

Networks Lab: Assignment #2

Swetha K V

AM.EN.P2CSN13024

Contents

Problem 1	3
-----------	---

Problem 1

Install wireshark to sniff capture

Installed wireshark : `sudo apt-get install wireshark`

commands used : `arp -n` //to list arp table

Captured TCP/IP packets by pinging to 10.30.56.103 and 4.2.2.1

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
[sudo] password for swe0523:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 65 used 29/29/6 probes 4 STALE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~$ arp -n
Address HWtype HWaddress Flags Mask Iface
10.30.56.1 (incomplete) eth0
10.30.56.112 (incomplete) eth0
10.30.56.103 (incomplete) eth0
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~$
```

ping 10.30.56.103

ping 4.2.2.1

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~$ 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=1.38 ms
64 bytes from 10.30.56.103: icmp_req=2 ttl=64 time=0.715 ms
64 bytes from 10.30.56.103: icmp_req=3 ttl=64 time=0.686 ms
64 bytes from 10.30.56.103: icmp_req=4 ttl=64 time=0.737 ms
^C
--- 10.30.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.686/0.880/1.385/0.293 ms
swe0523@swe0523-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=343 ms
64 bytes from 4.2.2.1: icmp_req=4 ttl=55 time=246 ms
64 bytes from 4.2.2.1: icmp_req=5 ttl=55 time=239 ms
^C
--- 4.2.2.1 ping statistics ---
6 packets transmitted, 3 received, 50% packet loss, time 5019ms
rtt min/avg/max/mdev = 239.700/276.827/343.930/47.538 ms
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~$
```

ping 224.0.0.1 // multicast

```
swe0523@swe0523-HP-Compaq-Pro-6300-MT:~/024/Network$ ping 224.0.0.1
PING 224.0.0.1 (224.0.0.1) 56(84) bytes of data.
^C
--- 224.0.0.1 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8062ms
```

8	3.024236	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request id=0x07fa, seq=43/11008, ttl=1
9	3.071058	10.30.56.108	10.30.59.255	NBNS	92 Name query NB WORKGROUP<id>
10	3.196068	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x122b, seq=1020/64515, ttl=1
11	4.032092	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request id=0x07fa, seq=44/11264, ttl=1
12	4.203978	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x122b, seq=1021/64771, ttl=1
13	5.040192	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request id=0x07fa, seq=45/11520, ttl=1
14	5.212055	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x122b, seq=1022/65027, ttl=1
15	5.700554	0c:3b:e5:3e:0a:44	Broadcast	ARP	42 Who has 10.30.56.103? Tell 10.30.56.124
16	5.787204	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
17	5.787217	10.30.56.124	10.30.56.103	ICMP	98 Echo (ping) request id=0x10c6, seq=1/256, ttl=64
18	5.787916	10.30.56.103	10.30.56.124	ICMP	98 Echo (ping) reply id=0x10c6, seq=1/256, ttl=64
19	6.048070	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request id=0x07fa, seq=46/11776, ttl=1
20	6.220015	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x122b, seq=1023/65283, ttl=1
21	6.234509	Hewlett- 98:d7:a6	Broadcast	ARP	60 Who has 10.30.56.1? Tell 10.30.56.147
22	6.788051	10.30.56.124	10.30.56.103	ICMP	98 Echo (ping) request id=0x10c6, seq=2/512, ttl=64
23	6.788744	10.30.56.103	10.30.56.124	ICMP	98 Echo (ping) reply id=0x10c6, seq=2/512, ttl=64
24	7.056130	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request id=0x07fa, seq=47/12032, ttl=1
25	7.093040	10.30.56.147	10.30.56.255	BROWSER	252 Domain/Workgroup Announcement IPINFUSION, NT Workstation, Domain Enum
26	7.228141	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request id=0x122b, seq=1024/4, ttl=1
27	7.788068	10.30.56.124	10.30.56.103	ICMP	98 Echo (ping) request id=0x10c6, seq=3/768, ttl=64
28	7.788730	10.30.56.103	10.30.56.124	ICMP	98 Echo (ping) reply id=0x10c6, seq=3/768, ttl=64

* Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 * Ethernet II, Src: 6c:3b:e5:3e:0a:44 (6c:3b:e5:3e:0a:44), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 * Address Resolution Protocol (request)

14	4.232529	10.30.56.124	4.2.2.1	ICMP	98 Echo (ping) request	id=0x10eb, seq=3/768, ttl=64
15	5.040894	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=154/39424, ttl=1
16	5.211269	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1131/27396, ttl=1
17	5.240527	10.30.56.124	4.2.2.1	ICMP	98 Echo (ping) request	id=0x10eb, seq=4/1024, ttl=64
18	5.487363	4.2.2.1	10.30.56.124	ICMP	98 Echo (ping) reply	id=0x10eb, seq=4/1024, ttl=55
19	6.048227	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=155/39680, ttl=1
20	6.219884	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1132/27652, ttl=1
21	6.242236	10.30.56.124	4.2.2.1	ICMP	98 Echo (ping) request	id=0x10eb, seq=5/1280, ttl=64
22	6.481923	4.2.2.1	10.30.56.124	ICMP	98 Echo (ping) reply	id=0x10eb, seq=5/1280, ttl=55
23	7.056200	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=156/39936, ttl=1
24	7.227255	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1133/27980, ttl=1
25	7.243800	10.30.56.124	4.2.2.1	ICMP	98 Echo (ping) request	id=0x10eb, seq=6/1536, ttl=64
26	7.536771	4.2.2.1	10.30.56.124	ICMP	98 Echo (ping) reply	id=0x10eb, seq=6/1536, ttl=55
27	8.064284	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=157/40192, ttl=1
28	8.235240	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1134/28164, ttl=1
29	9.072502	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=158/40448, ttl=1
30	9.243358	10.30.56.115	224.0.0.1	ICMP	98 Echo (ping) request	id=0x122b, seq=1135/28420, ttl=1
Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)						
Ethernet II, Src: 6c:3b:e5:3e:0a:44 (6c:3b:e5:3e:0a:44), Dst: Cisco_f2:bc:c9 (00:1f:9d:f2:bc:c9)						
Internet Protocol Version 4, Src: 10.30.56.124 (10.30.56.124), Dst: 4.2.2.1 (4.2.2.1)						
TCP, Seq=155, Win=0, Len=0						
0000 00 1f 9d f2 bc c9 6c 3b e5 3e 0a 44 00 00 45 00l; .>.D..E..						
0010 00 54 00 00 40 00 40 01 f2 0c 0a 1e 38 7c 04 02 ..T..@.8]..						
0020 02 01 08 00 06 ef 10 eb 00 05 df 91 20 52 00 00 R...						
0030 00 00 00 00 00 00 00 00 00 00 11 12 13 14 15						

29	11.546496	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=2/512, ttl=1
30	12.094888	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=990/56835, ttl=1
31	12.518560	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=563/13058, ttl=1
32	12.554476	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=3/768, ttl=1
33	13.102825	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=991/57091, ttl=1
34	13.526471	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=564/13314, ttl=1
35	13.562452	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=4/1024, ttl=1
36	14.110993	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=992/57347, ttl=1
37	14.534462	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=565/13570, ttl=1
38	14.578464	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=5/1280, ttl=1
39	15.119645	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=993/57603, ttl=1
40	15.542492	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=566/13826, ttl=1
41	15.578479	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=6/1536, ttl=1
42	16.126949	10.30.56.114	224.0.0.1	ICMP	98 Echo (ping) request	id=0x0f7a, seq=994/57859, ttl=1
43	16.550390	10.30.56.109	224.0.0.1	ICMP	98 Echo (ping) request	id=0x173f, seq=567/14002, ttl=1
44	16.586463	10.30.56.124	224.0.0.1	ICMP	98 Echo (ping) request	id=0x11b6, seq=7/1792, ttl=1