EE673 – Lab

Packet capture and Analysis from remote node

Module 1:

(Refer to the lab sheet for lab-2 to work on this module. You will need topology.pdf and tetsbed-ip.pdf as reference documents. The command set to be used in this module has been given in lab sheet for lab-2)

1. Create a network with point to point links using appropriate ip addr and subnet mask.
2. Check that neighbors are reachable by ping < ip addr of neighbor >
3. Set up static routing in forward and reverse directions to set up a topology
4. Enable intermediate nodes to act as router by setting ip_forward
   (Path name is /proc/sys/net/ipv4/ip_forward)

Module 2: (iperf)

Generate Traffic using iperf

Run iperf as a server on one node

```
% iperf -s
```

Run iperf as client

```
% iperf -c <server ip>
```

Note down the bandwidth.

Data formatting: (-f argument)

The -f argument can display the results in the desired format: bits(b), bytes(B), kilobits(k), kilobytes(K), megabits(m), megabytes(M), gigabits(g) or gigabytes(G).

Generally the bandwidth measures are displayed in bits (or Kilobits, etc ...) and an amount of data is displayed in bytes (or Kilobytes, etc ...).

```
% iperf -c <server ip> -f b
```

use the command `netstat -an | more` to see the ports being used by iperf. By default server runs on port 5001

Stop the server and the client and test the following for udp traffic

```
% iperf -s -u -i 1
% iperf -c <server-ip> -u -b 10m
```

Observer the output.

Module 3: (tcpdump)

```
% tcpdump -i <eth1|eth2>
```

read output format section of tcpdump man pages to understand the output of tcpdump

Module 4: (Making sense of tcpdump with add-on enhancements)

wireshark: Application to Interactively dump and analyze network traffic . To be executed on front end system.

```
% ssh root@<eth0 ip> “tcpdump -i <eth1|eth2> -w -”|wireshark -k
-n -i -
```

Enter the password when asked.

Locate the entry for ping after selection capture --> stop

Look up ethernet header, ip header and upper layer headers.