



Report

Assignment 1

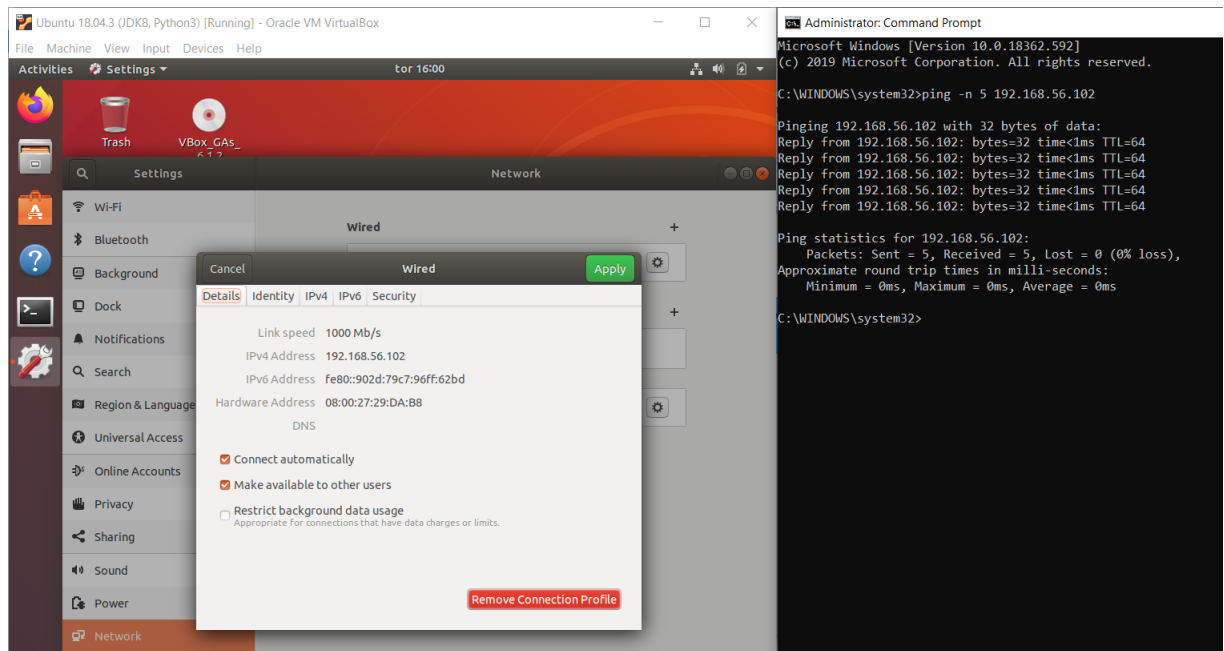


Author: LOIC GALLAND
Email: lg222sv@student.lnu.se
Semester: Spring 2020
Area: Computer Science
Course code: 1DV701

Contents

1	Problem 1	1
1.1	Discussion	1
2	Problem 2	1
2.1	Discussion	2
3	Problem 3	3
3.1	Discussion	3
4	Problem 4	3
4.1	Discussion	3
5	Problem 5	5
5.1	Discussion	5

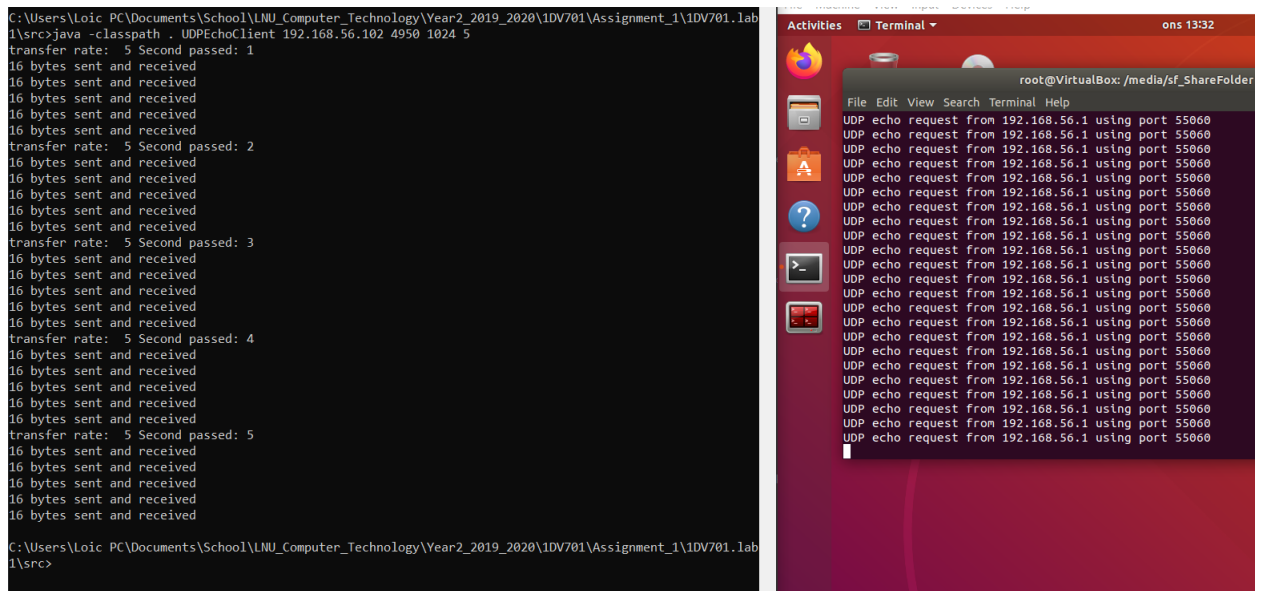
1 Problem 1



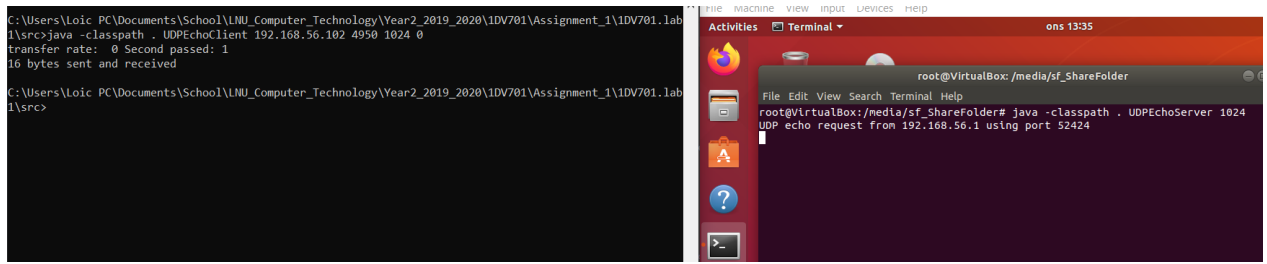
1.1 Discussion

The screenshot above shows what happens when we are pinging the server with the CMD. The server was ping five times and was successful five times. The command used varies a little bit "ping -n 5 <IP>" instead of "ping -c 5 <IP>".

2 Problem 2



This picture above shows the UDP echo server and client talking to each other. It also shows that 5 messages are being sent every second.



2.1 Discussion

In the picture above, when the transfer rate is set to 0 then only one message is going to the server and comes back to the client and shutdown. **To check the validity of the IP address:**

1. Looks if each part between the "." of the IP address are numbers
2. Check if those numbers are between 0 and 255

To check the validity of the Port:

1. Check if argument is a number
2. Check if number is between 0 and 65535

To check the validity of the Buffer Rate:

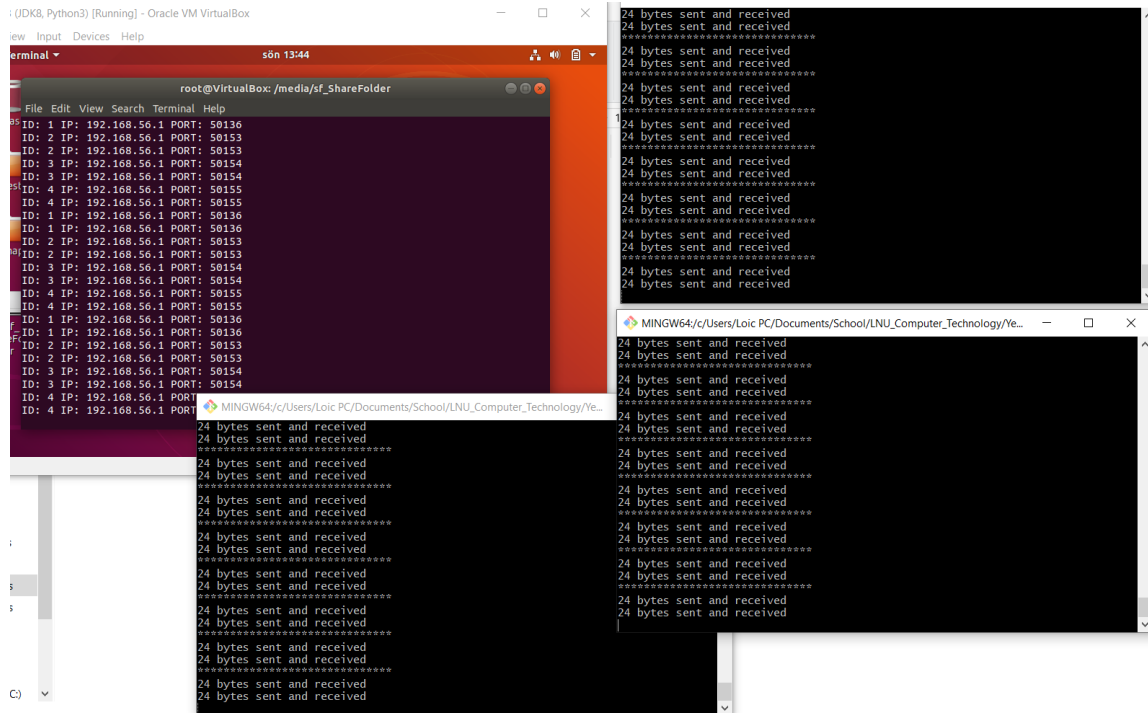
1. Check if argument is a number
2. Check if number is between 1 and 2048

To check the validity of the Transfer Rate:

1. Check if argument is a number
2. Check if number is more than/equal to 0

This check should cover enough exception that might occur with a wrong input.

3 Problem 3



3.1 Discussion

The picture above shows the VM running the EchoServer with TCP on the top left corner and 3 CMD running the Echo Client for TCP. It shows that multiple client are handled by the server. The server is run infinitely manual termination

4 Problem 4

8	30.634000	192.168.56.1	50390 → 4950 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_	192.168.56.102	TCP
9	30.634418	192.168.56.102	4950 → 50390 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	192.168.56.1	TCP
10	30.634576	192.168.56.1	50390 → 4950 [ACK] Seq=1 Ack=1 Win=2102272 Len=0	192.168.56.102	TCP
11	30.636246	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=24	192.168.56.102	TCP
12	30.636556	192.168.56.102	4950 → 50390 [ACK] Seq=1 Ack=25 Win=64256 Len=0	192.168.56.1	TCP
13	30.645984	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=1 Ack=25 Win=64256 Len=24	192.168.56.1	TCP
14	30.686687	192.168.56.1	50390 → 4950 [ACK] Seq=25 Ack=25 Win=2102272 Len=0	192.168.56.102	TCP
15	30.730832	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=25 Ack=25 Win=2102272 Len=24	192.168.56.102	TCP
16	30.731165	192.168.56.102	4950 → 50390 [ACK] Seq=25 Ack=49 Win=64256 Len=0	192.168.56.1	TCP
17	30.732331	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=25 Ack=49 Win=64256 Len=24	192.168.56.1	TCP
18	30.772195	192.168.56.1	50390 → 4950 [ACK] Seq=49 Ack=49 Win=2102272 Len=0	192.168.56.102	TCP
19	31.634653	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=49 Ack=49 Win=2102272 Len=24	192.168.56.102	TCP
20	31.634978	192.168.56.102	4950 → 50390 [ACK] Seq=49 Ack=73 Win=64256 Len=0	192.168.56.1	TCP
21	31.635554	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=49 Ack=73 Win=64256 Len=24	192.168.56.1	TCP
22	31.635851	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=73 Ack=73 Win=2102272 Len=24	192.168.56.102	TCP
23	31.636510	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=73 Ack=97 Win=64256 Len=24	192.168.56.1	TCP
24	31.676857	192.168.56.1	50390 → 4950 [ACK] Seq=97 Ack=97 Win=2102272 Len=0	192.168.56.102	TCP
25	32.634669	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=97 Ack=97 Win=2102272 Len=24	192.168.56.102	TCP
26	32.635410	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=97 Ack=121 Win=64256 Len=24	192.168.56.1	TCP
27	32.635743	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=121 Ack=121 Win=2102272 Len=24	192.168.56.102	TCP
28	32.636292	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=121 Ack=145 Win=64256 Len=24	192.168.56.1	TCP
29	32.675653	192.168.56.1	50390 → 4950 [ACK] Seq=145 Ack=145 Win=2102016 Len=0	192.168.56.102	TCP
31	33.635658	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=145 Ack=145 Win=2102016 Len=24	192.168.56.102	TCP
32	33.636495	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=145 Ack=169 Win=64256 Len=24	192.168.56.1	TCP
33	33.636968	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=169 Ack=169 Win=2102016 Len=24	192.168.56.102	TCP
34	33.637718	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=169 Ack=193 Win=64256 Len=24	192.168.56.1	TCP
35	33.677613	192.168.56.1	50390 → 4950 [ACK] Seq=193 Ack=193 Win=2102016 Len=0	192.168.56.102	TCP
36	34.636347	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=193 Ack=193 Win=2102016 Len=24	192.168.56.102	TCP
37	34.637016	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=193 Ack=217 Win=64256 Len=24	192.168.56.1	TCP
38	34.637352	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=217 Ack=217 Win=2102016 Len=24	192.168.56.102	TCP
39	34.637903	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=217 Ack=241 Win=64256 Len=24	192.168.56.1	TCP
40	34.678320	192.168.56.1	50390 → 4950 [ACK] Seq=241 Ack=241 Win=2102016 Len=0	192.168.56.102	TCP
41	35.635663	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=241 Ack=241 Win=2102016 Len=24	192.168.56.102	TCP
42	35.636776	192.168.56.102	4950 → 50390 [PSH, ACK] Seq=241 Ack=265 Win=64256 Len=24	192.168.56.1	TCP
43	35.637240	192.168.56.1	50390 → 4950 [PSH, ACK] Seq=265 Ack=265 Win=2102016 Len=24	192.168.56.102	TCP

4.1 Discussion

The first picture represent the connections between the server and client using TCP and the second one is with using UDP instead. Starting with TCP, the first column shows the

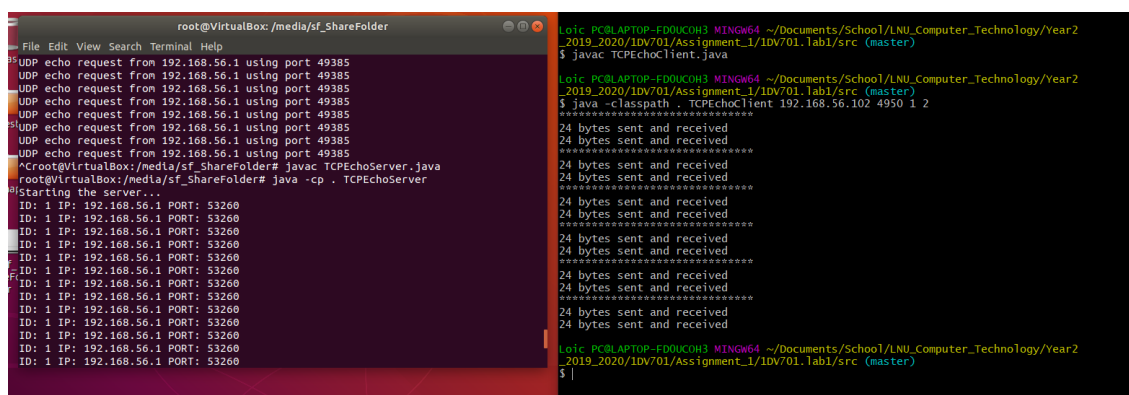
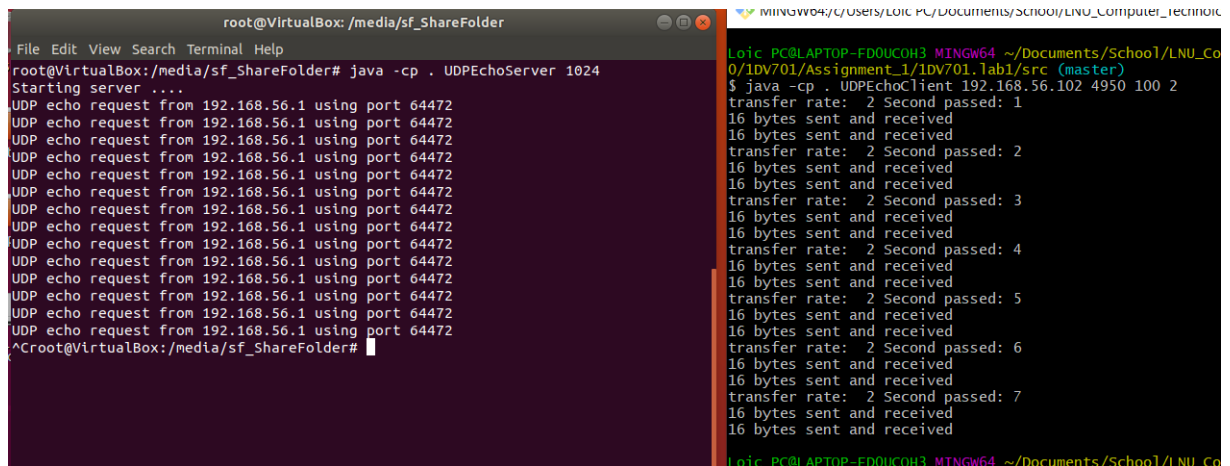
No.	Time	Source	Info	Destination	Protocol	Length
35	6.999635	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
36	7.001621	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
37	7.998563	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
38	7.999388	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
39	7.999838	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
40	8.001432	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
41	8.997930	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
42	8.998406	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
43	8.998856	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
44	8.999557	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
45	9.997919	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
46	9.998414	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
47	9.998968	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
48	9.999487	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
49	10.998656	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
50	10.999076	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
51	10.999482	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
52	11.000393	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
53	11.998684	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
54	11.999191	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
55	11.999652	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
56	12.001115	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
57	12.997793	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
58	12.998355	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
59	12.998944	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
60	13.000020	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
61	13.998114	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
62	13.998713	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
63	13.999284	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
64	14.001704	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
65	14.998598	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
66	14.999154	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
67	14.999669	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
68	15.000751	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	
69	15.998695	192.168.56.1	54659 → 4950 Len=16	192.168.56.102	UDP	
70	15.999155	192.168.56.102	4950 → 54659 Len=16	192.168.56.1	UDP	

number of the connection registered. The second is the time at which the connection happened. Then it is the source IP address, Port of the machine that made the request and port of the destination port, some info that explain what type of connection it is, destination IP address, type of protocol (TCP, UDP). In the screenshot there are two different type of connection: ACK, PSH. ACK indicates that the Acknowledgment filed is significant. PSH is a push function that asks to push all the buffered data to the receiving application. The main difference between UDP and TCP is that TCP is a reliable bidirectional stream of bytes where UDP is just a simple but unreliable message delivery.

When looking at connection number 11 of the picture, we can see that the type is [PSH, ACK] because the Client send the packet and acknowledge it and then waits for the server ACK. On the ligne under it, it is the response from the server with ACK that shows that the server has received the packets and has sent it back. This cycle will continue until some errors appears or when the server is terminated manually.

On the second picture, we can see the different connections made between the VM and Client using UDP. On the first ligne we can see the connection from the client to the server and then the ligne under it is the response from the server to say that it received the packet. And the cycle continues until the manual termination of the server.

5 Problem 5



5.1 Discussion

The first picture represents UDP connection with a buffer size of 100 and the second picture represents TCP connections with buffer size of 100. Wireshark did not show any changes from normal. Just that it is possible to have a buffer of 1 byte for TCP because it is stream but for UDP if the buffer size is bigger than the message then the client will not be able to receive the whole message.