Advanced Computer Networks: Assignment #2

Praveen. S

Contents

Problem 1

1.Install sniffer capture tool sniff packets while pinging an IP address. Ensure ARP table is empty before pinging. Analyse the output save the file.
Installed Wireshark.
Commands: $ arp -n *To list ARP table*
$ arp -a -d ipaddress *To delete the entry from the ARP cache*

```
praveen@Praveen:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.125                     (incomplete)                              eth1
10.30.56.117                     (incomplete)                              eth1
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth1
praveen@Praveen:~$
```

Launch Wireshark
Command: $ sudo wireshark
Start capturing packets & ping the ipaddress
Command: $ ping ipaddress

```
praveen@Praveen:~$ ping 10.30.56.125
PING 10.30.56.125 (10.30.56.125) 56(84) bytes of data.
64 bytes from 10.30.56.125: icmp_req=1 ttl=64 time=1.31 ms
64 bytes from 10.30.56.125: icmp_req=2 ttl=64 time=0.556 ms
64 bytes from 10.30.56.125: icmp_req=3 ttl=64 time=0.773 ms
64 bytes from 10.30.56.125: icmp_req=4 ttl=64 time=0.557 ms
64 bytes from 10.30.56.125: icmp_req=5 ttl=64 time=0.743 ms
64 bytes from 10.30.56.125: icmp_req=6 ttl=64 time=0.573 ms
^Z
[4]+  Stopped                 ping 10.30.56.125
praveen@Praveen:~$
```

Stop capturing packets save the file

No.	Time	Source	Destination	Protocol	Length	Info
35	50.004523	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
36	52.006747	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
37	53.819753	6c:3b:e5:3e:0a:cc	Broadcast	ARP	42	Who has 10.30.56.125? Tell 10.30.56.115
38	53.820484	88:51:fb:42:80:89	6c:3b:e5:3e:0a:cc	ARP	60	10.30.56.125 is at 88:51:fb:42:80:89
39	53.820496	10.30.56.115	10.30.56.125	ICMP	98	Echo (ping) request id=0x1484, seq=1/256, ttl=64
40	53.821178	10.30.56.125	10.30.56.115	ICMP	98	Echo (ping) reply id=0x1484, seq=1/256, ttl=64
41	54.004325	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
42	54.821316	10.30.56.115	10.30.56.125	ICMP	98	Echo (ping) request id=0x1484, seq=2/512, ttl=64
43	54.821922	10.30.56.125	10.30.56.115	ICMP	98	Echo (ping) reply id=0x1484, seq=2/512, ttl=64
44	56.004543	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
45	58.005826	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
46	58.138693	Cisco_7f:1b:2e	CDP/VTP/DTP/PAgP/UDLD	CDP	404	Device ID: SW3.CY-FO.AMP1.amrita.edu Port ID: FastEthernet0/46
47	58.832684	88:51:fb:42:80:89	6c:3b:e5:3e:0a:cc	ARP	60	Who has 10.30.56.115? Tell 10.30.56.125

Check the ARP table and see if its updated.

```
praveen@Praveen:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.125             ether   88:51:fb:42:80:89   C                     eth1
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth1
praveen@Praveen:~$
```

Problem 2

2. Using sniffer capture analyse the output and save the file when pinging www.google.com
Launch Wireshark start capturing packets.
Ping www.google.com Command: $ ping www.google.com

```
praveen@Praveen:~$ ping www.google.com
PING www.google.com (74.125.236.116) 56(84) bytes of data.
64 bytes from bom03s01-in-f20.1e100.net (74.125.236.116): icmp_req=1 ttl=56 time=7
3.9 ms
64 bytes from bom03s01-in-f20.1e100.net (74.125.236.116): icmp_req=2 ttl=56 time=8
5.5 ms
^Z
[1]+  Stopped                 ping www.google.com
praveen@Praveen:~$ ping www.google.com
PING www.google.com (74.125.236.114) 56(84) bytes of data.
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=1 ttl=56 time=5
9.1 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=2 ttl=56 time=6
0.3 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=3 ttl=56 time=5
4.5 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=4 ttl=56 time=5
8.8 ms
64 bytes from bom03s01-in-f18.1e100.net (74.125.236.114): icmp_req=5 ttl=56 time=5
5.2 ms
^Z
[2]+  Stopped                 ping www.google.com
praveen@Praveen:~$
```

Stop capturing packets save the file

No.	Time	Source	Destination	Protocol	Length	Info
17	18.617807	8.8.8.8	10.30.56.115	DNS	154	Standard query response A 74.125.236.116 A 74.125.236.113 A 74.125.236.112 A 74.125.236.114
18	18.618263	10.30.56.115	74.125.236.116	ICMP	98	Echo (ping) request id=0x09dd, seq=1/256, ttl=64
19	18.692170	74.125.236.116	10.30.56.115	ICMP	98	Echo (ping) reply id=0x09dd, seq=1/256, ttl=56
20	18.692453	10.30.56.115	8.8.8.8	DNS	87	Standard query PTR 116.236.125.74.in-addr.arpa
21	18.803423	8.8.8.8	10.30.56.115	DNS	126	Standard query response PTR bom03s01-in-f20.1e100.net
22	19.618471	10.30.56.115	74.125.236.116	ICMP	98	Echo (ping) request id=0x09dd, seq=2/512, ttl=64
23	19.703953	74.125.236.116	10.30.56.115	ICMP	98	Echo (ping) reply id=0x09dd, seq=2/512, ttl=56
24	19.704212	10.30.56.115	8.8.8.8	DNS	87	Standard query PTR 116.236.125.74.in-addr.arpa
25	19.804556	8.8.8.8	10.30.56.115	DNS	126	Standard query response PTR bom03s01-in-f20.1e100.net
26	19.809826	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
27	20.618595	10.30.56.115	74.125.236.116	ICMP	98	Echo (ping) request id=0x09dd, seq=3/768, ttl=64
28	20.716598	74.125.236.116	10.30.56.115	ICMP	98	Echo (ping) reply id=0x09dd, seq=3/768, ttl=56
29	20.716831	10.30.56.115	8.8.8.8	DNS	87	Standard query PTR 116.236.125.74.in-addr.arpa
30	20.864004	8.8.8.8	10.30.56.115	DNS	126	Standard query response PTR bom03s01-in-f20.1e100.net
31	21.810771	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e