Computer Networks

Lab 7

802.11 WiFi v8.0

Student Name: Dương Gia Lâm

Student No:2211806

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

```
SSID: "30 Munroe St"
```

2. What are the intervals of time between the transmissions of the beacon frames 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).

```
[Time delta from previous captured frame: 0.004165000 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).

```
> Source address: CiscoLinksys_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??

```
> 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?

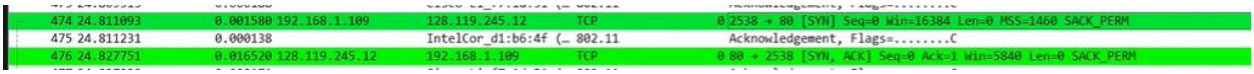
```
BSS Id: 50:2b:25:67:22:94 (50:2b:25:67:22:94)
```

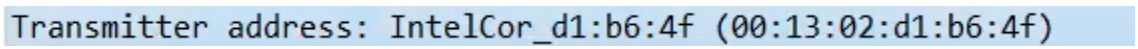
6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

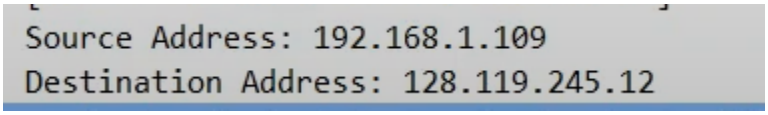
Supported Rates

Extended Supported Rates

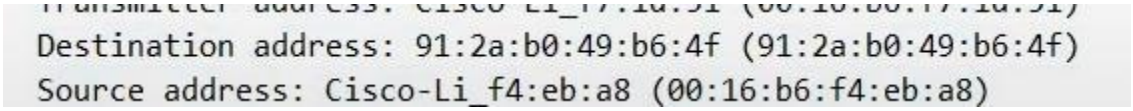
7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? 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.



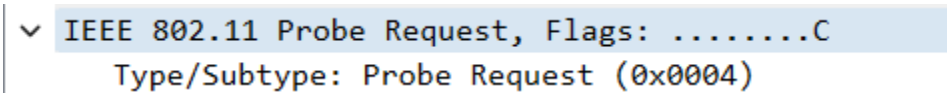




8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address 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).



9. 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?



10. Examine the trace file and look for AUTHENICATION 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? .

Zero

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

```
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0001
Status code: Successful (0x0000)
```

No need key

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

No

13. 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 AUTHENICATION frames sent from the host to and AP and vice versa. At what times are 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 == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

```
2156 2007-06-29 09:06:10.240544 Intel_d1:b6:4f          CiscoLinksys_f7:1d:51    802.11    58 Authentication, SN=1647, FN=0, Flags=........C
2158 2007-06-29 09:06:10.241528 CiscoLinksys_f7:1d:51   Intel_d1:b6:4f           802.11    58 Authentication, SN=3726, FN=0, Flags=........C
```

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to 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.)

```
2164 2007-06-29 09:06:10.243149 CiscoLinksys_f7:1d:51   Intel_d1:b6:4f           802.11    58 Authentication, SN=3727, FN=0, Flags=........C
```

15. 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.

by looking at the **Association Request** and **Association Response** frames and examining the **Supported Rates** and **Extended Supported Rates**, you can determine the transmission rates the host and the AP are willing to use.

16. 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).

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

Purpose: This is the **unique identifier** of a specific wireless access point (AP) or a Basic Service Set (BSS).

BSS ID: Broadcast (ff:ff:ff:ff:ff:ff)

- **Purpose**: This is the **broadcast address**, used to send frames to all devices in a wireless network.