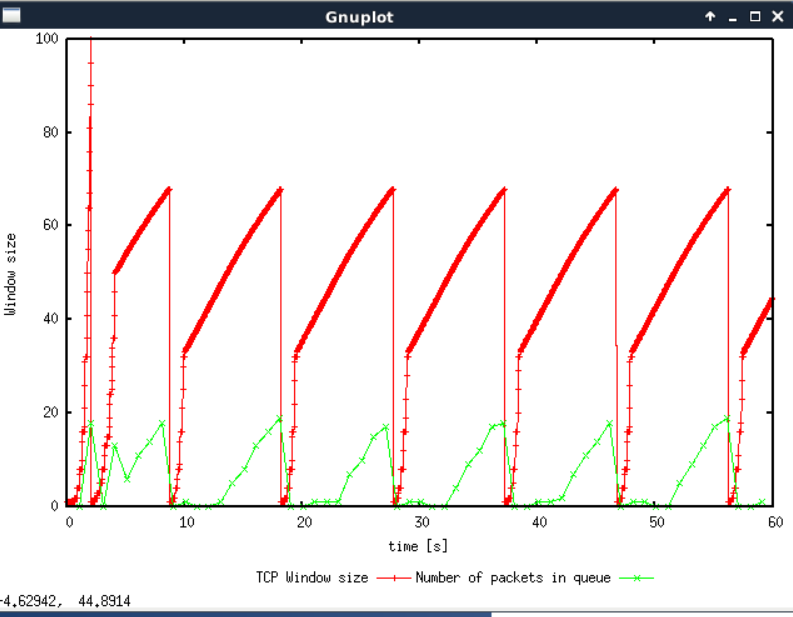
Lab05

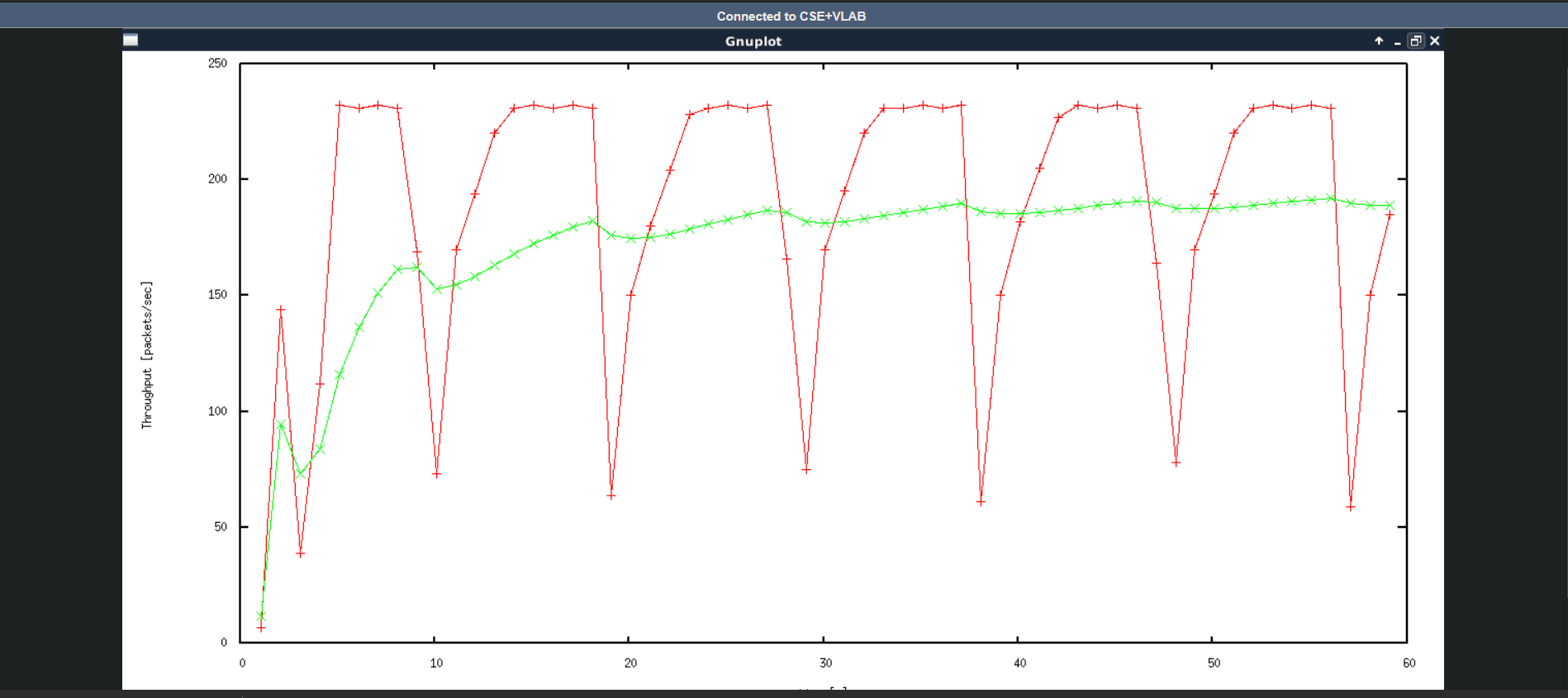
Exercise 1.

1.1

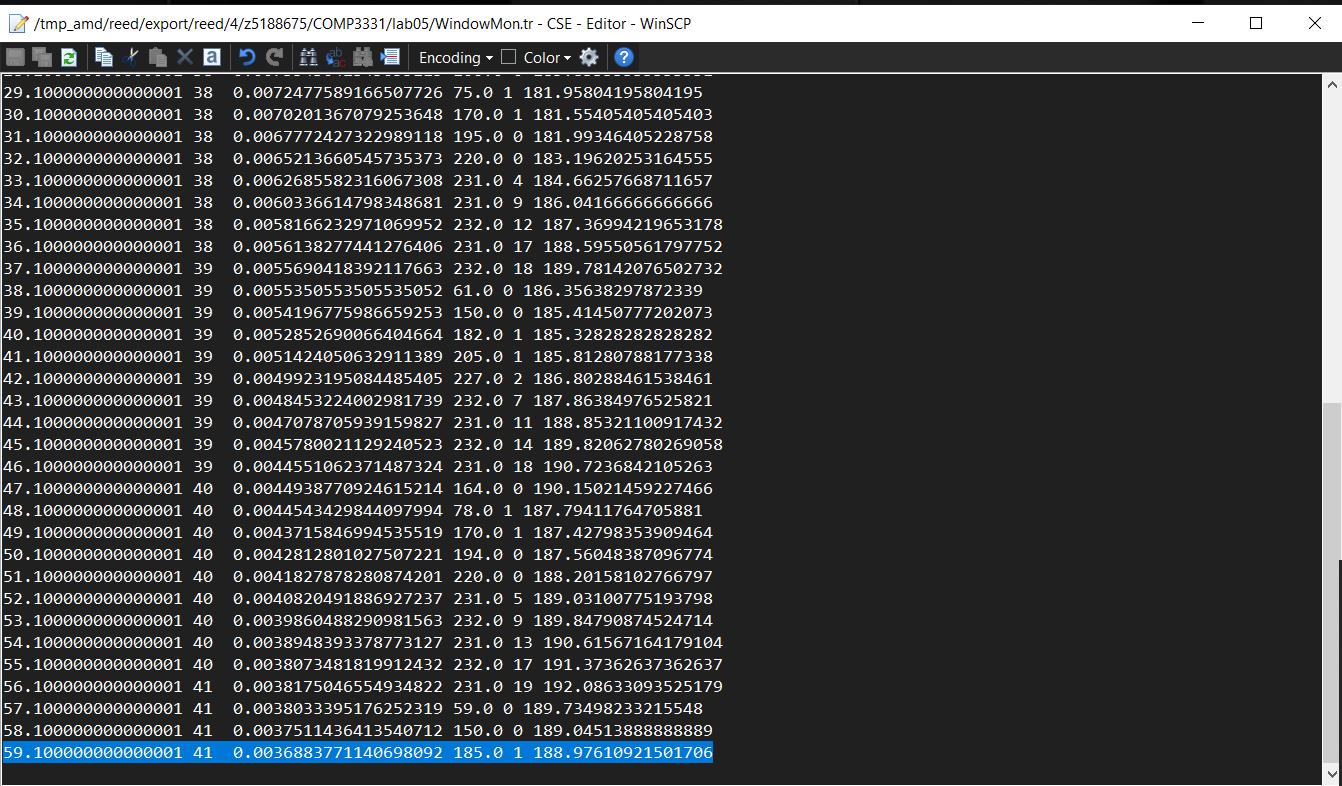


The max window size is 100 in this case, however the tcp congestion control mechanism will decrease the size of the window to 1 after the tcp flow reaches the value of 68 after the first ‘wave’.This is due to the congestion control of tcp. After the size of the window is decreased to 1, the slow start phase will start again with the window size of 1.

1.2



For this question we need to calculate two throughputs, one for the useful throughputs(excluding the headers), and the throughputs for any kinds of data(including headers)



From the last row of windowMon.tr, we can get the average throughputs since the start of the simulation

Throughputs = 188.97610921501706 packets/s

Payload = 500 bytes

payload \_with\_headers = (500 + 20 + 20) = 540 bytes

useful throughputs

= Throughputs \* payload

= 188.97610921501706 packets/s \* 500 bytes

= 94488.05460750853 bytes/s

Any kinds of data throughputs

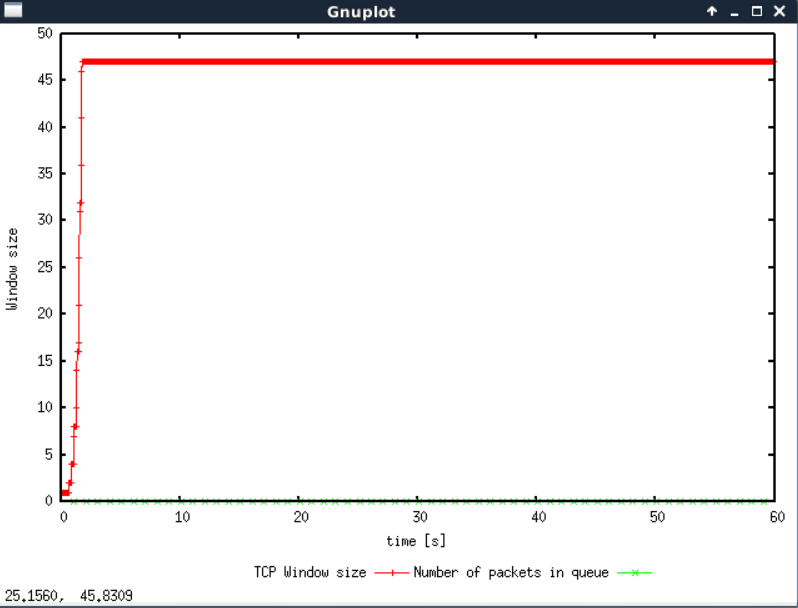
= Throughputs \* payload\_with\_headers

= 188.97610921501706 packets/s \* 540 bytes

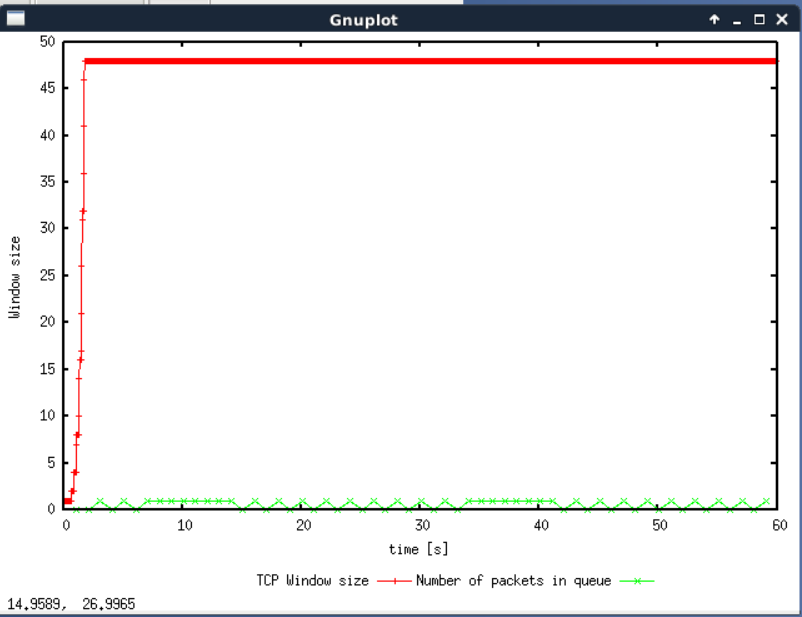
= 102047.0989761092 bytes/s

1.3

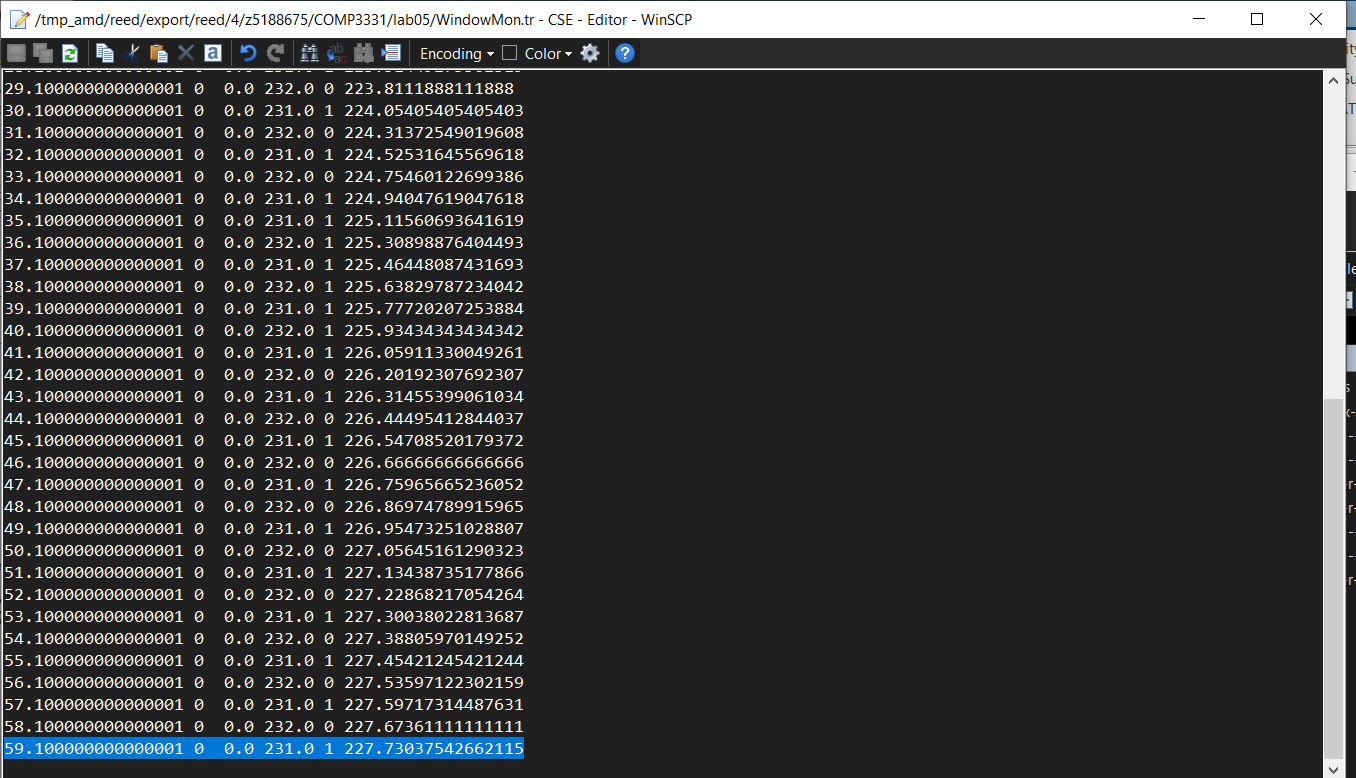
Window size = 47



Window size = 48



As the window size decreases, the number of oscillations decreases. Once the max window size is down till 48, then there is only one oscillation and if the max window size is lower than 48(eg.47), there will not be any oscillation.



The average throughput is 227.73037542662115

packets per second \*from WindowMon.tr Average throughput = (500 + 20 + 20) \* 227.73037542662115 = 122974.40273037543 bytes per second

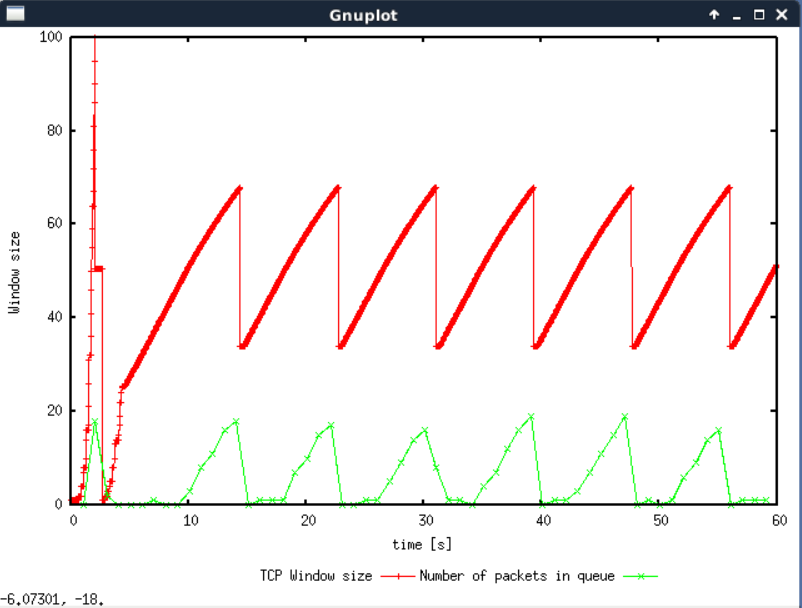
Link = 125000 bytes/s

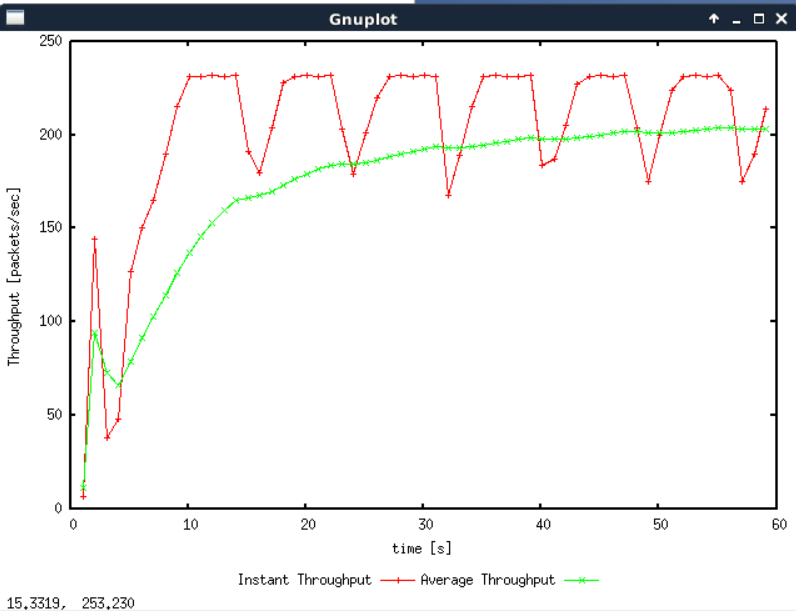
Link capacity

= 100% \* (122974.40273037543/125000)

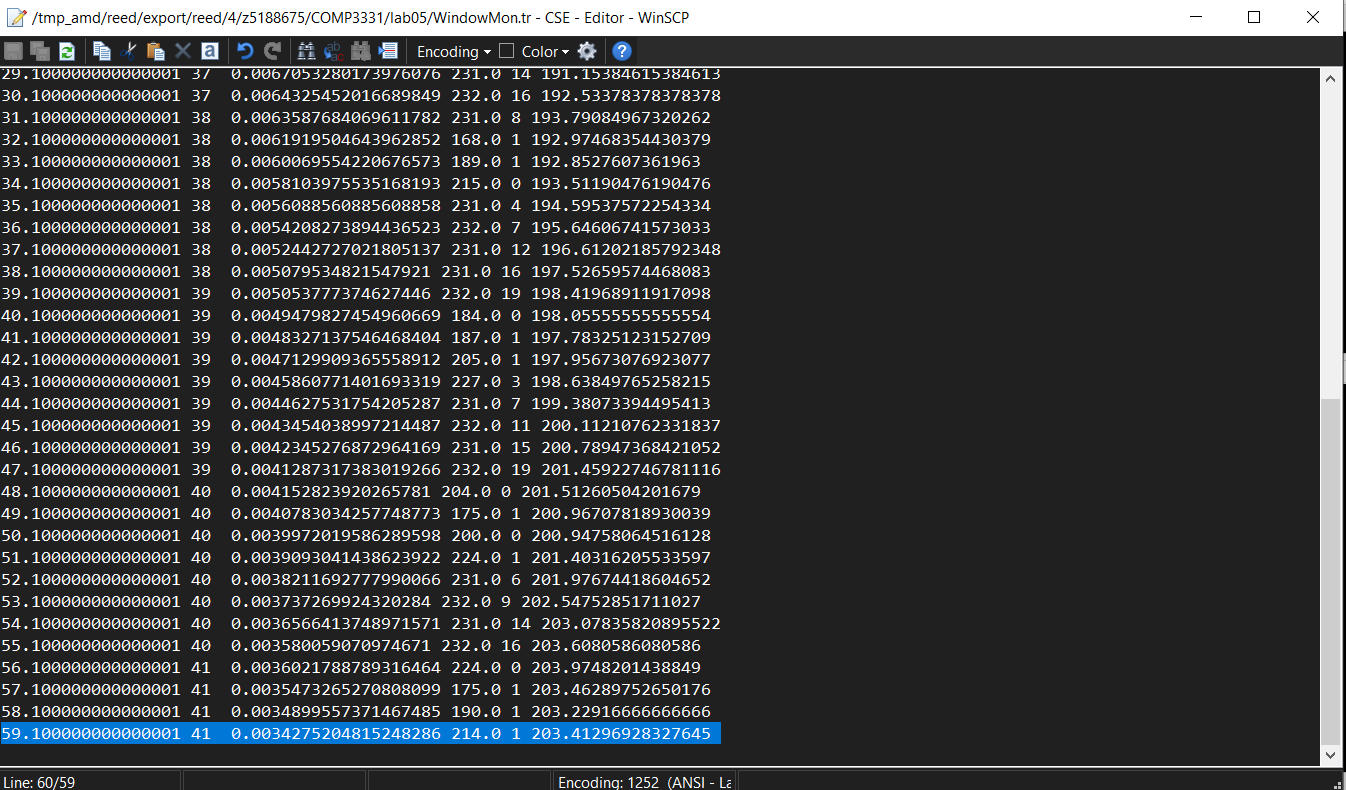
= 98.37952218430034%

1.4





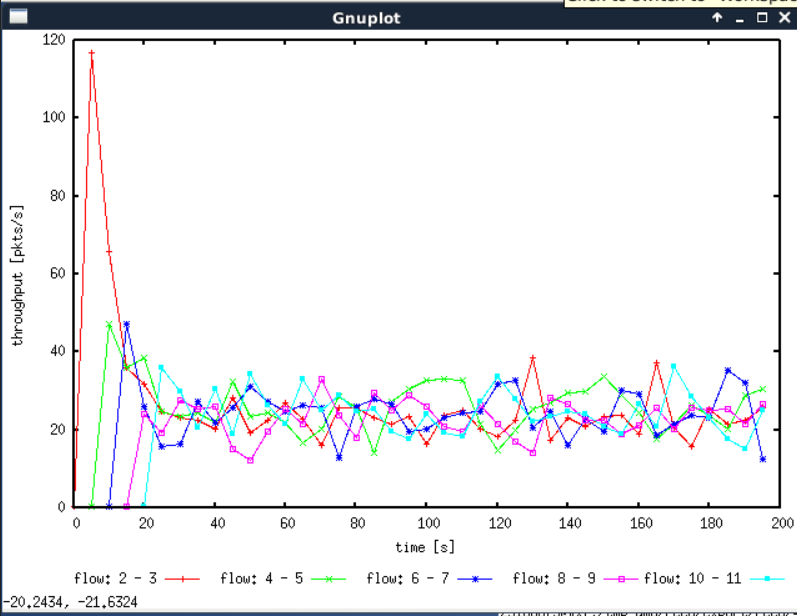
The average throughput of Reno



The window size only hit zero once after a slow start phase for Reno. The average throughput is higher for Reno (203.41296928327645) than Tahoe (188.97610921501706).

Exercise 2.

2.1



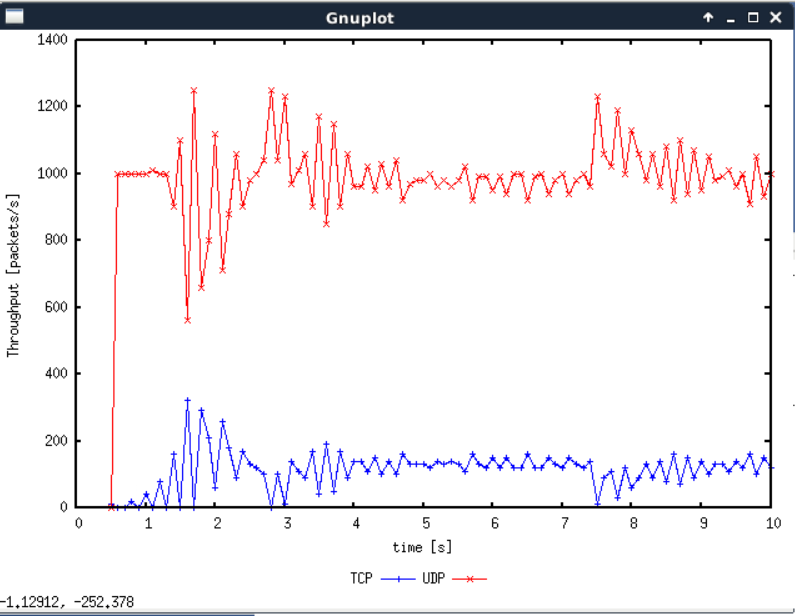
Yes, each flow gets an equal share of the capacity of the common link.Although at the start each flow has a different share of common link, as time goes by, the throughput of each flow is gradually stabilized within the interval of 20 – 40 packets per second.

2.2.

Throughput of pre-existing TCP flows will decrease when a new flow is created to provide equal share. The congestion window size increases rapidly during the slow start phase which causes congestion. Thus, all flows will adjust to adapt the network. I would consider this behaviour to be fair because the design of an internet system is always about trade off, in this case the decrease of the bandwidth of all the users will be used to guarantee the stability of the network. And all the users will be benefited from it.

Exercise3.

3.1



TCP has congestion control, while UDP has no congestion control which means under the same internet condition, the bandwidth of TCP will dominate the bandwidth of UDP

3.2

The flow with higher throughput is udp(mentioned in previous section) which does not provide congestion control mechanism, it provides best-effort datagram where application needs to provide its own reliability and flow control. The flow with lower throughput is tcp(mentioned in the previous section) which has a congestion control mechanism. It will provide a stable connection and not overload the link by changing the window size based on conditions.

3.3

Advantages using UDP over TCP

- Higher average throughput

- Transfer rate based off link bandwidth

- Smaller packet size

Disadvantages using UDP over TCP

- No congestion control

- The order of arriving packets are not guaranteed

- The application will need to have their own measure to deal with packages loss and corrupted packages

As it is mentioned in the section 1, if everyone started using UDP over TCP, then the performance of the network system will be terribly impacted as there is neither congestion control design which helps the network conjectures nor safety guaranteed information transmission which will cause the application without having security measures have the risk of losing packets and unable to deal with corrupted packets.