**CS3506 Lab 3: Worksheet**

## Beacon Frames

1. What are the SSIDs observed in the trace? You can find the SSID in the contents of each Beacon frame. To allow you to focus on Beacon frames try clicking the top of the “info” column to sort frames alphanumerically or else filter for beacon frames only (using wlan.fc.type\_subtype == 8 as given in the “cheat sheet”).

30 Munroe St

linksys12

A malformed packet with SSID "6c69ee0104e2273a32"

1. What are the intervals of time between the transmissions of Beacon frames by the “30 Monroe St” access point?

Approx at around 0.1 seconds

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

Source address: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51)

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

BSS Id: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51)

1. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*? Why is the Beacon sent with this address?

The destination MAC address in these beacon frames is set to ff:ff:ff:ff:ff:ff (broadcast address). This is typical in beacon frames, as they are broadcast to all nearby devices to announce the presence of the network.

1. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four “Supported” data rates and eight additional “Extended Supported” rates. List both the Supported and Extended rates. The Extended rates field is needed for 802.11g, why?

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]

Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

The Extended Supported Rates field is necessary for compatibility with 802.11g networks, as 802.11g introduced additional data rates that were not part of the original 802.11b standard.

**Data Transfer**

Locate the packet that has the HTTP GET request (for file wireshark-labs/alice.txt) and answer the following questions (Hint: use filter HTTP to locate the packet)

1. What is the IP address of the host sending the request? Is it a private or public address?

Source Address: 192.168.1.109

1. What is the IP address of the web-server?

Destination Address: 128.119.245.12

1. What is the DNS server assigned to the host? (Hint: remove the filter and check previous packets) Is the DNS server located in the same subnet as the host?

DNS Server assigned to host: 192.168.1.109

The IP address **192.168.1.109** is in the same subnet as the other devices (following the 192.168.1.x convention), indicating that the DNS server is located within the same local network or subnet as the host.

1. What is the first ARP request sent by the device running the HTTP client? Why?

* **First ARP Request**: The first ARP request in your screenshot (Frame 45, Time: 2.236534) is from CnetTechnolo\_73:8d:... requesting the MAC address of 192.168.1.103 to tell 192.168.1.100.
* **Reason**: ARP requests are used to resolve IP addresses to MAC addresses, enabling devices to communicate on a local network. Here, the device at 192.168.1.100 is looking to communicate with the device at 192.168.1.103 but first needs its MAC address.

1. Find the 802.11 frame containing the **SYN-ACK** segment for this TCP session. Which MAC address in this frame corresponds to (i) the host, (ii) the access point, (ii) the first-hop router?

 **(i) the host**: The host would have the MAC address of the device making the initial HTTP GET request or ARP request.

 **(ii) the access point**: This would be the device facilitating wireless communication between the host and the router.

 **(iii) the first-hop router**: The router's MAC would likely appear as a destination in responses to the host or in responses from the web server to the access point.

To find the exact SYN-ACK frame:

Apply a filter like tcp.flags.syn == 1 and tcp.flags.ack == 1 to locate SYN-ACK packets.

Identify the corresponding MAC addresses in the frame details.

1. Every correctly received frame is followed by an ACK frame in response. What would be sent if the sent frame is not received correctly?

**Response to Unreceived Frame**: If a frame is not received correctly (such as due to interference or collision), the sender will not receive an ACK. Consequently, after a timeout period, the sender will typically retransmit the frame until it receives an acknowledgment or reaches a retry limit.

**Association/Disassociation**

Use the filter expression “wlan.fc.type == 0” to display only the management frames in this trace.

1. An ASSOCIATE REQUEST from host to AP is usually followed by an ASSOCIATE RESPONSE. At what time is there an ASSOCIATE REQUEST to the “30 Monroe St” AP? What message number is the ASSOCIATE RESPONSE?

**Frame 2162**

To find the **ASSOCIATE RESPONSE** frame:

* Look for the next frame from the "30 Monroe St" access point to the requesting device after this timestamp, typically in a similar time range. You may need to scroll or apply a filter in Wireshark, such as wlan.fc.type\_subtype == 0x0001, to view only association responses.

1. You can see that the first AUTHENTICATION from the host to the AP is sent at t = 49.638857. There is no reply from the *linksys\_ses\_24086* AP. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring (i.e., not responding to) requests for open access. 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? Note that you can use the filter " wlan.fc.subtype == 11 and wlan.fc.type == 0" to show only AUTHENTICATION frames.

When is there a reply AUTHENTICATION sent from that AP to the host?

1. **Time of First AUTHENTICATION Frame from Host to "30 Monroe St" AP**
   * According to your screenshot, the first AUTHENTICATION frame from the host (source Intel\_d1:b6:4f) to the "30 Monroe St" AP appears around 49.638857 seconds.
2. **Reply AUTHENTICATION Frame from the AP to Host**
   * The next AUTHENTICATION frame that you should see in the sequence after the host sends an authentication request should be a response from the AP. Based on the information, it seems that there is an exchange happening within seconds after the initial authentication request from the host.

To view this precisely, follow these steps in Wireshark:

* Apply the filter wlan.fc.subtype == 11 and wlan.fc.type == 0 to display only authentication frames.
* Look for the sequential AUTHENTICATION frame that matches the destination address of the host (Intel\_d1:b6:4f).

**Radio Information**

1. Examine the first Beacon frame in the trace. Find the 802.11 Radio Information. Wifi usually operates in either the 2.5 GHz or 5 GHz portions of the radio spectrum. Can you tell which one this Access Point is operating? Can you tell which radio channel within that spectrum it using?

Channel frequency: 2437 [2.4 GHz 6]

**Frequency Band**: The access point is operating in the **2.4 GHz** frequency band.

**Radio Channel**: It is using **Channel 6**.