1. What is the layer 2 protocol and the associated physical layer represented in this capture? How can you tell? Layer 2 is the IEEE protocol that is represented by the 802.11 Wireless LAN we can tell in the packet information display.

2. Is frame 13 a management, control, or data frame? What is the frame subtype? What type of address is the layer 2 destination address? Why is this type of address being used?

Frame 13 is a control frame, the frame subtype is management. The type of address for the destination is a broadcast address (ff:ff:ff:ff:ff:ff). This address is being used because it is used to target all systems on a specific subnet network instead of single hosts.

3. What is the name of the Access Point (AP) broadcasting this frame? What is the filter syntax for the field containing the AP's name? Explain how the name of the filter makes sense logically based on your knowledge of frame types and the field you are interested in.

The access point that is broadcasting the frame is a Beacon. The filter syntax for this field that contains the AP's is BSS which is the network topology that allows all wireless devices to communicate with each other through the access point. The name of Beacon makes logical sense because the signals are transmitted periodically, similar to a light beacon.

4. What is the BSSID of the AP in frame 7?

The SSID for frame 7 is CMY

5. Create a filter based on the BSSID of frame 7, where you only want to see traffic that was sent from that AP. Apply the filter. How many frames are displayed? What is the only other type of management frame seen from this AP? What generic type of frames are the remaining frames?

Based on the filter that is applied to the BSSID on frame 7, there were 35 frames that were sent using that specific access point. The only other type of frames was a probe response. The probe response is determining what network is available on that channel.

6. Where is the radiotap header info derived from, how is it created? Is this transmitted in the frame?

The radiotap header is derived from the userspace applications to the driver for transmission. This is being transmitted in all of the frames in this file.

7. What channel was this traffic collected on? What is the filter syntax for this?

The channel that this frames traffic is collected on is at a frequency of 2437, with a complementary code keying flag. The filter syntax for this channel is radiotap.channelfreq == 2437, which filters only the frames that are using this specific channel frequency.

8. Is frame 1 a control, management, or data packet? What is the frame subtype? Explain the function of this frame. Frame 1 is a management frame, the frames subtype is 4 which is a probe response subtype. This subtype is requesting information from either a specific access point, specified by SSID, or all access points in the area, specified with the broadcast SSID.

9. What would you expect in response to frame 1? What traffic is caused by the actions of frame 1? Specify the frame numbers. In response to frame 1 the ipad is starting up and is sending out a probe request to the broadcast of SSID.

10. What is the client's layer 2 address? What are the layer 2 addresses of the devices that responded to the client after the initial probe request? The clients layer two address is connecting to the wlan01 and then hpsetup.

11. Which device does the client choose to connect to? How do you know? Any idea why it did not connect to the other device? The device that the client decided to connect to is the ipad that has the address of Apple_47:33:97. The client did not connect to another device because the ipad is the one trying to connect.

12. What is happening in frames 10, 11, and 12? Which device initiates this?

In frames 10,11, and 12 the device is being authenticated, the device that initiates this is the iPad to the Cisco receiver, which is the router. It has to authenticate the mac address before connecting.

13. What is this field telling the client?

This field is telling the client that the process by which the iPad securely accesses the server is exchanging a Digital Certificate.

14. At this point what type of authentication algorithm was implemented? Is this what was listed by the AP as the authentication scheme, why is this? The authentication algorithm that was used is the open system. This is not listed as the AP for an authentication scheme this is because an access point is not required for authentication.

15. What happens after the initial authentication process? Which device initiates this? What is happening during this process? After the initial authentication process is completed the Cisco device initiates the next transmission that goes to the ipad where the Cisco network is running the authentication after the iPad transmitted that it wanted to connect.

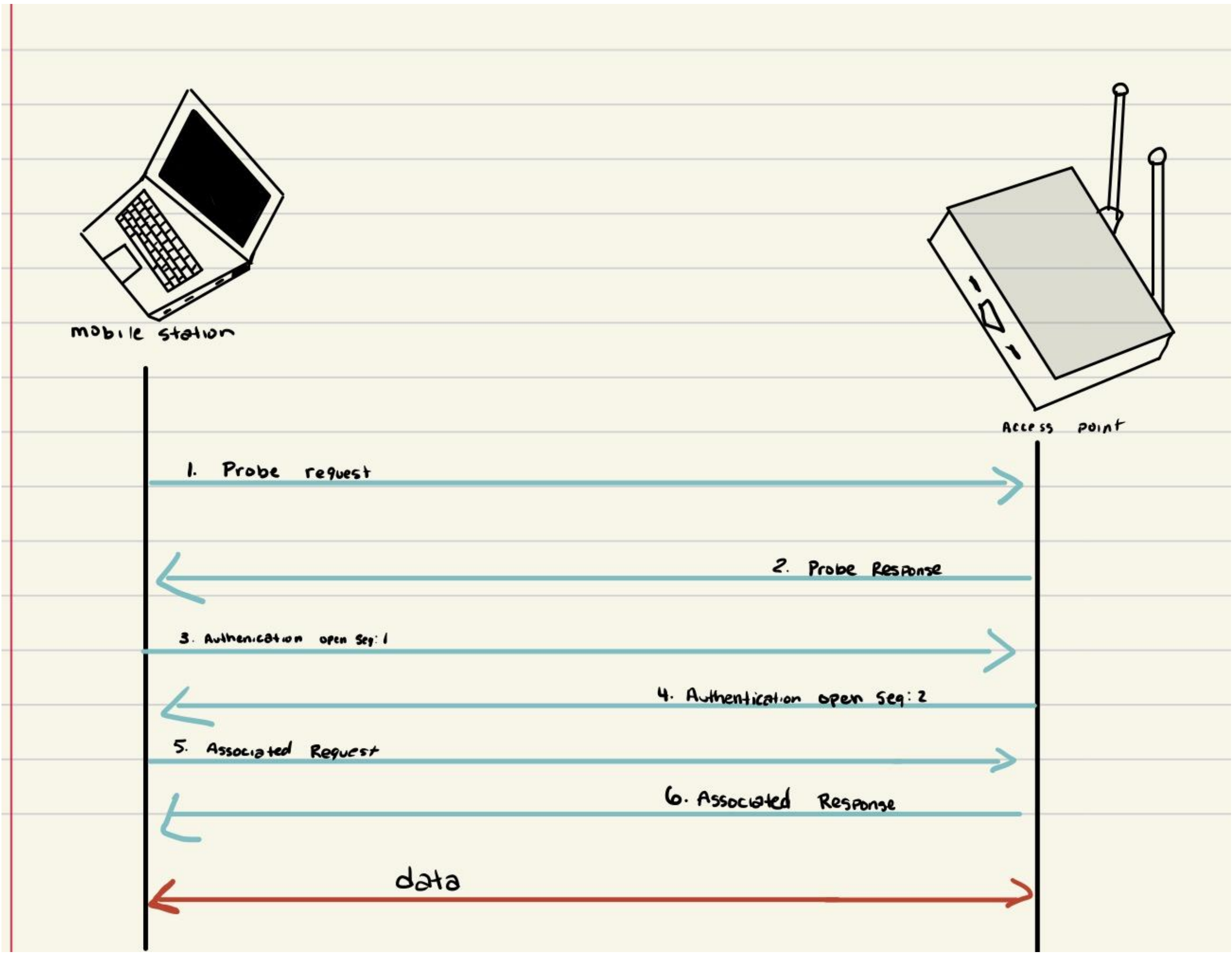
16. What is happening in frames 17-20? Why is this happening after association? In frames 17-20 a key is being sent through the four frames which have four separate parts. The Association occurs after the Shared Key Authentication or Open System Authentication Algorithm. There cannot be a STA that is Associated but not Authenticated. If the STA fails Authentication, it does not move to Association.

17. Are frames 25-65 control, management, or data frames? Why can we not read the data encapsulated in these frames? The frames 25-65 are data frames, we can see the bytes of data that are being transmitted. For example the frame 25 is sending 348 bytes worth of data.

18. There are three main types of frames. We have seen two of them in this capture, what is the third type. Give some examples of what this additional type of frame is used for. The third frame is the control frame that we have not seen, some examples of this is required to describe the conditions and tolerances of a geometric control on a part's feature. The feature control frame includes four parts: GD&T symbol/control symbol.

19. What is the only ‘type’ of frame intended to be forwarded to the wired network? Why is this the case? On Ethernet networks, frames contain a source MAC address and a destination MAC address. Switches receive a frame from the source device and quickly forward it toward the destination device.

20. Diagram the entire process of a client identifying an AP and connecting to an AP using WPA authentication. (You can ignore any control frames for this question)


mobile station
Access point
1. Probe request
2. Probe Response
3. Authenication open Seq: 1
4. Authentication open Seq: 2
5. Associated Request
6. Associated Response
data