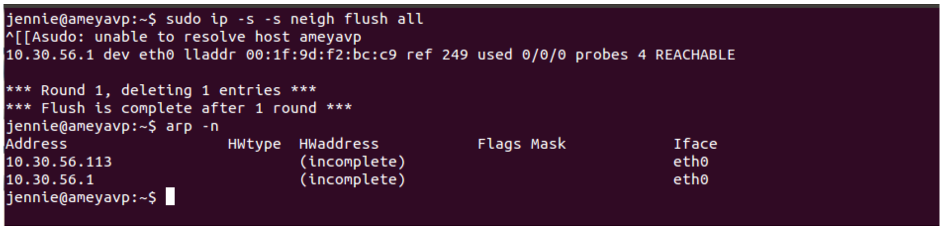
ADVANCED COMPUTER NETWORKS - LAB: ASSIGNMENT 2

Ameya V P

AM.EN.P2CSN13003

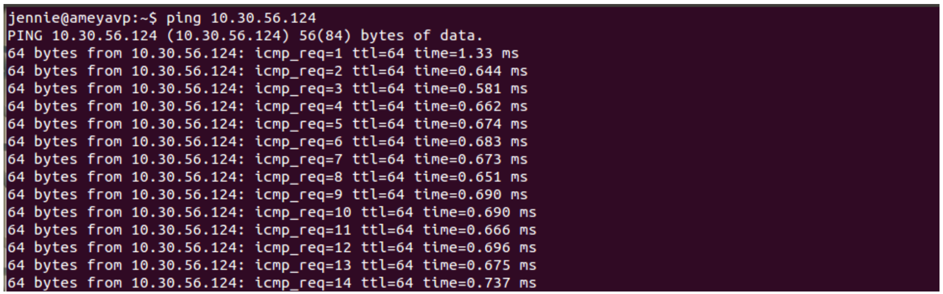
Problem 1

1. Install wireshark to sniffer capture
Wireshark is a open source network packet analyzer. It is used for netwrok troubleshooting and analysis.
1) command used : sudo apt-get install wireshark
Installed wireshark
2) sudo wireshark
Run wireshark for capturing packets.
3) sudo ip -s -s neigh flush all :to flush arp table
arp -n : to list arp table

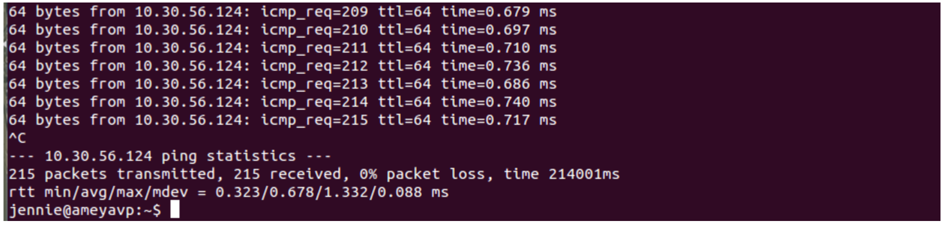


```
jennie@ameyavp:~$ sudo ip -s -s neigh flush all
^[[Asudo: unable to resolve host ameyavp
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 249 used 0/0/0 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
jennie@ameyavp:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.113                     (incomplete)                              eth0
10.30.56.1                       (incomplete)                              eth0
jennie@ameyavp:~$ 
```

4) ping a local machine :
ping 10.30.56.124

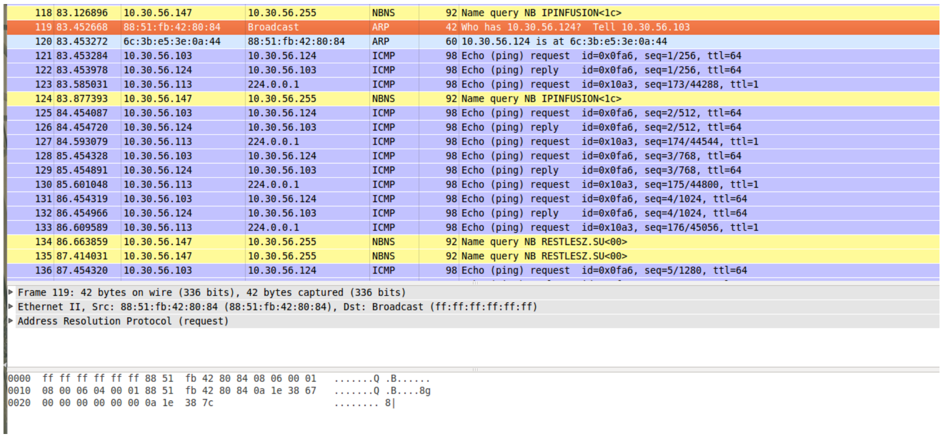


```
jennie@ameyavp:~$ ping 10.30.56.124
PING 10.30.56.124 (10.30.56.124) 56(84) bytes of data.
64 bytes from 10.30.56.124: icmp_req=1 ttl=64 time=1.33 ms
64 bytes from 10.30.56.124: icmp_req=2 ttl=64 time=0.644 ms
64 bytes from 10.30.56.124: icmp_req=3 ttl=64 time=0.581 ms
64 bytes from 10.30.56.124: icmp_req=4 ttl=64 time=0.662 ms
64 bytes from 10.30.56.124: icmp_req=5 ttl=64 time=0.674 ms
64 bytes from 10.30.56.124: icmp_req=6 ttl=64 time=0.683 ms
64 bytes from 10.30.56.124: icmp_req=7 ttl=64 time=0.673 ms
64 bytes from 10.30.56.124: icmp_req=8 ttl=64 time=0.651 ms
64 bytes from 10.30.56.124: icmp_req=9 ttl=64 time=0.690 ms
64 bytes from 10.30.56.124: icmp_req=10 ttl=64 time=0.690 ms
64 bytes from 10.30.56.124: icmp_req=11 ttl=64 time=0.666 ms
64 bytes from 10.30.56.124: icmp_req=12 ttl=64 time=0.696 ms
64 bytes from 10.30.56.124: icmp_req=13 ttl=64 time=0.675 ms
64 bytes from 10.30.56.124: icmp_req=14 ttl=64 time=0.737 ms
```



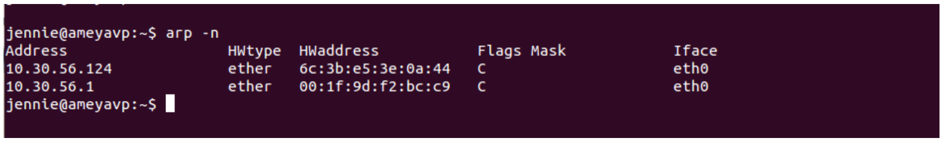
```
64 bytes from 10.30.56.124: icmp_req=209 ttl=64 time=0.679 ms
64 bytes from 10.30.56.124: icmp_req=210 ttl=64 time=0.697 ms
64 bytes from 10.30.56.124: icmp_req=211 ttl=64 time=0.710 ms
64 bytes from 10.30.56.124: icmp_req=212 ttl=64 time=0.736 ms
64 bytes from 10.30.56.124: icmp_req=213 ttl=64 time=0.686 ms
64 bytes from 10.30.56.124: icmp_req=214 ttl=64 time=0.740 ms
64 bytes from 10.30.56.124: icmp_req=215 ttl=64 time=0.717 ms
^C
--- 10.30.56.124 ping statistics ---
215 packets transmitted, 215 received, 0% packet loss, time 214001ms
rtt min/avg/max/mdev = 0.323/0.678/1.332/0.088 ms
jennie@ameyavp:~$ 
```

Table is stored



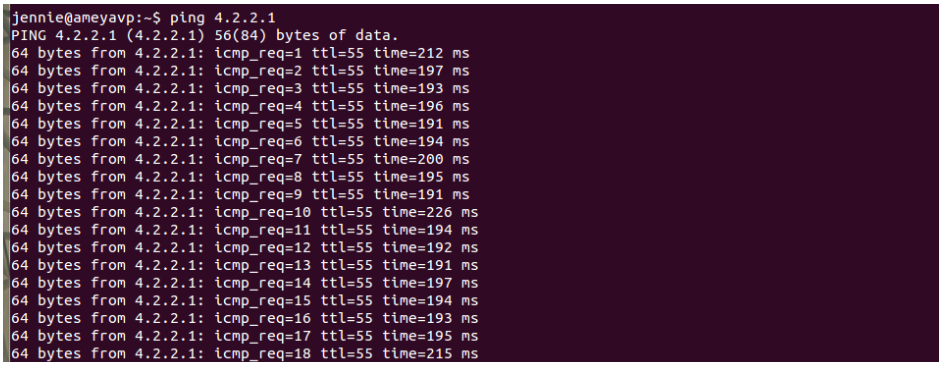
```
118 83.126896  10.30.56.147       10.30.56.255       NBNS   92 Name query NB IPINFUSION<1c>
119 83.452668  88:51:fb:42:80:84  Broadcast          ARP    42 Who has 10.30.56.124?  Tell 10.30.56.103
120 83.453272  6c:3b:e5:3e:0a:44  88:51:fb:42:80:84  ARP    60 10.30.56.124 is at 6c:3b:e5:3e:0a:44
121 83.453284  10.30.56.103       10.30.56.124       ICMP   98 Echo (ping) request  id=0x0fa6, seq=1/256, ttl=64
122 83.453978  10.30.56.124       10.30.56.103       ICMP   98 Echo (ping) reply    id=0x0fa6, seq=1/256, ttl=64
123 83.585031  10.30.56.113       224.0.0.1          ICMP   98 Echo (ping) request  id=0x10a3, seq=173/44288, ttl=1
124 83.877393  10.30.56.147       10.30.56.255       NBNS   92 Name query NB IPINFUSION<1c>
125 84.454087  10.30.56.103       10.30.56.124       ICMP   98 Echo (ping) request  id=0x0fa6, seq=2/512, ttl=64
126 84.454720  10.30.56.124       10.30.56.103       ICMP   98 Echo (ping) reply    id=0x0fa6, seq=2/512, ttl=64
127 84.593079  10.30.56.113       224.0.0.1          ICMP   98 Echo (ping) request  id=0x10a3, seq=174/44544, ttl=1
128 85.454328  10.30.56.103       10.30.56.124       ICMP   98 Echo (ping) request  id=0x0fa6, seq=3/768, ttl=64
129 85.454891  10.30.56.124       10.30.56.103       ICMP   98 Echo (ping) reply    id=0x0fa6, seq=3/768, ttl=64
130 85.601048  10.30.56.113       224.0.0.1          ICMP   98 Echo (ping) request  id=0x10a3, seq=175/44800, ttl=1
131 86.454319  10.30.56.103       10.30.56.124       ICMP   98 Echo (ping) request  id=0x0fa6, seq=4/1024, ttl=64
132 86.454966  10.30.56.124       10.30.56.103       ICMP   98 Echo (ping) reply    id=0x0fa6, seq=4/1024, ttl=64
133 86.609589  10.30.56.113       224.0.0.1          ICMP   98 Echo (ping) request  id=0x10a3, seq=176/45056, ttl=1
134 86.663859  10.30.56.147       10.30.56.255       NBNS   92 Name query NB RESTLESZ.SU<00>
135 87.414031  10.30.56.147       10.30.56.255       NBNS   92 Name query NB RESTLESZ.SU<00>
136 87.454320  10.30.56.103       10.30.56.124       ICMP   98 Echo (ping) request  id=0x0fa6, seq=5/1280, ttl=64

▸ Frame 119: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: 88:51:fb:42:80:84 (88:51:fb:42:80:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 88 51  fb 42 80 84 08 06 00 01   .......Q .B......
0010  08 00 06 04 00 01 88 51  fb 42 80 84 0a 1e 38 67   .......Q .B....8g
0020  00 00 00 00 00 00 0a 1e  38 7c                     ........ 8|
```

Updated arp table.

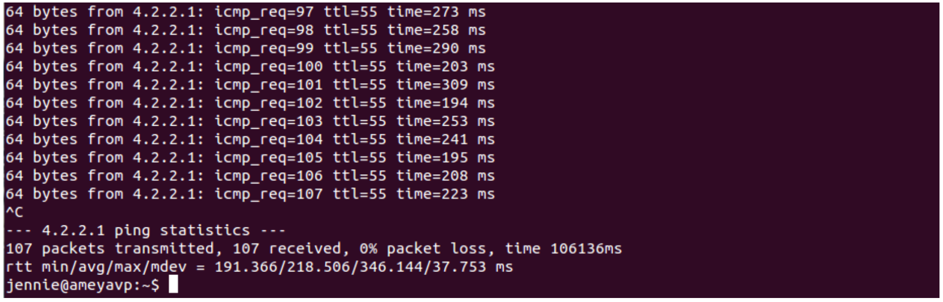


```
jennie@ameyavp:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.124             ether   6c:3b:e5:3e:0a:44   C                     eth0
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
jennie@ameyavp:~$ 
```

5) capturing network packets by pinging with 4.2.2.1
ping 4.2.2.1

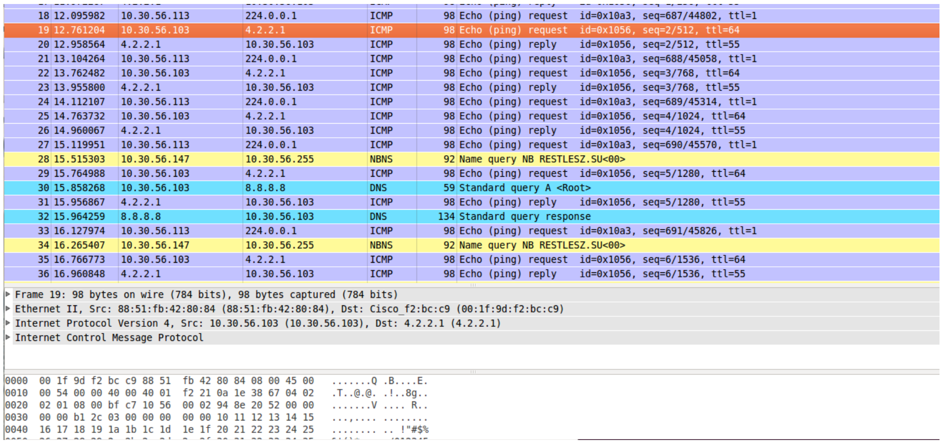


```
jennie@ameyavp:~$ ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1) 56(84) bytes of data.
64 bytes from 4.2.2.1: icmp_req=1 ttl=55 time=212 ms
64 bytes from 4.2.2.1: icmp_req=2 ttl=55 time=197 ms
64 bytes from 4.2.2.1: icmp_req=3 ttl=55 time=193 ms
64 bytes from 4.2.2.1: icmp_req=4 ttl=55 time=196 ms
64 bytes from 4.2.2.1: icmp_req=5 ttl=55 time=191 ms
64 bytes from 4.2.2.1: icmp_req=6 ttl=55 time=194 ms
64 bytes from 4.2.2.1: icmp_req=7 ttl=55 time=200 ms
64 bytes from 4.2.2.1: icmp_req=8 ttl=55 time=195 ms
64 bytes from 4.2.2.1: icmp_req=9 ttl=55 time=191 ms
64 bytes from 4.2.2.1: icmp_req=10 ttl=55 time=226 ms
64 bytes from 4.2.2.1: icmp_req=11 ttl=55 time=194 ms
64 bytes from 4.2.2.1: icmp_req=12 ttl=55 time=192 ms
64 bytes from 4.2.2.1: icmp_req=13 ttl=55 time=191 ms
64 bytes from 4.2.2.1: icmp_req=14 ttl=55 time=197 ms
64 bytes from 4.2.2.1: icmp_req=15 ttl=55 time=194 ms
64 bytes from 4.2.2.1: icmp_req=16 ttl=55 time=193 ms
64 bytes from 4.2.2.1: icmp_req=17 ttl=55 time=195 ms
64 bytes from 4.2.2.1: icmp_req=18 ttl=55 time=215 ms
```



```
64 bytes from 4.2.2.1: icmp_req=97 ttl=55 time=273 ms
64 bytes from 4.2.2.1: icmp_req=98 ttl=55 time=258 ms
64 bytes from 4.2.2.1: icmp_req=99 ttl=55 time=290 ms
64 bytes from 4.2.2.1: icmp_req=100 ttl=55 time=203 ms
64 bytes from 4.2.2.1: icmp_req=101 ttl=55 time=309 ms
64 bytes from 4.2.2.1: icmp_req=102 ttl=55 time=194 ms
64 bytes from 4.2.2.1: icmp_req=103 ttl=55 time=253 ms
64 bytes from 4.2.2.1: icmp_req=104 ttl=55 time=241 ms
64 bytes from 4.2.2.1: icmp_req=105 ttl=55 time=195 ms
64 bytes from 4.2.2.1: icmp_req=106 ttl=55 time=208 ms
64 bytes from 4.2.2.1: icmp_req=107 ttl=55 time=223 ms
^C
--- 4.2.2.1 ping statistics ---
107 packets transmitted, 107 received, 0% packet loss, time 106136ms
rtt min/avg/max/mdev = 191.366/218.506/346.144/37.753 ms
jennie@ameyavp:~$ 
```

Table is stored.



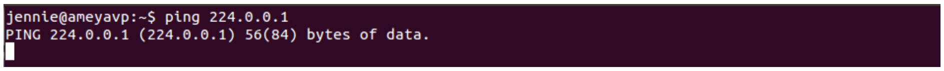
```
   18 12.095982  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x10a3, seq=687/44802, ttl=1
   19 12.761204  10.30.56.103    4.2.2.1         ICMP     98 Echo (ping) request  id=0x1056, seq=2/512, ttl=64
   20 12.958564  4.2.2.1         10.30.56.103    ICMP     98 Echo (ping) reply    id=0x1056, seq=2/512, ttl=55
   21 13.104264  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x10a3, seq=688/45058, ttl=1
   22 13.762482  10.30.56.103    4.2.2.1         ICMP     98 Echo (ping) request  id=0x1056, seq=3/768, ttl=64
   23 13.955800  4.2.2.1         10.30.56.103    ICMP     98 Echo (ping) reply    id=0x1056, seq=3/768, ttl=55
   24 14.112107  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x10a3, seq=689/45314, ttl=1
   25 14.763732  10.30.56.103    4.2.2.1         ICMP     98 Echo (ping) request  id=0x1056, seq=4/1024, ttl=64
   26 14.960067  4.2.2.1         10.30.56.103    ICMP     98 Echo (ping) reply    id=0x1056, seq=4/1024, ttl=55
   27 15.119951  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x10a3, seq=690/45570, ttl=1
   28 15.515303  10.30.56.147    10.30.56.255    NBNS     92 Name query NB RESTLESZ.SU<00>
   29 15.764988  10.30.56.103    4.2.2.1         ICMP     98 Echo (ping) request  id=0x1056, seq=5/1280, ttl=64
   30 15.858268  10.30.56.103    8.8.8.8         DNS      59 Standard query A <Root>
   31 15.956867  4.2.2.1         10.30.56.103    ICMP     98 Echo (ping) reply    id=0x1056, seq=5/1280, ttl=55
   32 15.964259  8.8.8.8         10.30.56.103    DNS     134 Standard query response
   33 16.127974  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x10a3, seq=691/45826, ttl=1
   34 16.265407  10.30.56.147    10.30.56.255    NBNS     92 Name query NB RESTLESZ.SU<00>
   35 16.766773  10.30.56.103    4.2.2.1         ICMP     98 Echo (ping) request  id=0x1056, seq=6/1536, ttl=64
   36 16.960848  4.2.2.1         10.30.56.103    ICMP     98 Echo (ping) reply    id=0x1056, seq=6/1536, ttl=55
▶ Frame 19: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: 88:51:fb:42:80:84 (88:51:fb:42:80:84), Dst: Cisco_f2:bc:c9 (00:1f:9d:f2:bc:c9)
▶ Internet Protocol Version 4, Src: 10.30.56.103 (10.30.56.103), Dst: 4.2.2.1 (4.2.2.1)
▶ Internet Control Message Protocol

0000  00 1f 9d f2 bc c9 88 51  fb 42 80 84 08 00 45 00   .......Q .B....E.
0010  00 54 00 00 40 00 40 01  f2 21 0a 1e 38 67 04 02   .T..@.@. .!..8g..
0020  02 01 08 00 bf c7 10 56  00 02 94 8e 20 52 00 00   .......V .... R..
0030  00 00 b1 2c 03 00 00 00  00 00 10 11 12 13 14 15   ...,.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
```

6) Determine MAC address of

a) Braodcast : ff:ff:ff:ff:ff:ff

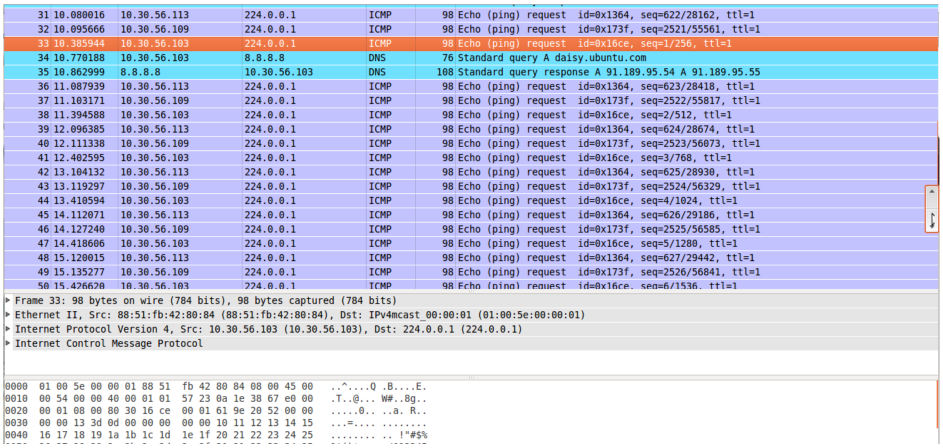
b) Multicast : 01.00.5e.00.00.01

ping 22.0.0.1



```
jennie@ameyavp:~$ ping 224.0.0.1
PING 224.0.0.1 (224.0.0.1) 56(84) bytes of data.
```

Sniffer Table is stored :



```
   31 10.080016  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=622/28162, ttl=1
   32 10.095666  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2521/55561, ttl=1
   33 10.385944  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=1/256, ttl=1
   34 10.770188  10.30.56.103    8.8.8.8         DNS      76 Standard query A daisy.ubuntu.com
   35 10.862999  8.8.8.8         10.30.56.103    DNS     108 Standard query response A 91.189.95.54 A 91.189.95.55
   36 11.087939  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=623/28418, ttl=1
   37 11.103171  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2522/55817, ttl=1
   38 11.394588  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=2/512, ttl=1
   39 12.096385  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=624/28674, ttl=1
   40 12.111338  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2523/56073, ttl=1
   41 12.402595  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=3/768, ttl=1
   42 13.104132  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=625/28930, ttl=1
   43 13.119297  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2524/56329, ttl=1
   44 13.410594  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=4/1024, ttl=1
   45 14.112071  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=626/29186, ttl=1
   46 14.127240  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2525/56585, ttl=1
   47 14.418606  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=5/1280, ttl=1
   48 15.120015  10.30.56.113    224.0.0.1       ICMP     98 Echo (ping) request  id=0x1364, seq=627/29442, ttl=1
   49 15.135277  10.30.56.109    224.0.0.1       ICMP     98 Echo (ping) request  id=0x173f, seq=2526/56841, ttl=1
   50 15.426620  10.30.56.103    224.0.0.1       ICMP     98 Echo (ping) request  id=0x16ce, seq=6/1536, ttl=1
▶ Frame 33: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: 88:51:fb:42:80:84 (88:51:fb:42:80:84), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
▶ Internet Protocol Version 4, Src: 10.30.56.103 (10.30.56.103), Dst: 224.0.0.1 (224.0.0.1)
▶ Internet Control Message Protocol

0000  01 00 5e 00 00 01 88 51  fb 42 80 84 08 00 45 00   ..^....Q .B....E.
0010  00 54 00 00 40 00 01 01  57 23 0a 1e 38 67 e0 00   .T..@... W#..8g..
0020  00 01 08 00 80 30 16 ce  00 01 61 9e 20 52 00 00   .....0.. ..a. R..
0030  00 00 13 3d 0d 00 00 00  00 00 10 11 12 13 14 15   ...=.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
```