

Advanced Computer Networks: Assignment #2

ARCHANA B S

Contents

| | |
|------------------|----------|
| Problem 1 | 3 |
| Problem 2 | 5 |
| Problem 3 | 7 |

Problem 1

SNIFFER CAPTURE : LOCAL IP

Install wireshark. Start sniffing packets. Ping IP. Analyze. Save file.

Clear the ARP table.

Commands : arp -n

sudo ip -s -s neigh flush all

PING to Ip.

```
archana@archana-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  Hwtype  Hwaddress    Flags Mask          Iface
10.30.56.1                ether   08:1f:9d:f2:bc:c9    C
archana@archana-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
10.30.56.1 dev eth0 lladdr 08:1f:9d:f2:bc:c9 ref 44 used 8/5/8 probes 4 REACHABLE
*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
archana@archana-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  Hwtype  Hwaddress    Flags Mask          Iface
10.30.56.1                (incomplete)
archana@archana-HP-Compaq-Pro-6300-MT:~$ ping 10.30.56.123
PING 10.30.56.123 (10.30.56.123) 56(84) bytes of data:
64 bytes from 10.30.56.123: icmp_req=1 ttl=64 time=1.31 ms
64 bytes from 10.30.56.123: icmp_req=2 ttl=64 time=0.739 ms
64 bytes from 10.30.56.123: icmp_req=3 ttl=64 time=0.591 ms
64 bytes from 10.30.56.123: icmp_req=4 ttl=64 time=0.569 ms
64 bytes from 10.30.56.123: icmp_req=5 ttl=64 time=0.747 ms
64 bytes from 10.30.56.123: icmp_req=6 ttl=64 time=0.758 ms
64 bytes from 10.30.56.123: icmp_req=7 ttl=64 time=0.729 ms
^C
--- 10.30.56.123 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 600ms
rtt min/avg/max/mdev = 0.569/0.777/1.312/0.232 ms
archana@archana-HP-Compaq-Pro-6300-MT:~$
```

Screenshots from WIRESHARK.

eth0 [Wireshark 1.6.7]

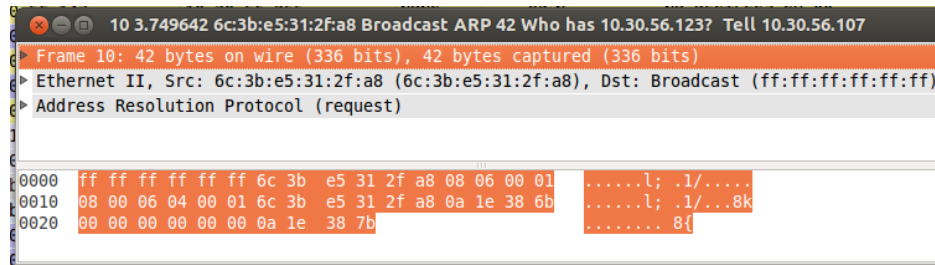
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------------|-------------------|----------|--------|--|
| 4 | 3.346445 | 10.30.56.107 | 173.194.36.22 | TLSv1 | 175 | Application Data |
| 5 | 3.408797 | 173.194.36.22 | 10.30.56.107 | TCP | 66 | https > 49465 [ACK] Seq=1 Ack=1419 Win=1115 Len=0 TSval=656654893 TSecr=5470487 |
| 6 | 3.408809 | 173.194.36.22 | 10.30.56.107 | TCP | 66 | https > 49465 [ACK] Seq=1 Ack=2071 Win=1115 Len=0 TSval=656654893 TSecr=5470487 |
| 7 | 3.401878 | 173.194.36.22 | 10.30.56.107 | TCP | 66 | https > 49465 [ACK] Seq=1 Ack=2180 Win=1115 Len=0 TSval=656654893 TSecr=5470487 |
| 8 | 3.413758 | 6c:3b:e5:31:2f:a8 | Broadcast | ARP | 42 | Who has 10.30.56.123? Tell 10.30.56.107 |
| 9 | 3.414339 | 6c:3b:e5:31:2f:a5 | 6c:3b:e5:31:2f:a8 | ARP | 60 | 10.30.56.123 is at 6c:3b:e5:31:2f:a5 |
| 10 | 3.414345 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=1/256, ttl=64 |
| 11 | 3.415057 | 10.30.56.123 | 10.30.56.107 | ICMP | 98 | Echo (ping) reply id=0x1328, seq=1/256, ttl=64 |
| 12 | 3.797486 | 173.194.36.22 | 10.30.56.107 | TLSv1 | 534 | Application Data |
| 13 | 3.797504 | 173.194.36.22 | 10.30.56.107 | TLSv1 | 109 | Application Data |
| 14 | 3.797508 | 173.194.36.22 | 10.30.56.107 | TLSv1 | 122 | Application Data |
| 15 | 3.797510 | 173.194.36.22 | 10.30.56.107 | TLSv1 | 99 | Application Data |
| 16 | 3.797675 | 10.30.56.107 | 173.194.36.22 | TCP | 66 | 49465 > https [ACK] Seq=2180 Ack=601 Win=613 Len=0 TSval=5470600 TSecr=656655289 |
| 17 | 4.415129 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=2/512, ttl=64 |
| 18 | 4.415856 | 10.30.56.123 | 10.30.56.107 | ICMP | 98 | Echo (ping) reply id=0x1328, seq=2/512, ttl=64 |
| 19 | 5.415604 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=3/768, ttl=64 |
| 20 | 5.416378 | 10.30.56.123 | 10.30.56.107 | ICMP | 98 | Echo (ping) reply id=0x1328, seq=3/768, ttl=64 |
| 21 | 6.415657 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=4/1024, ttl=64 |
| 22 | 6.416204 | 10.30.56.123 | 10.30.56.107 | ICMP | 98 | Echo (ping) reply id=0x1328, seq=4/1024, ttl=64 |
| 23 | 7.415605 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=5/1280, ttl=64 |
| 24 | 7.416337 | 10.30.56.123 | 10.30.56.107 | ICMP | 98 | Echo (ping) reply id=0x1328, seq=5/1280, ttl=64 |
| 25 | 8.415602 | 10.30.56.107 | 10.30.56.123 | ICMP | 98 | Echo (ping) request id=0x1328, seq=6/1536, ttl=64 |

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on eth0
 Ethernet II, Src: 6c:3b:e5:31:2f:a5 (6c:3b:e5:31:2f:a5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 6c 3b e5 31 2f a5 08 06 00 01:./1/.....
 0010 00 00 00 00 00 01 6c 3b e5 31 2f a5 0a 1e 38 7b:./1/...8(
 0020 00 00 00 00 00 0a 1e 38 01 00 00 00 00 00 008.....
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 archana@archana-HP-Compaq-Pro-6300-MT:~\$



Problem 2

SNIFFER CAPTURE :PING 4.2.2.1.

Open sniffer capture. Ping 4.2.2.1 Save file.

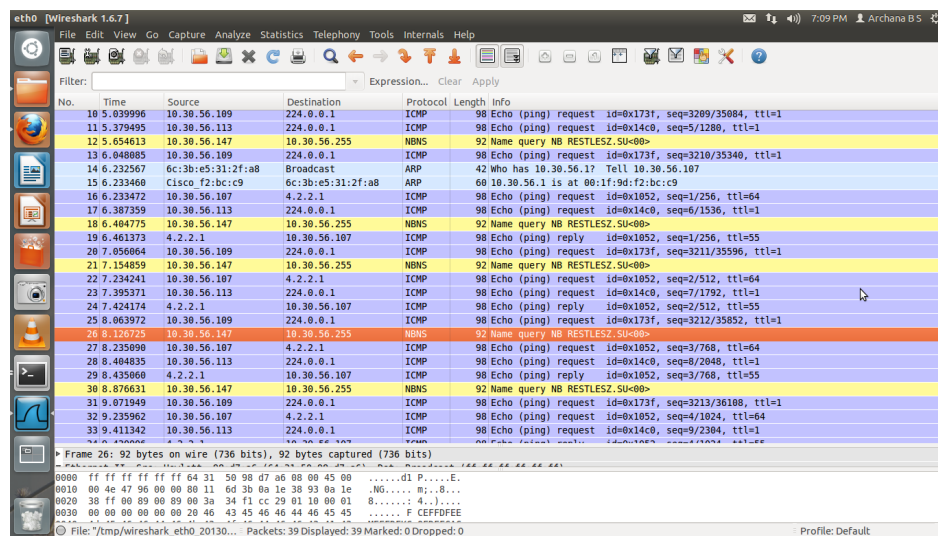
Clear arp.

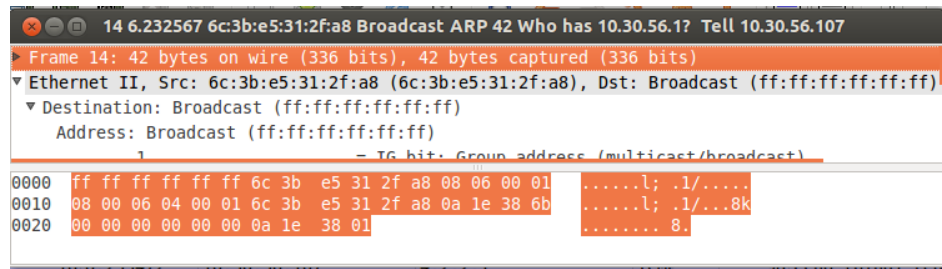
PING 4.2.2.1

```
archana@archana-HP-Compaq-Pro-6300-MT: ~
archana@archana-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1                (incomplete)
archana@archana-HP-Compaq-Pro-6300-MT:~$ ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1) 56(84) bytes of data.
64 bytes from 4.2.2.1: icmp_req=1 ttl=55 time=211 ms
64 bytes from 4.2.2.1: icmp_req=2 ttl=55 time=211 ms
64 bytes from 4.2.2.1: icmp_req=3 ttl=55 time=186 ms
64 bytes from 4.2.2.1: icmp_req=4 ttl=55 time=189 ms
^C
--- 4.2.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 186.910/199.900/211.630/11.757 ms
archana@archana-HP-Compaq-Pro-6300-MT:~$ clear

archana@archana-HP-Compaq-Pro-6300-MT:~$ clear
```

Screenshots from WIRESHARK.





Problem 3

SNIFFER CAPTURE : MULTICAST
PING 224.0.0.1

Screenshots from WIRESHARK.

The screenshot displays the Wireshark 1.6.7 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The packet list pane shows a series of ICMP Echo (ping) requests and responses. The packet details pane for frame 23 shows an Ethernet II frame with destination IPv4multicast_00:00:01 (01:00:5e:00:00:01) and source 6c:3b:e5:31:2f:a8 (6c:3b:e5:31:2f:a8). The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|--------------------------------|--------------------------------|----------|--------|--|
| 4 | 3.292266 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=1/256, ttl=1 |
| 5 | 3.564599 | 10.30.56.147 | 10.30.56.255 | NBNS | 92 | Name query NB RESTLESZ.SU<00> |
| 6 | 4.292183 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=2/512, ttl=1 |
| 7 | 4.314922 | 10.30.56.147 | 10.30.56.255 | NBNS | 92 | Name query NB RESTLESZ.SU<00> |
| 8 | 5.292201 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=3/768, ttl=1 |
| 9 | 6.292184 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=4/1024, ttl=1 |
| 10 | 7.292180 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=5/1280, ttl=1 |
| 11 | 8.271008 | 10.30.56.147 | 10.30.56.255 | NBNS | 92 | Name query NB DEVICESTA.RU<00> |
| 12 | 8.292175 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=6/1536, ttl=1 |
| 13 | 9.021419 | 10.30.56.147 | 10.30.56.255 | NBNS | 92 | Name query NB DEVICESTA.RU<00> |
| 14 | 9.292156 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=7/1792, ttl=1 |
| 15 | 9.771663 | 10.30.56.147 | 10.30.56.255 | NBNS | 92 | Name query NB DEVICESTA.RU<00> |
| 16 | 10.292179 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=8/2048, ttl=1 |
| 17 | 11.292154 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=9/2304, ttl=1 |
| 18 | 12.292183 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=10/2560, ttl=1 |
| 19 | 13.210526 | fe80::6e3b:e5ff:fe31::ff02::fb | fe80::8a51:fbff:fe42::ff02::fb | MDNS | 356 | Standard query response PTR touch-able.tcp.local PTR AB351678AB35.touch-able.tc |
| 20 | 13.217080 | fe80::8a51:fbff:fe42::ff02::fb | fe80::6e3b:e5ff:fe31::ff02::fb | MDNS | 186 | Standard query response PTR workstation.tcp.local PTR touch-able.tcp.local PTR |
| 21 | 13.217735 | 10.30.56.117 | 224.0.0.251 | ICMP | 332 | Standard query response PTR touch-ables.tcp.local PTR AB351678AB35.touch-able.tc |
| 22 | 13.224275 | 10.30.56.102 | 224.0.0.251 | MDNS | 166 | Standard query response PTR workstation.tcp.local PTR touch-able.tcp.local PTR |
| 23 | 13.292176 | 10.30.56.107 | 224.0.0.1 | ICMP | 98 | Echo (ping) request id=0x138e, seq=11/2816, ttl=1 |
| 24 | 13.806736 | 173.194.36.22 | 10.30.56.107 | TLSv1 | 121 | Application Data |
| 25 | 13.844123 | 10.30.56.107 | 173.194.36.22 | TCP | 66 | 49465 > https [ACK] Seq=1 Ack=56 Win=613 Len=0 TSval=5541000 TSecr=656936854 |

Frame 16: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 Ethernet II, Src: 6c:3b:e5:31:2f:a8 (6c:3b:e5:31:2f:a8), Dst: IPv4multicast_00:00:01 (01:00:5e:00:00:01)
 Destination: IPv4multicast_00:00:01 (01:00:5e:00:00:01)
 Source: 6c:3b:e5:31:2f:a8 (6c:3b:e5:31:2f:a8)
 Type: IP (0x0800)

```

0000 01 00 5e 00 00 01 6c 3b e5 31 2f a8 08 00 45 00  ..^...l; .1/...E.
0010 00 54 00 00 40 00 01 01 57 1f 0a 1e 38 6b e0 00  .T..@... W...8k..
0020 00 01 08 00 06 1b 13 8e 00 0b 41 a8 20 52 00 00  ....n... ..A. R..
0030 00 00 4f 7e 06 00 00 00 00 00 10 11 12 13 14 15  ..0~.....
  
```