10.30.56.125	74.125.236.102	ICMP	98	Echo (ping) request id=0x0e77, seq=2/512, ttl=64
10	3.305541	74.125.236.102	10.30.56.125	ICMP	98	Echo (ping) reply id=0x0e77, seq=2/512, ttl=56
11	3.305788	10.30.56.125	8.8.8.8	DNS	87	Standard query PTR 102.236.125.74.in-addr.arpa
12	3.409500	8.8.8.8	10.30.56.125	DNS	125	Standard query response PTR bom03s01-in-f6.1e100.net
13	4.000070	Cisco_7f:1b:2e		Spanning-tree-(for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
14	4.232515	10.30.56.125	74.125.236.102	ICMP	98	Echo (ping) request id=0x0e77, seq=3/768, ttl=64
15	4.335335	74.125.236.102	10.30.56.125	ICMP	98	Echo (ping) reply id=0x0e77, seq=3/768, ttl=56

The packet details pane for the selected packet (No. 15) shows:

- Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- IEEE 802.3 Ethernet
- Logical-Link Control
- Spanning Tree Protocol

Line No.3 shows that the system is sending a query to the Domain Name System asking for the IP of google.com

Line No.4 shows that the system got reply to the query indicating the IP of google.com as 74.125.236.102

Line No.5 shows that the system sent a ping request to the host with IP address as 74.125.236.102

Line No.6 shows that google replied to my system with IP 10.30.56.125.