

CS620:Advanced Computer Networks : Assignment 2

Lakshmi Devi K

Contents

Problem 1	3
Problem 2	4

Problem 1

Ping a local ip address and analyse the sniffer capture using wireshark.

Steps: 1)Clear the arp table

```

lakshmi@lakshmi:~$ arp -n
Address                  HWtype  HWaddress          Flags Mask  Iface
10.30.56.1                ether    00:1f:9d:f2:bc:c9  C           eth0
lakshmi@lakshmi:~$ sudo ip -s -s neigh flush all
[sudo] password for lakshmi:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 17 used 32/32/8 probes 1 STALE
*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
lakshmi@lakshmi:~$

```

2)start the wireshark sniffer analyser by typing the command sudo wireshark in the terminal. 3)start the capture session 4)Open the terminal and type the command ping 10.30.56.107(any local ip address) 5)check the arp table in the wildshark.

```

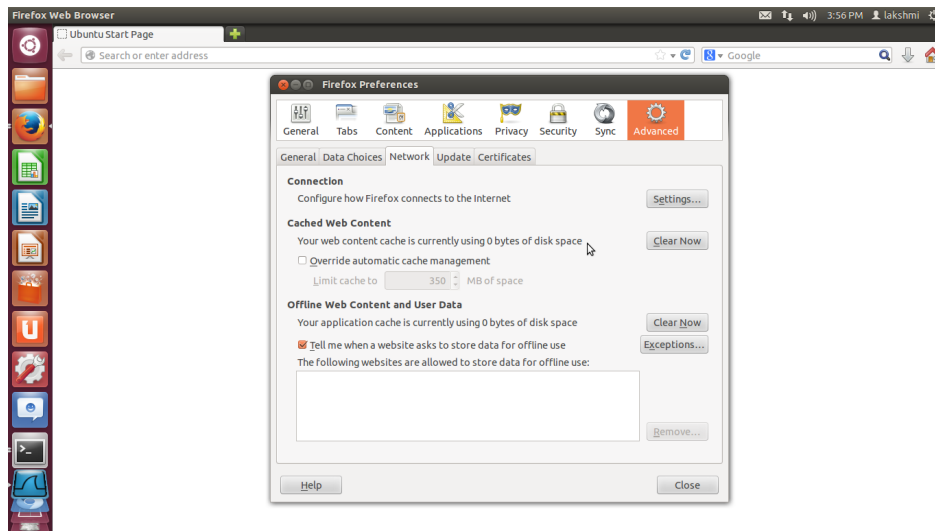
Capturing from eth0 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
20 15.586865 10.30.56.101 10.30.56.112 ICMP 98 Echo (ping) reply id=0x8942, seq=3/788, ttl=64
21 15.998655 Cisco 7f:1b:2e Spanning-tree-(for-br)STP 60 Conf. Root = 32768/15/00-8c:31:65-a9-00 Cost = 4 Port = 0x802e
22 16.585329 10.30.56.112 10.30.56.101 ICMP 98 Echo (ping) request id=0x8942, seq=4/1024, ttl=64
23 16.585884 10.30.56.101 10.30.56.112 ICMP 98 Echo (ping) reply id=0x8942, seq=4/1024, ttl=64
24 16.737285 HewlettP f8:ca:b0 Cisco f2:bc:c9 ARP 42 Who has 10.30.56.1? Tell 10.30.56.112
25 16.738432 Cisco f2:bc:c9 HewlettP f8:ca:b0 ARP 60 10.30.56.1 is at 00:1f:9d:f2:bc:c9
26 17.585385 10.30.56.112 10.30.56.101 ICMP 98 Echo (ping) request id=0x8942, seq=5/1280, ttl=64
27 17.585715 10.30.56.101 10.30.56.112 ICMP 98 Echo (ping) reply id=0x8942, seq=5/1280, ttl=64
28 17.998680 Cisco 7f:1b:2e Spanning-tree-(for-br)STP 60 Conf. Root = 32768/15/00-8c:31:65-a9-00 Cost = 4 Port = 0x802e
29 18.585392 10.30.56.112 10.30.56.101 ICMP 98 Echo (ping) request id=0x8942, seq=6/1536, ttl=64
30 18.585998 10.30.56.101 10.30.56.112 ICMP 98 Echo (ping) reply id=0x8942, seq=6/1536, ttl=64
31 18.586919 88:51:fb:42:80:72 HewlettP f8:ca:b0 ARP 60 Who has 10.30.56.112? Tell 10.30.56.101
32 18.586932 HewlettP f8:ca:b0 88:51:fb:42:80:72 ARP 42 10.30.56.112 is at 00:b3:cc:f8:ca:b0
* Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
* IEEE 802.3 Ethernet
* Logical-Link Control
* Spanning Tree Protocol
0000 01 00 c2 00 00 00 0d ed 7f 1b 2e 00 26 42 42 .....680
0010 03 00 00 00 00 00 0f 00 0c 31 65 a9 00 00 00 .....le...
0020 00 04 80 0f 00 0d ed 7f 1b 00 80 2e 01 00 14 00 .....
0030 02 00 0f 00 00 00 00 00 00 00 00

```

Problem 2

ping google.com and analyse the sniffer capture.

Steps: 1)clear the browser cache



2)Start the capture session in wireshark.In terminal,type ping google.com.Check the arp table .

