

Assignment 12

210010033

Part 1:

1. SSID "30 Munroe St" and "linksys12" are the ones issuing most of the beacon frames in this trace.
2. Beacon Interval is 0.102400 [Seconds] for "30 Munroe St" and Beacon Interval is 0.102400 [Seconds] for "linksys12"
3. Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
4. Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
5. BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
6. The supported rates are as follows:

```
▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  Tag Number: Supported Rates (1)
  Tag length: 4
  Supported Rates: 1(B) (0x82)
  Supported Rates: 2(B) (0x84)
  Supported Rates: 5.5(B) (0x8b)
  Supported Rates: 11(B) (0x96)
```

The extended rates are as follows(in Mbps):

```
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag Number: Extended Supported Rates (50)
  Tag length: 8
  Extended Supported Rates: 6(B) (0x8c)
  Extended Supported Rates: 9 (0x12)
  Extended Supported Rates: 12(B) (0x98)
  Extended Supported Rates: 18 (0x24)
  Extended Supported Rates: 24(B) (0xb0)
  Extended Supported Rates: 36 (0x48)
  Extended Supported Rates: 48 (0x60)
  Extended Supported Rates: 54 (0x6c)
```

Part 2:

1.

The respective address are as follows:

```
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

The TCP SYN message is contained in the frame sent at t=24.811093 seconds.(Frame No. 474)

The MAC address corresponding to the wireless host is 00:13:02:d1:b6:4f.

The MAC address corresponding to the Access point is 00:16:b6:f7:1d:51

The MAC address corresponding to the First hop router is 00:16:b6:f7:1d:51

Source IP:192.168.1.109

Destination IP: 128.119.245.12

2.

Receiver address: 91:2a:b0:49:b6:4f

Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)

BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)

The TCP SYNACK message is received at t=24.827751 seconds into the trace.(Frame No. 476)

The MAC address corresponding to the wireless host is 00:16:b6:f7:1d:51.

The MAC address corresponding to the Access point is 91:2a:b0:49:b6:4f

The MAC address corresponding to the BSS is 00:16:b6:f7:1d:51

Server IP: 128.119.245.12

Part 3:

1.

```
1733 07:35:56.656072 192.168.1.109 192.168.1.1 DHCP 398 DHCP Release - Transaction ID 8aea5a526
1734 07:35:56.656228 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
1735 07:35:56.682074 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 54 Deauthentication, SN=1685, RN=0, Flags=.....C
1736 07:35:56.682227 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
```

The two actions taken include DHCP release(frame 1733) and Deauthentication (frame 1735)

The action which was expected here was a disassociation message.

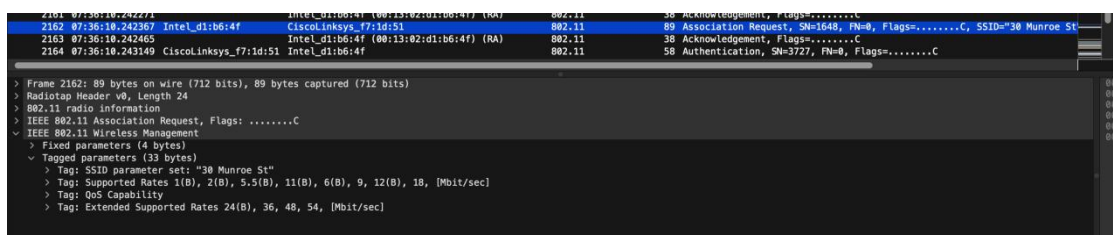
2. 15 Authentication messages were sent.

3. Yes, the host wants authentication to be open.

4. No, I don't see reply AUTHENTICATION from the linksys_ses_24086 AP in the trace.

5. AUTHENTICATION frame from the host to 30 Munroe St. AP at: 63.168087s (Frame No. 2156)
Reply AUTHENTICATION sent from that AP to the host reply at: 63.169071s (Frame No. 2158)
AUTHENTICATION frame retransmitted from host to 30 Munroe St. AP at: 63.169707s (Frame No. 2160)
Reply AUTHENTICATION sent from that AP to retransmitted host reply at: 63.170692s(Frame No. 2164)

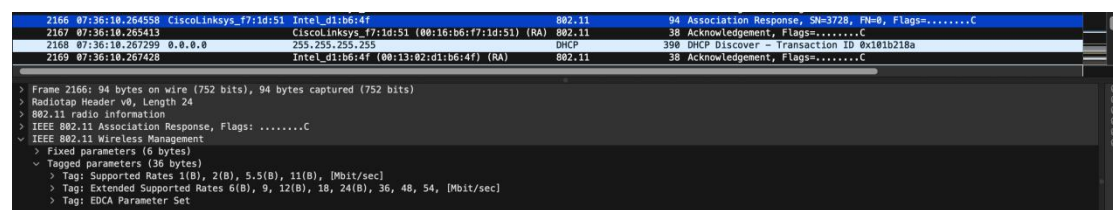
6.



```
2161 07:36:10.242771 Intel_d1:b6:4f (08:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
2162 07:36:10.242367 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 89 Association Request, SN=1648, FN=0, Flags=.....C, SSID="30 Munroe St"
2163 07:36:10.242465 Intel_d1:b6:4f (08:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
2164 07:36:10.243149 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 58 Authentication, SN=3727, FN=0, Flags=.....C

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on 0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Wireless Management
> Fixed parameters (4 bytes)
> Tagged parameters (33 bytes)
> Tag: SSID parameter set: "30 Munroe St"
> Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 6(0), 9, 12(0), 18, [Mbit/sec]
> Tag: QoS Capability
> Tag: Extended Supported Rates 24(0), 36, 48, 54, [Mbit/sec]
```

Frame: 2162 at time = 7:36:10.24 contains the association request from the host



```
2166 07:36:10.264558 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 94 Association Response, SN=3728, FN=0, Flags=.....C
2167 07:36:10.265413 CiscoLinksys_f7:1d:51 (08:16:b6:f7:1d:51) (RA) 802.11 38 Acknowledgement, Flags=.....C
2168 07:36:10.267299 0.0.0.0 255.255.255.255 DHCP 390 DHCP Discover - Transaction ID 0x101b218a
2169 07:36:10.267428 Intel_d1:b6:4f (08:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on 0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....C
> IEEE 802.11 Wireless Management
> Fixed parameters (6 bytes)
> Tagged parameters (36 bytes)
> Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), [Mbit/sec]
> Tag: Extended Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
> Tag: EDCA Parameter Set
```

Frame: 2166 at time = 7:36:10.2 contains the association response to the host.

7. Rates supported by host include: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

Rates supported by the AP include: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

Part 4:

1.

Respective addresses are

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
```

```
2120 07:36:09.213777 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb (00:10:39:f5:ba:bb) (RA) 802.11 38 Acknowledgement, Flags=.....C
2121 07:36:09.214408 Intel_d1:b6:4f Broadcast 802.11 98 Probe Request, SN=1644, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
2122 07:36:09.244408 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 58 Authentication, SN=1644, FN=0, Flags=.....C
2123 07:36:09.245403 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 58 Authentication, SN=1644, FN=0, Flags=.....R...C
2124 07:36:09.246527 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 58 Authentication, SN=1644, FN=0, Flags=.....R...C
2125 07:36:09.248099 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb (00:10:39:f5:ba:bb) (RA) 802.11 38 Acknowledgement, Flags=.....C
2126 07:36:09.249402 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SN=1645, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
2127 07:36:09.249999 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2128 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2129 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2130 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2131 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2132 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2133 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2134 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2135 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2136 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2137 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2138 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2139 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2140 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2141 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2142 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2143 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2144 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2145 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2146 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2147 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2148 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2149 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2150 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2151 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2152 07:36:09.250000 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 38 Acknowledgement, Flags=.....C
2153 07:36:10.214908 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 177 Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID="30 Munroe"
2154 07:36:10.215317 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 38 Acknowledgement, Flags=.....C
2155 07:36:10.233720 IntelLinksys_f7:1d:51 Broadcast 802.11 163 Beacon frame, SN=3725, FN=0, Flags=.....C, BI=100, SSID="30 Munroe"
2156 07:36:10.240544 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 58 Authentication, SN=1647, FN=0, Flags=.....C
2157 07:36:10.240679 Intel_d1:b6:4f Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
2158 07:36:10.241528 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 58 Authentication, SN=3726, FN=0, Flags=.....C
2159 07:36:10.242049 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f (00:16:b6:f7:1d:51) (RA) 802.11 38 Acknowledgement, Flags=.....C

> IEEE 802.11 radio information
  > IEEE 802.11 Probe Request, Flags: .....C
    Type/Subtype: Probe Request (0x0004)
    > Frame Control Field: 0x0000
    .000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 0000 = Fragment number: 0
    0110 0110 1100 .... = Sequence number: 1644
    Frame check sequence: 0x2fcfc513 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .....C]
  > IEEE 802.11 Wireless Management
```

Frame: 2121 contains the PROBE REQUEST

```
2153 07:36:10.214908 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 177 Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID="30 Munroe"
2154 07:36:10.215317 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 38 Acknowledgement, Flags=.....C
2155 07:36:10.233720 IntelLinksys_f7:1d:51 Broadcast 802.11 163 Beacon frame, SN=3725, FN=0, Flags=.....C, BI=100, SSID="30 Munroe"
2156 07:36:10.240544 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 58 Authentication, SN=1647, FN=0, Flags=.....C
2157 07:36:10.240679 Intel_d1:b6:4f Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C
2158 07:36:10.241528 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 58 Authentication, SN=3726, FN=0, Flags=.....C
2159 07:36:10.242049 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f (00:16:b6:f7:1d:51) (RA) 802.11 38 Acknowledgement, Flags=.....C

> IEEE 802.11 radio information
  > IEEE 802.11 Probe Response, Flags: .....C
    Type/Subtype: Probe Response (0x0005)
    > Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    .... 0000 = Fragment number: 0
    1110 1000 1100 .... = Sequence number: 3724
    Frame check sequence: 0xc29e2af [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .....C]
  > IEEE 802.11 Wireless Management
```

Frame: 2153 contains the PROBE RESPONSE

Probe Request Frames are sent by a device when it wants to discover nearby Wi-Fi networks. This frame is used by devices to search for available networks. When we turn on the Wi-Fi or manually search for networks on the device, it sends out Probe Request frames to find nearby access points.

Probe Response Frames: An access point (AP) or Wi-Fi router sends a Probe Response frame in response to a Probe Request from a client device. The Probe Response contains information about the access point, including its SSID (network name), supported Wi-Fi standards, security settings, and other network parameters. This information helps the client device decide which network to connect to.