CS 39006: Networks Lab

Assignment 1:
Use Wireshark for analyzing Network Packet Traces

SUBMITTED BY -

15CS10031 - PANKAJ DHURVE
15CS30025 - SACHIN KUMAR

OBJECTIVE:

The objective of this assignment is to understand the Wireshark tool and how you can analyse network packet traces. You have to use Wireshark for answering the questions.

STEPS:

(1) Open the terminal and run the command `sudo wireshark`.It opens the wireshark for further steps.

(2) Now run the command `iperf -c 10.5.20.128 -u -b 28000` in the terminal and filter result in Wireshark by setting the ip.addr==machine ip. Save the result and i/o graph .Now restart the capturing for further experiment.

(3)Repeat the step 2 with these commands

```
wget --no-proxy http://10.5.20.128:8000/pic1.jpg ,
wget --no-proxy http://10.5.20.128:8000/pic2.jpg
wget --no-proxy http://10.5.20.128:8000/pic3.jpg
wget --no-proxy http://10.5.20.128:8000/pic4.jpg
wget --no-proxy http://10.5.20.128:8000/pic5.jpg
```

OBSERVATIONS :

(1) List the different protocols that you observe in the packet trace, at application, transport and network layer for each of the UDP and TCP test cases.

UDP :

UDP Client (with 28 Kbps) for UDP performance measurement using command **iperf -c 10.5.20.128 -u -b 28000.**

This command will send UDP packets to the iperf server running at 10.5.20.128

Application Layer : NULL

Transport Layer : UDP

Network Layer : IPv4

TCP :

TCP Client: **wget --no-proxy http://10.5.20.128:8000/pic1.jpg**

This command uses the HTTP protocol to access the image fime pic1.jpg from the web server running at 10.5.20.128.

Application layer : HTTP protocol

Transport layer : TCP protocol

Network Layer : IPv4

Same Layers are observed in each TCP test case.

(2) Analyse the packet trace using Wireshark and compute the followings,

(a) How many TCP packets are transferred for each cases while accessing the files pic1.jpg to pic5.jpg? Are all the packets of same size? What are the different packet size you observe for each of the file access?

Pic1:

Number of TCP packets : 50

Sizes : 66, 74, 214, 829, 1514, 2962, 4410, 5858

Pic2:

Number of TCP packets : 4968

Sizes : 66, 74, 78, 86, 217, 1514, 2962, 4910, 5858, 7306, 8754, 10202, 11317, 13098, 14546, 15994, 17442, 20338, 21786, 23234, 24682, 26130, 29026, 30474

Pic3:

Number of TCP packets : 204

Sizes : 66, 74, 217, 1514, 2962, 3531, 4410, 5858, 7306, 8754, 11650, 13098, 14546

Pic4:

Number of TCP packets : 1038

Sizes : 66, 74, 90, 130, 138, 217, 1514, 2962, 4242, 4410, 5858, 7306, 8754, 10202, 11317, 13098, 14546, 15994, 17442

Pic5:

Number of TCP packets : 202

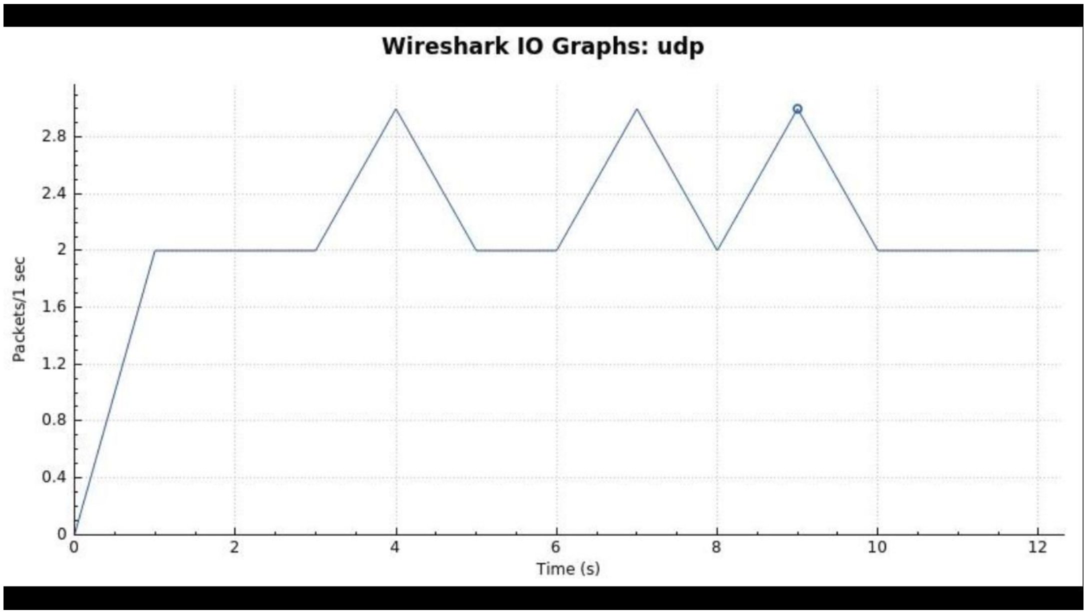
Sizes : 66, 74, 90, 217, 1514, 2962, 4094, 4410, 5858, 7306, 8754, 10202, 11317, 13098, 14546, 15994, 17442, 18890, 21786, 24682, 29026

(b) For the test case with UDP, are all the UDP packets of same size? If not, what are the different UDP packet sizes you observe?

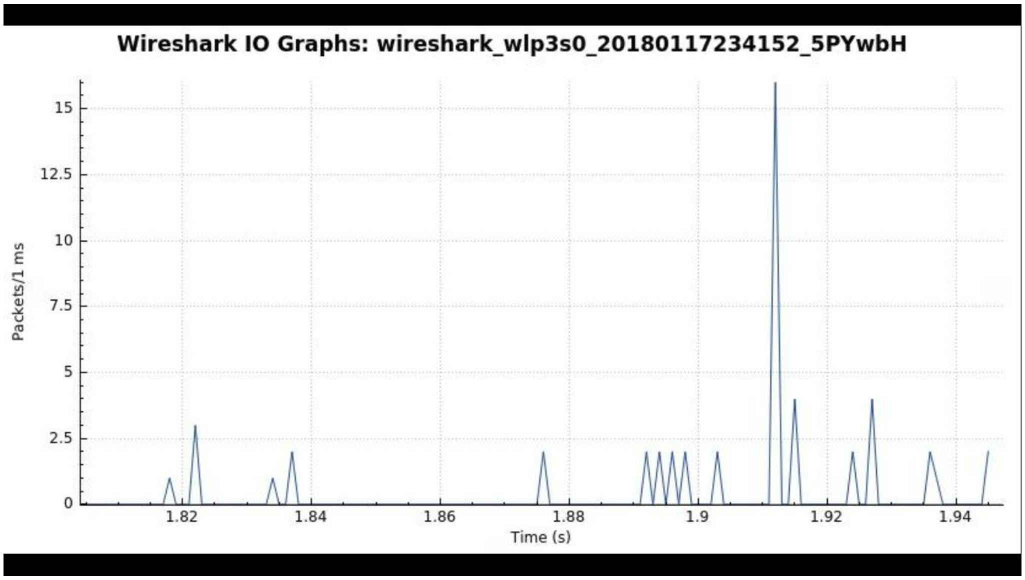
All UDP are of same size i.e 1512.

(c) Observe the TCP and the UDP throughput using Wireshark (Menu->Statistics->IO Graphs).

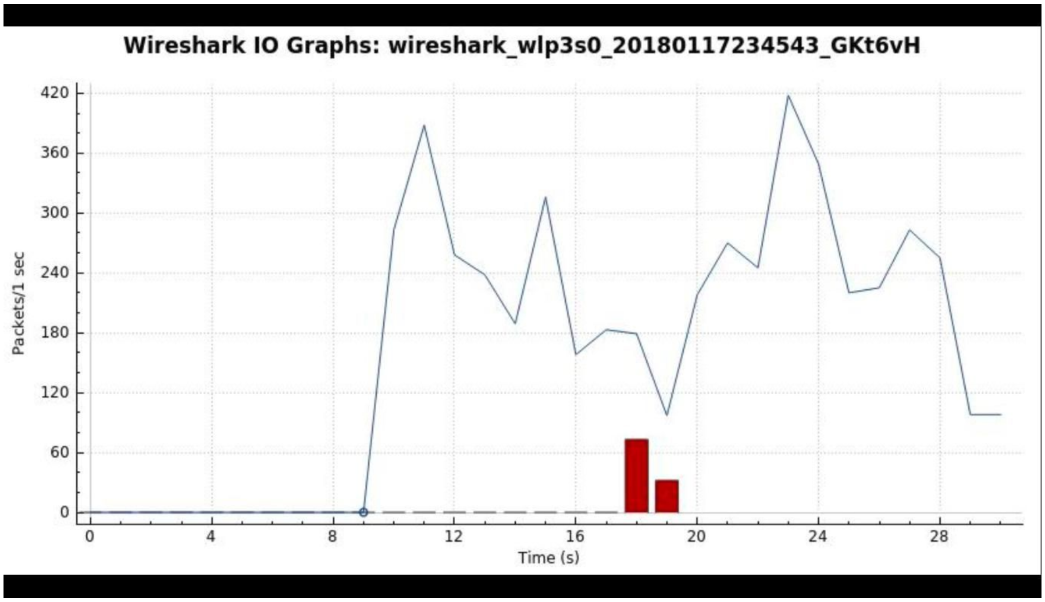
UDP:


Wireshark IO Graphs: udp
Packets/1 sec
0
0.4
0.8
1.2
1.6
2
2.4
2.8
Time (s)
0
2
4
6
8
10
12

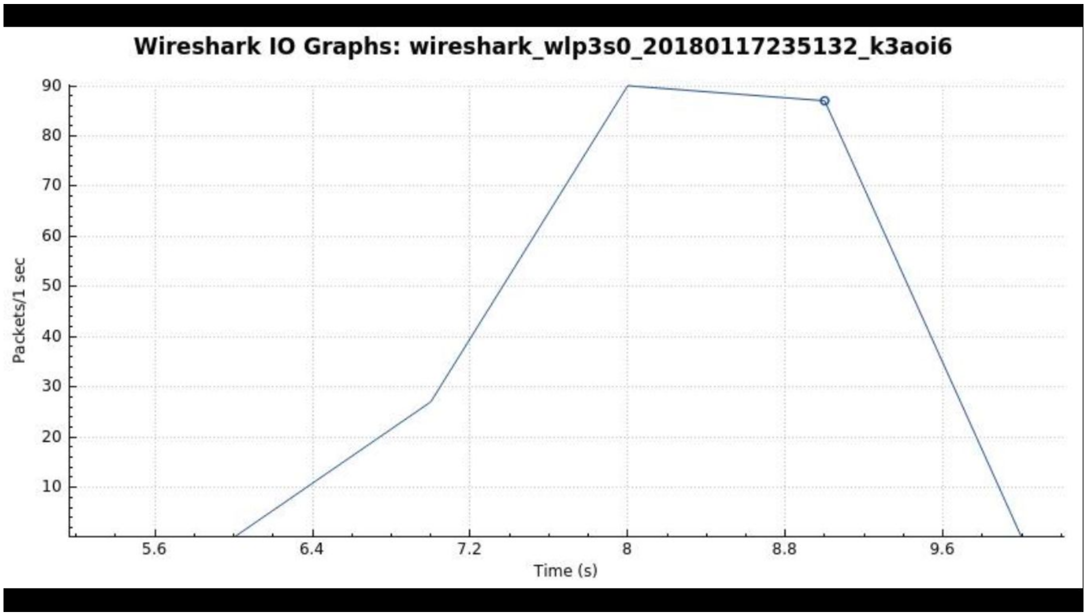
TCP-PIC1:


Wireshark IO Graphs: wireshark_wlp3s0_20180117234152_5PYwbH
Packets/1 ms
15
12.5
10
7.5
5
2.5
0
1.82
1.84
1.86
1.88
1.9
1.92
1.94
Time (s)

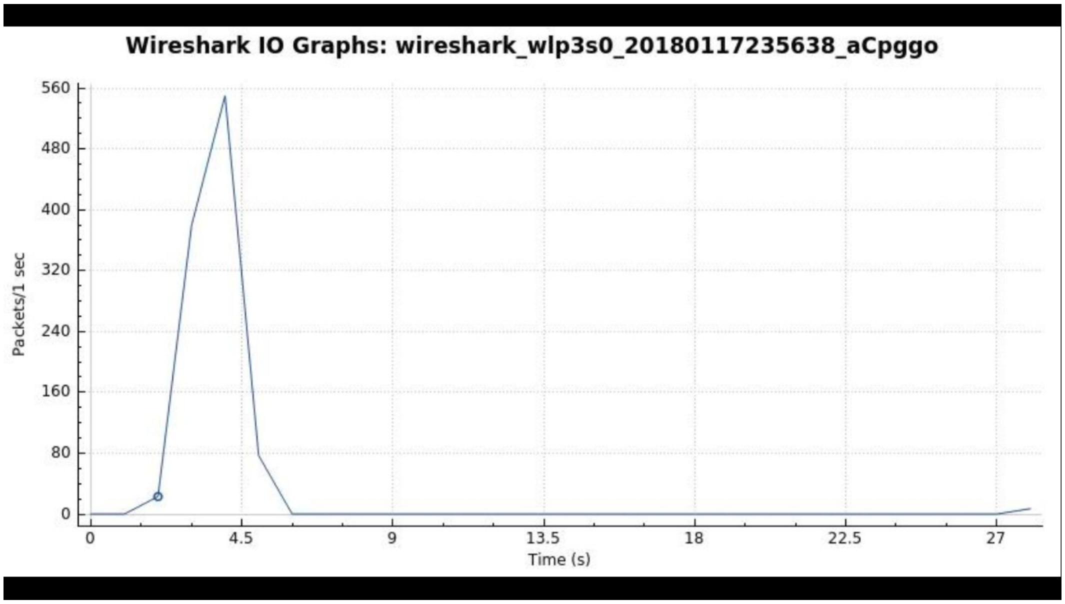
TCP-PIC2:


Wireshark IO Graphs: wireshark_wlp3s0_20180117234543_GKt6vH
Packets/1 sec
420
360
300
240
180
120
60
0
0
4
8
12
16
20
24
28
Time (s)

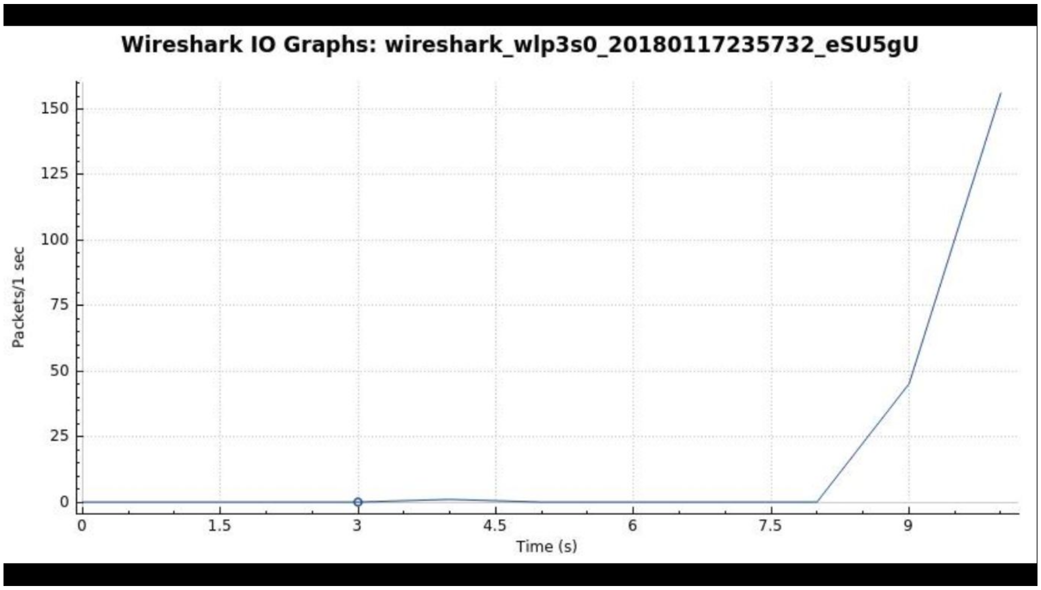
TCP- PIC3:



TCP-PIC4:



TCP-PIC5:



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

	Wireshark statistics	**Terminal**
(i) 64 Kbps :	8416 bytes/sec,	64 kbits/sec
(ii) 128 Kbps :	16,000 bytes/sec,	128 kbits/sec
(iii) 256 Kbps :	33,000 bytes/sec,	256 kbits/sec
(iv) 512 Kbps :	66,000 bytes/sec,	511 kbits/sec
(v) 1024 Kbps :	131,000 bytes/sec,	1.03 Mbits/sec
(vi) 2048 Kbps :	194,000 bytes/sec,	2.05 Mbits/sec

(3) Analyze the number of TCP packets retransmitted (Use: tcp.analysis.retransmission) from Wireshark, as shown in figure below.

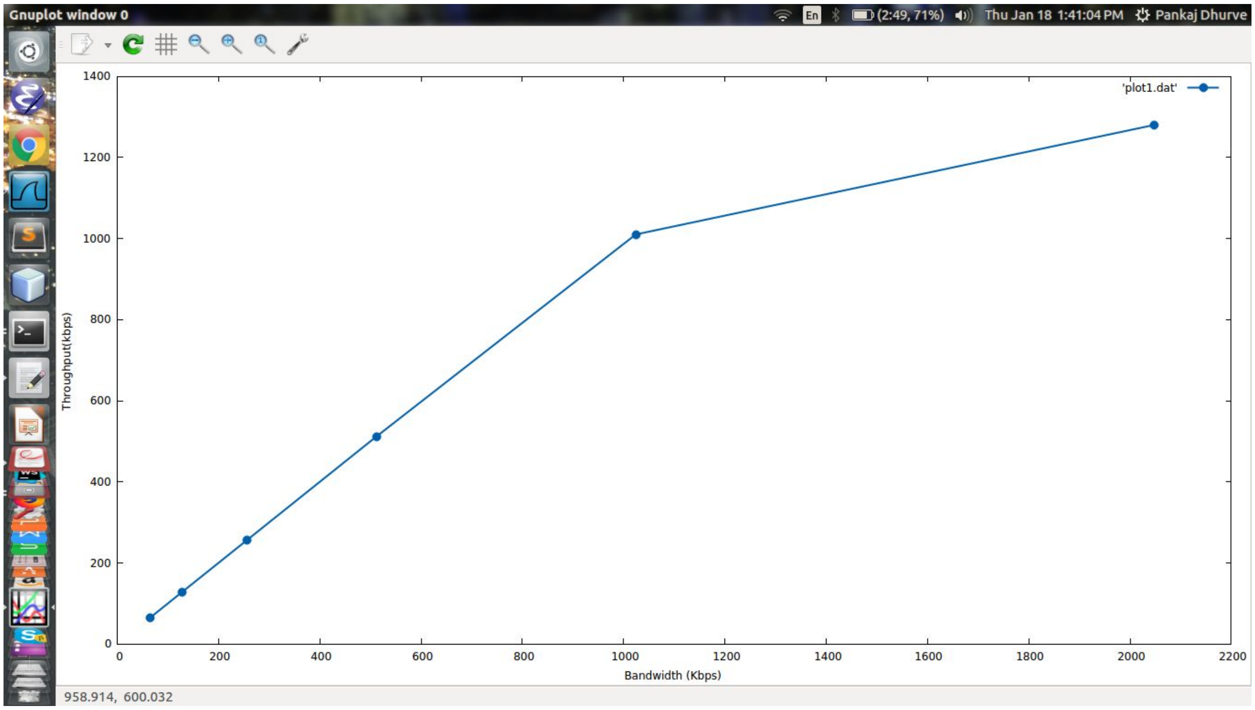
Pic2: 1

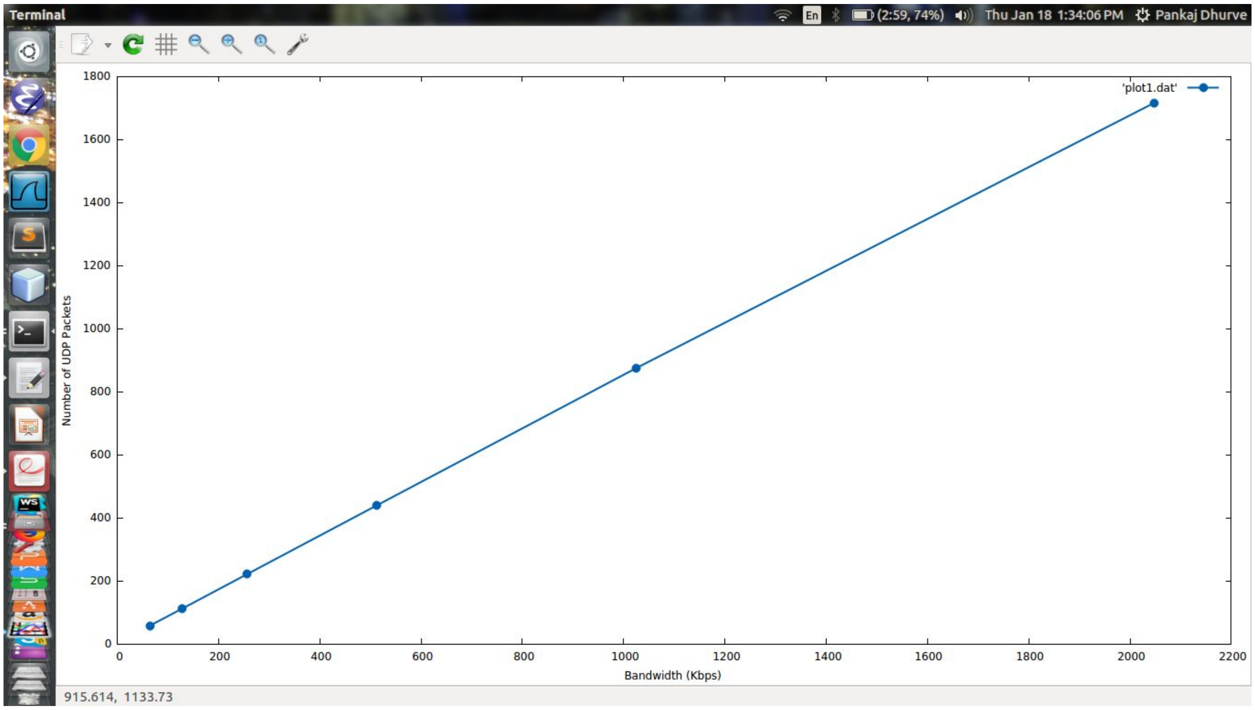
Pic2 is the only pic of large size and we have got TCP errors as well. So, this justifies tcp retransmission.

(4) Plot the following

1. UDP throughput with respect to the UDP bandwidth

2. Number of UDP packets transmitted with respect to UDP bandwidth


Gnuplot window 0
En
(2:49, 71%)
Thu Jan 18 1:41:04 PM
Pankaj Dhurve
'plot1.dat'
Throughput(kbps)
Bandwidth (Kbps)


Terminal
En
(2:59, 74%)
Thu Jan 18 1:34:06 PM
Pankaj Dhurve
'plot1.dat'
Number of UDP Packets
Bandwidth (Kbps)