

ADVANCED COMPUTER NETWORKS - LAB: ASSIGNMENT 2

Ameya V P

AM.EN.P2CSN13003

Problem 1

1. Install wireshark to sniffer capture

Wireshark is a open source network packet analyzer. It is used for network troubleshooting and analysis.

1) command used : `sudo apt-get install wireshark`

Installed wireshark

2) `sudo wireshark`

Run wireshark for capturing packets.

3) `arp -n` : to list arp table

```
jennie@ameyavp:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask          Iface
10.30.56.124             ether    00:1f:9d:f2:bc:c9   C                   eth0
10.30.56.1                ether    00:1f:9d:f2:bc:c9   C                   eth0
jennie@ameyavp:~$
```

4) capturing network packets by pinging 10.30.56.124

`ping 10.30.56.124`

```
jennie@ameyavp:~$ ping 10.30.56.124
PING 10.30.56.124 (10.30.56.124) 56(84) bytes of data:
64 bytes from 10.30.56.124: icmp_req=1 ttl=64 time=1.38 ms
64 bytes from 10.30.56.124: icmp_req=2 ttl=64 time=0.736 ms
64 bytes from 10.30.56.124: icmp_req=3 ttl=64 time=0.612 ms
64 bytes from 10.30.56.124: icmp_req=4 ttl=64 time=0.732 ms
64 bytes from 10.30.56.124: icmp_req=5 ttl=64 time=0.573 ms
64 bytes from 10.30.56.124: icmp_req=6 ttl=64 time=0.658 ms
64 bytes from 10.30.56.124: icmp_req=7 ttl=64 time=0.549 ms
64 bytes from 10.30.56.124: icmp_req=8 ttl=64 time=0.311 ms
64 bytes from 10.30.56.124: icmp_req=9 ttl=64 time=0.486 ms
64 bytes from 10.30.56.124: icmp_req=10 ttl=64 time=0.517 ms
64 bytes from 10.30.56.124: icmp_req=11 ttl=64 time=0.551 ms
64 bytes from 10.30.56.124: icmp_req=12 ttl=64 time=0.702 ms
64 bytes from 10.30.56.124: icmp_req=13 ttl=64 time=0.546 ms
64 bytes from 10.30.56.124: icmp_req=14 ttl=64 time=0.713 ms
64 bytes from 10.30.56.124: icmp_req=15 ttl=64 time=0.772 ms
64 bytes from 10.30.56.124: icmp_req=16 ttl=64 time=0.726 ms
64 bytes from 10.30.56.124: icmp_req=17 ttl=64 time=0.790 ms
64 bytes from 10.30.56.124: icmp_req=18 ttl=64 time=0.806 ms
64 bytes from 10.30.56.124: icmp_req=19 ttl=64 time=0.756 ms
64 bytes from 10.30.56.124: icmp_req=20 ttl=64 time=0.796 ms
64 bytes from 10.30.56.124: icmp_req=21 ttl=64 time=0.538 ms
64 bytes from 10.30.56.124: icmp_req=22 ttl=64 time=0.737 ms
64 bytes from 10.30.56.124: icmp_req=23 ttl=64 time=0.553 ms
64 bytes from 10.30.56.124: icmp_req=24 ttl=64 time=0.700 ms
64 bytes from 10.30.56.124: icmp_req=25 ttl=64 time=0.586 ms
64 bytes from 10.30.56.124: icmp_req=26 ttl=64 time=0.821 ms
64 bytes from 10.30.56.124: icmp_req=27 ttl=64 time=0.771 ms
64 bytes from 10.30.56.124: icmp_req=28 ttl=64 time=0.803 ms
64 bytes from 10.30.56.124: icmp_req=29 ttl=64 time=0.560 ms
64 bytes from 10.30.56.124: icmp_req=30 ttl=64 time=0.711 ms
64 bytes from 10.30.56.124: icmp_req=31 ttl=64 time=0.707 ms
64 bytes from 10.30.56.124: icmp_req=32 ttl=64 time=0.653 ms
^C
--- 10.30.56.124 ping statistics ---
32 packets transmitted, 32 received, 0% packet loss, time 31002ms
rtt min/avg/max/mdev = 0.311/0.682/1.382/0.174 ms
```

Table is stored

No.	Time	Source	Destination	Protocol	Length	Info
43	31.579837	Extreme-EEP	Extreme-EDP	EDP	338	EDP: Info Display
44	31.698023	10.30.56.125	224.0.0.251	MDNS	129	Standard query A system-of-a-down.local, "OM" question SRV amalji@system-of-a-down.local
45	31.696485	10.30.56.102	224.0.0.251	MDNS	181	Standard query response SRV, cache flush 0 0 5298 system-of-a-down.local AAAA, cache
46	31.741829	74.125.236.132	10.30.56.103	TLSv1	147	Application Data
47	31.741849	10.30.56.103	74.125.236.132	TCP	66	50248 > https [ACK] Seq=1 Ack=419 Win=331 Len=0 TSval=1752723 TSecr=33659230
48	32.257527	Cisco 7f:1b:2e	Spanning-tree-(for-br)STP	Spanning-tree-(for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x002e
49	33.842282	88:51:fb:42:80:84	Broadcast	ARP	42	Who has 10.30.56.124? Tell 10.30.56.103
50	33.842949	6c:3b:e5:3e:0a:44	88:51:fb:42:80:84	ARP	60	10.30.56.124 is at 6c:3b:e5:3e:0a:44
51	33.842961	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x16ea, seq=1/256, ttl=64
52	33.843640	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x16ea, seq=1/256, ttl=64
53	34.257531	Cisco 7f:1b:2e	Spanning-tree-(for-br)STP	Spanning-tree-(for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x002e
54	34.428223	10.30.56.103	74.125.236.117	TLSv1	103	Application Data
55	34.522144	74.125.236.117	10.30.56.103	TLSv1	103	Application Data
56	34.522172	10.30.56.103	74.125.236.117	TCP	66	33878 > https [ACK] Seq=38 Ack=38 Win=331 Len=0 TSval=1753418 TSecr=38275783
57	34.843770	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x16ea, seq=2/512, ttl=64
58	34.844491	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x16ea, seq=2/512, ttl=64
59	35.844607	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x16ea, seq=3/768, ttl=64
60	35.845201	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x16ea, seq=3/768, ttl=64
61	36.257419	Cisco 7f:1b:2e	Spanning-tree-(for-br)STP	Spanning-tree-(for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x002e
62	36.844645	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x16ea, seq=4/1024, ttl=64
63	36.845354	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x16ea, seq=4/1024, ttl=64
64	37.844623	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x16ea, seq=5/1280, ttl=64
65	37.845181	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x16ea, seq=5/1280, ttl=64

5) capturing network packets by pinging with google.com
ping google.com

```
jennie@ameyavp:~$ ping google.com
PING google.com (74.125.236.97) 56(84) bytes of data:
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=1 ttl=56 time=9
2.8 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=2 ttl=56 time=8
8.2 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=3 ttl=56 time=94.5 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=4 ttl=56 time=88.1 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=5 ttl=56 time=119 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=6 ttl=56 time=95.0 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=7 ttl=56 time=111 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=8 ttl=56 time=93.0 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=9 ttl=56 time=134 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=10 ttl=56 time=88.5 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=11 ttl=56 time=92.9 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=12 ttl=56 time=132 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=13 ttl=56 time=154 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=14 ttl=56 time=156 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=15 ttl=56 time=149 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=16 ttl=56 time=176 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=17 ttl=56 time=97.5 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=18 ttl=56 time=142 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=19 ttl=56 time=122 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=20 ttl=56 time=107 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=21 ttl=56 time=96.5 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=22 ttl=56 time=155 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=23 ttl=56 time=143 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=24 ttl=56 time=155 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=26 ttl=56 time=150 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=27 ttl=56 time=148 ms
64 bytes from bom03s01-in-f1.1e100.net (74.125.236.97): icmp_req=28 ttl=56 time=103 ms
^C
--- google.com ping statistics ---
28 packets transmitted, 27 received, 3% packet loss, time 27043ms
rtt min/avg/max/mdev = 88.118/121.948/176.667/27.358 ms
jennie@ameyavp:~$
```

Table is stored.

No.	Time	Source	Destination	Protocol	Length	Info
6	3.992393	Cisco 7f:1b:2e	Spanning-tree (for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
9	5.992551	Cisco 7f:1b:2e	Spanning-tree (for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
10	7.992426	Cisco 7f:1b:2e	Spanning-tree (for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
11	8.511595	10.30.56.103	8.8.8.8	DNS	70	Standard query A google.com
12	8.649140	8.8.8.8	10.30.56.103	DNS	246	Standard query response A 74.125.236.97 A 74.125.236.98 A 74.125.236.110 A 74.125.236.111
13	8.649568	10.30.56.103	74.125.236.97	ICMP	98	Echo (ping) request id=0x1759, seq=1/256, ttl=64
14	8.733405	74.125.236.97	10.30.56.103	ICMP	98	Echo (ping) reply id=0x1759, seq=1/256, ttl=56
15	8.733643	10.30.56.103	8.8.8.8	DNS	86	Standard query PTR 97.236.125.74.in-addr.arpa
16	8.884050	8.8.8.8	10.30.56.103	DNS	124	Standard query response PTR bon03s01-in-f1.1e100.net
17	9.642046	10.30.56.103	74.125.236.97	ICMP	98	Echo (ping) request id=0x1759, seq=2/512, ttl=64
18	9.730321	74.125.236.97	10.30.56.103	ICMP	98	Echo (ping) reply id=0x1759, seq=2/512, ttl=56
19	9.730585	10.30.56.103	8.8.8.8	DNS	86	Standard query PTR 97.236.125.74.in-addr.arpa
20	9.840496	8.8.8.8	10.30.56.103	DNS	124	Standard query response PTR bon03s01-in-f1.1e100.net
21	9.992436	Cisco 7f:1b:2e	Spanning-tree (for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	
22	10.643516	10.30.56.103	74.125.236.97	ICMP	98	Echo (ping) request id=0x1759, seq=3/768, ttl=64
23	10.738028	74.125.236.97	10.30.56.103	ICMP	98	Echo (ping) reply id=0x1759, seq=3/768, ttl=56
24	10.738281	10.30.56.103	8.8.8.8	DNS	86	Standard query PTR 97.236.125.74.in-addr.arpa
25	10.835874	8.8.8.8	10.30.56.103	DNS	124	Standard query response PTR bon03s01-in-f1.1e100.net
26	11.644922	10.30.56.103	74.125.236.97	ICMP	98	Echo (ping) request id=0x1759, seq=4/1024, ttl=64
27	11.733023	74.125.236.97	10.30.56.103	ICMP	98	Echo (ping) reply id=0x1759, seq=4/1024, ttl=56
28	11.733263	10.30.56.103	8.8.8.8	DNS	86	Standard query PTR 97.236.125.74.in-addr.arpa
29	11.825610	8.8.8.8	10.30.56.103	DNS	124	Standard query response PTR bon03s01-in-f1.1e100.net
30	11.992355	Cisco 7f:1b:2e	Spanning-tree (for-br)STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e	

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Filter: IEEE 802.3 Ethernet

Logical-Link Control

```
0000 01 00 c2 00 00 00 00 ed 7f 1b 2e 00 26 42 42 .....6B8
0010 03 00 00 00 00 00 00 00 0c 31 65 a9 00 00 00 .....le....
0020 00 04 00 0f 00 0d ed 7f 1b 00 00 2e 01 00 14 00 .....
0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

6) Updated arp table.

```
jennie@ameyavp:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.124              ether    6c:3b:e5:3e:0a:44    C                      eth0
10.30.56.1                ether    00:1f:9d:f2:bc:c9    C                      eth0
jennie@ameyavp:~$
```