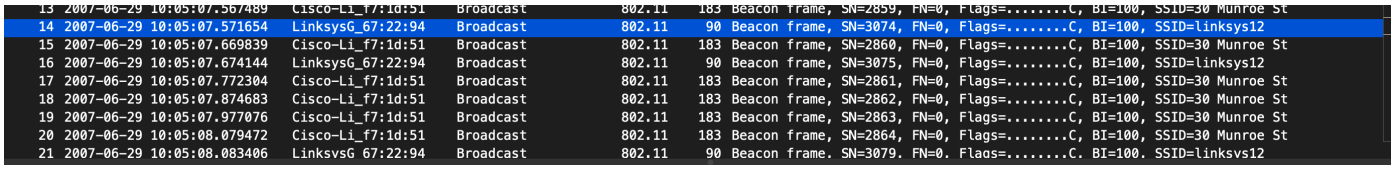
1 基于已捕获的 802.11 帧的数据文件Wireshark_802_11.pcap，分析

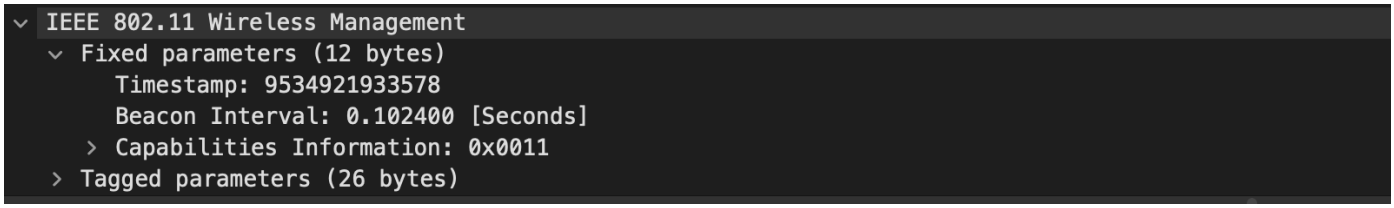
1.1 信标帧 Beacon Frames

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



如图，可以看到两个access points的SSID分别是说明文档中提到的linksys_ses_24086和30 Munroe st。

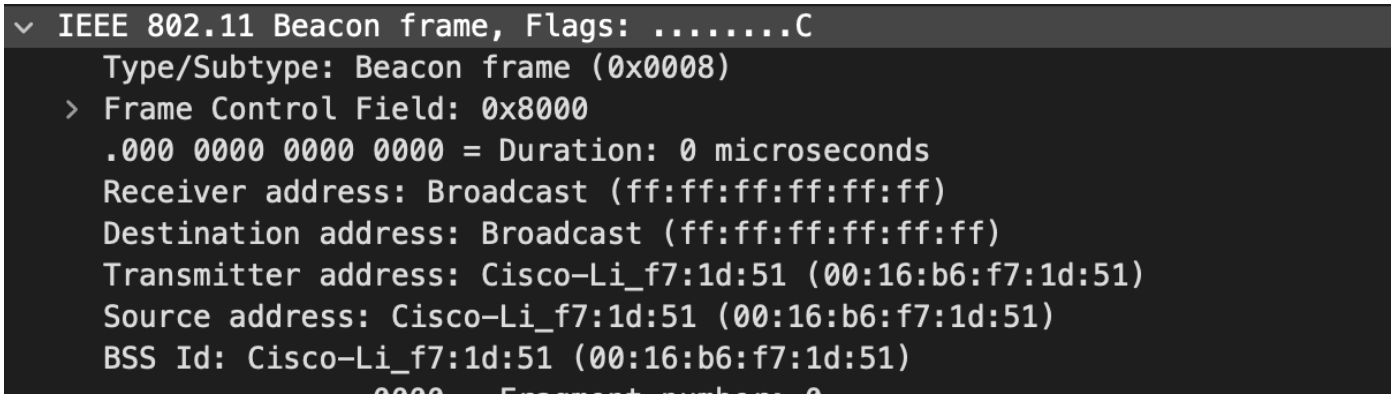
1.1.2 What are the intervals of time between the transmissions of the beacon frames the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).



如图，对于linksys_ses_24086，intervals是0.102400s。

对于30 Munroe St.，intervals也是0.102400s。

1.1.3 What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11standards document (cited above).



如图，source MAC address是00:16:b6:f7:1d:51。

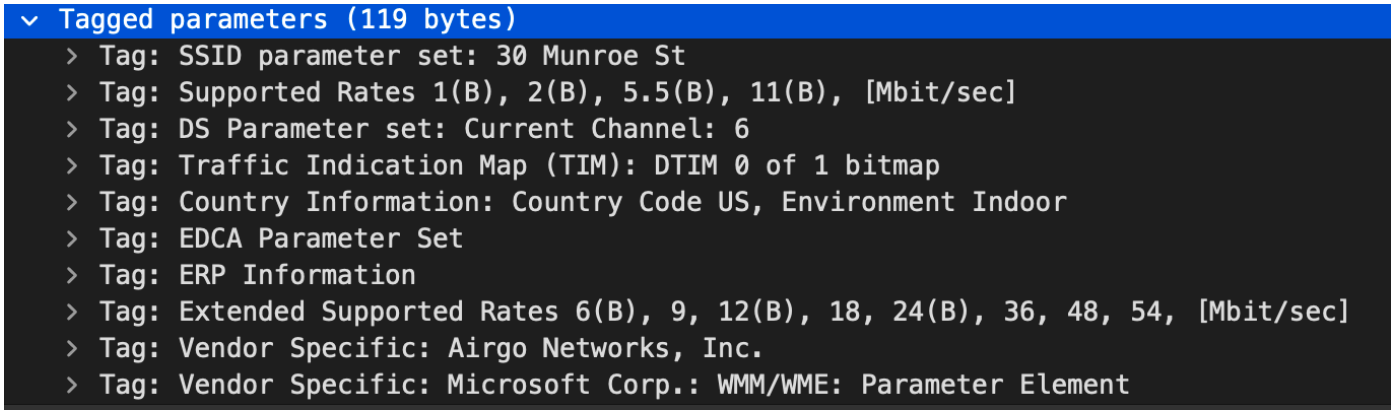
1.1.4 What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??

如1.1.3的图，这个是广播帧，destination MAC address是ff:ff:ff:ff:ff:ff。

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

如1.1.3的图，BSS Id是00:16:b6:f7:1d:51。

1.1.6 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?

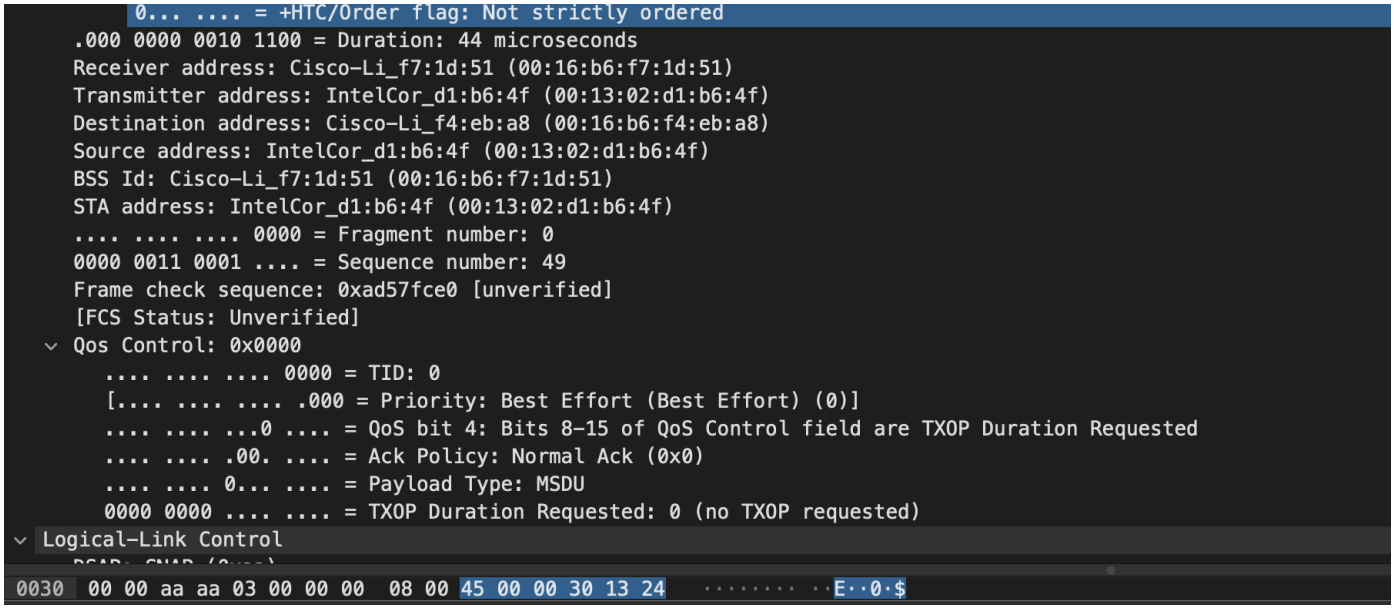


如图，四种数据率是1(B), 2(B), 5.5(B)和11(B) M bit/sec。

八种额外的拓展支持速率是6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbit/sec。

1.2 数据传输Data Transfer：

1.2.1 Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields 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 the 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 correspond to the host, access point, first-hop router, or some other network-attached device? Explain.



三个Mac address：

Receiver address：Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51),

Transmitter address和Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f),

Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。

wireless host是：IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)。

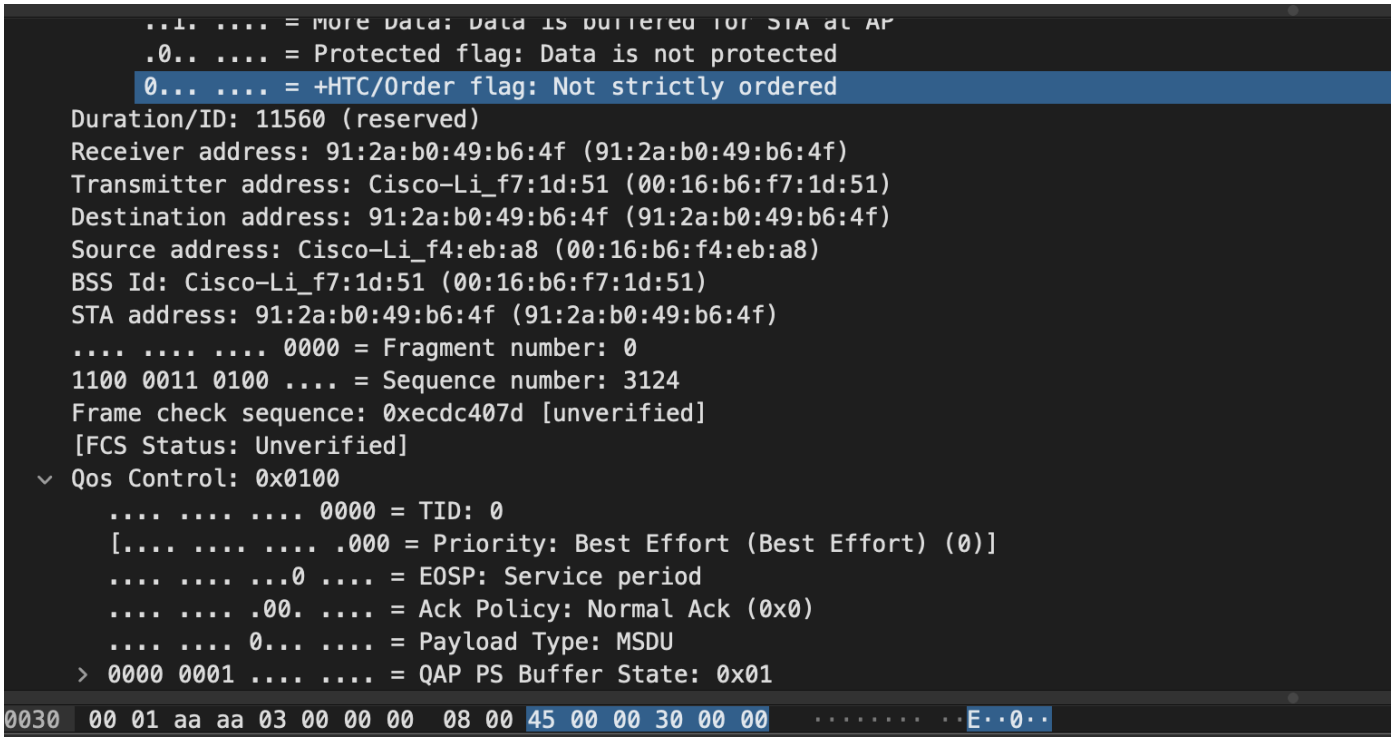
access point是：Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)。

first-hop router是：Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。

wireless host的IP address是：192.168.1.109 (没有在这个帧的信息中找到)。

destination IP address是： 128.119.245.12。这个IP address与服务器gaia.cs.umass.edu关联。

1.2.2 Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? 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? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).



三个Mac address：

Receiver address和Destination address：91:2a:b0:49:b6:4f,

Transmitter address：Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51),

Source address：Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。

wireless host是：91:2a:b0:49:b6:4f。**(和SYN TCP中host的address不一样？)**

access point是：Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)。

first-hop router是：Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。

wireless host的IP address是：192.168.1.109 (没有在这个帧的信息中找到)。

destination IP address是： 128.119.245.12。这个IP address与服务器gaia.cs.umass.edu关联。

sender MAC address与IP 地址不同，sender MAC address对应第一跳的路由器，IP 地址对应gaia.cs.umass.edu。

1.3 关联与去关联Association/Disassociation

1.3.1 What two actions are taken (i.e., 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 trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

是t = 49.583615的时候，一个DHCP release被host发送到DHCP server，告知它host要解除关联。

另一个是t = 49.609617的时候，host发送了一个deauthentication帧。

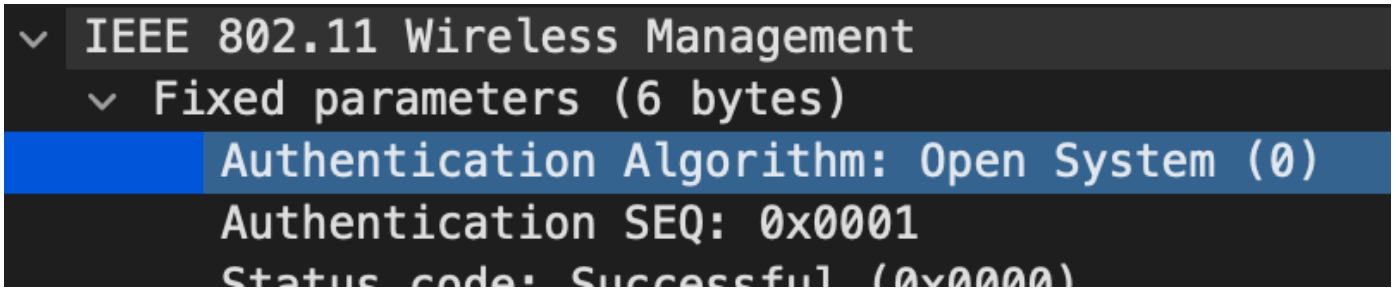
我期望看到一个disassociation的帧被发送，但没有。

1.3.2 Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are 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?* .

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C

从t = 49.638857开始，一共15条。

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

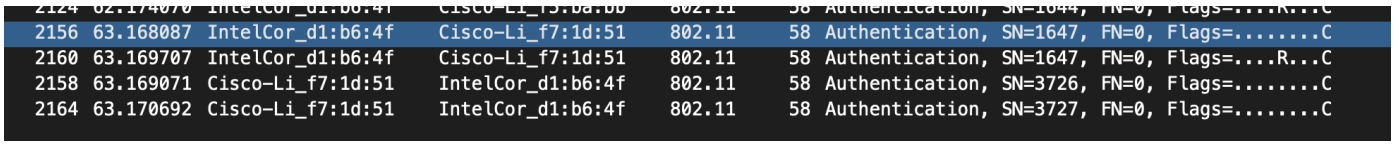


be open.

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

没有。

1.3.5 Now let's consider what happens as the host gives up trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENICATION frames sent from the host to and AP and 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 == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)



如图，t = 63.168087是第一条authentication发送从host到AP。

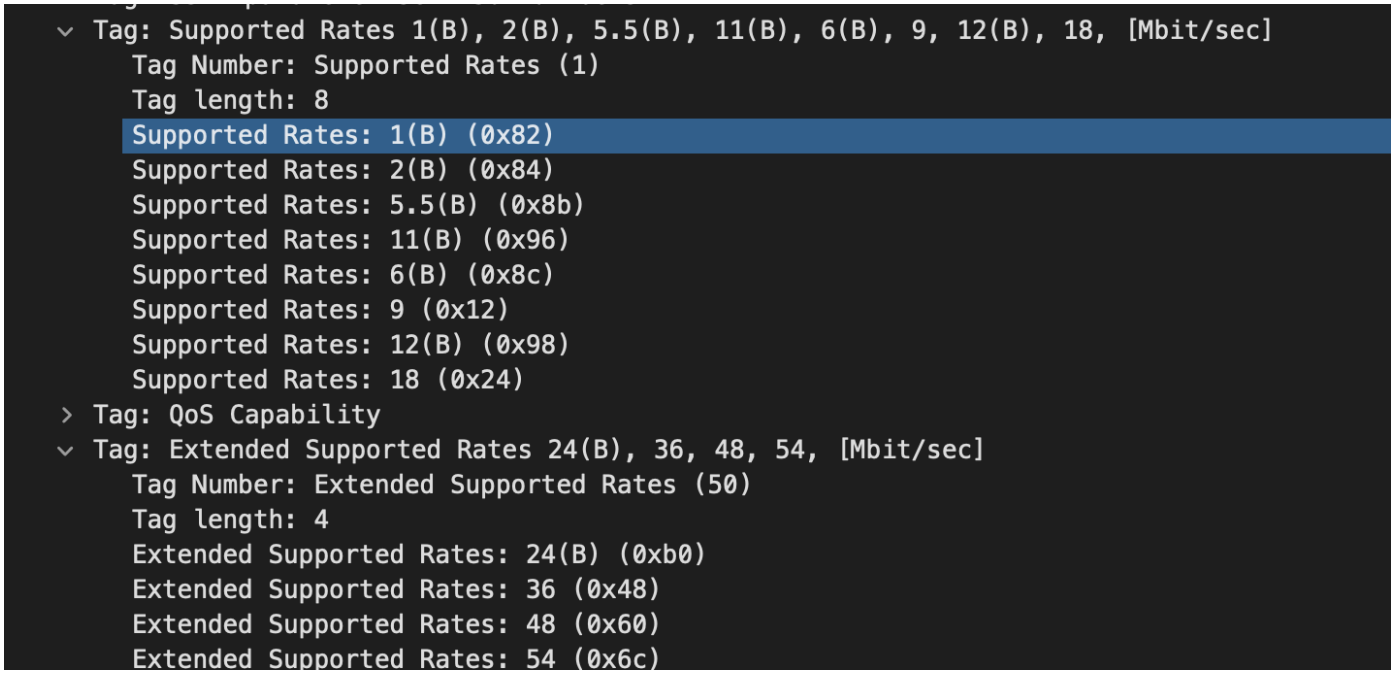
t = 63.169071是authentication发送从AP到host。

1.3.6 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.)

t = 63.196610是一个associate request帧，从host发送到AP。

t = 63.192101是一个associate response帧，从AP发送到host。

1.3.7 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.



这是associate request帧，标明支持的数据率为1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54。

associate response帧中也有相同的数据。

这表明了host和AP的传输速率。

1.4 其他帧类型Other Frame types

1.4.1 What are the sender, receiver and BSS ID MAC addresses in 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).

t = 2.297613的时候，有一个PROBE REQUEST帧，source的MAC address是00:12:f0:1f:57:13。receiver的MAC address是ff:ff:ff:ff:ff:ff，BSS ID是ff:ff:ff:ff:ff:ff。

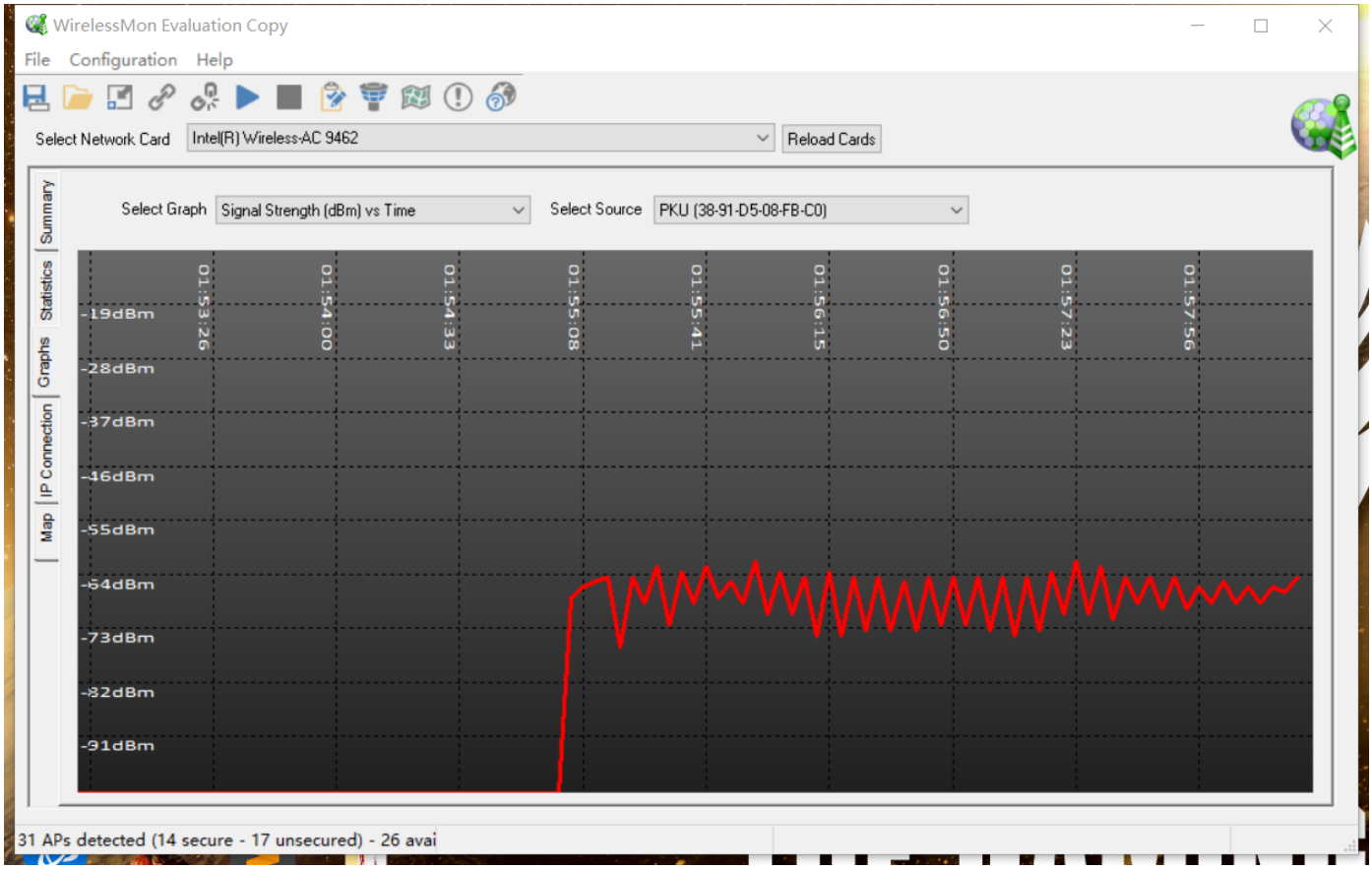
t = 2.300697的时候，有一个PROBE RESPONSE帧，source的MAC address是00:16:b6:f7:1d:51，receiver的MAC address是00:16:b6:f7:1d:51，BBS ID也是00:16:b6:f7:1d:51。

PROBE REQUEST帧是host用来主动扫描，寻找access point。

PROBE RESPONSE帧是access point发送给发送request的host作为回应。

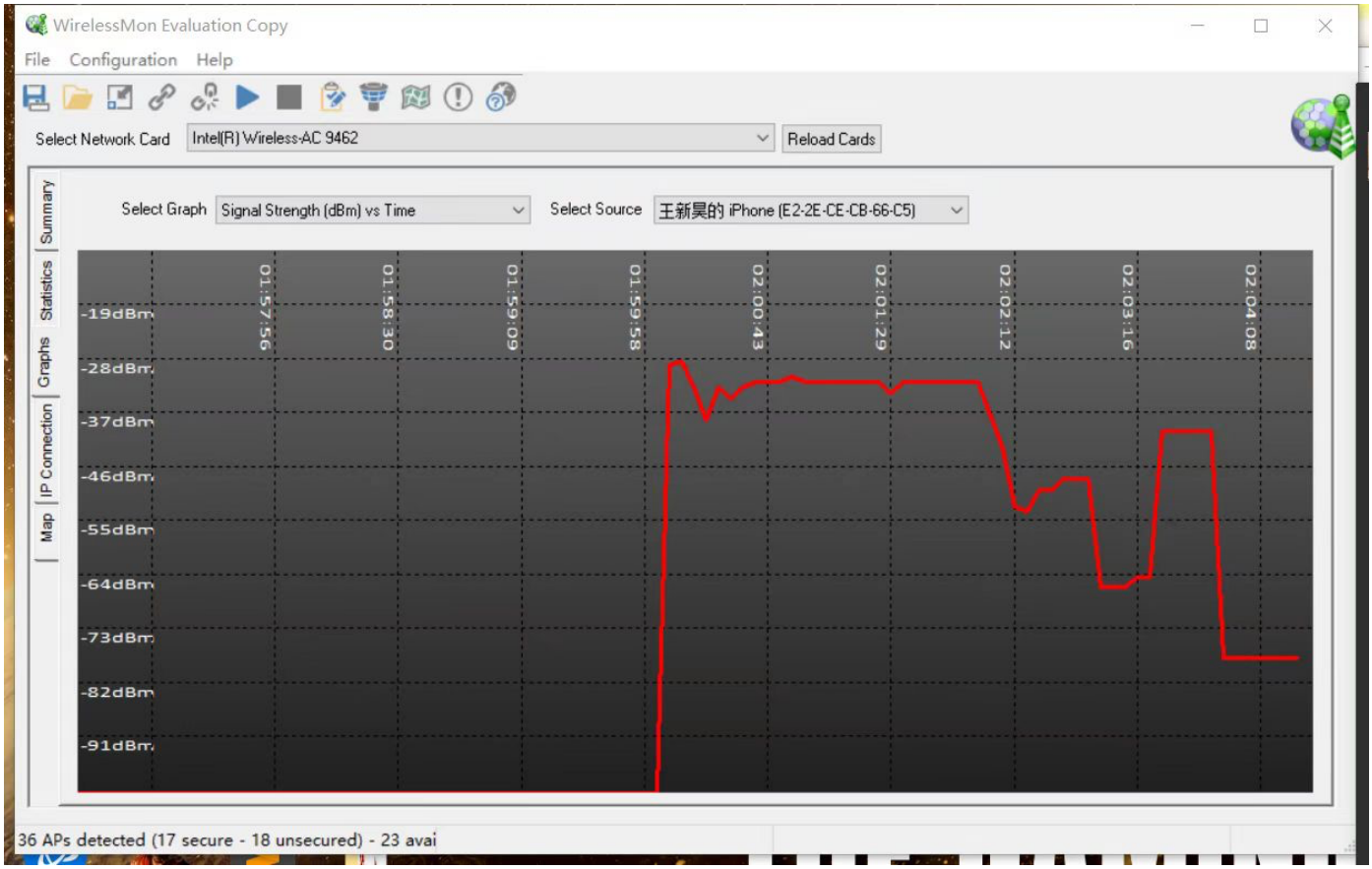
2 实验分析WIFI信号强度与数据率的关系

宏观感知



这是我测量1:55到1:58之间PKU wifi的信号强度。

wifi信号强度与距离



这是我测量我的手机热点随距离增加的信号强度变化。

其中1:58:58 - 2:02:12我是在电脑面前，2:02:12 - 2:03:16我是在寝室门口，2:03:16-2:04:08我是在门口之外，2:04:08之后我是在更远的地方。

可以很明显地看到，随着距离的增加，信号强度变弱。

wifi信号强度与障碍物

这是我测量我的手机热点信号强度与障碍物的关系。

2:13:12-2:15:59我在门外，但宿舍门开着；2:15:59-2:18:36我在门外，但宿舍门关着。

可以看到，信号强度几乎没有什么变化，wifi信号强度与障碍物的关系不大。

信号强度和网速

wirelessmon 软件之中，除了信号强度，还有一个叫做信号质量的参数。信号质量和信号强度都可以影响网速，所以并不是信号强度越强网速就一定越快。

总结

信号强度会随着距离的增加而衰减，衰减很快（至少不是线性衰减）。信号强度会因为障碍物的存在而减弱，但是 wifi 信号可以穿过一般障碍物。Wifi 信号是影响速度的一个因素，但是其他因素也还有很多。