Solutions to IEEE802.11 Wireshark Labs

1. The two access points that are issuing most of the beacon frames have an SSID of "30 Munroe St" and "linsys_SES_24086"

2. The beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless LAN Magement frane as .1024 seconds (i.e., just over 100 milliseconds). Note that the 30 Munroe St AP beacon frames show up in the trace at this regularity, but the beacons from the linsys_SES_24086 AP do not.

3. The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51

4. The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff, i.e., the broadcast address.

5. The MAC bssid address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51. Note that this is the same as for the source address (since this is a beacon frame)

6. The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps

7. The TCP SYN is sent at t = 24.811093 seconds into the trace. The MAC address for the host sending the TCP SYN is 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. Note that this is a NATed address. The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu. It is important to understand that the destination MAC address of the frame containing the SYN, is different from the destination IP address of the IP packet contained within this frame. Make sure you understand this distinction! (If you're a bit hazy on this, re-read pages 468 and 469 in the 4th edition of the text).

8. The TCP SYNACK is received at t = 24.827751 seconds into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached . The MAC address for the destination, which the host itself, is 91:2a:b0:49:b6:4f. (Curiously, this is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses - interesting!). The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu) The destination address is 192.168.1.109 (our wireless PC).

9. At *t* = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At *t* = 49.609617, the host sends a DEAUTHENTICATION frame (Frametype = 00 [Management], subframe type = 12[Deauthentication]). One might have expected to see a DISASSOCIATION request to have been sent.

10. The first AUTHENTICATION from the host to the AP is at *t* = 49.638857.

11. The host is requesting that the association be open (by specifying Authentication Algorithm: Open System).

12. I can't find any reply from the 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.

13. At *t* = 63.168087 there is a AUTHENTICATION frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At *t* = 63.169071 there is an AUTHENTICAN from sent in the reverse direction from the BSS to the wireless host.

14. At *t* = 63.169910 there is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At *t* = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host.

15. In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps. The same rates are advertised in the ASSOCIATION RESPONSE.

16. At *t* = 2.297613 there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSSID of ff:ff:ff:ff:ff:ff. At *t* = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 00:16:b6:f7:1d:51. A PROBE REQUEST is used by a host in *active scanning* to find an Access Point (see Figure 6.9 on page 531 in the text). A PROBE RESPONSE is sent by the access point to the host sending the request.