Networks Lab: Assignment #2

Archana Nair

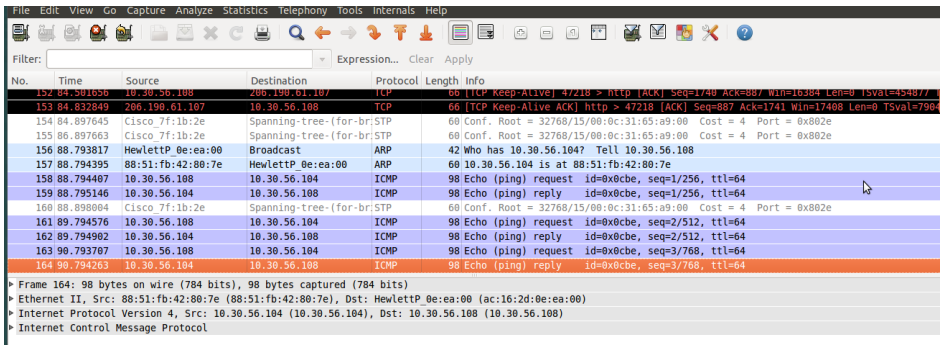
Contents

Problem 1

To install wireshark and capture the sniffer packets from a particular IP address.
The wireshark is installed using the command :
sudo apt-get install wireshark
Then the wireshark is opened using
sudo wireshark To get the mac address of an IP address :
arp -n

```
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$
```

The sniffer packets of an IP address using :
ping 10.30.56.105



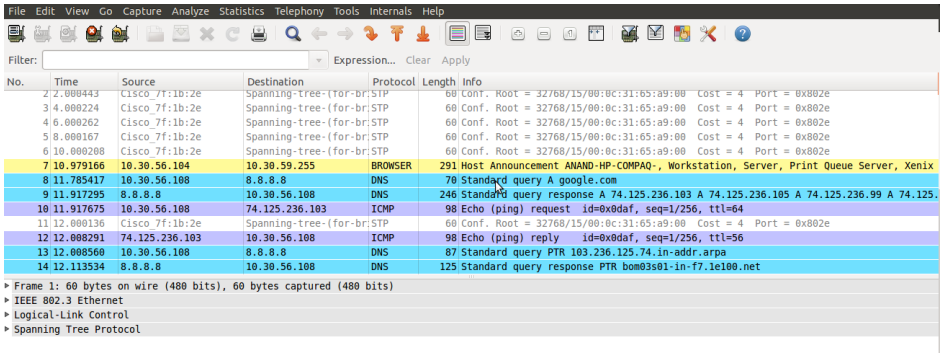
arp -n

```
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
10.30.56.104             ether   88:51:fb:42:80:7e   C                     eth0
10.30.56.119             ether   6c:3b:e5:3d:90:60   C                     eth0
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$
```

arp -d 10.30.56.104

```
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$ sudo arp -d 10.30.56.104
[sudo] password for archana:
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
10.30.56.104                     (incomplete)                              eth0
archana@archana-HP-Compaq-6200-Pro-MT-PC:~$
```

The sniffer packets from google.com is captured using :
ping google.com


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
2 2.000443 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 4.000224 Cisco_7f:1b:2e Spanning-tree-(for-br STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
4 6.000262 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 8.000167 Cisco_7f:1b:2e Spanning-tree-(for-br STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
6 10.000208 Cisco_7f:1b:2e Spanning-tree-(for-br STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
7 10.979166 10.30.56.104 10.30.59.255 BROWSER 291 Host Announcement ANAND-HP-COMPAQ-, Workstation, Server, Print Queue Server, Xenix
8 11.785417 10.30.56.108 8.8.8.8 DNS 70 Standard query A google.com
9 11.917295 8.8.8.8 10.30.56.108 DNS 246 Standard query response A 74.125.236.103 A 74.125.236.105 A 74.125.236.99 A 74.125.
10 11.917675 10.30.56.108 74.125.236.103 ICMP 98 Echo (ping) request id=0x0daf, seq=1/256, ttl=64
11 12.000136 Cisco_7f:1b:2e Spanning-tree-(for-br STP 60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
12 12.008291 74.125.236.103 10.30.56.108 ICMP 98 Echo (ping) reply id=0x0daf, seq=1/256, ttl=56
13 12.008560 10.30.56.108 8.8.8.8 DNS 87 Standard query PTR 103.236.125.74.in-addr.arpa
14 12.113534 8.8.8.8 10.30.56.108 DNS 125 Standard query response PTR bom03s01-in-f7.1e100.net
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol