22510064 PARSHWA HERWADE

CN 5 ASSIGNMENT

WIRESHARK LAB 802.11

***2. Beacon Frames***

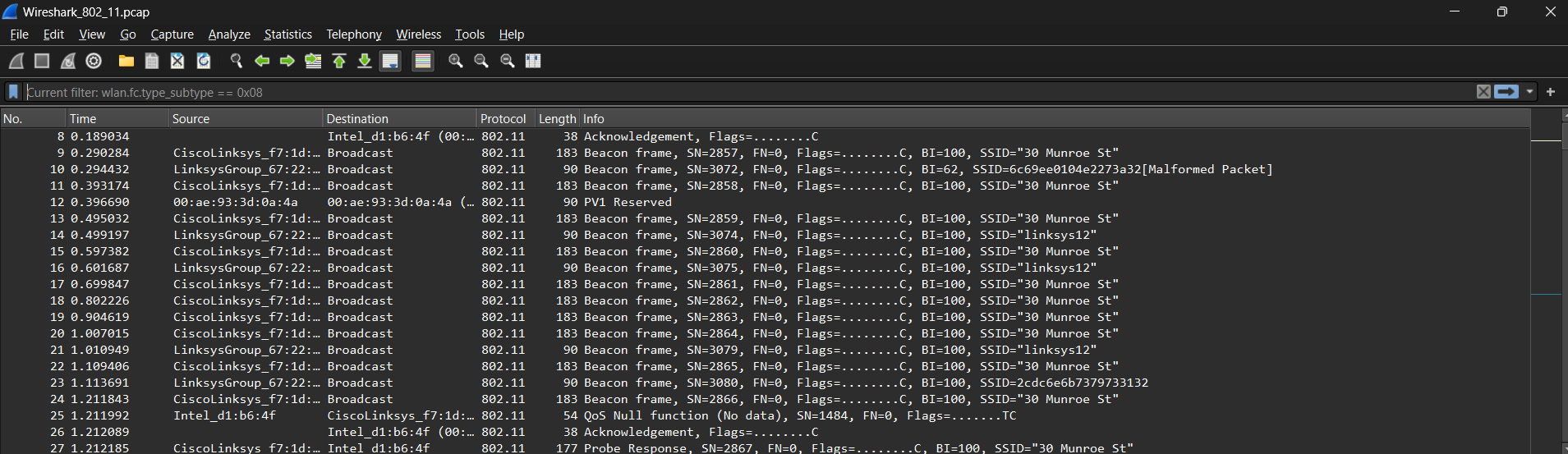
***Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer***

***some of the questions below, you’ll want to look at the details of the “IEEE 802.11”***

***frame and subfields in the middle Wireshark window.***

1. What are the SSIDs of the two access points that are issuing most of the

beacon frames in this trace?

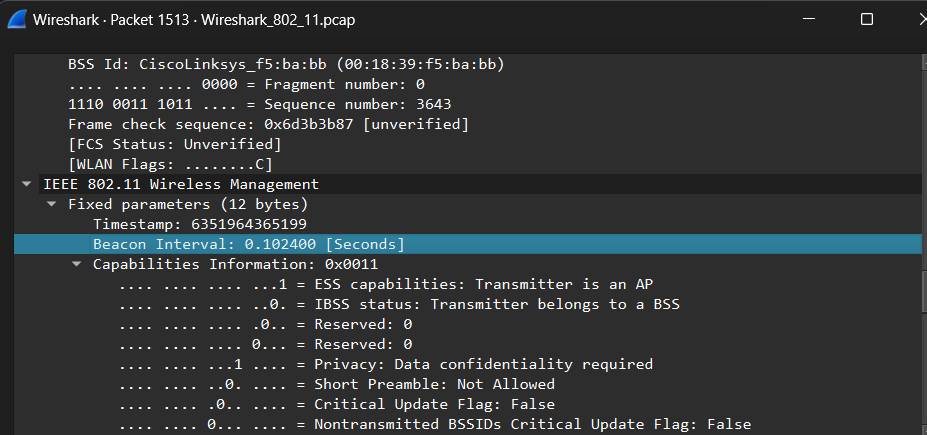
  
Ans= SSID=”linksys12”

SSID=”30 Munroe St”

2. 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.= 

Linksys\_ses\_24086 beacon time interval is 0.1024400 seconds

30 Monroe St beacon time interval is same too .

3. What (in hexadecimal notation) is the source MAC address on the beacon frame

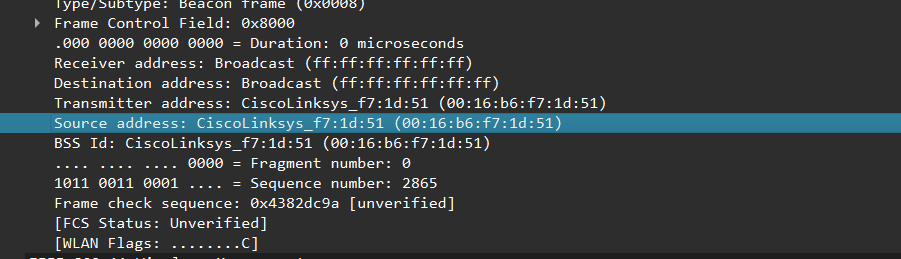
from 30 Munroe St? Recall from Figure 6.13 in the text that the source,

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.=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??

Ans= 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?

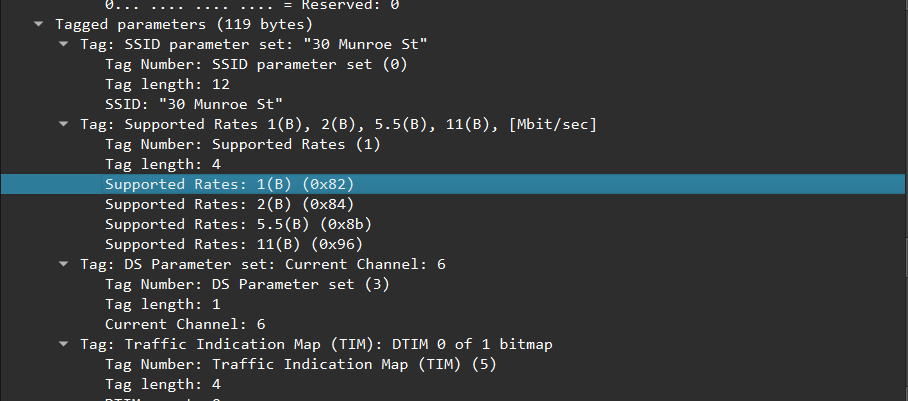
Ans.= BSS Id: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51)

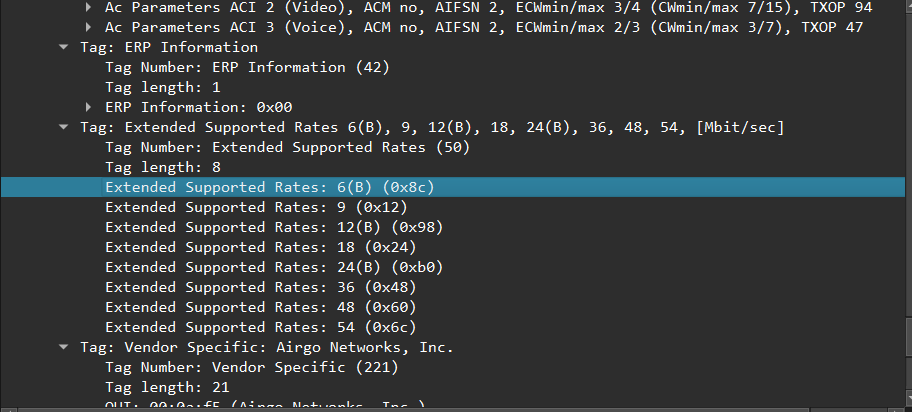
6. The beacon frames from the 30 Munroe St access point advertise that the access

point can support four data rates and eight additional “extended supported rates.”

What are these rates?

Ans.=





***3. Data Transfer***

***Since the trace starts with the host already associated with the AP, let first look at data***

***transfer over an 802.11 association before looking at AP association/disassociation.***

***Recall that in this trace, at t = 24.82, the host makes an HTTP request to***

***http://gaia.cs.umass.edu/wireshark- labs/alice.txt. The IP address of gaia.cs.umass.edu***

***is 128.119.245.12. Then, at t=32.82, the host makes an HTTP request to***

***http://www.cs.umass.edu.***

7. 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?

**Ans= 24.811 seconds**

--What are three MAC address fields in the 802.11 frame?

**Ans= Destination address: CiscoLinksys\_f4:eb:a8 (00:16:b6:f4:eb:a8)**

**Source address: Intel\_d1:b6:4f (00:13:02:d1:b6:4f)**

**Transmitter address: Intel\_d1:b6:4f (00:13:02:d1:b6:4f)**

--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?

Ans.= **Source address is the device itself.**

**Destination address is the access point**

**And transmitter address is the first hop router.**

--What is the IP address of the wireless host sending this TCP segment?

**Ans.= 192.168.1.109**

--What is the destination IP address?

**Ans.= 128.119.245.12**

-- 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.= Access point**

8. 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?

**Ans=24.82 seconds,**

**Transmitter address: CiscoLinksys\_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: CiscoLinksys\_f4:eb:a8 (00:16:b6:f4:eb:a8)**

--Which MAC address in this frame corresponds to the host?

To the access point?

To the first-hop router?

Ans= **Source address is the access point**

**Destination address is the device itself**

**And transmitter address is 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=yes it does.**

***3. Association/Disassociation***

***A host must first associate with an access point before sending data. Association in***

***802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP,***

***with a frame type 0) and the ASSOCIATE RESPONSE frame (sent by the AP to a host***

***with a frame type 0 and subtype of 1, in response to a received ASSOCIAT***

***REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34***

***(Section 7) of the 802.11 spec at http://gaia.cs.umass.edu/wireshark-labs/802.11-***

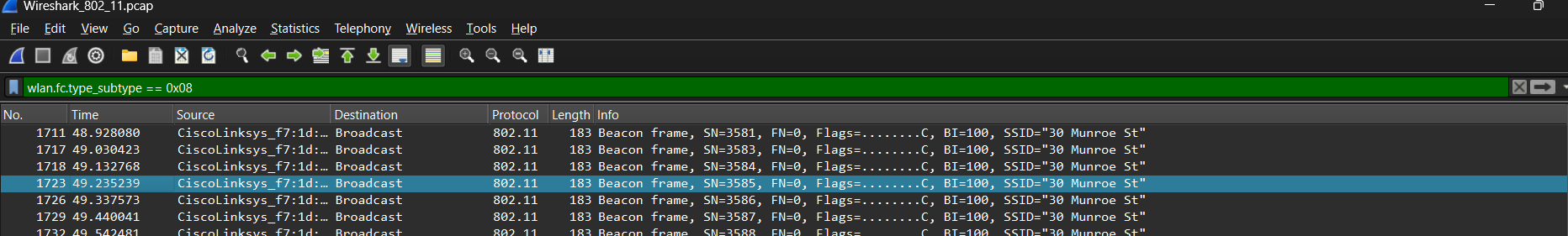
***1999.pdf.***

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, and at what times are these frames sent?

Ans.=time=>49.23 and so on after around every 0.10 seconds…



(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.=no ,there isn’t any.

10. 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.= 49.615 seconds**

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

Ans.= yes if the wifi network is secured by (WPA/WPA2/WPA3)

12. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the

trace?

Ans.= Yes.

13. 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

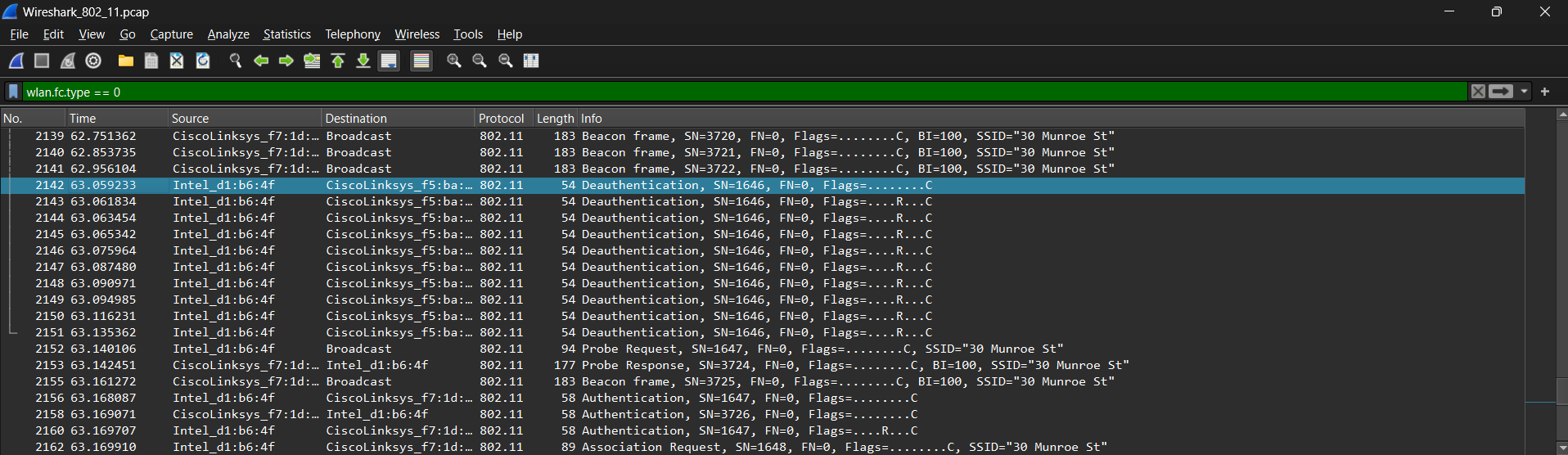
AUTHENTICATION sent from that AP to the host in reply? (Note that you can

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.=63.05 and 63.16 after time intervals of over 0.05 seconds



14. 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 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.= **ASSOCIATE REQUEST**

2162 63.169910 Intel\_d1:b6:4f CiscoLinksys\_f7:1d:51 802.11 89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"

**ASSOCIATE RESPONSE**

2166 63.192101 CiscoLinksys\_f7:1d:51 Intel\_d1:b6:4f 802.11 94 Association Response, SN=3728, 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.

Ans.= 1,2,5.5,6,9,11,12,24 and so on including the supported and extended rates.

***4. Other Frame types***

***Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.***

16. 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?

Ans**= PROBE REQUEST**

50 **2.297613** Intel\_1f:57:13 Broadcast 802.11 79 Probe Request, SN=576, FN=0, Flags=........C, SSID="Home WIFI"

**PROBE RESPONSE**

51 **2.300697** CiscoLinksys\_f7:1d:51 Intel\_1f:57:13 802.11 177 Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"

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.= **Probe Request** frames are sent by client devices (stations) to discover nearby Wi-Fi networks. When a client device is not currently connected to a network or is actively searching for available networks.These frames contain information such as the SSID (network name) being sought by the client device.

**Probe Response** frames are sent by access points (APs) in response to Probe Request frames sent by client devices. When an access point receives a Probe Request frame from a client device, it responds with a Probe Response frame.These frames contain information about the network, including the SSID, supported data rates, security parameters, and other network configuration details.