

# Assignment 1

Shubham Sharma, 2021099

## 1) a) Laptop connected to IIITD AP

```
shubham21099@SHUBHAM:~$ iwconfig
lo                no wireless extensions.

wlo1              IEEE 802.11  ESSID:"LAPTOP-S"
                  Mode:Managed  Frequency:5.745 GHz  Access Point: 00:5D:73:27:E9:AB
                  Bit Rate=650 Mb/s   Tx-Power=21 dBm
                  Retry short limit:7   RTS thr:off   Fragment thr:off
                  Power Management:on
                  Link Quality=44/70  Signal level=-66 dBm
                  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
                  Tx excessive retries:0  Invalid misc:8  Missed beacon:0
```

**SSID:-** LAPTOP-S

**BSSID:-** 00:5D:73:27:E9:AB

**Signal Strength:-** -66 dBm

**Bit Rate:-** 650 Mb/s

**Transmission Power:-** 21 dBm

**Frequency Band:-** 5.745 GHz

## b) Laptop connected to Hotspot

```
shubham21099@SHUBHAM:~$ iwconfig
lo                no wireless extensions.

wlo1              IEEE 802.11  ESSID:"OPPO A74 5G"
                  Mode:Managed  Frequency:5.18 GHz  Access Point: 6A:F1:93:EF:B7:04
                  Bit Rate=390 Mb/s   Tx-Power=20 dBm
                  Retry short limit:7   RTS thr:off   Fragment thr:off
                  Power Management:on
                  Link Quality=69/70  Signal level=-41 dBm
                  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
                  Tx excessive retries:0  Invalid misc:49  Missed beacon:0
```

**SSID:-** OPPO A74 5G

**BSSID:-** 6A:F1:93:EF:B7:04

**Signal Strength:-** -41 dBm

**Bit Rate:-** 390 Mb/s

**Transmission Power:-** 20 dBm

**Frequency Band:-** 5.18 GHz

I, noticed there is a difference in values of both measurements it is because these measurements depends on the factors like how far is AP from device, wireless standards, interference, and environmental conditions which impacts the wireless networks.

**2)** By using below commands I put my laptop in monitor mode then collect the **pcap trace** for 5 minutes using wireshark tool.

```
shubham21099@SHUBHAM:~$ sudo systemctl stop NetworkManager.service
[sudo] password for shubham21099:
shubham21099@SHUBHAM:~$ sudo ifconfig wlo1 down
shubham21099@SHUBHAM:~$ sudo iwconfig wlo1 mode monitor
shubham21099@SHUBHAM:~$ sudo ifconfig wlo1 up
shubham21099@SHUBHAM:~$ iwconfig
lo                no wireless extensions.

wlo1              IEEE 802.11  Mode:Monitor  Frequency:5.745 GHz  Tx-Power=20 dBm
                  Retry short limit:7   RTS thr:off   Fragment thr:off
                  Power Management:on
```

### **a) Identify #unique MAC addresses, #of APs, #of Clients**

For this part I exported that **pcap file** into a CSV file then run a python script on that CSV file which provides me the Total Unique MAC addresses, APs and Clients.

Results generated after running script on CSV file:-

#Unique MAC addresses:- **1788**

#APs:- **11**

#Clients:- **1628**

### **b) Compute the average signal strength of each client.**

For this part, again I write a python script which takes same CSV file input and gives me the average signal strength of each client.

*Not able to paste output because output is very large.*

**c) Compute the average bitrate of each client**

For this part, again I write a python script which takes same CSV file input and gives me the average signal strength of each client.

*Not able to paste output because output is very large.*

**d) Identify the number of clients of different standard 802.11 b/g/n or 802.11n/ac**

For this part I write a python script which read from CSV file and provides below output(unique clients):-

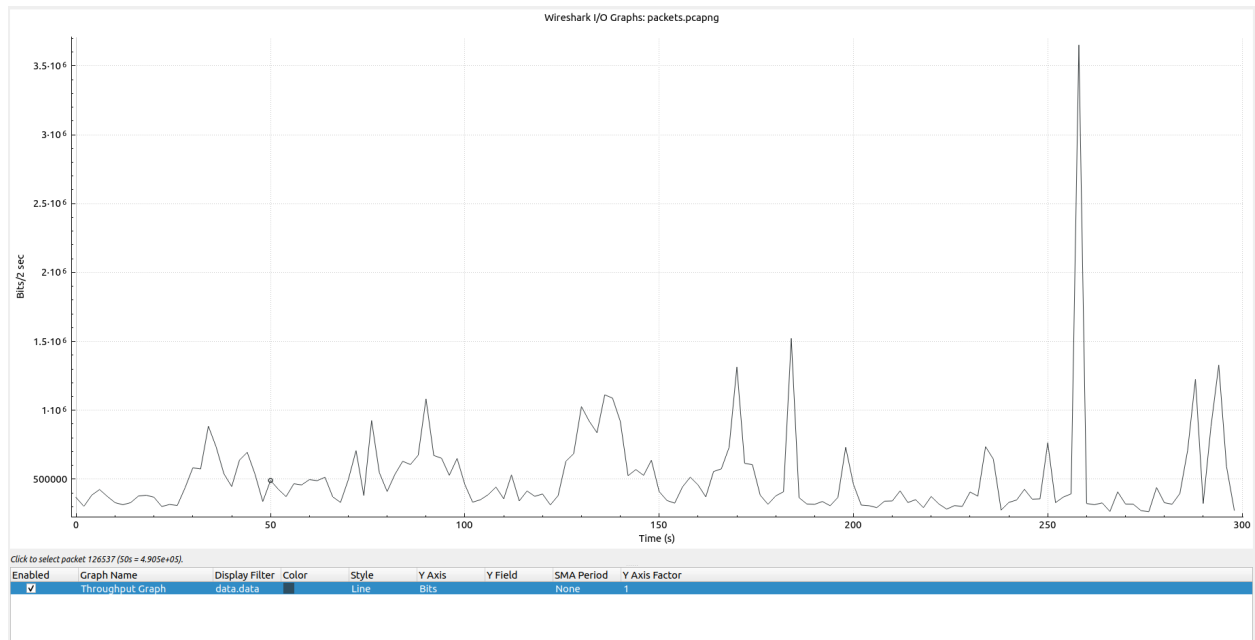
802.11a : **1623**

802.11ac : **3**

802.11n : **3**

**e) Compute the aggregate throughput of the network and plot with time.**

For this part I used wireshark's builtin graph generator tool which generates **bits/2sec vs time** graph. But it will generate graph for all captured packets but we need graph only for data packets so for this I used a filter **data.data** which filters only data packets and generate graph for data packets throughput vs time.



**3) a)** There are different types of frames that are exchanges before actual data transmission like there are some frames of standard DNS Queries for some background running tasks, some membership reports and TCP ack unseen segments frames.

**3) b)** I just applied **tcp** filter and get total TCP packets  
Total TCP Packets = **5862**

**3) c)** I just applied **udp** filter and get total UDP packets  
Total UDP Packets = **3007**

## BONUS QUESTION

**3 a)** Total TCP YouTube Packets = 31.

Calculated by applying specific filter for TCP and Youtube Packets.

**3 b)** Total UDP YouTube Packets = 72.

Calculated by applying specific filter for UDP and Youtube packets.