



Government Engineering College Thrissur

Network Programming Lab

Navaneeth D

TCR18CS043

S6, CSE

Experiment 7

Raw Sockets

AIM

- a) Display the header information of UDP and TCP packets during client-server communication using raw sockets.
- b) Develop a packet capturing and filtering application using raw sockets.

THEORY

Other sockets like stream sockets and data gram sockets receive data from the transport layer that contains no headers but only the payload. This means that there is no information about the source IP address and MAC address. If applications running on the same machine or on different machines are communicating, then they are only exchanging data.

The purpose of a raw socket is absolutely different. A raw socket allows an application to directly access lower level protocols, which means a raw socket receives un-extracted packets (see Figure 2). There is no need to provide the port and IP address to a raw socket, unlike in the case of stream and datagram sockets.

HOW TO USE?

1. Navigate to the main directory containing the program.
2. Open terminal 1
3. Type `$ gcc rawsock_tcp_a.c -o raw_tcp & gcc rawsock_udp_a.c -o raw_udp`
4. Enter `$ sudo ./raw_tcp` to see the output
5. Enter `$ sudo ./raw_udp` to see the output
6. Open a new terminal
7. Type `$ gcc packet_sniffer.c`
8. Enter `$ sudo ./a.out` to see the following output
9. Verify the output.

- a) Displayed the header information of UDP and TCP packets during client-server communication using raw sockets.
- b) Developed a packet capturing and filtering application using raw sockets.

```

TERMINAL 1
(Program a)

(base) navaneeth@navaneeth-lap:~/Documents/2021/Network Lab/Raw-socket/version p$ sudo ./raw_tcp
TCP header:
Source IP: 192.168.1.2 (33663168)
Source Port      : 1234
Destination Port : 80
Sequence Number  : 0
Acknowledge Number : 0
Packet Send. Length : 46

(base) navaneeth@navaneeth-lap:~/Documents/2021/Network Lab/Raw-socket/version p$ sudo ./raw_udp
UDP header:
Source IP: 192.168.1.2 (33663168)
Packet Send. Length : 47
Source Port      : 6666
Destination Port : 8622

TERMINAL 2
(Program b)

(base) navaneeth@navaneeth-lap:~/Documents/2021/Network Lab/Raw-socket/version p$ sudo ./sniffer
[sudo] password for navaneeth:
Starting...
TCP packets : 57

raw socket / version p / 2 log.txt
2
3 *****TCP Packet*****
4
5 IP Header
6 IP Header Length : 5 DWORDS or 20 Bytes
7 Source IP      : 157.240.228.60
8 Destination IP : 192.168.1.10
9
10 TCP Header
11 Source Port      : 443
12 Destination Port : 52378
13 Sequence Number  : 3138513399
14 Acknowledge Number : 2229111367
15 Header Length    : 8 DWORDS or 32 BYTES
16 | -Urgent Flag      : 0
17 | -Acknowledgement Flag : 1
18 | -Push Flag       : 0
19 | -Reset Flag      : 0
20 | -Synchronise Flag : 0
21 | -Finish Flag     : 0
22 | -Window          : 951
23 | -Checksum        : 13717
24 | -Urgent Pointer  : 0
25
26 | | | | | DATA Dump
27 IP Header
28 45 00 00 34 B4 5D 00 00 59 06 69 87 9D F0 E4 3C      E..4.]..Y.i...<
29 C0 A8 01 0A                                          ....
30 TCP Header
31 01 BB CC 9A BB 11 E9 F7 84 DD 8A 47 80 10 03 B7      .....6...
32 35 95 00 00 01 01 08 0A 88 5C A0 D2 9B 0D B2 D0      5.....\.....
33 Data Payload
```