Alyssa Ballestro

WireShark

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

frames in this trace? 30 Monroe St and linksys 12

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

linksys\_ses\_24086 access point? 2.138s and 8.384s   
From the 30 Munroe St. access point? 0.08s to 0.18s

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

from 30 Munroe St? 00:16:b6:f7:1d:51

4. What (in hexadecimal notation) is the destination MAC address on the beacon

frame from 30 Munroe St?? ff:ff:ff:ff:ff:ff

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

Munroe St? 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? 1B, 2B, 5.5B, 11B

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 802.11Receiver address: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)Transmitter address: IntelCor\_d1:b6:4f (00:13:02:d1:b6:4f)Destination address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)

Destination address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)

Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? Transmitter address: IntelCor\_d1:b6:4f (00:13:02:d1:b6:4f)

To the access point? Destination address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8) To the first-hop router? Receiver address: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)

What is the IP address of the wireless host

sending this TCP segment?ip.src == 192.168.1.109

What is the destination IP address? ip.dst == 128.119.240.19

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

Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? Transmitter address: IntelCor\_d1:b6:4f (00:13:02:d1:b6:4f)

To the access point? Destination address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)

To the first-hop router?Receiver address: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)

What is the IP address of the wireless host

sending this TCP segment?ip.src == 192.168.1.109

What is the destination IP address? ip.dst == 128.119.240.19

Does this destination IP address correspond to the host, access point, first-hop router, or

some other network-attached device? Corresponds to the access point.

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? No.

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? A SYN and and ACK pack

Looking at the 802.11 specification, is there another frame

that you might have expected to see, but don’t see here? Another acknowledgment from the system.

10. 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? 16

11. Does the host want the authentication to require a key or be open? No

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

Trace? Yes

13.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?frame.time\_relative == 49.020356 frame.time\_relative == 49.020948

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? frame.time\_relative == 49.651078When is the corresponding ASSOCIATE REPLY sent?frame.time\_relative == 63.192101

15. What transmission rates is the host willing to use? 1B, 2B, 5.5B, 11B The AP? 1B, 2B, 5.5B, 11B, 6B, 9B, 12B, 18, 24B, 36, 48, 54

16. What are the sender: wlan.sa == 00:12:f0:1f:57:13

receiver: wlan.da == ff:ff:ff:ff:ff:ff

BSS ID MAC addresses in these frames? BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

What is the purpose of these two types of frames? Their purpose is to negotiate and communicate the supported transmission rates between devices.