NWS Assignment 4 Report

Prepared by: Mrinal Aich   (CS16MTECH11009)
Shamik Kundu (CS16MTECH11015)

Q1.a Pie chart of MAC Management, Control, Data Traffic. Further division in Management and control frames (i.e., probe reqs, association reqs, RTS/CTS, power-saving, etc).
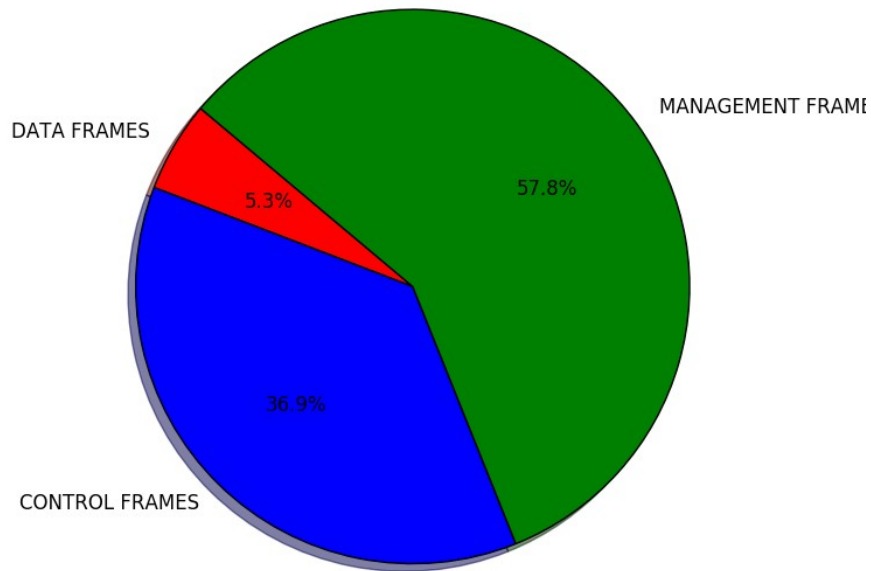

Fig1. Pie Chart of Control frame, Management Frame and Data Frame(TRACE1)

Observation : In TRACE 1, Mananagement frames appeared most in the TRACE and the number of management frames is 57.8% of all the frames.
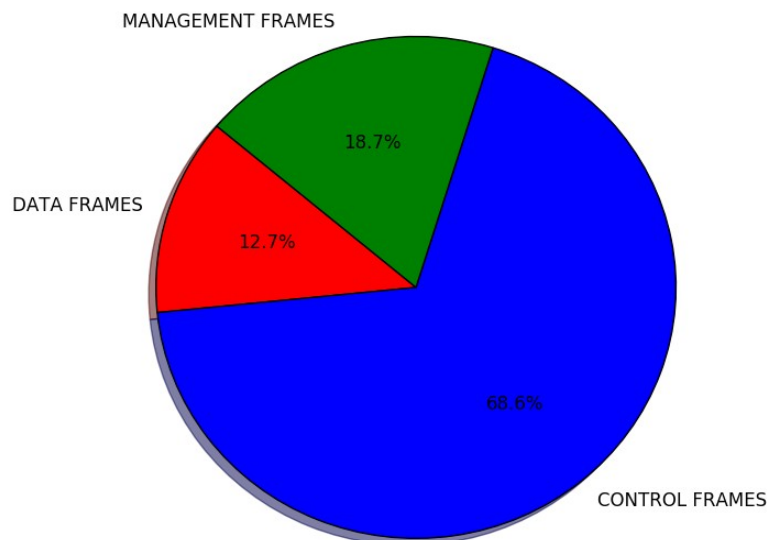

Fig2. Pie Chart of Control frame, Management Frame and Data Frame(TRACE2)

Observation : In TRACE 2, Controlt frames appeared most in the TRACE and the number of control frames is 68.6% of all the frames.

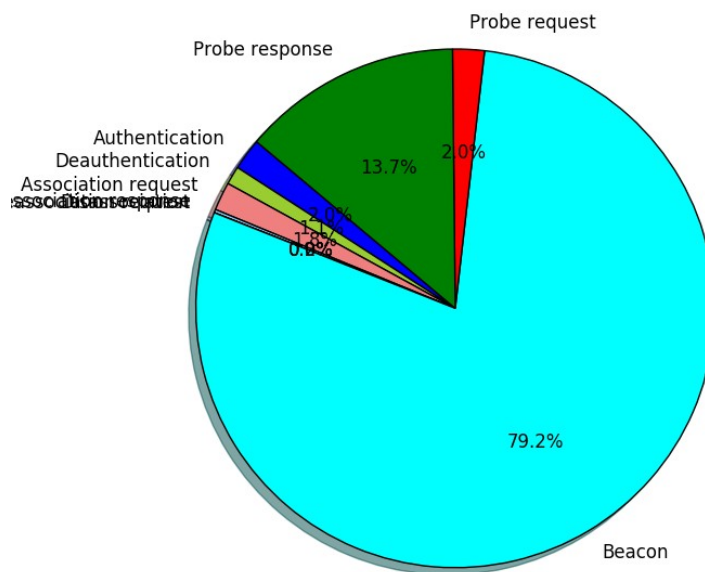## PIE CHART OF MANAGEMENT FRAMES:

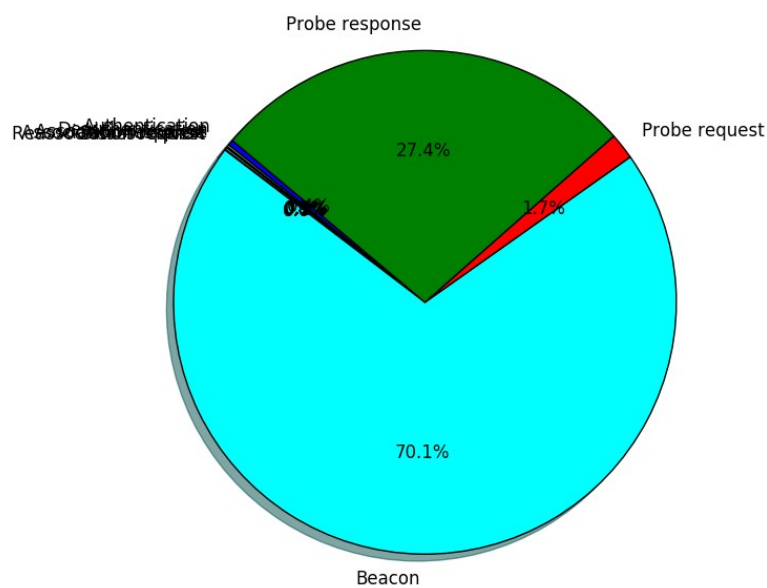Fig3. Pie Chart of different management frames(TRACE1)

Fig4. Pie Chart of different management frames(TRACE2)
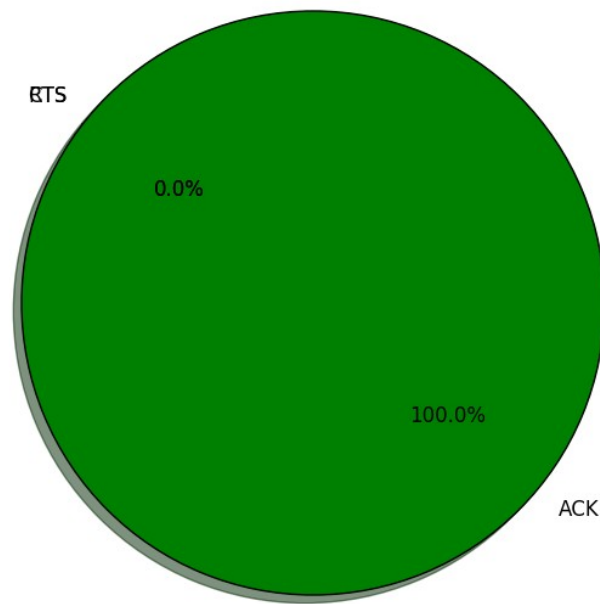
PIE CHART OF CONTROL FRAMES:

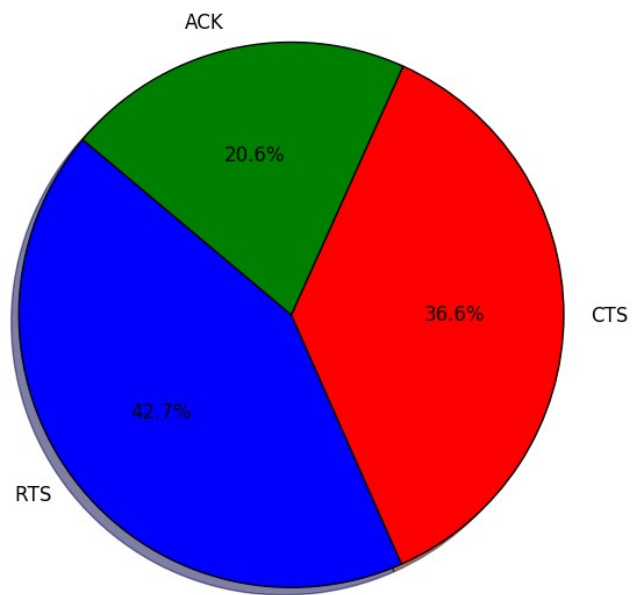Fig5. Pie Chart of different control frames(TRACE1)

Fig6. Pie Chart of different control frames(TRACE2)

Q1.b Pie Chart of Different Application/Network Layer Protocol Traffic:
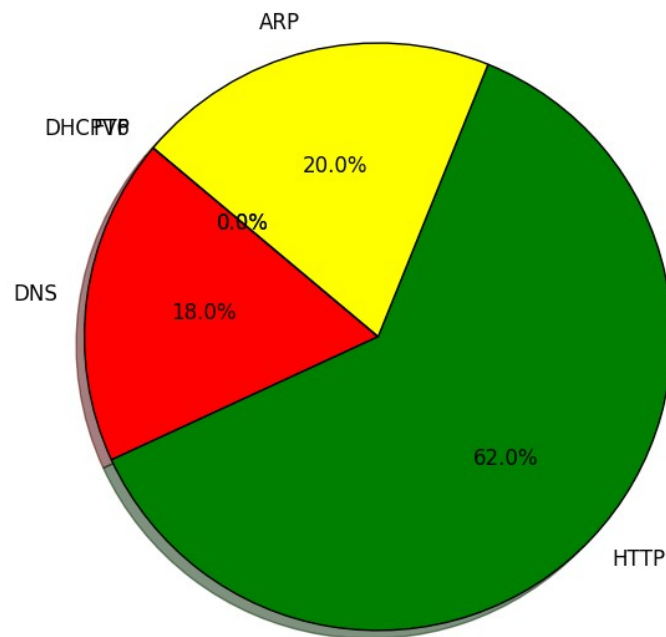
Fig7. Pie Chart of different application/network layer protocol traffic(TRACE1)
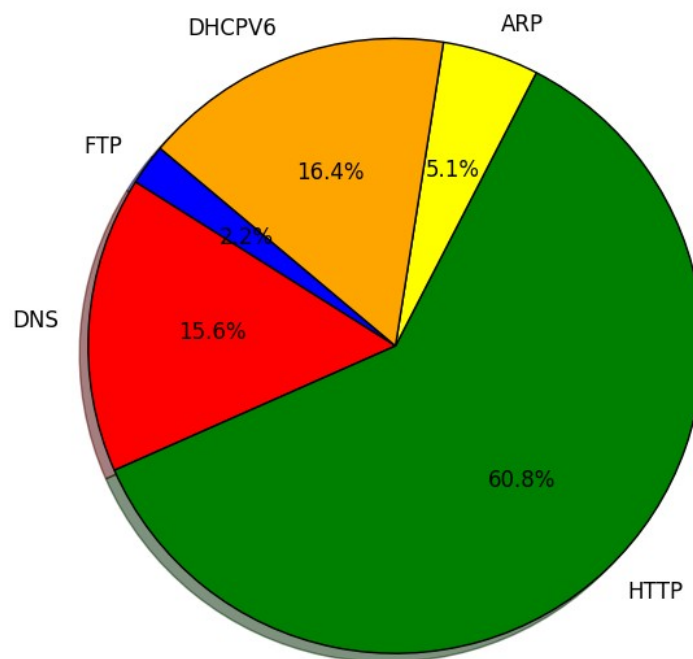
Fig8. Pie Chart of different application/network layer protocol traffic(TRACE2)

Q1.c Plot of avg packet size vs Time, Plot avg PHY data rate vs Time, Plot RSSI (received signal strength) vs Time and Plot Packet rate (pkts/sec) vs Time.

AVERAGE PACKET SIZE vs TIME:

Fig9. Plot of Avg. Packet size vs Time(TRACE1)
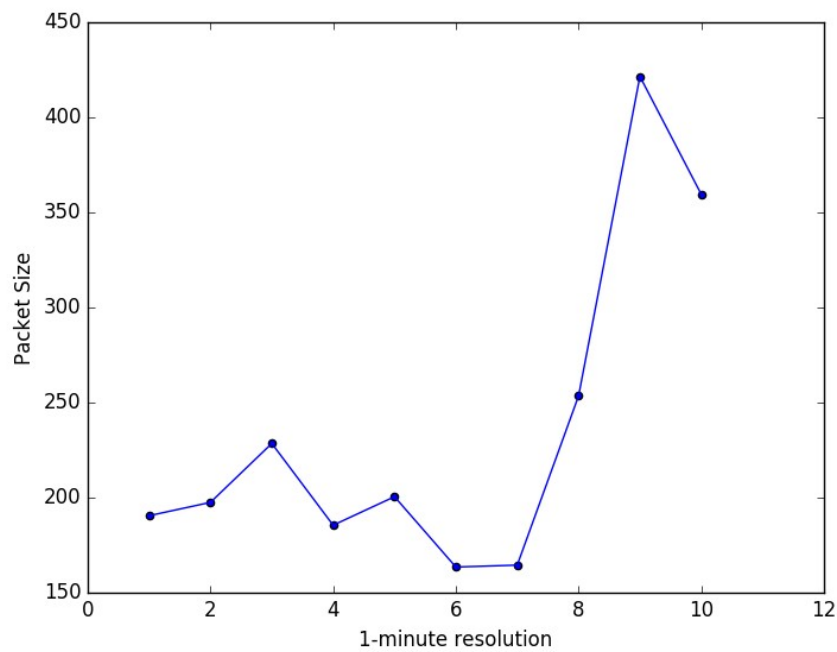
Fig10. Plot of Avg. Packet size vs Time(TRACE2)

PACKET RATE vs TIME:
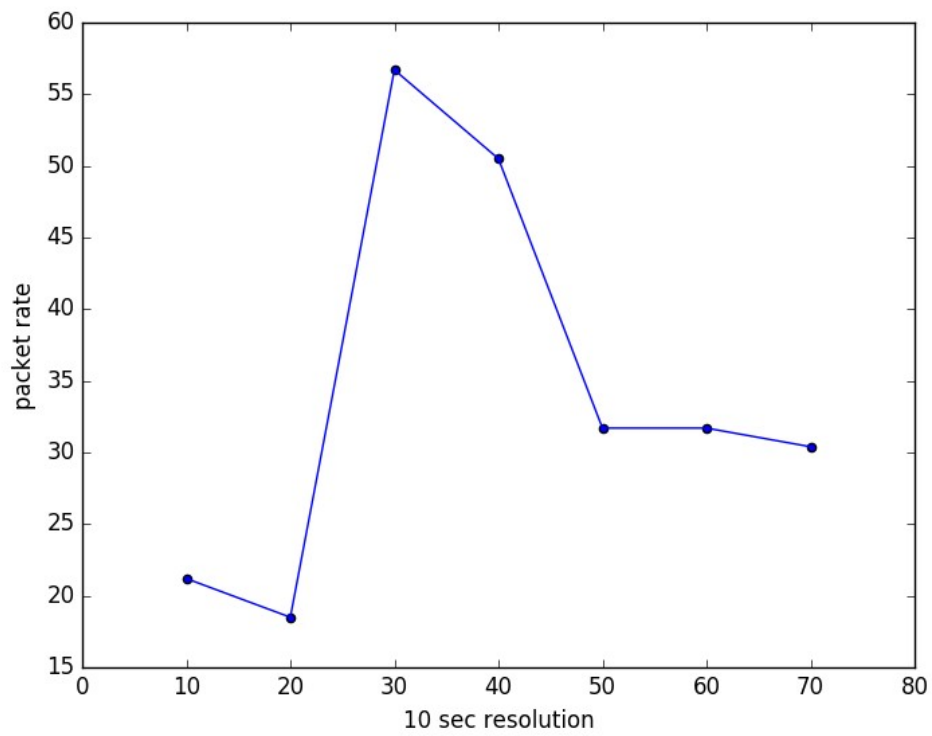
Fig11. Plot of Packet Rate vs Time(TRACE1)
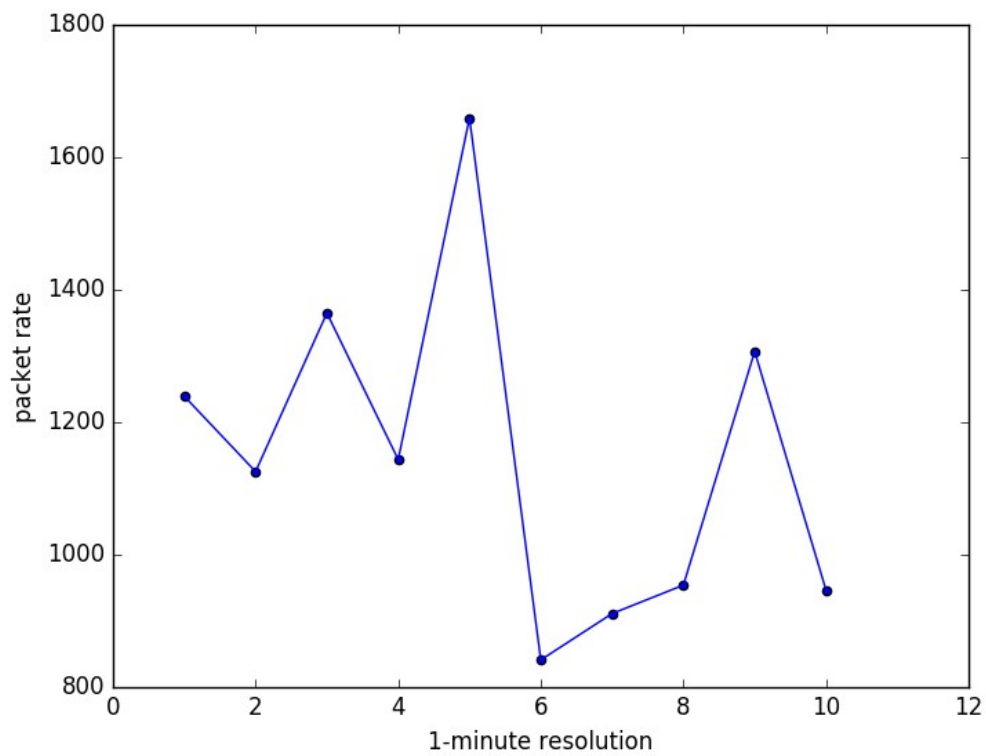
Fig12. Plot of Packet Rate vs Time(TRACE2)

Observation:

1. The number of packets in TRACE2 is much higer compared to TRACE1.
2. Fluctuation in packet rate is drastic in TRACE2.
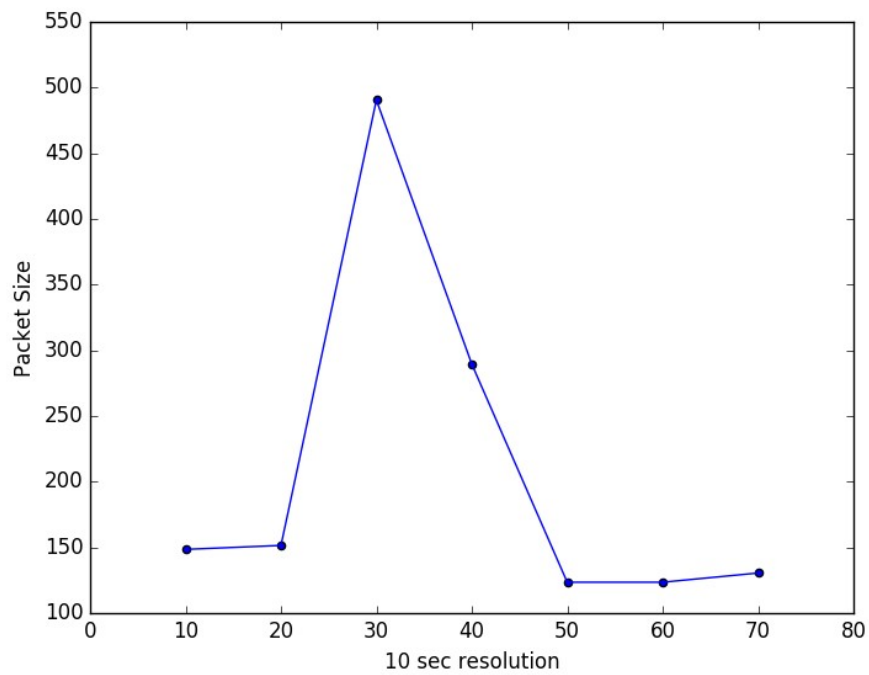3. In interval 4 -6, TRACE2 packet rate is high but avg packet size is small beacuse majority of the packets at this interval are beacon frames or authentication packets.
4. In interval 8 -10, TRACE2 packet rate is relatively less but high avg packet size because of the majority of the data packets.
5. In interval 0 -2, packet size is small and packet rate is relatively small indicating majority of beacon frames only.

RSSI vs TIME:
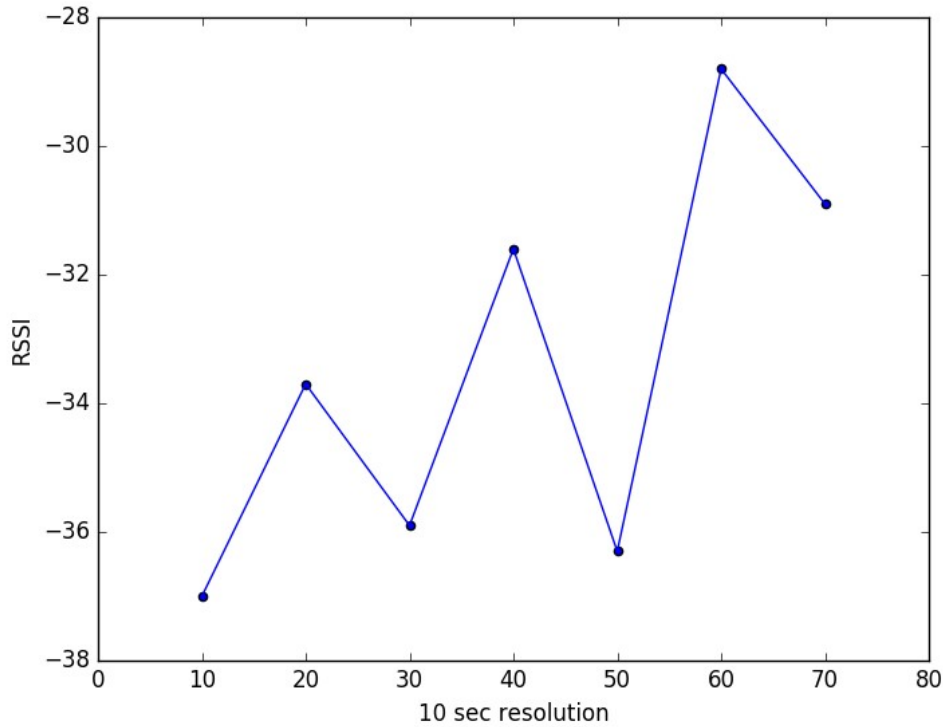
Fig13. RSSI vs Time(TRACE1)
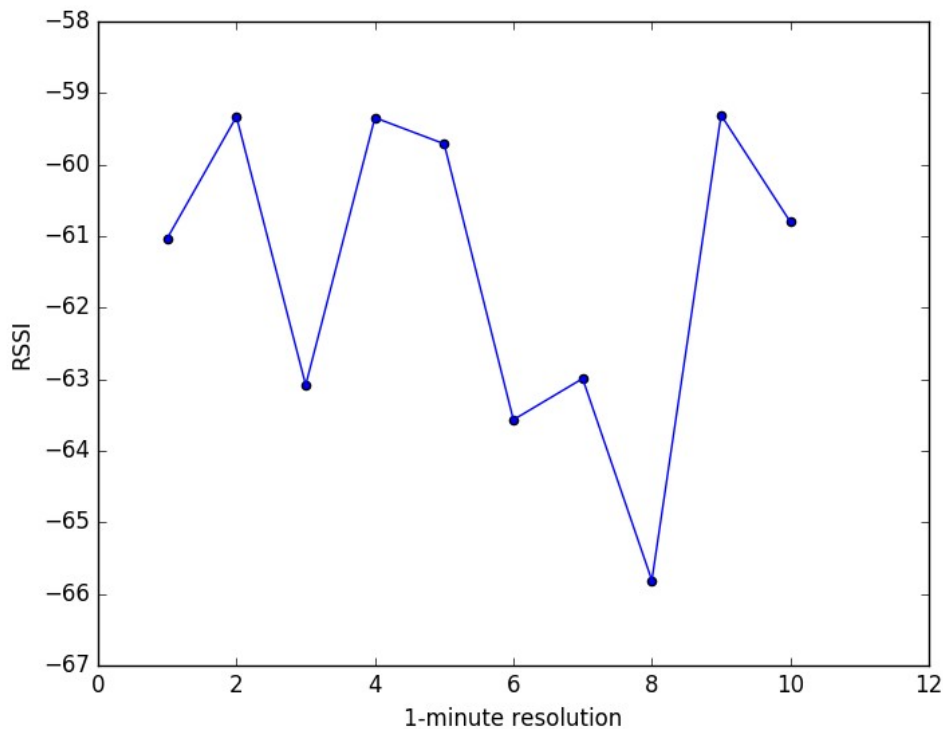
Fig14. RSSI vs Time(TRACE2)

PHY DATA RATE vs TIME:
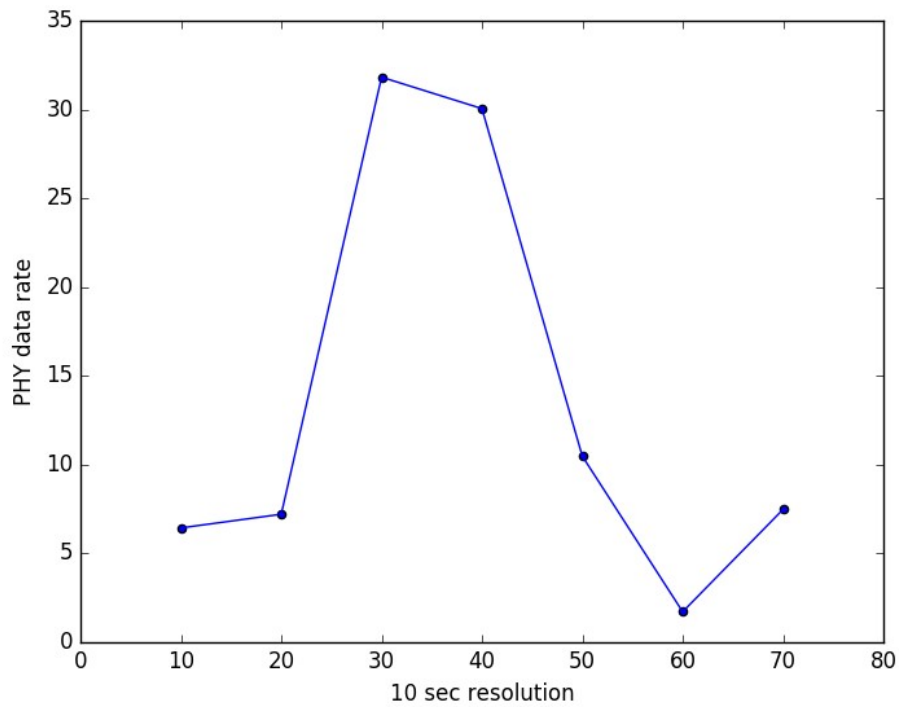
Fig15. PHY Data Rate vs Time(TRACE1)
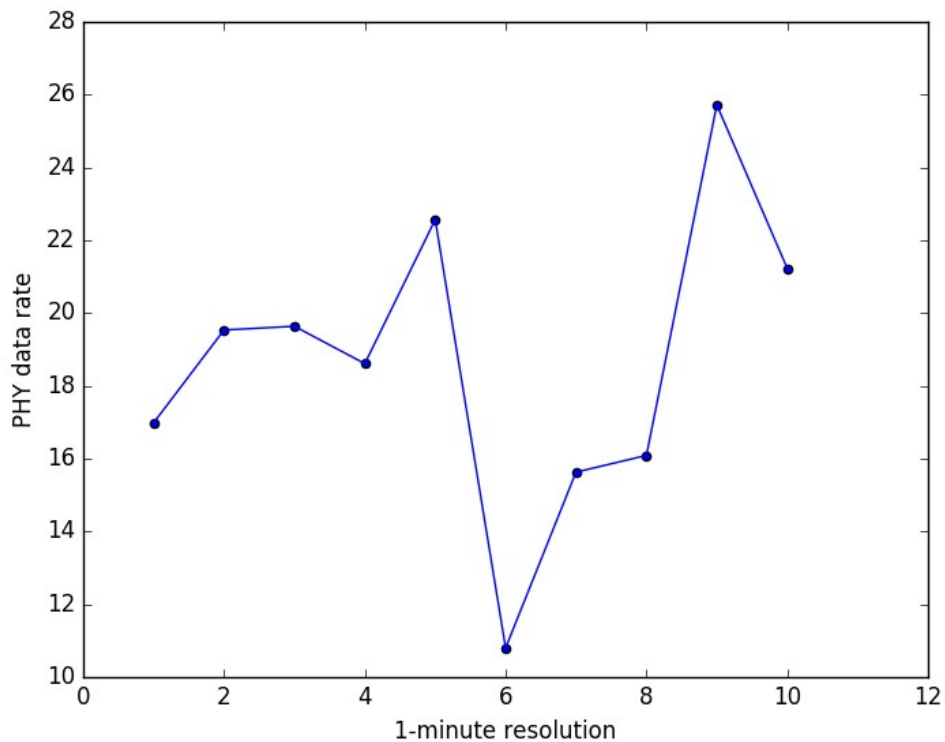
Fig16. PHY Data Rate vs Time(TRACE2)

Observation:

1. With decrease in singnal strength(RSSI), PHY data rate also decreases.

2. In interval 8 -10, assuming majority of data packets (from above) have been sent which may be due to high PHY data rate and RSSI value.

3. Although the highest data rate betwen the two TRACES belongs to TRACE1, average PHY data rate is higher in TRACE2.

Q1.d Histograms of packet sizes and PHY data rates.

Histograms:
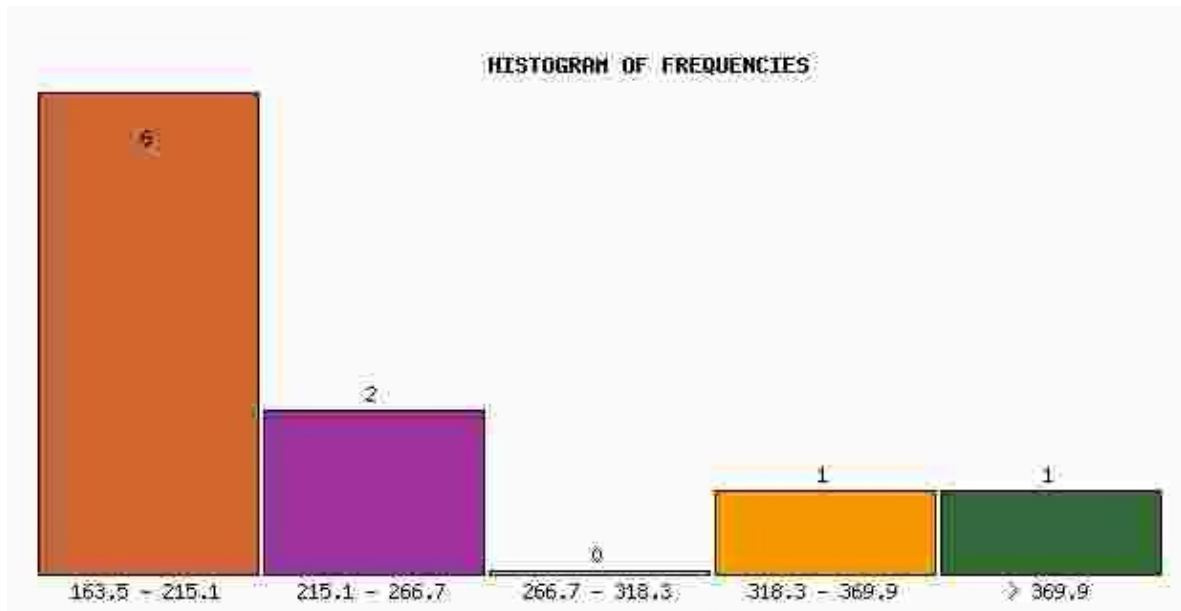
Fig17. Histogram of Packet size

Observation:
 The packet size in most of the cases varies between 163.5 to 215.1Bytes.
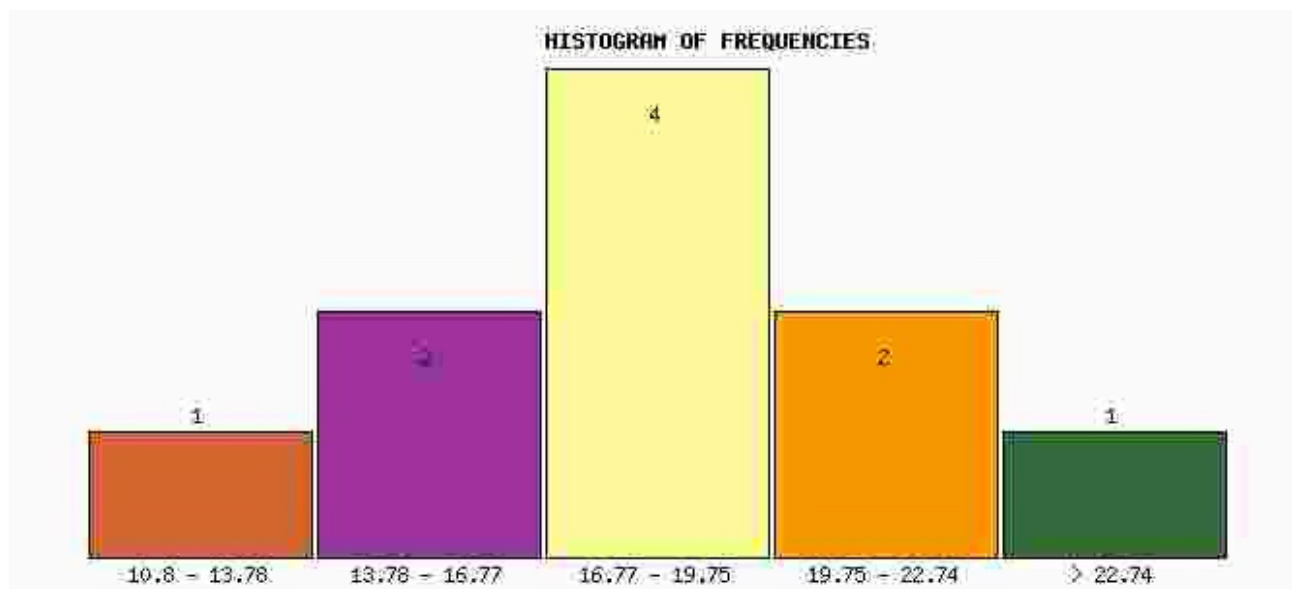
Fig18. Histogram of PHY Data rate(TRACE2)

Observation:
 PHY data rate raninging from 16.77 to 19.75 Mits/sec appeared most of the time in the TRACE2.
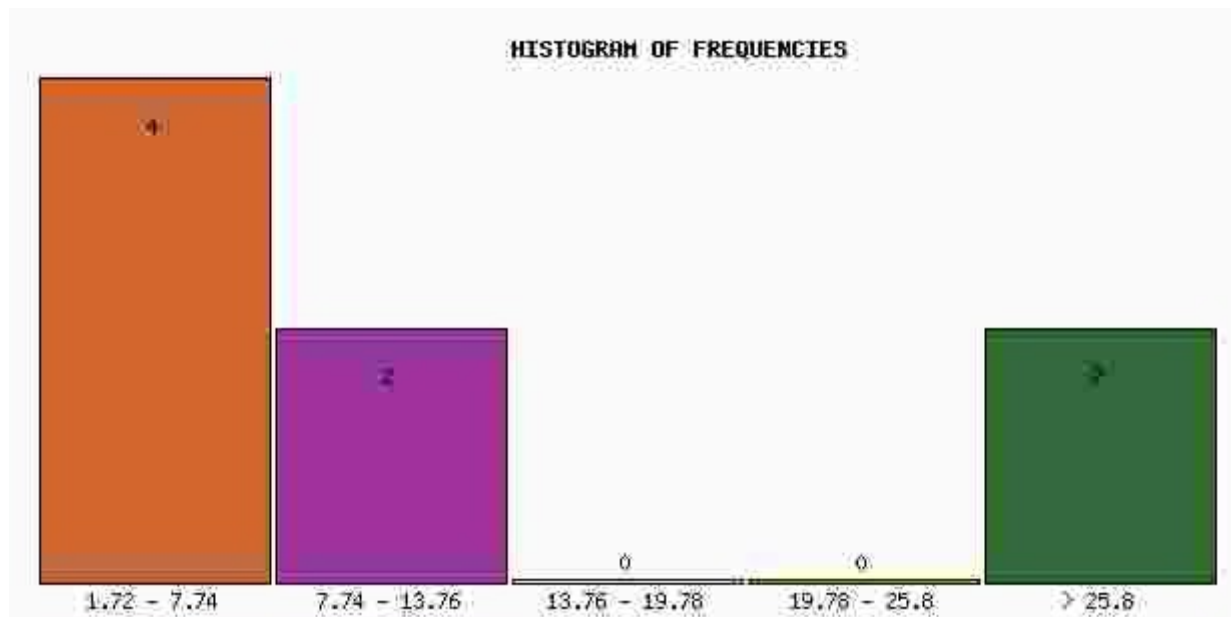
Fig19. Histogram of PHY Data rate(TRACE1)

Observation:
PHY data rate raninging from 1.72Mbits/sec to 7.74 Mits/sec appeared most of the time in TRACE1.

Q1.e Beacon important information.

IITH:
capabilities of AP:

```
Capabilities Information: 0x1421
    .... .... .... ...1 = ESS capabilities: Transmitter is an AP
    .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
    .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
    .... .... ...0 .... = Privacy: AP/STA cannot support WEP
    .... .... ..1. .... = Short Preamble: Allowed
    .... .... .0.. .... = PBCC: Not Allowed
    .... .... 0... .... = Channel Agility: Not in use
    .... ...0 .... .... = Spectrum Management: Not Implemented
    .... .1.. .... .... = Short Slot Time: In use
    .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
    ...1 .... .... .... = Radio Measurement: Implemented
    ..0. .... .... .... = DSSS-OFDM: Not Allowed
    .0.. .... .... .... = Delayed Block Ack: Not Implemented
    0... .... .... .... = Immediate Block Ack: Not Implemented
```

number of stations connected: 18 (LAN management frame-> Tagged parameters-> QBSS load element 802.11e CCA version-> Station count: 18)
channel utilization: 195 (76%)
rate supported: 9, 11, 12, 18, 24, 36, 48, 54 Mbit/sec

IITH-GUEST:
capabilities of AP:

```
Capabilities Information: 0x1431
    .... .... .... ...1 = ESS capabilities: Transmitter is an AP
    .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
    .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
    .... .... ...1 .... = Privacy: AP/STA can support WEP
    .... .... ..1. .... = Short Preamble: Allowed
    .... .... .0.. .... = PBCC: Not Allowed
    .... .... 0... .... = Channel Agility: Not in use
    .... ...0 .... .... = Spectrum Management: Not Implemented
    .... ..1. .... .... = Short Slot Time: In use
    .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
    ...1 .... .... .... = Radio Measurement: Implemented
    ..0. .... .... .... = DSSS-OFDM: Not Allowed
    .0.. .... .... .... = Delayed Block Ack: Not Implemented
    0... .... .... .... = Immediate Block Ack: Not Implemented
```

number of stations connected: 3 (LAN management frame-> Tagged parameters-> QBSS
load element 802.11e CCA version-> Station count: 3)
channel utilization: 182 (71%)
rate supported: 9, 11, 12, 18, 24, 36, 48, 54 Mbit/sec

Q2.a- Describe the whole procedure involved in setting up of your custom AP in the design document.

OS : Ubuntu 14.04 LTS
kernel : 4.4.0-43-generic

The following steps are involved in setting up the custom Acess Point. These are explained in detail later.

1. Installing hostapd and udhcpd packages.
2. Configuring udhcpd
3. Configuring hostapd
4. Setting static IP allocation for the Interface
5. Managing IP tables between the interfaces, IP-Forwarding
6. Starting hostapd and udhcpd services
7*. Debugging/Troubleshoting

(1) Hostapd and Udhcpd packages.
Hostapd - Hostapd (Host access point daemon) is a user space software access point capable of turning normal network interface cards into access points and authentication servers.
Udhcpd - Udhcpd is a DHCP server program using particular network interface cards.

Command : sudo apt-get install hostapd udhcpd

(2) Configuring udhcpd

1.Change in file: *etc/udhcpd.conf*

Changes:
```
start 192.168.101.2        # Starting address to be allocated to devices
end   192.168.101.20       # Last address to be allocated to devices
interface wlp2s0           # Interface that udhcpd will use
max_leases = 19            # difference between the starting address and ending address
opt subnet = 255.255.255.0
opt router = 192.168.101.1     # Address of the interface on which AP will be configured
```

2. Change in file: *etc/default/udhcpd*
From : DHCP_ENABLED="no"
To   : #DHCP_ENABLED="no"

(3). Configuring hostapd

1. Change in file: /etc/hostapd/hostapd.conf
Changes:
```
#Wireless Device
interface=wlp2s0           # AP netdevice name
driver=nl80211             # For all Linux mac80211 drivers


#Wireless Environment
ssid=wirelessAssignment        # Name of the SSID
hw_mode=g                  # Setting this to 802.11g is common, and has backwards
compatability.
channel=6


#Authentication and Encryption
macaddr_acl=0              # mac address filtering.
auth_algos=1               # Shared key Authentication
own_ip_addr=192.168.101.1      # AP's IP address
wpa=2                      # wpa2 authentication only
wpa_passphrase=12312312        # wpa-Passphrase
wpa_key_mgmt=WPA-PSK           # wpa-pre shared key
```

2. Change in file: *etc/default/hostapd*
To change the default configuration file.
From: DAEMON_CONF="/etc/usr/sbin/hostapd.conf"
To : DAEMON_CONF="/etc/hostapd/hostapd.conf"

(4). Allocating static IP Address for the AP Interface
1. Change in file: */etc/network/interfaces*

auto wlp2s0
iface wlp2s0 inet static
   address 192.168.101.1
   netmask 255.255.255.0

Note: Remove the following lines if any
auto wlp2s0 inet dhcp

2. Restart networking service for the above change to reflect
service networking restart

(5). Managing IP tables between the interfaces and enbale IP-forwarding
(Internet accessable interface and AP-interface)

1. Changing the iptable-persistent : To save Iptables Firewall Rules Permanently accross
reboots
 Note: Install iptables-persistent, if not: apt-get install iptables-persistent

Change in file: */etc/iptables/rules.v4*

Under the *nat section:
-A POSTROUTING -o enp1s0 -j MASQUERADE
-A FORWARD -i enp1s0 -o wlp2s0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i wlp2s0 -o enp1s0 -j ACCEPT
Line1: IP Masquerading: Linux IP Masquerading allows for internal interfaces to reach the
Internet even though these internal machines don't have an officially assigned IP address.
Line2: Forward traffic from in-interface 'enp1s0' to out-inferace 'wlp2s0' if state of the
packet is either RELATED or ESTABLISHED.
   ESTABLISHED meaning that the packet is associated with a connection which has seen
packets in both directions,
   RELATED meaning that the packet is starting a new connection, but is associated with an
existing connection, such as an FTP data transfer.
Line3: Forward traffic from in-interface 'wlp2s0' to out-inferace 'enp1s0'.
    -j ACCEPT: To let the packet through.

(OR) Manually in CLI: (root-user)
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT

2. Enabling IPv4 packet forwarding
Change in file: /etc/sysctl.conf
From: #net.ipv4.ip_forward=1
To: net.ipv4.ip_forward=1 (Uncomment)

(6). Starting Hostapd and Udhcpd services
service hostapd start
service udhcpd start

(7). Following commands may be used for troubleshooting purposes.
1. To check status of a service
systemctl status hostapd.service
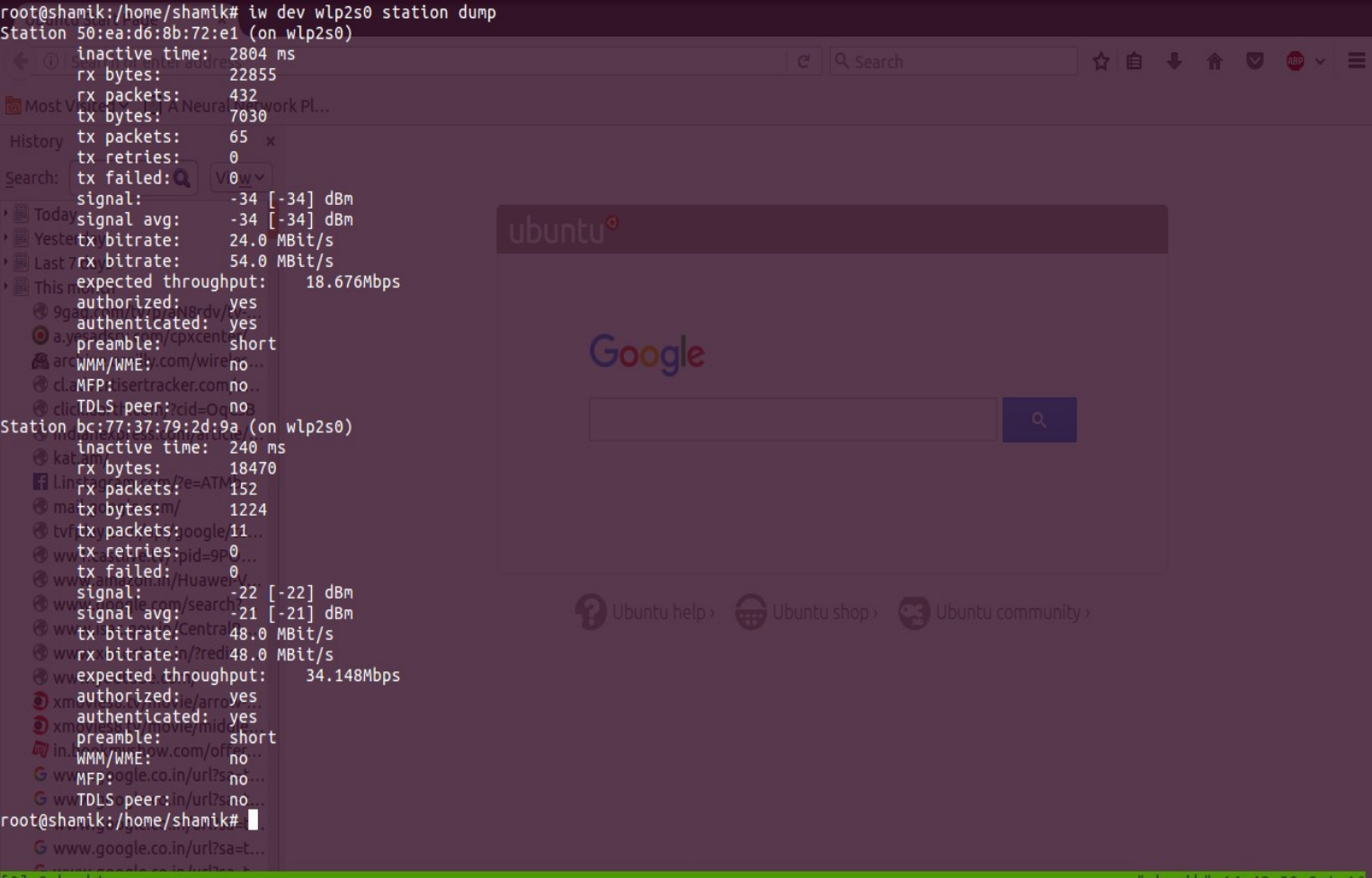systemctl status udhcpd.service

2. Debugging hostapd service
hostapd -d /etc/hostapd/hostapd.conf

3. Number of stations connected to an interface(Access-Point)
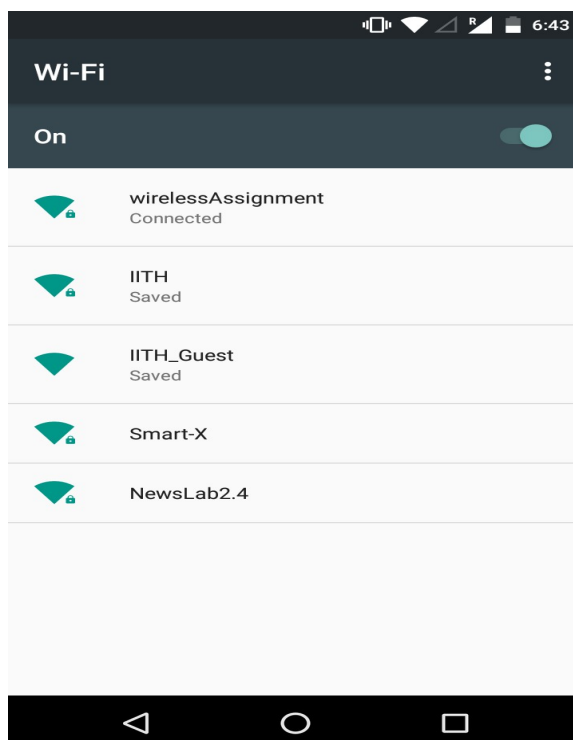iw dev wlp2s0 station dump

Screenshots:

1. Display stations connected to the Access Point at a given time.
(Laptop & a mobile phore are connected)

2. Station connected to the Access-Point – *wirelessAssignment.*

Q2.b Compare security features of your AP SSID, IITH-GUEST and IITH SSIDs. Write all messages exchanged during station association with above mentioned SSIDs. And comment on security messages exchange.

Security features:
IITH-Guest: None
IITH: WPA and WPA2 Enterprise,
        Authentication: Protected EAP,
        Inner Authentication: MSCHAPv2
wirelessassignment:WPA2 Personal

Messages exchanged during station association:

IITH-Guest Access-Point:

1. Probe request (STA to AP)
2. Probe response (AP to STA)
3. authentication request (STA to AP)
4. authentication response (AP to STA)
5. association request (STA to AP)
6. association response (AP to STA)

IITH Access-Point (802.1x Authentication):
1. Probe request (STA to AP)
2. Probe response (AP to STA)
3. authentication request (STA to AP)
4. authentication response (AP to STA)
5. association request (STA to AP)
6. association response (AP to STA)
7.EAP Request, Identity (AP to STA)
8. EAP Response, Identity (STA to AP)
9.EAP Request, TLS EAP (EAP-TLS) (AP to STA)
10.EAP Response, Legacy Nak (Response Only) (STA to AP)
11.EAP Request, Protected EAP (EAP-PEAP)(AP to STA)
12.TLSv1 Client Hello (STA to AP)
13.TLSv1 Server Hello, Certificate, Server Hello Done (AP to STA)
14.TLSv1 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message (STA to AP)
15.TLSv1 Change Cipher Spec, Encrypted Handshake Message(AP to STA)
16.EAP   Response, Protected EAP (EAP-PEAP) (STA to AP)
17.EAP Success(AP to STA)
18.EAPOL Key (Message 1 of 4)(AP to STA)
19.EAPOL Key (Message 2 of 4) (STA to AP)
20.EAPOL Key (Message 3 of 4) (AP to STA)
21.EAPOL Key (Message 4 of 4) (STA to AP)

wirelessassignment Access-Point (802.11i Authentication):
1. Probe request (STA to AP)
2. Probe response (AP to STA)
3. authentication request (STA to AP)
4. authentication response (AP to STA)
5. association request (STA to AP)
6. association response (AP to STA)
7. EAPOL Key (Message 1 of 4)(AP to STA)
8. EAPOL Key (Message 2 of 4) (STA to AP)
9. EAPOL Key (Message 3 of 4) (AP to STA)
10. EAPOL Key (Message 4 of 4) (STA to AP)

Security messages exchanged(IITH – 802.1x Authentication):
1. EAP: The EAP messages that appeared in the trace are EAP request from AP "IITH" and EAP response from STA. And finally a success message from AP.
2. TLSv1: TLSv1 is one of the EAP method that is being advertised by authentication server after getting EAP request from STA and then agreed upon by the corresponding STA.
3. EAPOL: EAPOL-Key frames are special key management frames used by STA to derive key information and establish secure communication. The EAPOL-Key frames are protected by a 128-bit key confirmation key(KCK) and a 128-bit key encryption key(KEK).
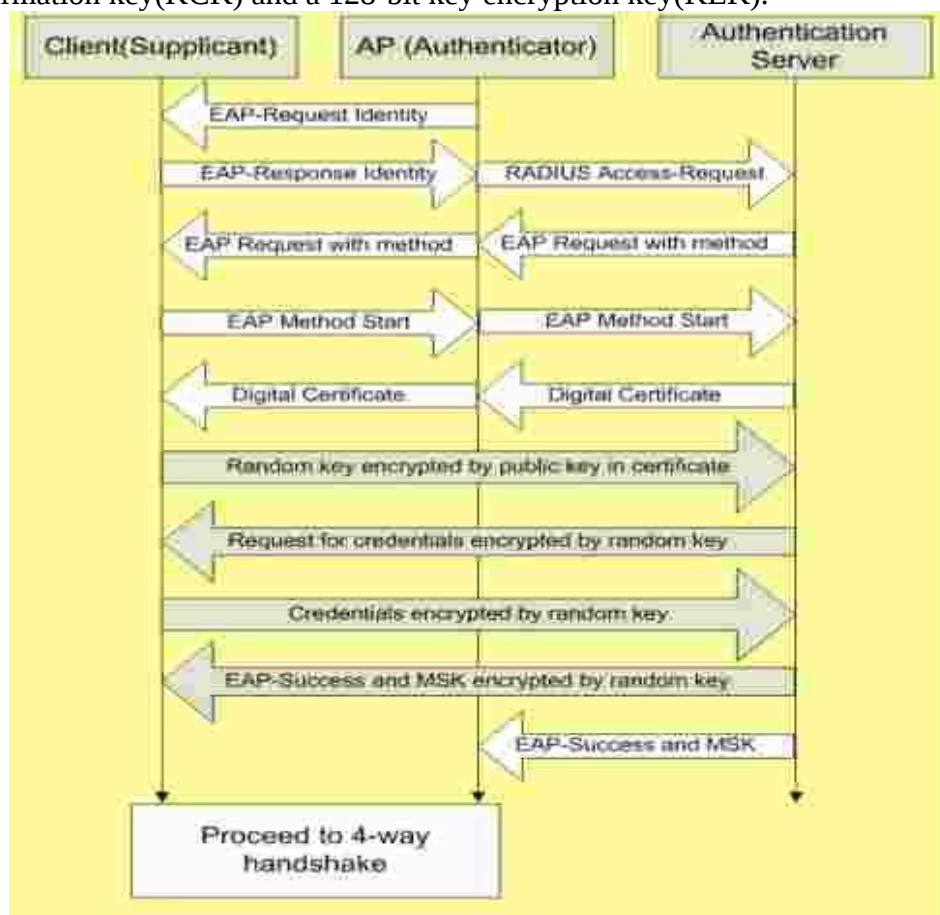
Security messages exchanged(wirelessassignment - 802.11i Authentication):
PSK(Pre-Shared Key) key: *wirelessassignement* AP is using 802.11i standard hence there is no RADIUS server and EAPOL messages.
This key is being used for 4-way handshake.

Q2c. Write a script for wireless clients to know about Number of stations connected to each SSID (IITH, IITH-Guest, Your AP) and connect to the SSID, which is having least number of clients. (You can connect to wireless AP using iw command from CLI).

Not Implemented.
Logic:
(1). Inside Beacon frames from Stations, QBSS Element contains Station count – The number of stations that are currently associated with the Access Point.

(2). Tshark package - is a paket capture tool that has powerful reading and parsing features for pcap analysis.

1. Capture network packets containing Beacon frames from all SSIDs.
   tshark -i wlp2s0 -w output_filename.pcap
2. Script reads the pcap using tshark.
   tshark -r output_filename.pcap
3. Script reads the output and searches for ssid and retreives the Station Count. Use grep command.
4. Depending on the station counts of all the SSIDs, the minimum loaded station will be connected using iw command.
   iw wlp2s0 connect <Chosen_SSID>

References:

1. The Evolution of 802.11 Wireless Security INF 795 - Kevin Benton
2. Linux man pages – iptables, systemctl, etc.
3. http://www.ibm.com/developerworks/library/l-wifiencrypthostapd/
4. http://elinux.org/RPI-Wireless-Hotspot
5. https://mrncciew.com/2014/10/08/*

Note: Used 4 out of the 5 remaining slip days.