

CS315: Assignment-12

Name: Shahil Patel

Roll No.: 200010039

Part-1: Beacon Frames

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

Ans: The two access points that are issuing most of the beacon frames have an SSID of **30 Munroe St** and **linksys12**.

```
Tag: SSID parameter set: 30 Munroe St
Tag Number: SSID parameter set (0)
Tag length: 12
SSID: 30 Munroe St
Tag: Supported Rates 1/(B) 2/(B) 5.5/(B) 11/(B)
```

```
Tag: SSID parameter set: linksys12
Tag Number: SSID parameter set (0)
Tag length: 9
SSID: linksys12
```

2. What are the intervals of time between the transmissions of the beacon frames and the *linksys_ses_24086* access point? From the *30 Munroe St.* access point? (Hint: this interval of time is contained in the beacon frame itself).

Ans: The interval of time between the transmissions of the beacon frames and the *linksys_ses_24086* access point is: **0.102400 seconds**.

```
Fixed parameters (12 bytes)
Timestamp: 9534921933578
Beacon Interval: 0.102400 [Seconds]
```

From the 30 Munroe St. access point: **0.102400 seconds**.

```
Fixed parameters (12 bytes)
Timestamp: 174319616391
Beacon Interval: 0.102400 [Seconds]
```

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

Ans: The source MAC address in hexadecimal notation on the beacon frame from 30 Munroe St. is: **00:16:b6:f7:1d:51**.

```
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??

Ans: The destination MAC address in hexadecimal notation on the beacon frame from 30 Munroe St is: **ff:ff:ff:ff:ff:ff**.

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
```

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?

Ans: The MAC BSS ID in hexadecimal notation on the beacon frame from 30 Munroe St is: **00:16:b6:f7:1d:51**

```
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

6. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

Ans: Supported rates: **1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]**

Extended supported rates: **6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]**

Part-2: Data Transfer

1. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads `alice.txt`). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

Ans: The 3 MAC addresses fields in the 802.11 frame are:

- Source Address: **00:13:02:d1:b6:4f**
- Destination Address: **00:16:b6:f4:eb:a8**
- BSS ID: **00:16:b6:f7:1d:51**

The Source address corresponds to the **host** device.

The Destination address corresponds to the **first-hop** device.

The BSS ID corresponds to the **access point**.

```
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

Source IP address: **192.168.1.109**

Destination IP address: **128.119.245.12**

Source IP address corresponds to the host address.

Destination address corresponds to the server.

2. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

Ans: The 3 MAC addresses fields in this 802.11 frames are:

- Source Address: **00:16:b6:f4:eb:a8**
- Destination Address: **91:2a:b0:49:b6:4f**
- BSS ID: **00:16:b6:f7:1d:51**

The source address corresponds to the *first-hop* device.

The destination address corresponds to the *host* device.

The BSS ID corresponds to the *access point*.

```
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

Source IP address: **128.199.245.12**

Destination IP address: **192.168.1.109**

Part-3: Association/Disassociation

1. What two actions are taken (i.e., frames are sent) by the host in the trace just after $t=49$, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

Ans: At $t = 49.583615$ a DHCP release is sent by the host to the DHCP server in the network that the host is leaving.

At $t = 49.609617$, the host sends a **DEAUTHENTICATION** frame

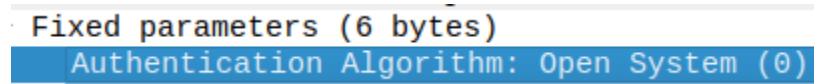
One might have expected to see a **DISASSOCIATION** request to have been sent.

2. Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksys_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around $t=49$?

Ans: Total **15** AUTHENTICATION messages were sent from the wireless host to the *linksys_ses_24086* AP.

3. Does the host want the authentication to require a key or be open?

Ans: The host is requesting that the **association be open** (by specifying *Authentication Algorithm: Open System*).



Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)

4. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?

Ans: I can't locate any reply from the AP. The AP is probably ignoring requests for open access (i.e. not responding to them) because it is set up to require a key when connecting to that AP.

5. Now let's consider what happens as the host gives up trying to associate with the *linksys_ses_24086* AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENTICATION frames sent from the host to an AP and vice versa. At what times is there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "*wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f*" to display only the AUTHENTICATION frames in this trace for this wireless host.)

Ans: *AUTHENTICATION* frame is sent from **00:13:02:d1:b6:4f** (the wireless host) to **00:16:b7:f7:1d:51** at $t = 63.168087$. (the BSS). At $t = 63.169071$ there is an *AUTHENTICATION sent* in the reverse direction from the *BSS to the wireless host*.

6. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that

you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

Ans: The wireless host at **00:13:02:d1:b6:4f** sends an ASSOCIATE REQUEST frame to **00:16:b7:f7:1d:51** at time $t = 63.169910$. (the BSS).

On the reverse route, from the BSS to the wireless host, an **ASSOCIATE RESPONSE** is sent at time $t = 63.192101$.

```
IEEE 802.11 Association Request, Flags: .....C
  Type/Subtype: Association Request (0x0000)
  ▶ Frame Control Field: 0x0000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... 0000 = Fragment number: 0
    0110 0111 0000 .... = Sequence number: 1648
    Frame check sequence: 0xfe3badc6 [unverified]
    [FCS Status: Unverified]
```

7. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

Ans: : The supported rates are listed as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps in the ASSOCIATION REQUEST frame. The ASSOCIATION RESPONSE also lists the same rates.

```
Tagged parameters (33 bytes)
  ▶ Tag: SSID parameter set: 30 Munroe St
  ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
  ▶ Tag: QoS Capability
  ▶ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

Part-4: Other Frame types

1. What are the sender, receiver and BSS ID MAC addresses in these frames?
What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).

Ans: At **t=2.297613** there is a *PROBE REQUEST* sent with source **00:12:f0:1f:57:13**, destination: *ff:ff:ff:ff:ff:ff*, and a BSS ID of *ff:ff:ff:ff:ff:ff*.

At **t=2.300697** there is a *PROBE RESPONSE* sent with source: **00:16:b6:f7:1d:51**, destination address of **00:16:b6:f7:1d:51** and a BSS ID of **00:16:b6:f7:1d:51**.

During active scanning, a host locates an Access Point by sending a *PROBE REQUEST*. The access point responds to the host making the request by issuing a *PROBE RESPONSE*.