EE450

802.11 Lab Report

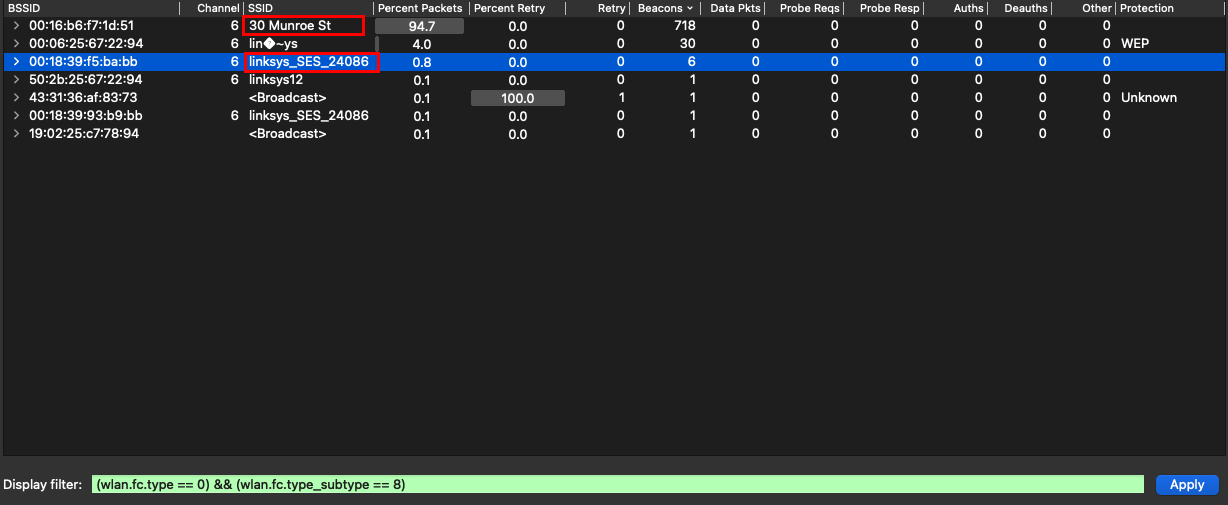
Yuhang Xiao

Abstract

This report investigates the behavior of the widely-used 802.11 wireless network protocol in detail. We will capture and analyze a trace of 802.11 frames, which consisting of a Linksys 802.11g combined access point/router, and frames are captured on channel 6. At first, the host is already associated with the 30 Munroe St AP, then it will make HTTP request to 128.119.245.12 and 128.119.240.19. After that, it will disconnect from the previous AP and try to connect to a new AP, linksys\_ses\_24086, and finally, it will re-connect with the original AP. During the process, multiple useful frames like beacon frame, AUTHENTICATION, DEAUTHENTICATION, ASSOCIATION REQUEST, ASSOCIATION RESPONSE, PROBE REQUEST and PROBE RESPONSE are captured. This report will dive into the details of these frames and help to understand the 802.11 protocol.

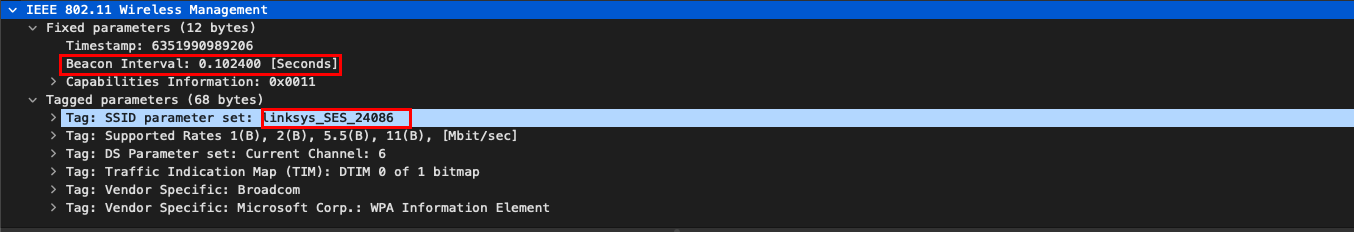
1.

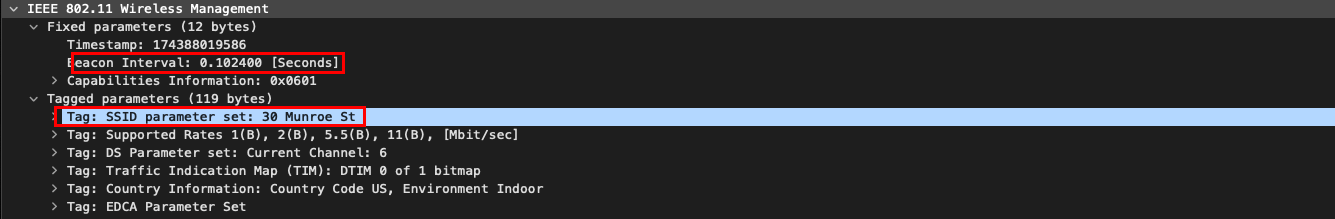
The two access points’ SSIDs are “30 Munroe St” and “linksys\_SES\_24086”.



2.

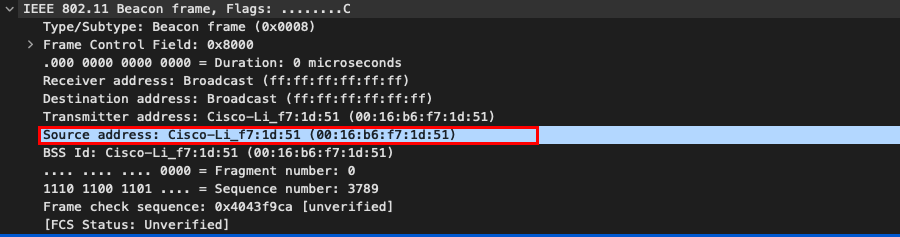
The beacon interval for both access points are 0.102400 seconds.





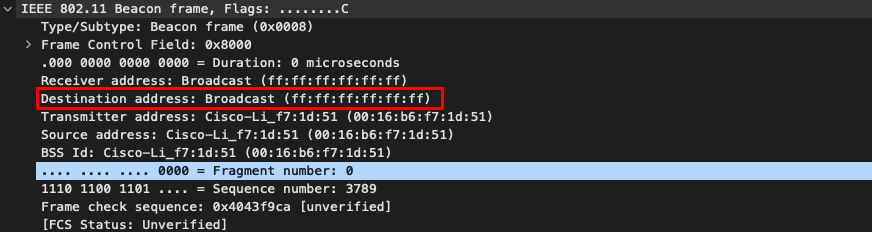
3.

The source MAC address is 00:16:b6:f7:1d:51.



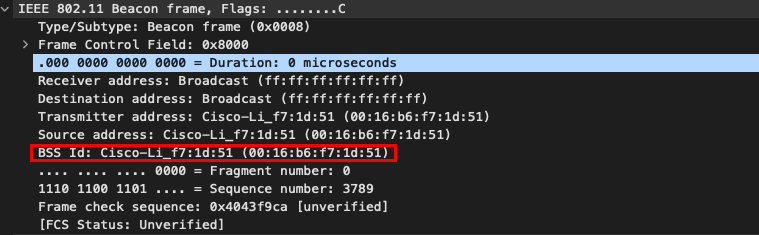
4.

The destination MAC address is ff:ff:ff:ff:ff:ff.



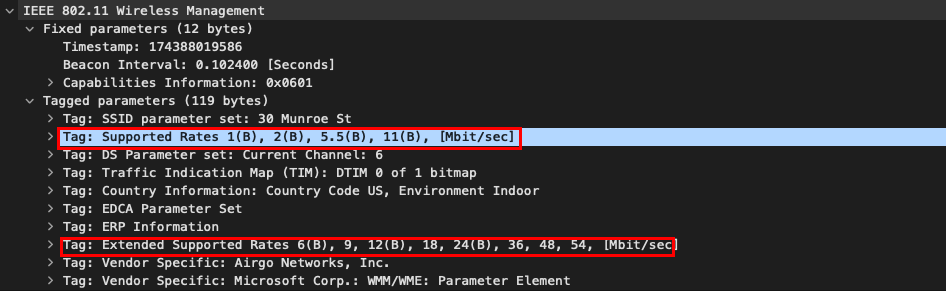
5.

The MAC BSS ID address is 00:16:b6:f7:1d:51.



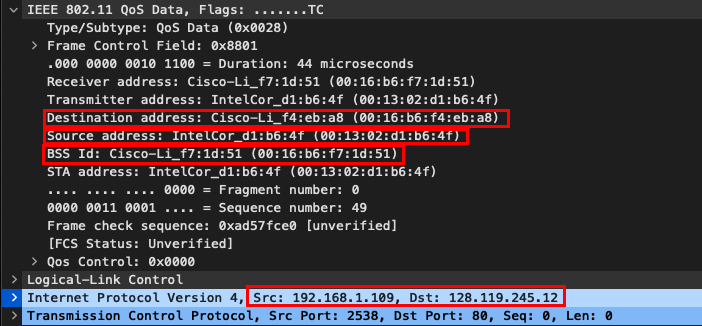
6.

The support rates are 1, 2, 5.5, 11 Mbps. The extended supported rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.



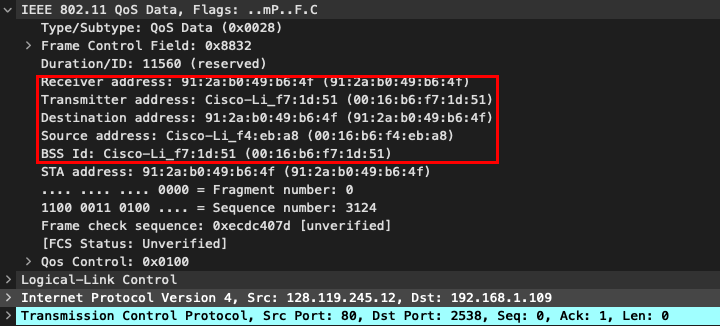
7.

The three MAC address field are 00:16:b6:f7:1d:51, 00:13:02:d1:b6:4f and 00:16:b6:f4:eb:a8. The MAC address for the wireless host is 00:13:02:d1:b6:4f. The MAC address for the access point is 00:16:b6:f7:1d:51. The MAC address for the first hop router is 00:16:b6:f4:eb:a8. The IP address of the host sending the TCP SYN is 192.168.1.109. The destination IP address is 128.119.245.12, which corresponds to the server gaia.cs.umass.edu.



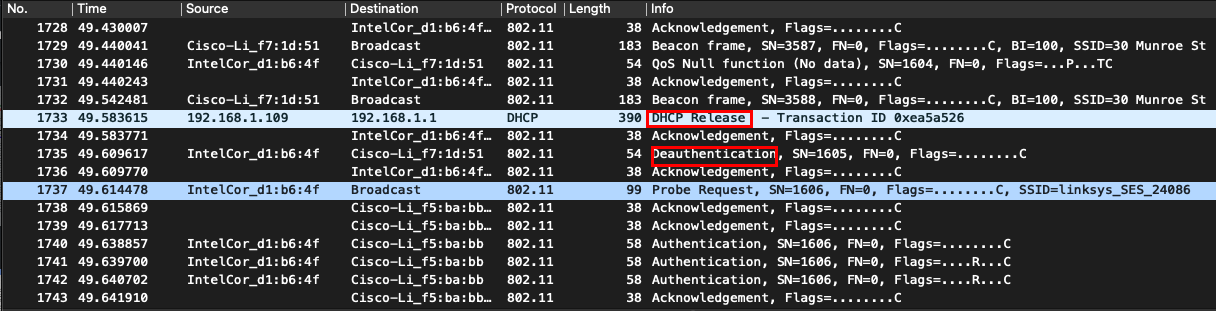
8.

The three MAC address field are 91:2a:b0:49:b6:4f, 00:16:b6:f7:1d:51 and 00:16:b6:f4:eb:a8. The MAC address for the host is 91:2a:b0:49:b6:4f. The MAC address for the access point is 00:16:b6:f7:1d:51. The MAC address for the first-hop router is 00:16:b6:f4:eb:a8, which is also the sender MAC address. The sender IP address is 128.199.245.12, which corresponds to gaia.cs.umass.edu. Thus, it doesn’t correspond to the sender MAC address.



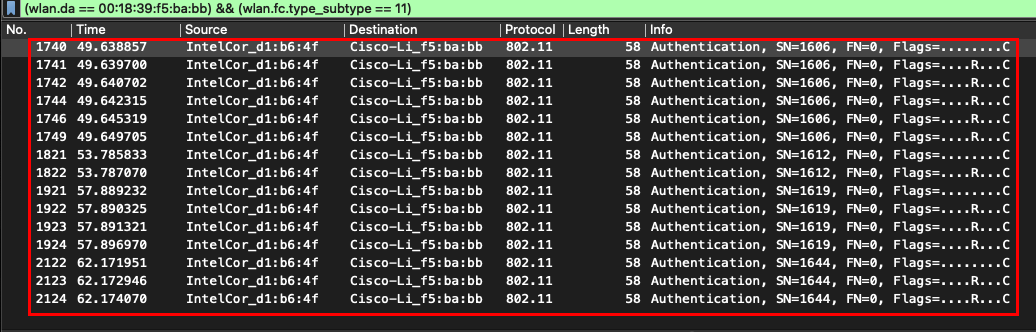
9.

A DHCP Release frame is sent by the host to the DHCP server. Then, the host sends a DEAUTHENTICATION frame. A DISASSOCIATION request frame is expected to send but don’t see here.



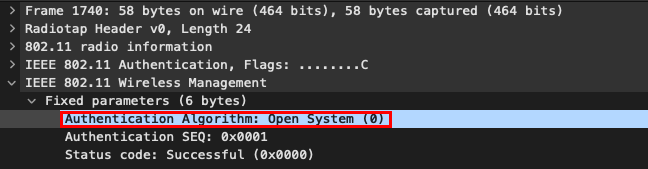
10.

There are 15 AUTHENTICATION messages sent from the wireless host to the linksys\_ses\_24086 AP starting at around t=49.



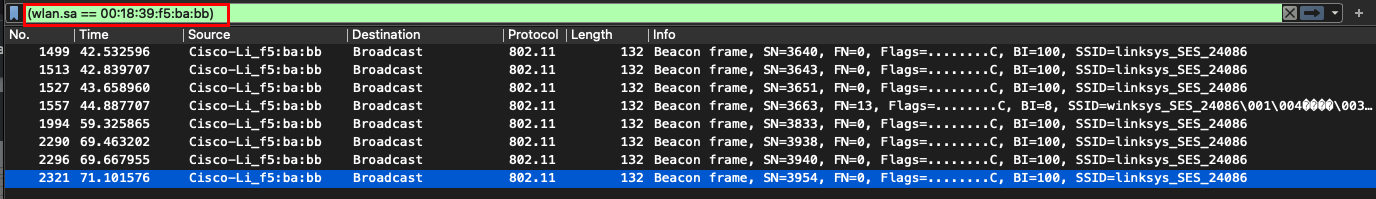
11.

The host wants the authentication to be open because the frame specifies the Authentication Algorithm is Open System.



12.

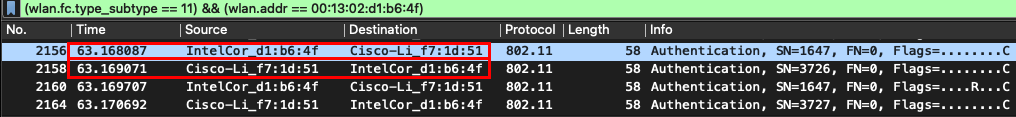
Applying the filter that the source address is the address of linksys\_ses\_24086 AP, there is no reply sent.



13.

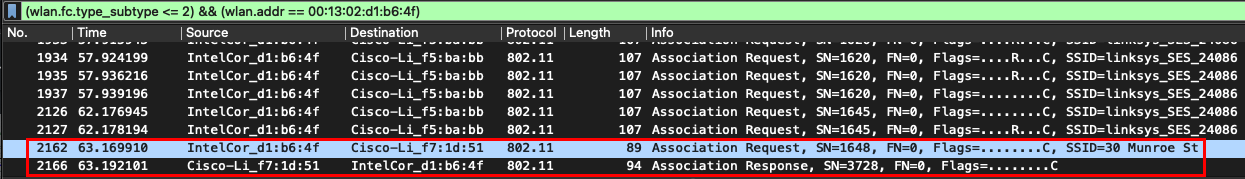
At t = 63.168087, there is an AUTHENTICATION frame sent from the wireless host to the 30

Munroe St AP. At t = 63.169071 there is a reply AUTHENTICATION frame sent from the AP to the host. There is another sending at t = 63.169707 and replying at t = 63.170692.



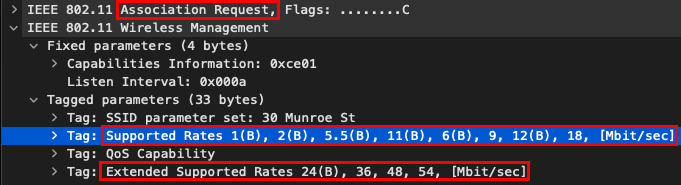
14.

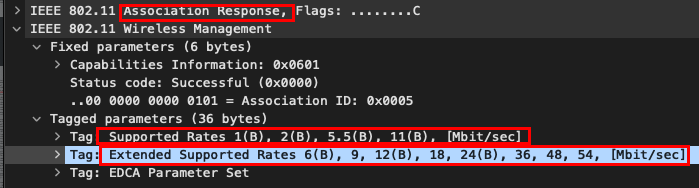
At t = 63.169910 there is an ASSOCIATION REQUEST frame sent from host to the 30 Munroe St AP. At t = 63.192101 there is an ASSOCIATION RESPONSE frame sent from the AP to the wireless host.



15.

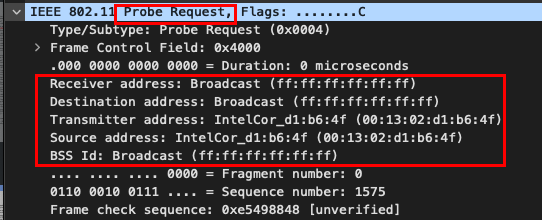
Looking into the ASSOCIATION REQUEST and ASSOCIATION RESPONSE frame, after combining the supported rate and extended supported rate, both host and the AP are willing to use the transmission rates of 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

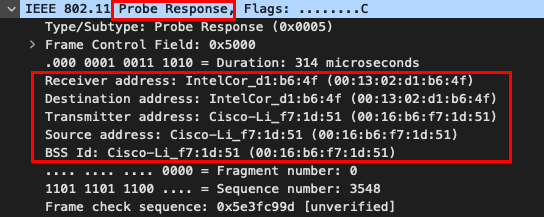




16.

In PROBE REQUEST frames, the sender MAC address is 00:13:02:d1:b6:4f, the receiver and BSS ID MAC address is ff:ff:ff:ff:ff:ff. In PROBE RESPONSE frames, the sender MAC address is 00:16:b6:f7:1d:51, which is also the BSS ID MAC address. The receiver MAC address is 00:13:02:d1:b6:4f. A PROBE REQUEST frame is a broadcast for a host to find an AP. A PROBE RESPONSE is a response message from the AP to the host. They are used for active scanning.





Conclusion

This report dived into the details of the ubiquitous 802.11 (WiFi) protocol. A trace of captured 802.11 frames was analyzed and discussed. First, the multiple MAC addresses inside the 802.11 frames were discussed and their purposes were clarified. Then, the AUTHENTICATION behavior in 802.11 protocol was explored. After that, the ASSOCIATION REQUEST and the ASSOCIATION RESPONSE frame were discussed in details when the host tried to reconnect with the original AP. Finally, the active association was briefly explored by the captured PROBE REQUEST and PROBE RESPONSE frame. Through this report, the main behaviors of 802.11 protocol are explored and clarified.