Paul Williams Diaz
CIS 151 Prof. Brown

Wireshark LAB: 802.11

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

   Answer: The SSID of the two access points that are issuing most of the beacons frames in this trace are `30 Munroe St` and `linksys_ses_24086.`

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?

   Answer: The intervals of time between the transmission of the beacon frames is

   `Beacon intervals: 0.102400 [ seconds].`

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 the three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the EEI 802.11 standard documents (cited above).

   Answer: The source MAC address on the beacon frame from 30 Munroe St is

   `Source address: Cisco-Li_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*?

   Answer: The destination MAC address on the beacon frame from *30 Munroe St* is

   `Destination address: Broadcast (ff:ff:ff:ff:ff:ff)`

5. What (hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St.*?

   Answer: The MAC BDD id on beacon frame from 30 *Munroe S*t is

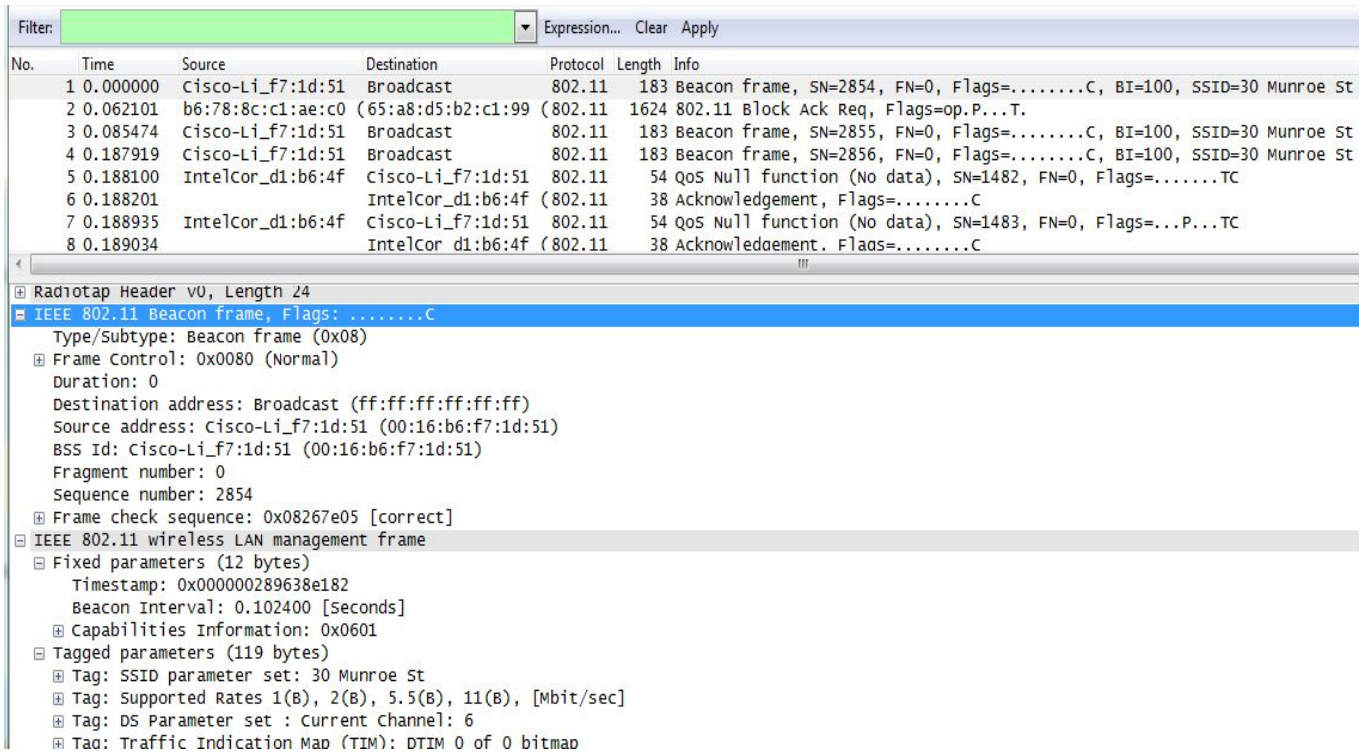
   `BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)`

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?

Answer: The beacon frames from the 30 Munroe St access point advertise that the access point can support four date rates and eight additional”extended supported rates”, these rates are...

```
Extended Supported Rates: 6(B)
Extended Supported Rates: 9
Extended Supported Rates: 12(B)
Extended Supported Rates: 18
Extended Supported Rates: 24(B)
Extended Supported Rates: 36
Extended Supported Rates: 48
Extended Supported Rates: 54 [Mbit/sec]
```



BEACON FRAME

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that

downloads alice.text). At what time is the TCP SYN sent? What are three MAC address field in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for this host)? To the access point? TO the first-hop-router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address corresponds to the host, access points, first-hop-router, 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).

Answer: The TCP SYN was sent at `t = 24.811093000 seconds.` The three MAC addresses fields in the 802.11 frame are 1. MAC address whose sending the TCP SYN or the `Source address: IntelCor_d1:b6:4f(00:13:02:d1:b6:4f)` 2. MAC address `Destination: Cisco-Li_f4:eb:a8(00:16:b6:f4:eb:a8)` 3. MAC address `BSS Id: Cisco-Li_f7:1a:51(00:16:b6:f7:1d:51)`. The IP address of the wireless host sending the TCP SYN is 192.168.1.109, and the destination IP address is 128.119.245.12. It corresponds with the server gaia.cs.umass.edu, the destination MAC address of the frame containing the first TCP segment is different from the destination IP address (containing the IP packet).

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 field in the 802.11 frame containing the SYNACK? Which MAC address in this frame corresponds to the host? To the access points? To 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?

   Answer: The TCP SYNACK was received at `t = 24.827751000 seconds.` The three MAC addresses fields in the 802.11 frame are 1. MAC `Source address: Cisco-Li_f4:eb:a8(00:16:b6:f4:eb:a8)`. 2. MAC `Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)`. 3. MAC `BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)`. The MAC address for the destination `(91:2a:b0:49:b6:4f)` is different from the MAC address of the host used that sends the TCP SYN.

9. What two actions are taken (e.i., 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 the trace

collection began, and at what are these frames were sent? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there any other frame that you might have expected to see, but don't see here?

Answer: The two actions taken by the host in the trace just after t = 49 are 1.DHCP (an IP-layer protocol) with a time of `t = 49.583615000 seconds` and 2. Deauthentication (802.11 protocol) with a time of `t = 49.609617000 seconds`. One might have expected to see a DISASSOCIATION request to have been sent.

10. Examine the trace file and look for AUTHENTICATION 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?

    Answer: The first AUTHENTICATION frame sent from the wireless host to the *linksys_ses_24086* is...

    `[Time since reference or first frame; 49.638857000 seconds]`

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

    Answer: By specifying Authentication Algorithm -Open System, the host is requesting that the association be open.

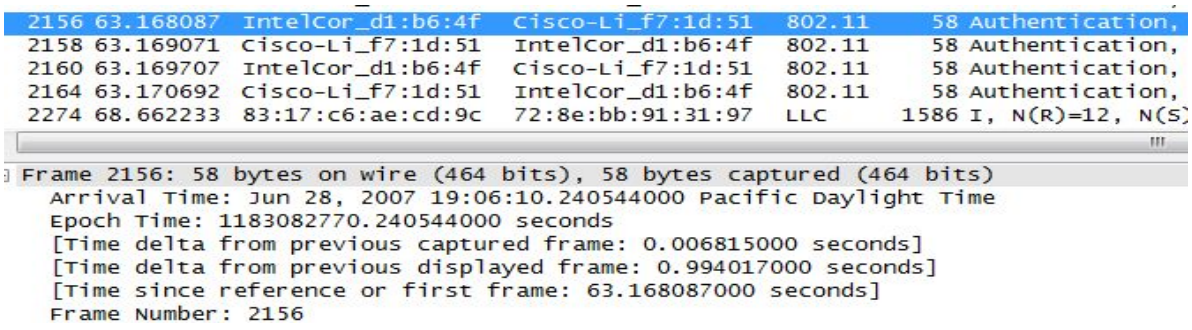
12. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?

    Answer: A request for open access is being ignored because AP is configured to require a key when associating. That is why there is no reply shown in the frame from the AP.

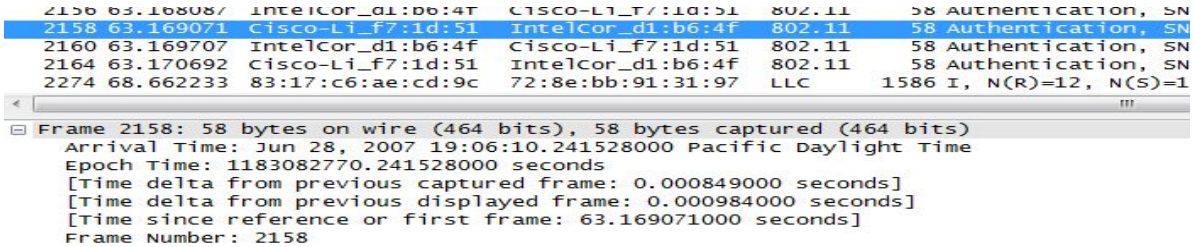
13. Now let's consider what happens as the host gives up (sometimes after *t=63.0*) trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe*

St. AP. Look for AUTHENTICATION frames sent from the host to and AP 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==1* and *wlan.fc.type==0* and *wlan.addr==IntelCo_d1:b6:4f"* to display only the AUTHENTICATION frames in this trace for this wireless host.)

Answer: The AUTHENTICATION frame from host to the 30 Munroe St AP is at `t = 63.168087000 seconds` and the reply was sent to the host at `t = 63.16907100 seconds.`



Authentication time after 63.0

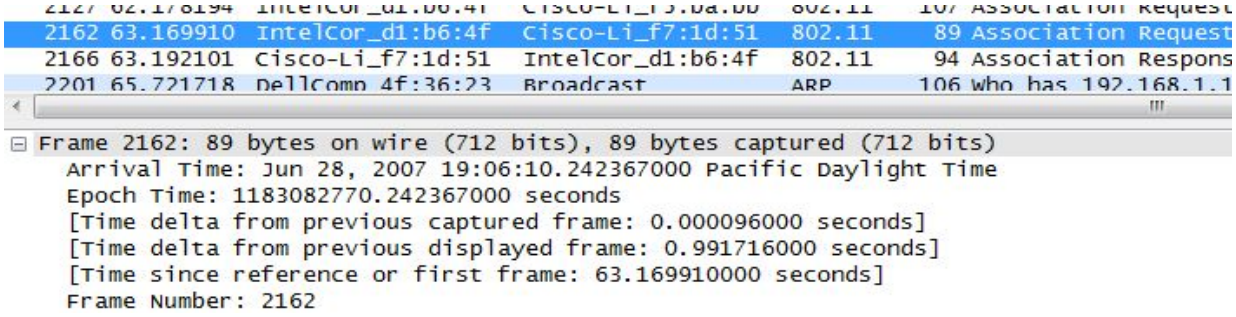


Authentication time of reply

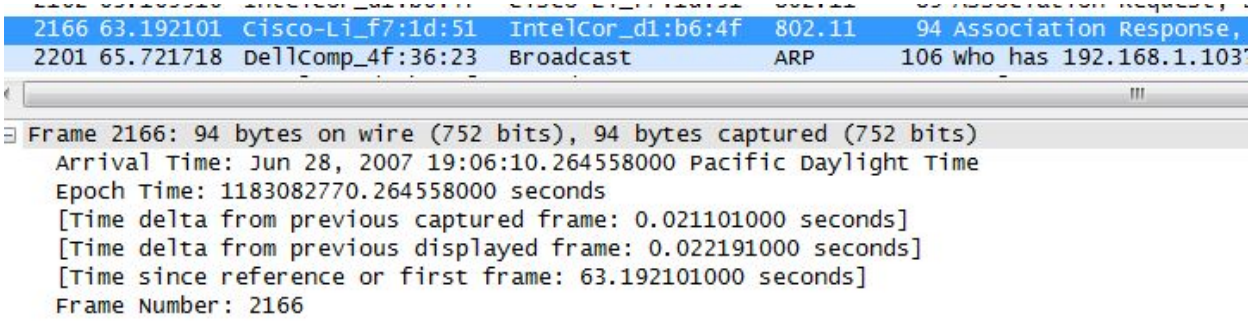
14. Let's continue on with the association between the wireless host and the 30 Munroe St. AP that happens after *t=63.0*. An ASSOCIATION from host to AP, and a corresponding

ASSOCIATE RESPONSE frame from an 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.)

Answer: The time of the ASSOCIATE REQUEST from host to the 30 Munroe ST was sent is at `t = 63.169910000 seconds` and the reply was sent at `t = 63.192101000 seconds.`



Association Request after 63.0

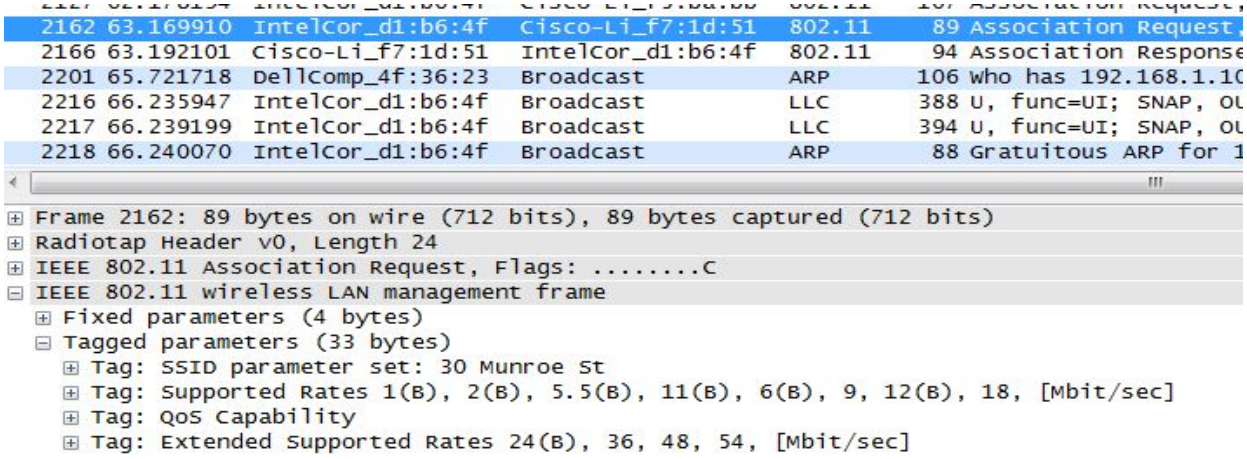


Association time of Reply

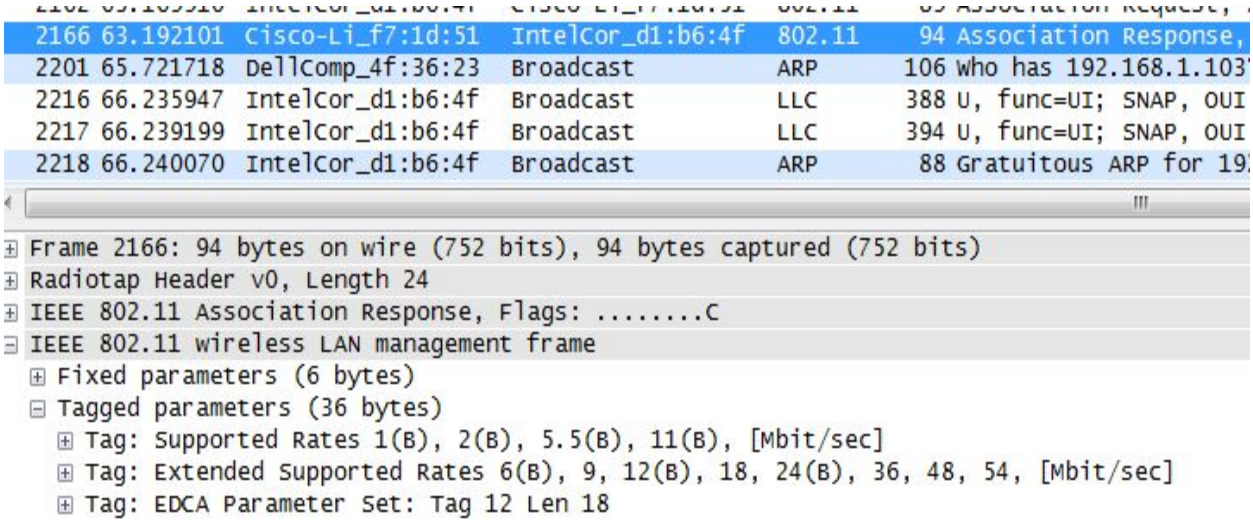
15. What transmission rates is the host willing to use? The AP? TO answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

Answer: The transmission rates that the host and the AP are willing to use are as follows...

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B),9,12(B), 18
          [Mbit/sec]
Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec].
```



ASSOCIATION REQUEST Parameters Field

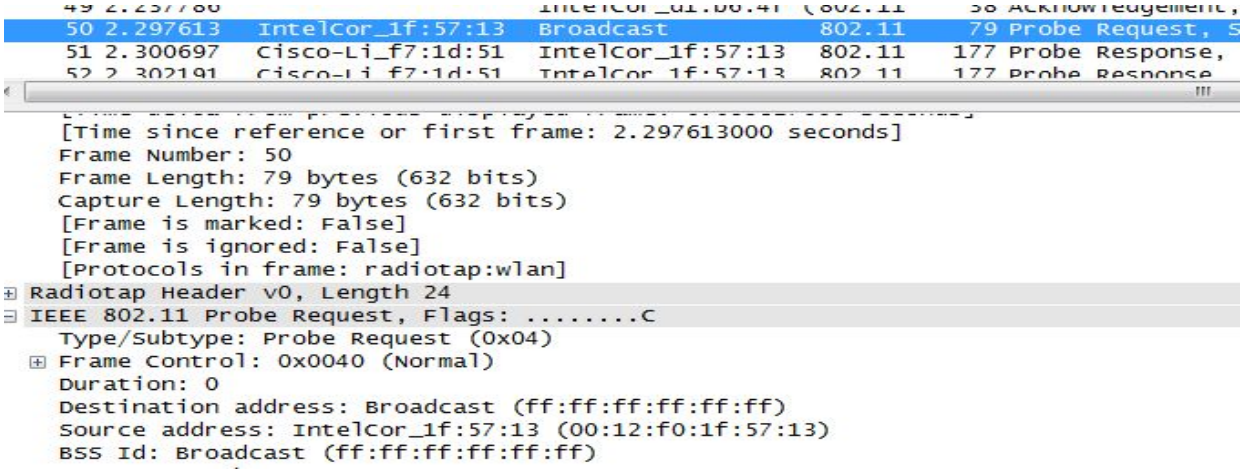


ASSOCIATION RESPONSE Parameters Field.

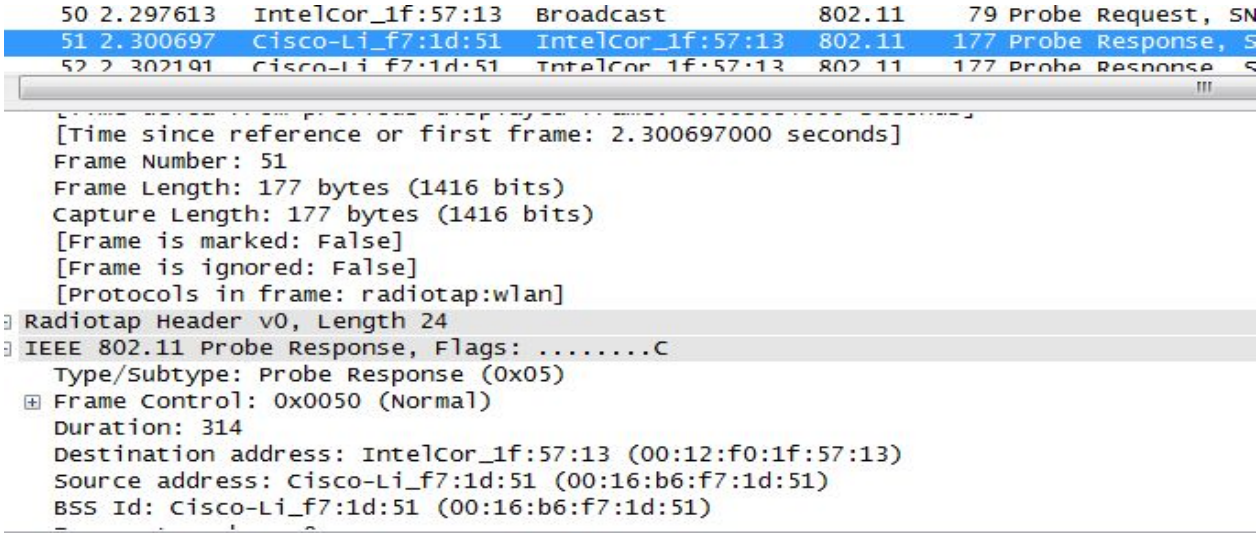
16. Consider the first PROBE REQUEST and soonest subsequent PROBE RESPONSE PAIR

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? 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).

Answer: The frame request was sent at `t = 2.297613000 seconds` with `Source address: InterCor_1f:57:13 (00:12:f0:1f:57:13)`, it's `Destination address: Broadcast (ff:ff:ff:ff:ff:ff)` and `BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)`. The frame response was sent at `t = 2.300697000 seconds` with `Source address:Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)`.A PROBE REQUEST is used by a host in active scanning to find an Access Point. A PROBE RESPONSE is sent by the Access Point to the host sending the request.



PROBE REQUEST after t = 2.0 seconds



PROBE RESPONSE after t = 2.0 seconds