Advanced computer networks: Assignment #2

Sreedhar R

Contents

Problem 1

Install sniffer capture and sniff packets when pinging a pingable ip address. Ensure that the ARP table is empty before pinging

Ans:

$ sudo arp -a -d 10.30.56.102 //To erase details of ip 10.30.56.102 from ARP table

$ arp -n //To display ARP table

```
sree@sree2612:~$ sudo arp -a -d 10.30.56.102
[sudo] password for sree:
sree@sree2612:~$ arp -n
Address             HWtype  HWaddress           Flags Mask       Iface
10.30.56.102                (incomplete)                         eth0
         Kate       ether   00:1f:9d:f2:bc:c9   C                eth0
                    ether   88:51:fb:42:80:89   C                eth0
```

$ ping 10.30.56.102

```
sree@sree2612:~$ ping 10.30.56.102
PING 10.30.56.102 (10.30.56.102) 56(84) bytes of data.
64 bytes from 10.30.56.102: icmp_req=1 ttl=64 time=1.44 ms
64 bytes from 10.30.56.102: icmp_req=2 ttl=64 time=0.569 ms
^C
```

output:

| 36 | 42.098034 | 6c:3b:e5:3d:90:08 | Broadcast | ARP | 42 | Who has 10.30.56.102? Tell 10.30.56.122 |
| 37 | 42.098695 | 88:51:fb:42:80:87 | 6c:3b:e5:3d:90:08 | ARP | 60 | 10.30.56.102 is at 88:51:fb:42:80:87 |

Problem 2

Using sniffer capture analyse the output when pinging google

$ 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=131 ms
64 bytes from bom03s01-in-f2.1e100.net (74.125.236.98): icmp_req=2 ttl=56 time=96.4 ms
^C
```

output:

13	13.998383	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	15.997949	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
15	17.997916	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
16	18.040605	10.30.56.122	8.8.8.8	DNS	70 Standard query A google.com
17	18.159220	8.8.8.8	10.30.56.122	DNS	246 Standard query response A 74.125.236.98 A 74.125.236.103 A 74.125.236.100
18	19.997824	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e
19	20.134211	Cisco_7f:1b:2e	CDP/VTP/DTP/PAgP/UDLD	CDP	404 Device ID: SW3.CY-FO.AMP1.amrita.edu Port ID: FastEthernet0/46
20	21.998690	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port = 0x802e