# PROGRAM 1

- 1. Download the file netdump.tar from <a href="ftp://dougj.net">ftp://dougj.net</a>.
  - a) Run the program to capture traffic in a text file. Look at the format stored in the file.
  - b) Modify the file to decode Ethernet Header. Print address in hex.
  - c) Based on type print Payload.
  - d) Add counters to count no. of packets.

>> run\_dump strings ./netdump | grep -q netdump ./netdump run\_dump: listening on bce0

Packet Header Information	(a)
Ethernet DA: 00: 0d: 65: d2: 4a: e0	····· (b)
Ethernet SA: 00: 22: 19: ad: 59: d9	(b)
Type: 0800	(b)
Payload: IP Packet	(c)
No of ARP Packets: 0	(d)
No of IP Packets: 1	(d)

000d 65d2 4ae0 0022 19ad 59d9 0800 4510 006c 2826 4000 4006 993d 81ba d728 81ba 9e7b 0016 c1ef bca8 5675 c652 4d43 5018 2014 7977 0000 b42a 9ef0 4046 46c7 d9de 87ab 3752 f522 d4e6 2a53 024a 6724 42e6 8d70 70f1 7470 6745 54bd bb23 a827 3003 f1d1 7c74 e5cf e5ce 01f3 3465 3230 8a42 208c e642 5aad f39e 68c9

## **Packet Header Information**

Ethernet Destination Address: ff: ff: ff: ff: ff: ff Ethernet Source Address: 02: 01: 81: ba: d7: 33

Type: 886f

No of ARP Packets: 0 No of IP Packets: 1

```
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 ffff
ff3f 0000 0000 ffff ffff ffff ff0f 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 ffff
ffff ffff ff0f ffff ffff ff0f 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000
```

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 3200  $0000\ 0100\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  $0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ 0000 0000 0000 0000 0000 0000

## **Packet Header Information**

Ethernet DA: 00: 0d: 65: d2: 4a: e0 Ethernet SA: 00: 22: 19: ad: 59: d9

Type: 0800 Payload: IP Packet No of ARP Packets: 0 No of IP Packets: 2

000d 65d2 4ae0 0022 19ad 59d9 0800 4510 006c 2826 4000 4006 993d 81ba d728 81ba 9e7b 0016 c1ef bca8 5675 c652 4d43 5018 2014 7977 0000 b42a 9ef0 4046 46c7 d9de 87ab 3752 f522 d4e6 2a53 024a 6724 42e6 8d70 70f1 7470 6745 54bd bb23 a827 3003 f1d1 7c74 e5cf e5ce 01f3 3465 3230 8a42 208c e642 5aad f39e 68c9

### **Packet Header Information**

Ethernet DA: 00: 0d: 65: d2: 4a: e0 Ethernet SA: 00: 22: 19: ad: 59: d9

Type: 0800 Payload: IP Packet No of ARP Packets: 0 No of IP Packets: 3

000d 65d2 4ae0 0022 19ad 59d9 0800 4510 006c 2826 4000 4006 993d 81ba d728 81ba

9e7b 0016 c1ef bca8 5675 c652 4d43 5018 2014 7977 0000 b42a 9ef0 4046 46c7 d9de 87ab 3752 f522 d4e6 2a53 024a 6724 42e6 8d70 70f1 7470 6745 54bd bb23 a827 3003 f1d1 7c74 e5cf e5ce 01f3 3465 3230 8a42 208c e642 5aad f39e 68c9

#### **Packet Header Information**

Ethernet DA: 00: 0d: 65: d2: 4a: e0 Ethernet SA: 00: 22: 19: ad: 59: d9

Type: 0800 Payload: IP Packet No of ARP Packets: 0 No of IP Packets: 4

000d 65d2 4ae0 0022 19ad 59d9 0800 4510 006c 2826 4000 4006 993d 81ba d728 81ba 9e7b 0016 c1ef bca8 5675 c652 4d43 5018 2014 7977 0000 b42a 9ef0 4046 46c7 d9de 87ab 3752 f522 d4e6 2a53 024a 6724 42e6 8d70 70f1 7470 6745 54bd bb23 a827 3003 f1d1 7c74 e5cf e5ce 01f3 3465 3230 8a42 208c e642 5aad f39e 68c9

.

.

^C

13 packets received by filter 0 packets dropped by kernel