CIS 375

Lab 05

2-25-2016

Rodney Fulk

Jason Carr

**Part 2. Beacon Frames**

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

#1 - 30 Munroe St

#2 - linksys12

**2. What are the intervals of time between the transmissions of the beacon frames the linksys\_ses\_24086 access point?**

0.102400 seconds

**From the 30 Munroe St?**

0.102400 seconds

**3. What (in hex) is the source MAC address on the beacon frame from 30 Munroe St?**

00:16:b6:f7:1d:51

**4. What (in hex) is the destination Mac address on the beacon frame from 30 Munroe St?**

ff:ff:ff:ff:ff:ff

**5. What (in hex) is the MAC BSSID 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?**

data: 1(B), 2(B), 5.5(B), 11(B) [Mbit/sec]

extended: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 [Mbit/sec]

**Part 3. Data Transfer**

**7. Find the 802.11 frame containing the SYN TCP segment for this TCP session. At what time is the TCP SYN sent?**

24.81

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

Receiver: 00:16:b6:f7:1d:51

Transmitter: 00:13:02:d1:b6:4f

Destination: 00:16:b6:f4:eb:a8

**Which MAC address in this frame corresponds to: the (1) the wireless host of the MAC address for the host?**

Transmitter: 00:13:02:d1:b6:4f

**(2) to the access point?**

Receiver: 00:16:b6:f7:1d:51

**(3) to the first-hop router?**

Destination: 00:16:b6:f4:eb:a8

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

192.168.1.109

**What is the destination IP address?**

128.119.245.12

**Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device?**

Access point

**8. Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received?**

24.82

**What are three MAC address fields in the 802.11 frame containing the SYNACK?**

Receiver: 91:2a:b0:49:b6:4f

Transmitter: 00:16:b6:f7:1d:51

Source Address: 00:16:b6:f4:eb:a8

**Which MAC address in this frame corresponds to (1) the host?**

Receiver: 91:2a:b0:49:b6:4f

**(2) to the access point?**

Transmitter: 00:16:b6:f7:1d:51

**(3) to the first-hop router?**

Source Address: 00:16:b6:f4:eb:a8

**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?**

They appear to yes

**Part 4. Association/Disassociation**

**9. What two actions are taken (i.e., ALL frames types that 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?.**

DHCP release at 49.58 and Deauthentication at 49.60

**Looking at the 802.11 specification, is there another frame that you might have expected to see, but don’t see here?**

Disassociation Frame, so that the 30 Munroe St AP can relinquish memory allocations and remove the host from the association table.

**10. Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP. 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?**

49.63

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

be an open system

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

no, just beacon broadcasts

**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 AUTHENTICATION frames sent from the host to this AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when the AUTHENTICATION reply is sent from that AP to the host?**

Authentication is at 63.16 and reply is 63.16

**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 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? 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.)**

request at 63.16

response at 63.19

**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 Asso Req and Res frames.**

Data rate is 54.0Mb/s using BG Channel 6 on 2.4Ghz