

Computer Networks Lab, Assignment 12

Suyash Gaurav

210010054

1 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?

the SSIDs of the two access points that are issuing most of the beacon frames in the trace are **"30 Munroe St"** and **"linksys12."**

2. What are the beacon intervals in the *linksys_ses₂4086* access point and the 30 Munroe St. access point?

The time interval between the transmissions of the beacon frames and the *linksys_ses₂4086* access point is **0.102400 seconds**.



Beacon Interval: 0.102400 [Seconds]

Figure 1: Q2. time interval

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).

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

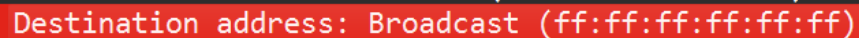


Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)

Figure 2: Q3. hexadecimal notation

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

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

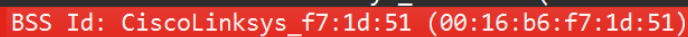


Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Figure 3: Q4. destination MAC address

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

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



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

Figure 4: Q5. MAC BSS ID

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 are 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec] Extended supported rates are: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

2 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?

The 3 MAC address 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 (**00:13:02:d1:b6:4f**) corresponds to the wireless host.

The Destination Address (**00:16:b6:f4:eb:a8**) corresponds to the first-hop router.

The BSS ID (**00:16:b6:f7:1d:51**) corresponds to the access point.

Source IP address: **192.168.1.109**

Destination IP address: **128.119.245.12**

Source IP address corresponds to **host address** and 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 of these are the MAC addresses corresponding to the host sending SYNACK, destination, and BSS? What is the IP address of the server sending the TCP SYNACK?

The 3 MAC address 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.

Source IP address: **128.199.245.12**

Destination IP address: **192.168.1.109**

3 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?

The two actions taken by the host to end the association with the 30 Munroe St AP are:

At $t = 49.583615$, the host sends a **DHCP** release to the DHCP server in the network, indicating its intention to relinquish its IP address lease and end its association with the network at the IP-layer.

At $t = 49.609617$, the host sends a **DEAUTHENTICATION** frame at the 802.11-layer, indicating its intention to terminate the association with the access point.

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_es24086* AP (which has a MAC address of *Cisco_Lif5 : ba : bb*) starting at around $t=49$?

Total **15 AUTHENTICATION** messages were sent from the wireless host to the AP with the MAC address "*Cisco_Lif5 : ba : bb*" starting at around $t=49$.

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

Yes, the host wants the authentication to be open, as

indicated by specifying the Authentication Algorithm as "Open System" in the authentication frames.

4. Do you see a reply AUTHENTICATION from the *linksys_es24086* AP in the trace?

there doesn't seem to be a reply authentication from the "*linksys_es24086*" AP in the trace. It's likely that the AP is configured to require authentication with a key and is ignoring requests for open access, hence not responding to them.

5. Now let's consider what happens as the host gives up trying to associate with the *linksys_es24086* 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 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host reply? (Note that you can use the filter expression `\wlan.fc.subtype == 11wlan.fc.type == 0wlan.addr == IntelCor_d1 : b6 : 4f` to display only the AUTHENTICATION frames in this trace for this wireless host.)

An **AUTHENTICATION** frame is sent from the wireless host (00:13:02:d1:b6:4f) to the BSS (00:16:b7:f7:1d:51) at **t = 63.168087**.

A reply **AUTHENTICATION** frame is sent in the reverse direction from the BSS (30 Munroe St AP) to the wireless host at **t = 63.169071**.

This sequence indicates the successful exchange of authentication frames between the wireless host and the

”30 Munroe St” AP during the association process.

6. An ASSOCIATE REQUEST from the host to AP and a corresponding ASSOCIATE RESPONSE frame from AP to the host is used for the host to be associated with an AP. At what time is there an ASSOCIATE REQUEST from the host to 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression `\wlan.fc.subtype < 2wlan.fc.type == 0wlan.addr == IntelCord1 : b6 : 4f`” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

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 $t = 63.192101$.

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.

both the host and the AP are willing to use the following transmission rates:

1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps.

These rates are listed in the parameters fields of the ASSOCIATION REQUEST frame sent by the host

and in the **ASSOCIATION RESPONSE** frame sent by the AP.

4 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).

In the PROBE REQUEST frame:

- Sender MAC address: **00:12:f0:1f:57:13**
- Receiver MAC address: **ff:ff:ff:ff:ff:ff**
- BSS ID MAC address: **ff:ff:ff:ff:ff:ff**

In the PROBE RESPONSE frame:

- Sender MAC address: **00:16:b6:f7:1d:51**
- Receiver MAC address: **00:16:b6:f7:1d:51**
- BSS ID MAC address: **00:16:b6:f7:1d:51**

The purpose of the **PROBE REQUEST** frame is for the host to discover available access points in its vicinity. The **PROBE RESPONSE** frame is sent by an access point in response to a PROBE REQUEST, providing information about its capabilities and services, allowing the host to select an appropriate access point for association.