

Assignment 1 Networks Lab(CS39006) Spring 2020

Submitted By -Group 18

Prakhar Bindal-17CS10036

Gaurav Goyal-17CS30013

Problem Statement : Using Wireshark for analysing network packet traces

1) Steps-

1) UDP Client (with 28 Kbps) for UDP performance measurement using iperf :
iperf -c 10.5.18.163 -u -b 28000

This command will send UDP packets to the iperf server running at 10.5.18.163. You can specify the time for which you want to send UDP packets. Please check iperf documentation.

2) TCP Client:

wget --no-proxy http://10.5.18.163:8000/1.jpg

This command uses the HTTP protocol to download the image file 1.jpg from the web server running

at 10.5.18.163. You can change the URI to access 1.jpg to 7.jpg.

Observation:

UDP Case:

Application Layer- NIL

Transport Layer- UDP

Network Layer- IP Version 4

TCP Case:

Application Layer- HTTP

Transport Layer- TCP

Network Layer- IP Version 4

Justification: In case of TCP, we used wget which is an application layer tool sending HTTP requests and iperf is a transport layer tool with -u flag specifying to send UDP packets.

2) a)

Steps:

- 1."ip.addr=10.5.18.163 && ip.addr=client_ip" is used in the filter to monitor only the Packets that are concerned without our experiment
2. Client_id found using the \$ifconfig command
3. I/O graphs are obtained from wireshark menu Menu->Statistics->IO Graphs

Observation:In all the cases 2 SYN and ACK Packets are observed at the beginning. 1 HTTP "OK" packet and 1 TCP "OK" packet were observed at the end. There was an ACK packet after each of the received packets.

Pic1-186 data packets
Pic2- 621 data packets
Pic3- 1362 data packets
Pic4- 845 data packets
Pic5- 855 data packets

Justification: Since the pictures are of different sizes and are using a TCP protocol, number of data packets are different in all cases.

No, all the packets are not of same size and there were various sizes ranging from few 60's to a few thousands. Generally the ACK packets are of less size than data packets.

Some packet sizes for each of the pic in bytes are:

Pic1-60,66,82,228,252,1514,18890 etc

Pic2-60,66,119,270,7386,8654,11297 etc

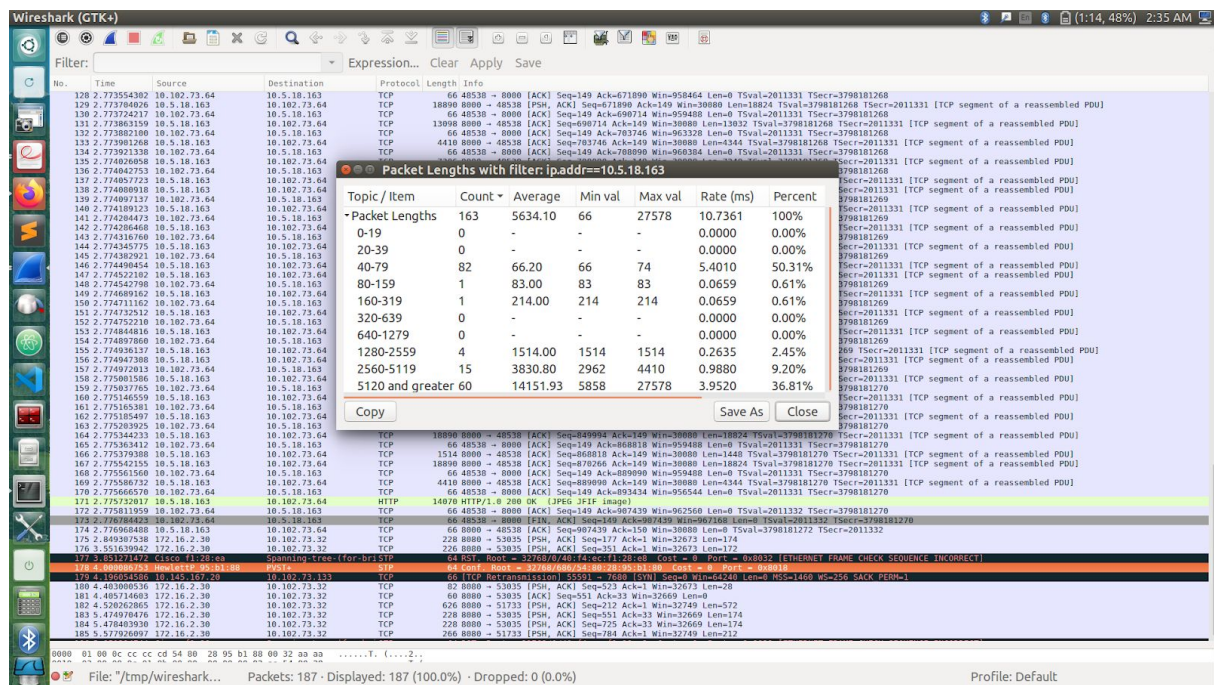
Pic3-66,73016,9472,18654 etc

Pic4-66,119,2962,3412,4572 etc

Pic5-66,105,119,136,2964,4410 etc

Details-

Pic-1



Pic-2

Filter: **ip.addr==10.5.18.163** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
564	2.053604900	10.5.18.163	10.102.73.64	TCP	2962	8000 → 4854 [ACK] Seq=2926426 Ack=149 Win=30000 Len=2096 Tsv=3798735798 Tsc=2149961 [TCP segment of a reassembled PDU]
565	2.053615523	10.5.18.163	10.102.73.64	TCP	4410	8000 → 4854 [ACK] Seq=2929322 Ack=149 Win=30000 Len=4344 Tsv=3798735799 Tsc=2149961 [TCP segment of a reassembled PDU]
566	2.053620914	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2933666 Win=1210368 Len=0 Tsv=2149961 Tsc=3798735799
567	2.053709602	10.5.18.163	10.102.73.64	TCP	10202	8000 → 4854 [ACK] Seq=2933666 Ack=149 Win=30000 Len=10136 Tsv=3798735799 Tsc=2149961 [TCP segment of a reassembled PDU]
568	2.053733239	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2943802 Win=1210368 Len=0 Tsv=2149961 Tsc=3798735799
569	2.053809987	10.5.18.163	10.102.73.64	TCP	11650	8000 → 4854 [ACK] Seq=2943802 Ack=149 Win=30000 Len=11584 Tsv=3798735799 Tsc=2149961 [TCP segment of a reassembled PDU]
570	2.053840565	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2955386 Win=1211192 Len=0 Tsv=2149961 Tsc=3798735799
571	2.053877761	10.5.18.163	10.102.73.64	TCP	7386	8000 → 4854 [ACK] Seq=2955386 Ack=149 Win=30000 Len=7240 Tsv=3798735799 Tsc=2149961 [TCP segment of a reassembled PDU]
572	2.053968820	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
573	2.054074438	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
574	2.054106330	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
575	2.054174402	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
576	2.054152733	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
577	2.054277550	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
578	2.054298846	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
579	2.054338648	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
580	2.054408264	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
581	2.054492886	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
582	2.054510236	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
583	2.054552343	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
584	2.054584674	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
585	2.054620731	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
586	2.054687456	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
587	2.054726661	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
588	2.054811131	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
589	2.054856782	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
590	2.054901644	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
591	2.054907134	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
592	2.055012080	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
593	2.055062351	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
594	2.055124159	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
595	2.055178880	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
596	2.055257626	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
597	2.055377175	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
598	2.055317580	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
599	2.055448911	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
600	2.055464397	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
601	2.055480741	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
602	2.055500420	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
603	2.055519923	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
604	2.055600992	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
605	2.055647440	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
606	2.055709774	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
607	2.055731608	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
608	2.055777580	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
609	2.055835980	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
610	2.055897920	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
611	2.055907710	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
612	2.055935334	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
613	2.057310920	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
614	2.059013350	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
615	2.054731765	172.16.2.30	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=2967626 Win=1205636 Len=0 Tsv=2149961 Tsc=3798735799
616	2.050843020	Cisco:11:28:ea	Spanning tree (for-bc151f)	STP	64	Root = 32768/0/40:14cc:11:28:ea Cost = 0 Port = 0/8032 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
618	2.775928007	172.16.2.30	10.102.73.64	TCP	270	8000 → 51120 [PSH, ACK] Seq=124 Ack=552 Win=32864 Len=284 Tsv=281679208 Tsc=2150046
619	2.777540927	10.102.73.64	10.5.18.163	TCP	570	51120 → 8000 [PSH, ACK] Seq=0 Ack=124 Win=2710 Len=512 Tsv=2150046 Tsc=281679208
620	2.777651526	10.102.73.64	172.16.2.30	TCP	66	8000 → 4854 [ACK] Seq=1175720 Ack=150 Win=30000 Len=0 Tsv=3798735803 Tsc=2149962
621	3.450421949	Cisco:11:28:ea	CDP/VTP/DTF/Pag/UDP	CDP	162	Device ID: 40f4ec128eb Port ID: gi2

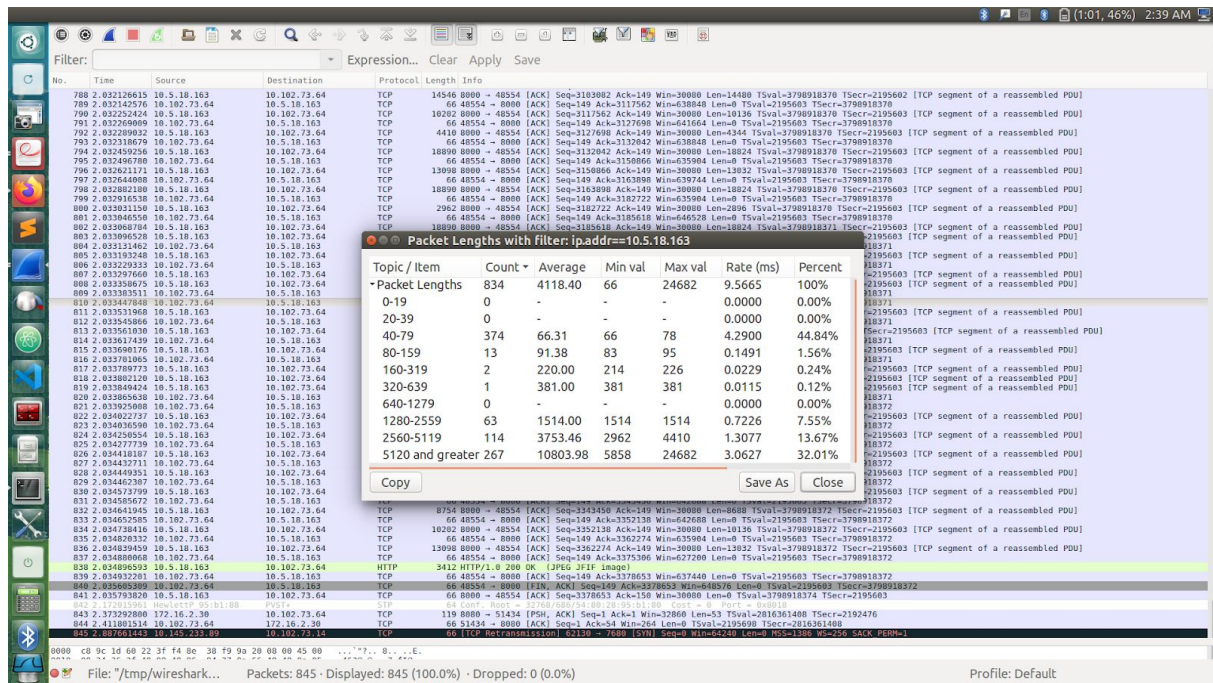
File: /tmp/wireshark... Packets: 621 (100.0%) - Dropped: 0 (0.0%) Profile: Default

Pic-3

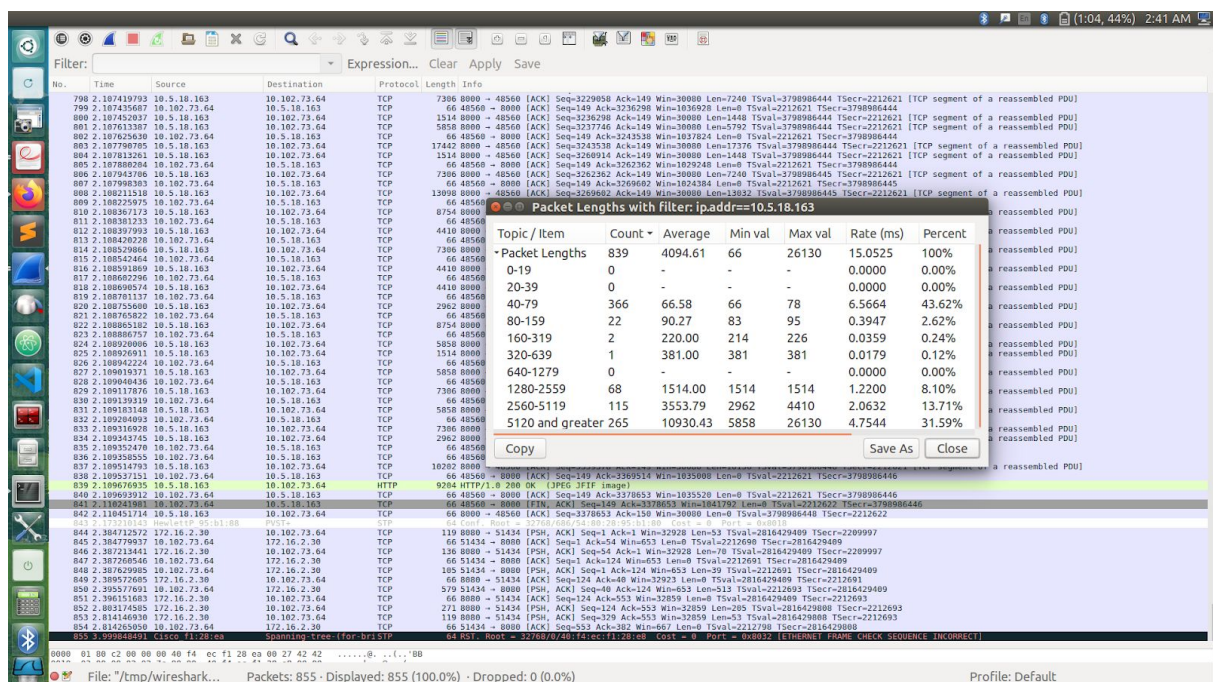
Filter: **ip.addr==10.5.18.163** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1365	3.657079163	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6582626 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843994 [TCP segment of a reassembled PDU]
1366	3.657229208	10.5.18.163	10.102.73.64	TCP	18890	8000 → 4854 [ACK] Seq=6582626 Ack=149 Win=30000 Len=18824 Tsv=3798843994 Tsc=2177809 [TCP segment of a reassembled PDU]
1367	3.657234241	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6581450 Win=1116800 Len=0 Tsv=2177809 Tsc=3798843994
1368	3.657392677	10.5.18.163	10.102.73.64	TCP	18890	8000 → 4854 [ACK] Seq=6601450 Ack=149 Win=30000 Len=18824 Tsv=3798843994 Tsc=2177809 [TCP segment of a reassembled PDU]
1369	3.657399100	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6602674 Win=1116800 Len=0 Tsv=2177809 Tsc=3798843994
1370	3.657457177	10.5.18.163	10.102.73.64	TCP	15446	8000 → 4854 [ACK] Seq=6602674 Ack=149 Win=30000 Len=14480 Tsv=3798843994 Tsc=2177809 [TCP segment of a reassembled PDU]
1371	3.657560940	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6634754 Win=1116816 Len=0 Tsv=2177809 Tsc=3798843994
1372	3.657716653	10.5.18.163	10.102.73.64	TCP	10202	8000 → 4854 [ACK] Seq=2933666 Ack=149 Win=30000 Len=10136 Tsv=3798843994 Tsc=2177809 [TCP segment of a reassembled PDU]
1373	3.657722422	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6644890 Win=1122560 Len=0 Tsv=2177809 Tsc=3798843994
1374	3.657777995	10.5.18.163	10.102.73.64	TCP	10202	8000 → 4854 [ACK] Seq=6644890 Ack=149 Win=30000 Len=10136 Tsv=3798843995 Tsc=2177809 [TCP segment of a reassembled PDU]
1375	3.657786593	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6655926 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1376	3.657935728	10.5.18.163	10.102.73.64	TCP	24602	8000 → 4854 [ACK] Seq=6655926 Ack=149 Win=30000 Len=24616 Tsv=3798843995 Tsc=2177809 [TCP segment of a reassembled PDU]
1377	3.657959602	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6679642 Win=1112960 Len=0 Tsv=2177809 Tsc=3798843995
1378	3.658112166	10.5.18.163	10.102.73.64	TCP	20338	8000 → 4854 [ACK] Seq=6679642 Ack=149 Win=30000 Len=20272 Tsv=3798843995 Tsc=2177809 [TCP segment of a reassembled PDU]
1379	3.658120020	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6699914 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1380	3.658277577	10.5.18.163	10.102.73.64	TCP	20338	8000 → 4854 [ACK] Seq=6699914 Ack=149 Win=30000 Len=20272 Tsv=3798843995 Tsc=2177809 [TCP segment of a reassembled PDU]
1381	3.658280151	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1382	3.658437092	10.5.18.163	10.102.73.64	TCP	15948	8000 → 4854 [ACK] Seq=6720186 Ack=149 Win=30000 Len=15928 Tsv=3798843995 Tsc=2177809 [TCP segment of a reassembled PDU]
1383	3.658447594	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1384	3.658605706	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1385	3.658657786	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1386	3.658810353	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1387	3.658871476	10.102.73.64	10.5.18.163	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1388	3.659040742	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=149 Ack=6720186 Win=1115776 Len=0 Tsv=2177809 Tsc=3798843995
1389	3.659095123	10.5.18.163	10.102.73.64	TCP	66	4854 → 8000 [ACK] Seq=

Pic-4



Pic-5

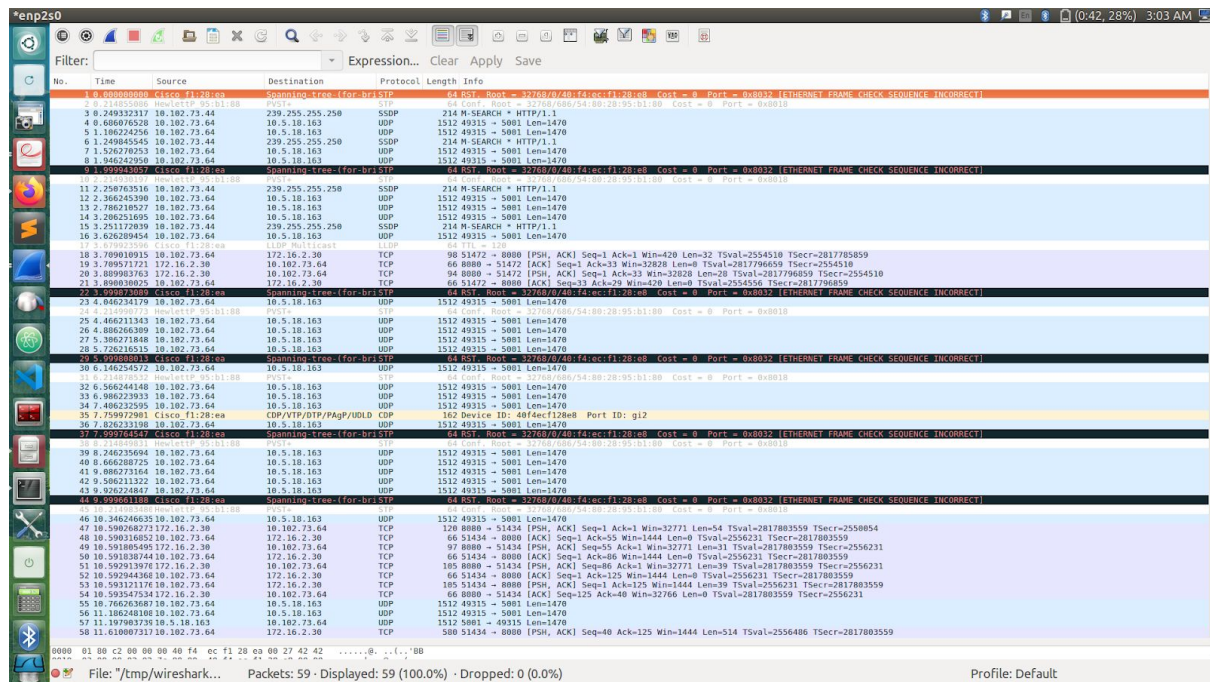


2.b)

All the UDP Packets are of same size- 1512 bytes length per packet.

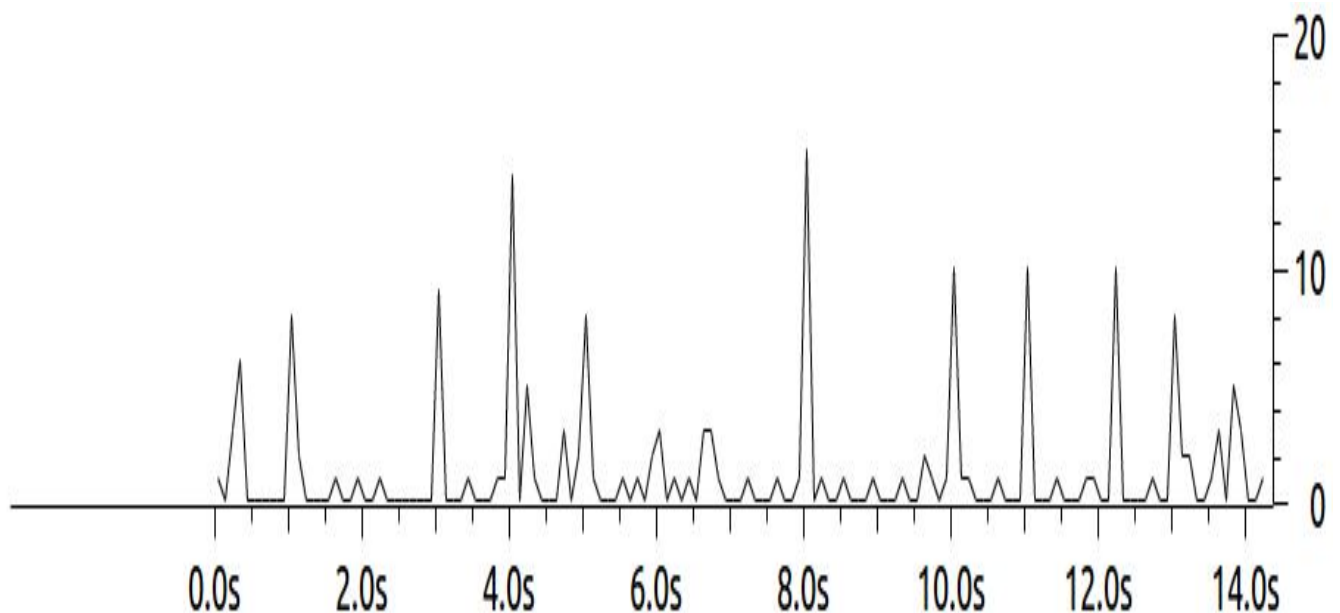
Justification-All packets are of same size because of the iperf server sending it that way.

Pic for Reference:

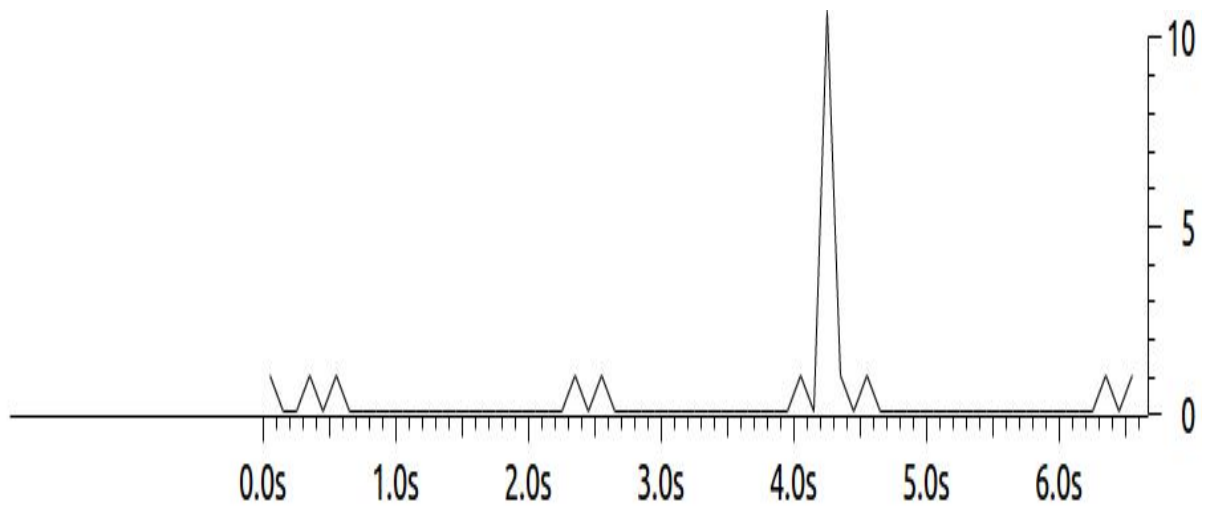


2.c) Throughout using Wireshark

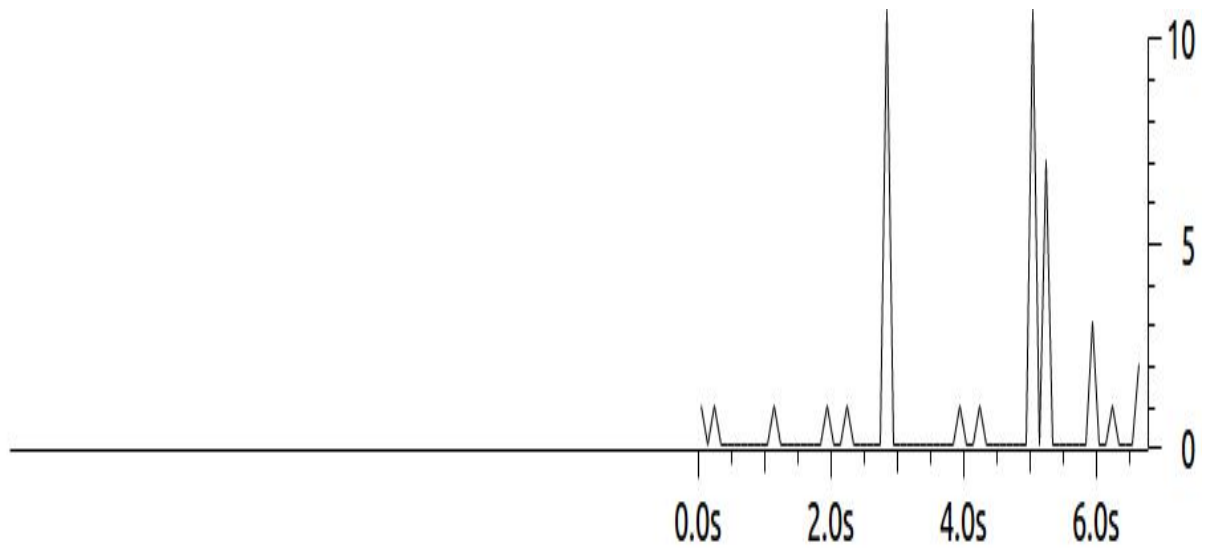
UDP Case:



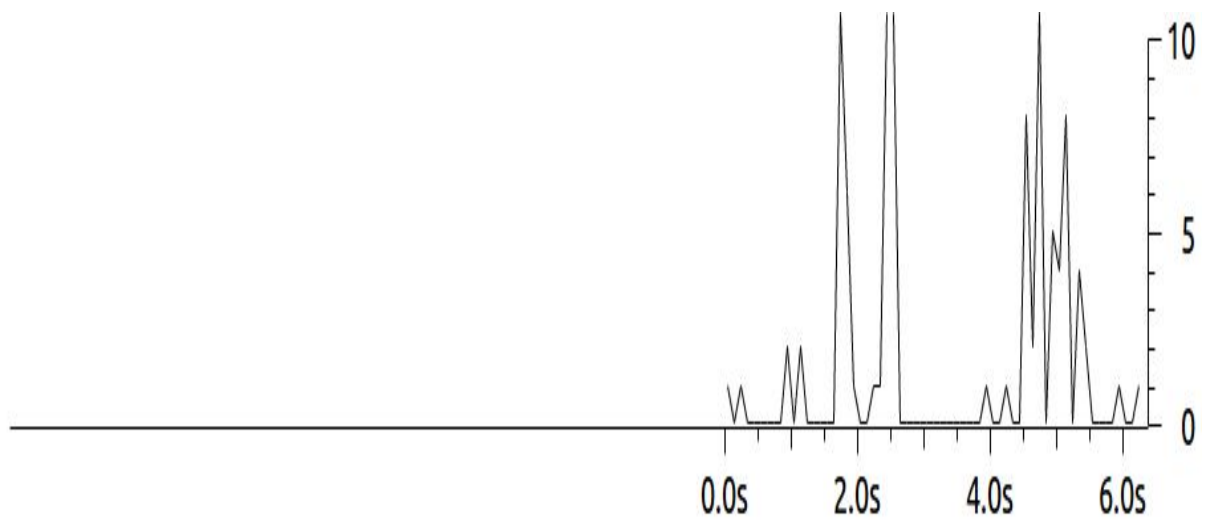
TCP Case:
Pic 1:



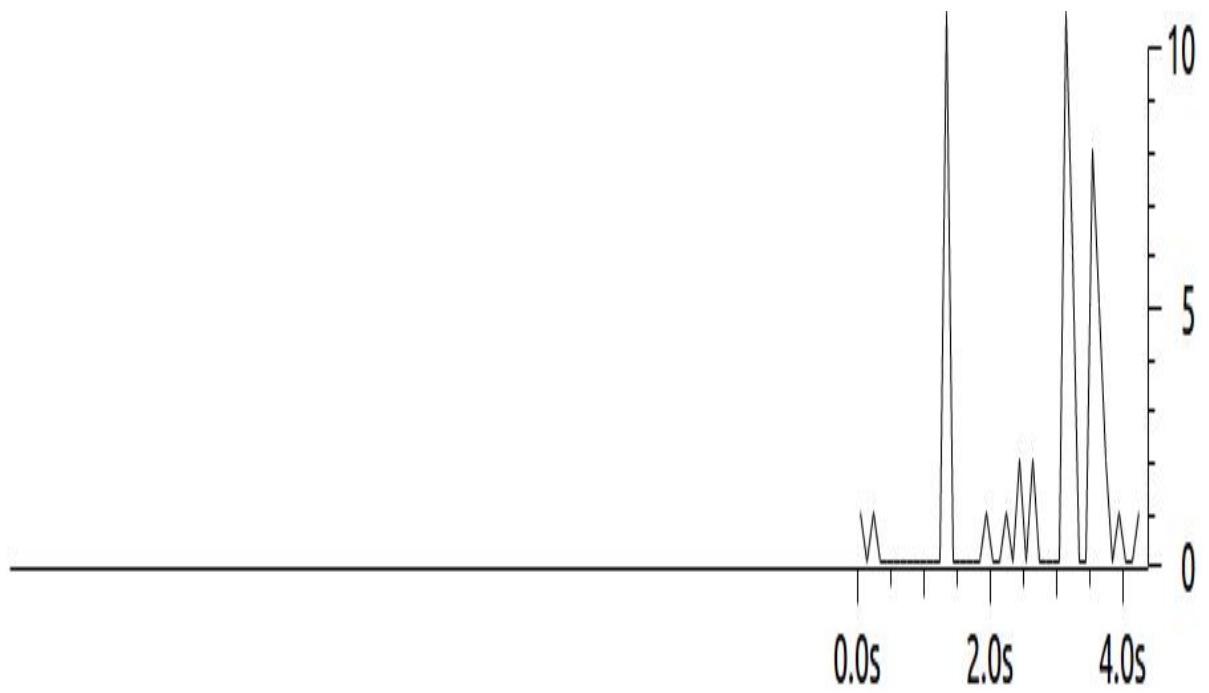
Pic 2:



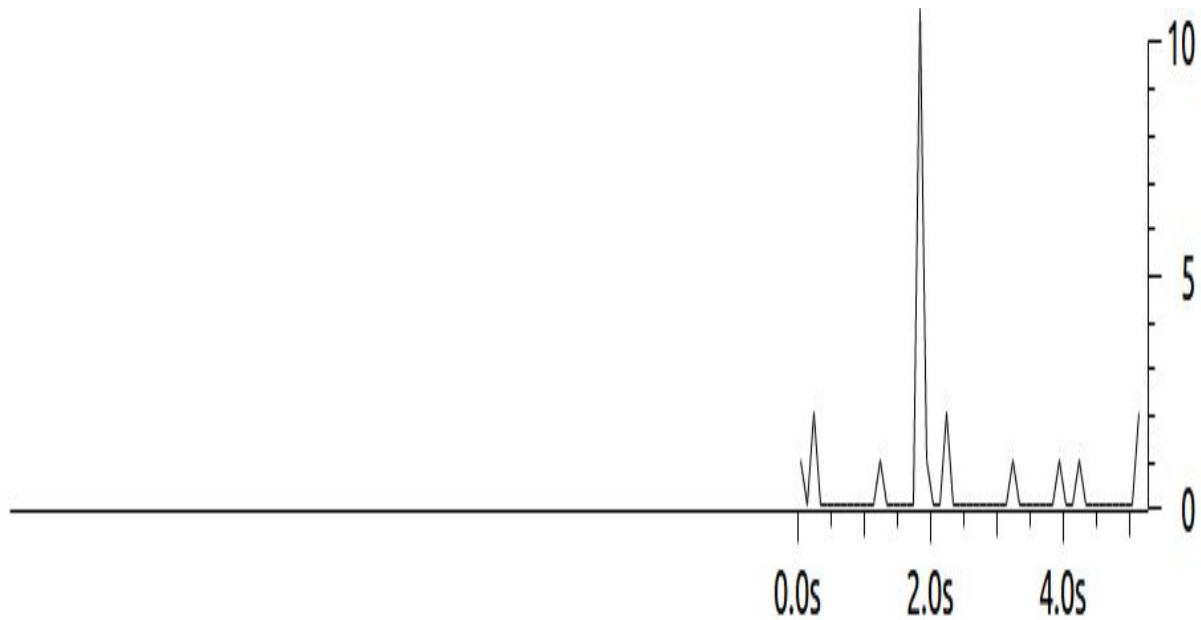
Pic 3:



Pic 4:



Pic 5:



Justification-Since, the request for all the pictures are sent one after the other, the set of packets for each image are received consecutively for 5 pictures. Since each picture is requested only after receiving the previous picture, each peak corresponds to one picture only.

d) The UDP throughput (amount of UDP data received per second) for the following cases of UDP traffic generation rates (bandwidth)

1. 64 Kbps
Data Transfer=80.4 Kbytes
Uplink throughput=64.0 kbps
Downlink throughput=64.3 kbps
Datagrams Sent-56
2. 128 kbps
Data Transfer=158 Kbytes
Uplink throughput=128 kbps
Downlink throughput=130 kbps
Datagrams Sent-110
3. 256 kbps
Data Transfer=314 Kbytes
Uplink throughput=256 kbps
Downlink throughput=256 kbps
Datagrams Sent-219
4. 512 kbps
Data Transfer=627 Kbytes
Uplink throughput=512 kbps
Downlink throughput=519 kbps
Datagrams Sent-437

5. 1024 kbps
Data Transfer=1.22 MB
Uplink throughput=1.02 Mbps
Downlink throughput=1.02 Mbps
Datagrams Sent-872
6. 2048 kbps
Data Transfer=2.44 MB
Uplink throughput=2.05 Mbps
Downlink throughput=2.08 Mbps
Datagrams Sent-1743

Justification-It is clear that the uplink throughput is limited by the network condition and the bandwidth of the host machines and the bandwidth used by the client. In most of the cases the network has sufficient capability to have uplink throughput equal to the bandwidth.

3)

The image displays a Wireshark packet capture analysis. The top pane shows a list of packets with several TCP Retransmission entries highlighted in orange. The middle pane shows the details of a selected packet (Frame 5983), identifying it as a suspected retransmission of a TCP segment. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Filter: tcp.analysis.retransmission

No.	Time	Source	Destination	Protocol	Length	Info
280	30.533883744	10.117.20.124	10.102.75.153	TCP	66	[TCP Retransmission] Seq=51731 - 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
281	32.554129224	10.117.20.124	10.102.75.153	TCP	66	[TCP Retransmission] Seq=51731 - 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
301	34.050601265	10.102.75.64	172.16.2.30	TCP	151	[TCP Retransmission] Seq=51454 - 8088 [PSH, ACK] Seq=51454 Ack=40 Win=1075 Len=85 TSval=3516313 TSecr=2821641610
860	36.554971711	10.117.20.124	10.102.75.153	TCP	66	[TCP Retransmission] Seq=51731 - 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2113	44.535266404	10.117.20.124	10.102.75.153	TCP	66	[TCP Retransmission] Seq=51731 - 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3412	58.390555681	10.102.75.64	172.16.2.30	TCP	381	[TCP Retransmission] Seq=51682 - 8088 [PSH, ACK] Seq=28235 Ack=3739 Win=1444 Len=235 TSval=3520396 TSecr=2821657860
3498	60.40349444	10.102.75.64	172.16.2.30	TCP	1402	[TCP Retransmission] Seq=51650 - 8088 [PSH, ACK] Seq=7800 Ack=5214 Win=1444 Len=1236 TSval=3535499 TSecr=2821662010
3942	112.81886378	10.102.75.64	172.16.2.30	TCP	917	[TCP Retransmission] Seq=51602 - 8088 [PSH, ACK] Seq=72679 Ack=39588 Win=1444 Len=831 TSval=3535863 TSecr=2821721660
3943	112.81886378	10.102.75.64	172.16.2.30	TCP	168	[TCP Retransmission] Seq=51602 - 8088 [PSH, ACK] Seq=72679 Ack=39588 Win=1444 Len=831 TSval=3535863 TSecr=2821721660
4045	129.56253768	10.102.75.64	172.16.2.30	TCP	570	[TCP Retransmission] Seq=51454 - 8088 [PSH, ACK] Seq=7077 Ack=701 Win=1075 Len=554 TSval=3540189 TSecr=2821765310

Frame 5983: 1287 bytes on wire (10296 bits), 1287 bytes captured (10296 bits) on interface 0

- Ethernet II, Src: Dell (f8:9a:20:f4:8e:38:f9:9a:20), Dst: Cisco (60:22:3f:c8:9c:1d:60:22:3f)
- Internet Protocol Version 4, Src: 10.102.75.64, Dst: 172.16.2.30
- Transmission Control Protocol, Src Port: 51658, Dst Port: 8088, Seq: 54852, Ack: 6131, Len: 1221
 - Source Port: 51658
 - Destination Port: 8088
 - [Stream index: 2]
 - [TCP Segment Len: 1221]
 - Sequence number: 54852 (relative sequence number)
 - [Next sequence number: 56075 (relative sequence number)]
 - Acknowledgment number: 6131 (relative ack number)
 - 1080 ... = Header Length: 32 bytes (8)
 - Flags: 0x010 (PSH, ACK)
 - Window size value: 1444
 - [Calculated window size: 1444]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0xa45a (Unverified)
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [SEQ/ACK analysis]
 - (Bytes in flight: 7618)
 - (Bytes sent since last PSH flag: 1221)
 - [TCP Analysis Flags]
 - [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
 - [The RTT for this segment was: 0.013483823 seconds]
 - [Info based on delta from frame: 3932]
 - [Timestamps]
 - TCP payload (1221 bytes)
 - Retransmitted TCP segment data (1221 bytes)

0000 48 9c 18 00 22 3f f4 8e 38 f9 9a 20 00 00 00 00
0010 04 f9 0e 20 40 00 00 00 20 83 0a 06 40 40 ac 10 ... (0.0.0.0)..
0020 02 1e c9 ca 1f 90 87 e7 08 53 3f ba f3 c3 00 10
0030 05 40 0a 1a 0f 00 01 01 00 0a 00 35 f3 ba 00 30
0040 03 68 79 29 0f f1 81 73 26 1c 09 09 17 45 ea 37 ... 4.50.0

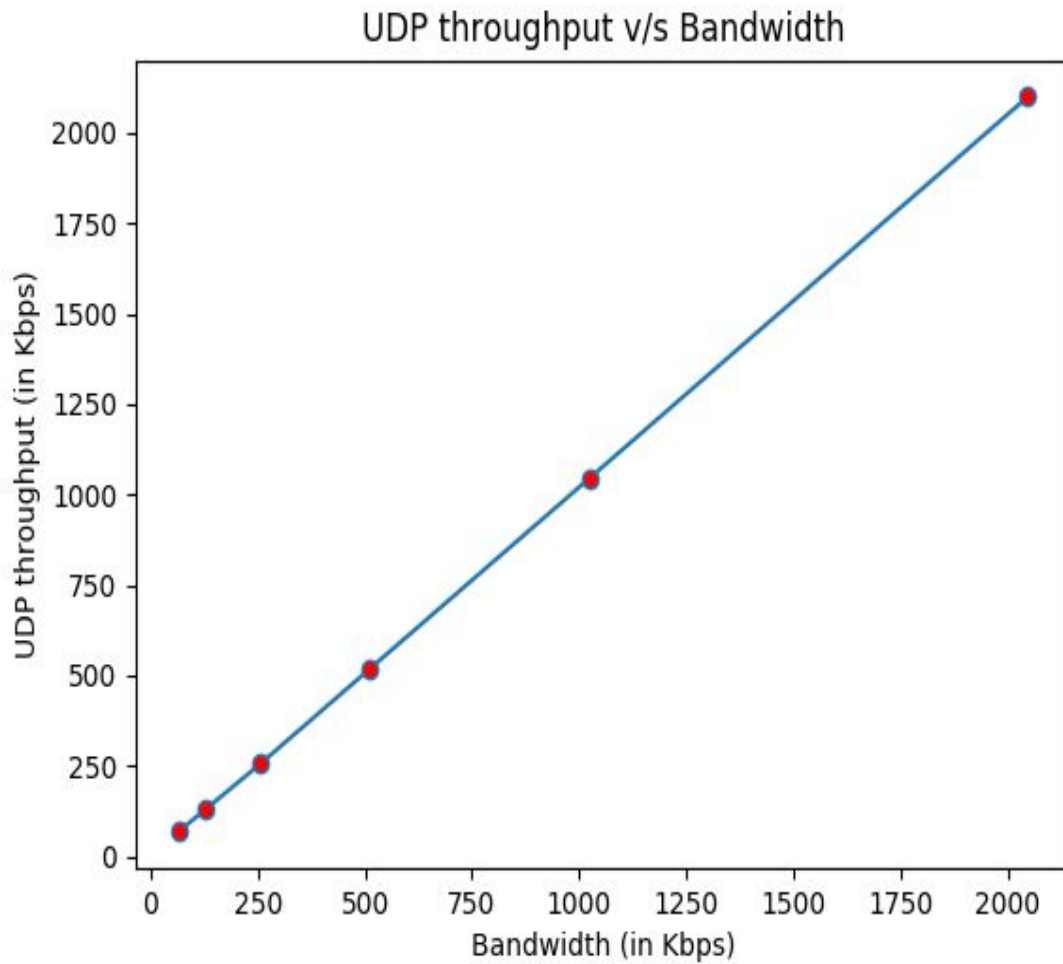
Frame (frame), 1287 ... Packets: 4606 · Displayed: 10 (0.2%) · Dropped: 0 (0.0%) Profile: Default

Observation:Number of retransmission packets lost depends on the traffic and the strength of network connection

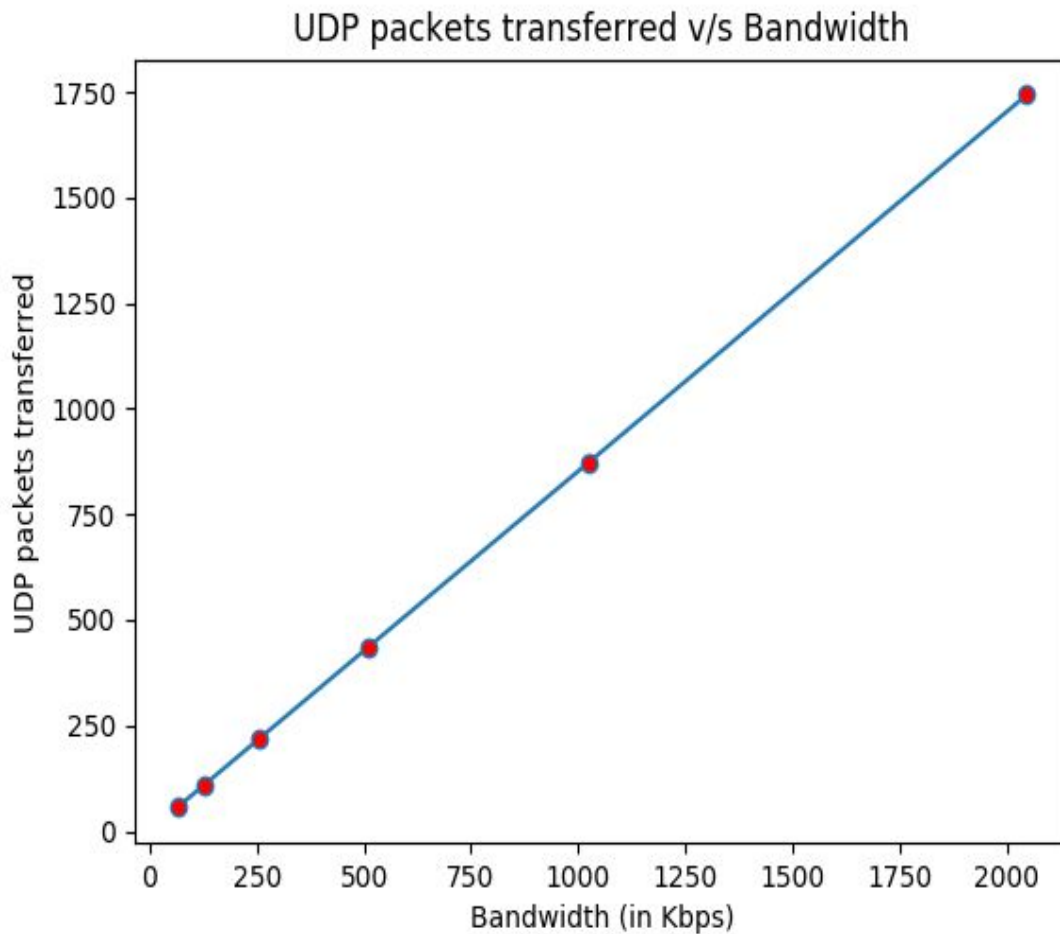
4) Plots

Using a *matplotlib* script, generate the graph that shows the relation between UDP throughput vs bandwidth, and also between the number of packets that are transmitted vs bandwidth.

UDP throughput vs UDP bandwidth



Number of UDP packet transmitted vs UDP bandwidth



Observations:

- UDP throughput is almost equal to the bandwidth specification using *iperf*. This shows the network is showing no latency at all. It can be observed that for very high data rate the throughput reaches a limiting value. This limiting value is due to network limitations.
- As bandwidth increases more number of packets were transferred in the same span of time. This can be observed by the increasing number of datagrams sent