**East West University**

**Department of CSE**

**Lab Report 03**

**CSE 453**

**Wireless Networking**

**Submitted To:**

Md. Mahir Ashhab

Lecturer

Department of Computer Science and Engineering

**Submitted By:**

Adri Saha

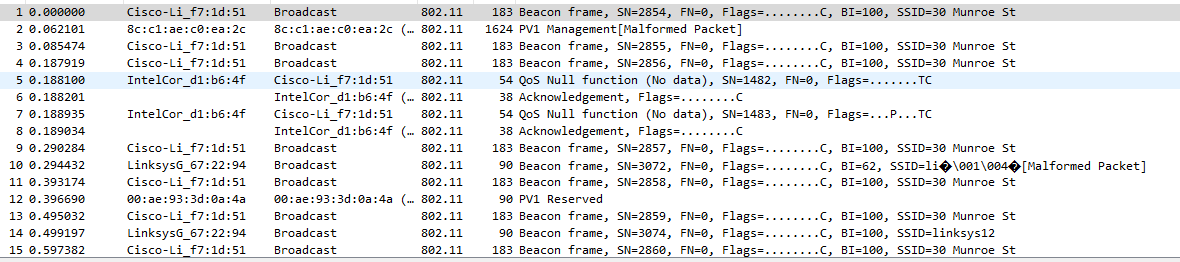
ID: 2019-1-60-024

Submission Date: 31 August 2022

**Wireshark Traces Answers**

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

**Ans:** 30 Munroe St is issuing most of the beacon frames in this trace. And then ‘linsys\_SES\_24086’ are also seen which is issuing the same.



1. **What are the intervals of time between the transmission 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).**

**Ans:** We see, beacon interval from both ‘linksys\_ses\_24086’ and ‘30 Munroe St.’ is: 0.102400 Seconds.

Graphical user interface, text, application

Description automatically generated

1. **What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 6.13 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:** Receiver address: Broadcast (ff: ff: ff: ff: ff: ff)

Source MAC address: *00:16:b6:f7:1d:51*

Text, letter

Description automatically generated

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

**Ans:** Destination MAC address: Broadcast (ff:ff:ff:ff:ff:ff)

Text, letter

Description automatically generated

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

**Ans:** MAC BSS id on beacon frame: Cisco-Li\_f7:1d:51 (00: 16: b6: f7: 1d: 51)

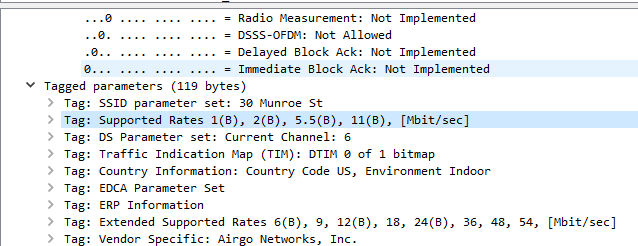
Text, letter

Description automatically generated

1. **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 4 data rates are: 1(B), 2(B), 5.5(B), 11(B) Mbps and

Eight additional extended supported rates are: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbps.



1. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). At what time is the TCP SYN sent? 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. (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the corresponding part of the next question. It’s particularly important that you understand this).**

**Ans:** The TCP SYN is sent at t = 24.811093 seconds into the

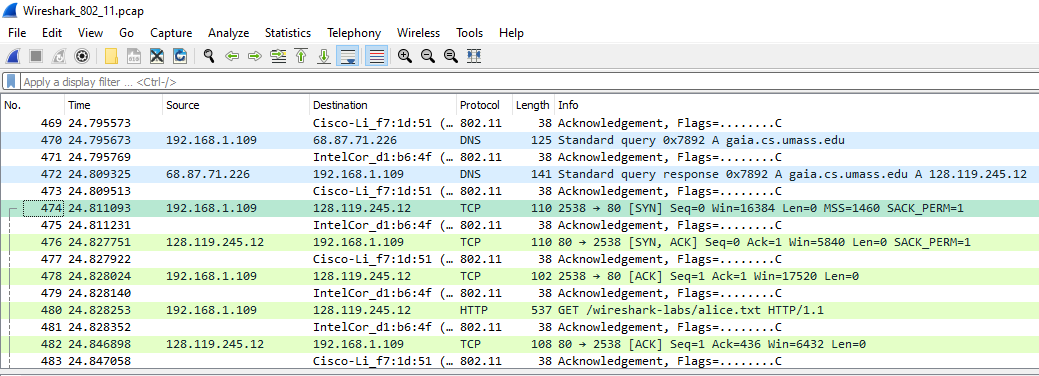
trace. The MAC address for the host sending the TCP SYN is

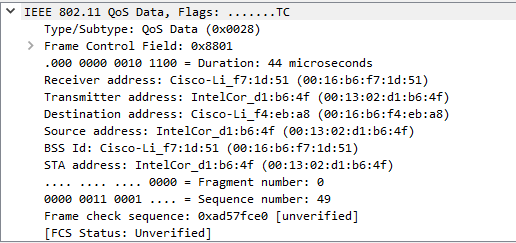
transmitter address: 00:13:02:d1:b6:4f.

The MAC address for the destination: which the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8.

The MAC address for the BSS is 00:16:b6:f7:1d:51.

The IP address of the host sending the TCP SYN is 192.168.1.109.





1. **Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received? What are three MAC address fields in the 802.11 frame containing the SYNACK? 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?**

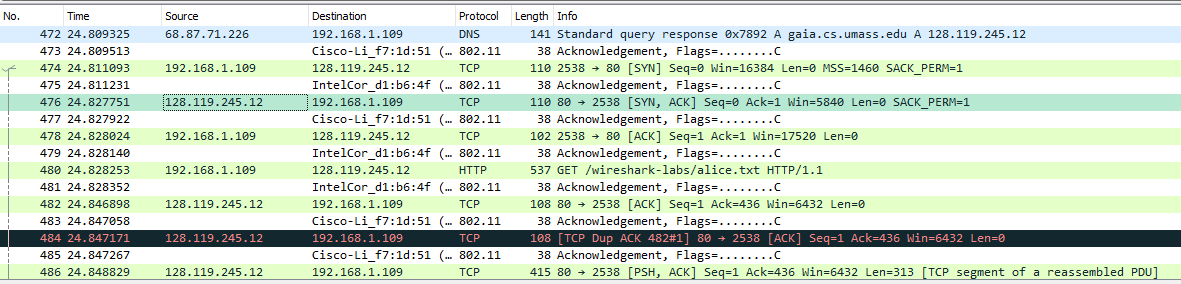
**Ans:** At time t = 24.827751 seconds into the trace, a TCP SYNACK is received.

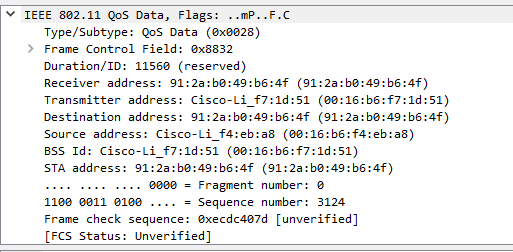
The first hop router to which the host is connected is identified by the MAC address 00:16:b6:f4:eb:a8 as the sender of the 802.11 frame containing the TCP SYNACK segment.

The host itself, the destination, and its MAC address are 91:2a:b0:49:b6:4f.

The BSS's MAC address is 00:16:b6:f7:1d:51.

The server sending the TCP SYNACK has the IP address 128.199.245.12.



1. 
2. **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, and at what times are these frames sent? (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 49.583615 sec, we see the host transmits DHCP release to the DHCP server in the network they are leaving (whose IP address is 192.168.1.1).

At time 49.609617, the host transmits a DEAUTHENTICATION frame (subframe type 12 [Deauthentication]; frametype 00 [Management]). A DISASSOCIATION request might have been anticipated to have been sent, for example.

A picture containing graphical user interface

Description automatically generated

1. **Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION frame 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:** The host authenticates for the first time to the AP at time = 49.638857.

Graphical user interface, text

Description automatically generated

A screenshot of a computer

Description automatically generated

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

**Ans:** Yes. The host requests that the association be open by giving the authentication algorithm.

Text

Description automatically generated

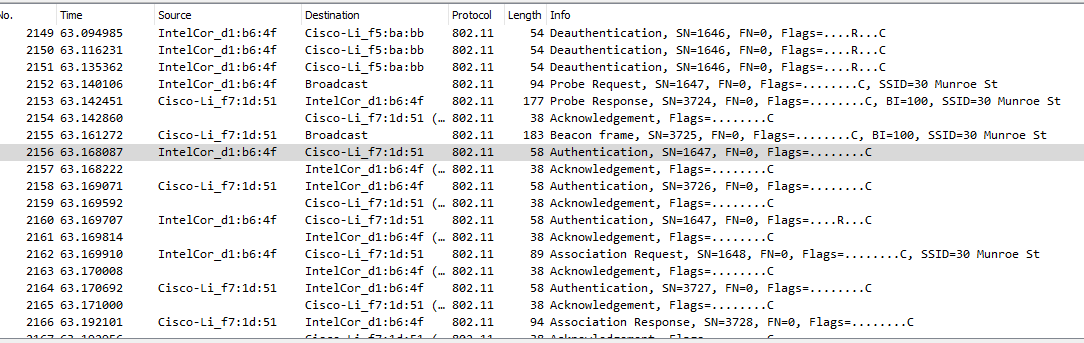
1. **Do you see a reply to AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?**

**Ans:** I am unable to find a reply from the AP. This is most likely because the AP is set up to require a key before connecting to it, and as a result, it is probably disregarding requests for open access.

1. **Now let’s consider what happens as the host gives up (sometime after t = 63.0) 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.)**

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

An AUTHENTICATION is transmitted from the BSS to the wireless host in the reverse direction at t = 63.169071.



Text, letter

Description automatically generated

1. **Let’s continue on with the association between the wireless host and the 30 Munroe St AP that happens after t = 63.0. An ASSOCIATE from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associate 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:** At time t = 63.169910, an ASSOCIATE REQUEST frame is sent from the wireless host, 00:13:02:d1:b6:4f, to 00:16:b7:f7:1d:51 (the BSS).

At time t = 63.192101, an ASSOCIATE RESPONSE is sent from the BSS to the wireless host in the other way.

**Text

Description automatically generated with low confidence**

Text

Description automatically generated

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

**Ans:** The supported rates are given 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.

1. **Consider the first PROBE REQUEST and the soonest subsequent PROBE RESPONSE PAIR occurs after *t =* 2.0 seconds in the trace. When are these frames sent and what are the sender, receiver, and BSS ID MAC addresses for 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:** A PROBE REQUEST with the source 00:12:f0:1f:57:13, destination ff:ff:ff:ff:ff, and BSSID ff:ff:ff:ff:ff:ff is issued at t = 2.297613.

A PROBE RESPONSE with the source and destination of 00:16:b6:f7:1d:51 and a BSSID of 00:16:b6:f7:1d:51 is transmitted at t = 2.300697.

A host uses a PROBE REQUEST during active scanning to identify an Access Point. The access point responds to the host making the request by issuing a PROBE RESPONSE.