LAB-4

Network Data Analysis using tcpdump

Lab Exercises:

1) While tcpdump host your-host is running one command window, run ping 127.0.0.1 from another command window. From the ping output, is the 127.0.0.1 interface on? Can you see any ICMP message from your host in the tcpdump output? Why?

ans:- Terminal 1:

$ sudo tcpdump host 172.16.59.39 (pc ip)

Terminal 2:

$ ping 127.0.0.1

Yes, the interface is on since packets are transmitted in the same host.

No, we do not see any ICMP messages sent from host since "127.0.0.1" is the loopback address.

ICMP is a network layer protocol. It is used to communicate with the source of a data packet about transmission issues. So, if a datagram is not delivered, ICMP might not report this back to the host. While using loop backaddress, the packets won't be leaving our system. So ICMP won't be reported.

$ ping 172.16.59.57 (neighbour pc ip)

This gives ICMP requests & and replies because it happens between two systems. (Packet exchanging)

#FMI : man tcpdump

3) Explain briefly the purposes of the following tcpdump expressions.

a) tcpdump udp port 520

ans:- Shows traffic of ~~Data~~ ~~protocol~~ User Datagram Protocol with either server or client on port 520.

b) tcpdump -x -s 120 ip proto 89

ans:- ~~-x : prints data of each packet contents in both hex and ascii~~

-s : defines the snaplength (size) of the capture in bytes. Here -s 120 implies that the size is reduced to 120 bytes.

-x : When parsing and printing, in addition to printing the headers of each packet, it prints the data of each packet (minus its link level header) in hex (-xx including " " ")

ip proto : lets you target a specific protocol. Here ipv4. number
∴ the command prints header of ipv4 protocol 89 (OSPF) in hexa and captures 120 bytes of data.

c) tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip. addr3)

ans:- -x : same as above

-s 70 : snaplength = 70 ⇒ captures 70 bytes of data

This command searches for those packets where ip address of host is that of ip addr1 and (either that of ip-addr2 or ip-addr3)

d) tcpdump -x -s 70 host ip addr1 and no ip addr2

ans:- -x : same as above

-s 70 : captures 70 bytes of data.
This command lists all packets where ip address is ~~equ~~ same as ip addr1 and is not equal to ip addr2.