Student Name : ______________________________

Group : ______________________________

Date : ______________________________

## LAB 3: ANALZING NETWORK DATA LOG

You will be provided with the data file, in .csv format, in the working directory. Write the program to extract the following informations.

### EXERCISE 3A: TOP TALKERS AND LISTENERS

One of the most commonly used function in analyzing data log is finding out the IP address of the hosts that send out large amount of packet and hosts that receive large number of packets, usually know as TOP TALKERS and LISTENERS. Based on the IP address we can obtained the organization who owns the IP address.

List the TOP 5 TALKERS

| Rank | IP address | # of packets | Organisation |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

TOP 5 LISTENERS

| Rank | IP address | # of packets | Organisation |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

### EXERCISE 3B: TRANSPORT PROTOCOL

Using the IP protocol type attribute, determine the percentage of TCP and UDP protocol

| | Header value | Transport layer protocol | # of packets |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| | | | |

### EXERCISE 3C: APPLICATIONS PROTOCOL

Using the Destination IP port number determine the most frequently used application protocol.

| Rank | Destination IP port number | # of packets | Service |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

## EXERCISE 3D: TRAFFIC INTENSITY

The traffic intensity is an important parameter that a network engineer needs to monitor closely to determine if there is congestion. You would use the IP packet size to calculate the estimated total traffic over the monitored period of 15 seconds. (Assume the sampling rate is 1 in 1000)

| | |
|---|---|
| Total Traffic( MB) | |

## EXERCISE 3E: ADDITIONAL ANALYSIS (BONUS MARKS)

Please described additional analysis of the data and how it is useful. Please use a separate sheet to submit your new graphs and observations. Your report for this exercise is limited to 2 pages. The answer template and the two page additional analysis are to be submitted to your e-learning drive.

Examples

- Visulisation using scatter graph of port and IP address to determine if a specific node been port scanned by another node.
- Which is the most popular node that provide service on port 80, port= 443 ?

You must analise and explain the graphs. Please do not be limited by the above examples.

## EXERCISE 3F: SOFTWARE CODE

Please attach a softcopy of your code to the e-learning drive.