Networks Lab: Assignment #2

Swetha K V

AM.EN.P2CSN13024

Contents

Problem 1

Install wireshark to sniffer capture
Installed wireshark : sudo apt-get install wireshark
commands used : arp -n //to list arp table
Captured TCP/IP packets by pinging to google.com and 10.30.56.103

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~/024/Network$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
```

ping 10.30.56.103

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~/024/Network$ ping 10.30.56.103
PING 10.30.56.103 (10.30.56.103) 56(84) bytes of data.
64 bytes from 10.30.56.103: icmp_req=1 ttl=64 time=1.46 ms
64 bytes from 10.30.56.103: icmp_req=2 ttl=64 time=0.649 ms
64 bytes from 10.30.56.103: icmp_req=3 ttl=64 time=0.730 ms
64 bytes from 10.30.56.103: icmp_req=4 ttl=64 time=0.669 ms
^C
--- 10.30.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.649/0.877/1.460/0.337 ms
```

87	42.796702	8.8.8.8	10.30.56.124	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.55
88	44.442818	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
89	44.997623	74.125.236.132	10.30.56.124	TLSv1	147	Application Data
90	44.997644	10.30.56.124	74.125.236.132	TCP	66	40265 > https [ACK] Seq=1 Ack=325 Win=1345 Len=0 TSval=1632549 TSecr=32934353
91	46.442787	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
92	48.400032	10.30.56.124	74.125.236.118	TLSv1	103	Application Data
93	48.442788	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
94	48.506795	74.125.236.118	10.30.56.124	TLSv1	103	Application Data
95	48.506816	10.30.56.124	74.125.236.118	TCP	66	40443 > https [ACK] Seq=75 Ack=75 Win=345 Len=0 TSval=1633426 TSecr=37547525
96	49.100984	6c:3b:e5:3e:0a:44	Broadcast	ARP	42	Who has 10.30.56.103? Tell 10.30.56.124
97	49.101738	88:51:fb:42:80:84	6c:3b:e5:3e:0a:44	ARP	60	10.30.56.103 is at 88:51:fb:42:80:84
98	49.101751	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) request id=0x0f2a, seq=1/256, ttl=64
99	49.102419	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f2a, seq=1/256, ttl=64
100	49.737550	10.30.56.104	10.30.59.255	NBNS	92	Name query NB WORKGROUP<1d>
101	50.102525	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) request id=0x0f2a, seq=2/512, ttl=64
102	50.103158	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f2a, seq=2/512, ttl=64
103	50.442786	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
104	51.103084	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) request id=0x0f2a, seq=3/768, ttl=64
105	51.103798	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f2a, seq=3/768, ttl=64
106	52.103088	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) request id=0x0f2a, seq=4/1024, ttl=64

ping google.com

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~/024/Network$ ping google.com
PING google.com (74.125.236.98) 56(84) bytes of data.
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=1 ttl=56 time=1
06 ms
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=2 ttl=56 time=9
4.4 ms
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=3 ttl=56 time=9
9.1 ms
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=5 ttl=56 time=9
3.8 ms
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=6 ttl=56 time=1
00 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 5013ms
rtt min/avg/max/mdev = 93.824/98.896/106.232/4.549 ms
```

34	8.218292	10.30.56.124	8.8.8.8	DNS	70	Standard query A google.com
35	8.348195	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x14af, seq=333/19713, ttl=64
36	8.348218	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x14af, seq=333/19713, ttl=64
37	8.427156	8.8.8.8	10.30.56.124	DNS	246	Standard query response A 74.125.236.98 A 74.125.236.105 A 74.125.236.102 A 74.125.
38	8.427628	10.30.56.124	74.125.236.98	ICMP	98	Echo (ping) request id=0x0f9d, seq=1/256, ttl=64
39	8.605670	74.125.236.98	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f9d, seq=1/256, ttl=56
40	8.605951	10.30.56.124	8.8.8.8	DNS	86	Standard query PTR 98.236.125.74.in-addr.arpa
41	8.723742	8.8.8.8	10.30.56.124	DNS	124	Standard query response PTR bom03s01-in-f2.1e100.net
42	9.348250	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x14af, seq=334/19969, ttl=64
43	9.348274	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x14af, seq=334/19969, ttl=64
44	9.428671	10.30.56.124	74.125.236.98	ICMP	98	Echo (ping) request id=0x0f9d, seq=2/512, ttl=64
45	9.521406	74.125.236.98	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f9d, seq=2/512, ttl=56
46	9.521659	10.30.56.124	8.8.8.8	DNS	86	Standard query PTR 98.236.125.74.in-addr.arpa
47	9.616363	8.8.8.8	10.30.56.124	DNS	124	Standard query response PTR bom03s01-in-f2.1e100.net
48	10.003946	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
49	10.348138	10.30.56.103	10.30.56.124	ICMP	98	Echo (ping) request id=0x14af, seq=335/20225, ttl=64
50	10.348160	10.30.56.124	10.30.56.103	ICMP	98	Echo (ping) reply id=0x14af, seq=335/20225, ttl=64
51	10.430350	10.30.56.124	74.125.236.98	ICMP	98	Echo (ping) request id=0x0f9d, seq=3/768, ttl=64
52	10.593771	74.125.236.98	10.30.56.124	ICMP	98	Echo (ping) reply id=0x0f9d, seq=3/768, ttl=56
53	10.594022	10.30.56.124	8.8.8.8	DNS	86	Standard query PTR 98.236.125.74.in-addr.arpa
54	10.753249	8.8.8.8	10.30.56.124	DNS	124	Standard query response PTR bom03s01-in-f2.1e100.net