

# CCN - Assignment

Chandra Kiran G

S20190010029

**Q1. Basic client-server application with a data rate of 50mbps, 5ms delay.**

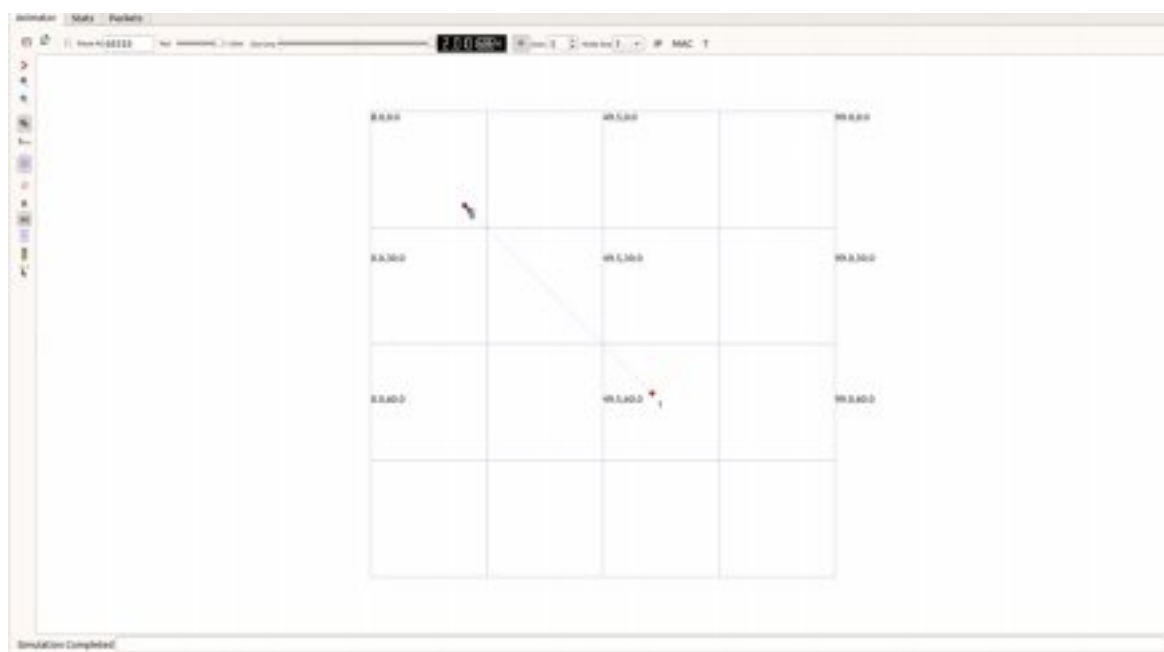
**Assume the server port number to be 32.**

**The Output for the above is:**

```
Chandu@kiran: ~/Desktop/ns-allinone-3.33/ns-3.33 > ./waf --run scratch/First.cc
Waf: Entering directory `/home/karalius/Desktop/ns-allinone-3.33/ns-3.33/build'
Waf: Leaving directory `/home/karalius/Desktop/ns-allinone-3.33/ns-3.33/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (1.008s)
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
At time +2s client sent 1024 bytes to 10.1.1.2 port 32
At time +2.00517s server received 1024 bytes from 10.1.1.1 port 49153
At time +2.00517s server sent 1024 bytes to 10.1.1.1 port 49153
At time +2.01034s client received 1024 bytes from 10.1.1.2 port 32
```

**Q2. Nodes are taken at (20,20) and (60,60).**

**NetAnim simulation:**



**Trace metrics illustrating Throughput/Goodput :**

TraceMetrics - a trace analyzer for Network Simulator 3

File Tools Help

Simulation Nodes Throughput / Goodput Little's Result Streams

Node	Throughput	Goodput
0	524.2894236795767	509.3685748062417
1	524.2894236795767	509.3685748062417

Q3.

## Pcap analysis with the help of tcpdump tool and illustration in the Wireshark

```
Chandu@kiran: ~/Desktop/ns-allinone-3.33 > tcpdump -nn -tt -r animation-0-0.pcap
reading from file animation-0-0.pcap, link-type PPP (PPP)
2.000000 IP 10.1.1.1.49153 > 10.1.1.2.32: UDP, length 1024
2.010337 IP 10.1.1.2.32 > 10.1.1.1.49153: UDP, length 1024

Chandu@kiran: ~/Desktop/ns-allinone-3.33 > tcpdump -nn -tt -r animation-1-0.pcap
reading from file animation-1-0.pcap, link-type PPP (PPP)
2.005168 IP 10.1.1.1.49153 > 10.1.1.2.32: UDP, length 1024
2.005168 IP 10.1.1.2.32 > 10.1.1.1.49153: UDP, length 1024
```

➤ In pcap analysis we get different .pcap files for client and server.

➤ We need to analyse individually for client and server for this pcap analysis.

### Pcap Analysis for Client:

No.	Time	Source	Destination	Protocol
1	0.000000	10.1.1.1	10.1.1.2	UDP
2	0.010337	10.1.1.2	10.1.1.1	UDP

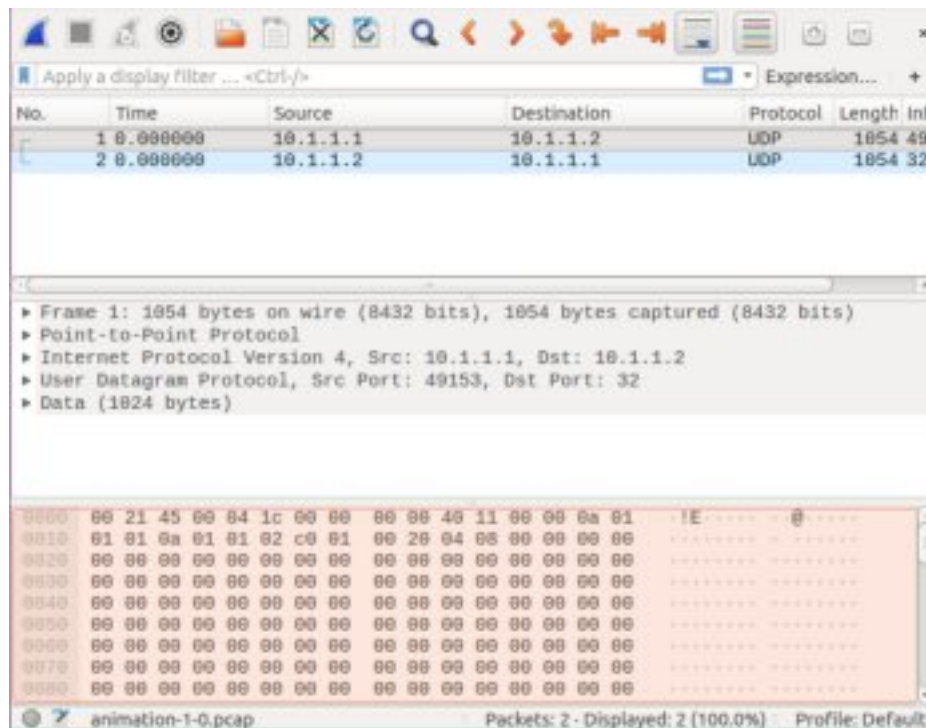
  

▶ Frame 1: 1054 bytes on wire (8432 bits), 1054 bytes captured (8432 bit) on interface 0  
 ▶ Point-to-Point Protocol  
 ▶ Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.2  
 ▶ User Datagram Protocol, Src Port: 49153, Dst Port: 32  
 ▶ Data (1024 bytes)

0000	00 21 45 00 04 1c 00 00	00 00 40 11 00 00 0a 01	!E----	@
0010	01 01 0a 01 01 02 c0 01	00 20 04 08 00 00 00 00	-----	
0020	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	-----	

animation-0-0.pcap      Packets: 2 · Displayed: 2 (100.0%)      Prof

### Pcap Analysis for Server:



### Summary:

- In this Assignment we implemented a basic client-server program and simulated with ns3 simulator.
- Through NS3 simulator we get a clear-cut picture of the simulation.
- With help of trace metrics we analysed the Throughput / Goodput of our program.
- Wireshark(Packet sniffer tool) is used here to analyse IP address of source,destination and port number, type of protocol, etc. of that packet.