

计算机网络 课程实验报告

学号：202000130143	姓名： 郑凯饶	班级： 2020 级 1 班
实验题目：802.11 WiFi		
实验学时：2	实验日期： 2022-5-31	
实验目的： 研究 802.11 WiFi 协议		
硬件环境： Dell Latitude 5411 Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz (8GPUs), ~2.6GHz		
软件环境： Windows 10 家庭中文版 64 位 (10.0, 版本 18363) Wireshark-win64-3.6.2		
实验步骤与内容： 1. 问题： (1) 发送最多信标帧的两个接入点的 SSID？ (2) 24086 和 30 Munroe St. 接入点的信标帧传输间隔是多少？ (3) 30 Munroe St. 接入点的 MAC 地址。说明源地址、目的地址、BSS 的地址是什么？ (4) 30 Munroe St. 接入点的信标帧目的地址的 16 进制表示？ (5) 30 Munroe St. 接入点的 BSS ID 地址？ (6) 30 Munroe St. 接入点的信标帧宣告接入点可以支持 4 种数据速率和 8 种额外的“扩展支持速率”，这些速率是多少？ (7) 找到包含第 1 个 TCP SYN TCP 报文（下载 alice.txt）的 802.11 帧。帧中 3 个 MAC 地址是什么？说明和无线主机、接入点、第 1 跳路由的对应关系？发送此 TCP 报文的无线主机 IP 是什么？目的 IP 是什么？解释他们之间的对应关系？ (8) 找到包含此 TCP 会话 SYN ACK 报文的 802.11 帧。回答问题类同（7）。 (9) 49 时刻在跟踪中使用哪 2 个方法解除在跟踪之前与 30 Munroe St. 建立的关联？ (10) 找到主机发送给 AP 的 AUTHENTICATION 帧，同时找到无线 AP 的回复响应帧。49 时刻之后无线主机向 24086 发送了多少 AUTHENTICATION 消息？ (11) 主机认证是希望通过 key 还是 be open？ (12) 是否在跟踪中看到来自 24086 AP 回复 AUTHENTICATION？ (13) 分析主机放弃与 24086 AP 的关联并且尝试与 30 Munroe St. AP 关联的过程。查找从诸暨发送到 AP 的 AUTHENTICATION 帧以及无线 AP 的回复响应帧。 (14) 主机到 AP 的关联请求以及 AP 到主机的请求响应被用于主机和 AP 之间的关联。查找关联的请求以及响应。 (15) 主机愿意使用什么传输速率？ (16) 回答 PROBE REQUEST 帧和 PROBE RESPONSE 帧的 3 个 MAC 地址，并解释这些帧的作用是什么？ 2. 阐述基本方法		

Version: 版本号

目前802.11只有一个版本，故为0

Type: 帧类型

00 - 管理帧、01 - 控制帧、10 - 数据帧、11 - 保留

Subtype: 帧子类型

要根据**Type**来判断子类型代表什么，例如**Type = 00**为管理帧，**Subtype = 1000**对应为Beacon帧

Frame Control Flags: 帧控制字段

bit_7: 按序传输位，**bit = 1** 为帧和帧片段必须严格按序传输

bit_6: 保护位，**bit = 1** 为帧主体部分被加密

bit_5: 更多数据位，与省电相关，**bit = 1**为至少有一帧待发送给休眠中的STA

bit_4: 电源管理位，**bit = 1**为完成当前基本帧交换之后进入省电模式，对于AP来说，因为要进行一些重要的管理功能，所以该bit一定为0，但对于STA来说，该bit可以为1

bit_3: 重传位，**bit = 1**为该帧是重传帧

bit_2: 更多碎片位，**bit = 1**为上层封包经过mac层需要分片，只有分片的最后一个片段该bit为0，其余片段均为1

bit_1 & bit_0: From DS位 & To DS位，00 - 所有管理帧和控制帧、01 - STA发出的数据帧、10 - STA收到的数据帧、11 - 无线桥接器上的数据帧

Duration: 持续时间

该字段有多种功能，在这的功能是用来设置NAV（网络分配矢量），通俗的来讲就是占用信道多长时间（单位 us），STA要根据收到的所有帧的MAC头，实时更新NAV，同时会阻止其它STA使用信道

Destination: 目的MAC地址

因为Beacon帧为广播，所以目的地址全部为FF

Source: 源MAC地址

因为Beacon是从AP发出的，所以源MAC地址为AP的MAC地址

BSSID: 基本服务集标识

一般为AP的MAC地址，用来判断收到的帧是否属于该网络

Seq Number: 顺序编号

当上层帧交付 MAC 传送时，会被赋予一个 sequence number，相当于已传帧的计数器取 4096 的模（modulo）；此计数器由 0 起算，MAC 每处理一个上层封包就会累加 1；如果上层封包被分片处理，所有帧片段都会具有相同的顺序编号；如果是重传帧，则顺序编号不会累加。

Frag Number: 片段编号

帧片段之间的差异在于fragment number，第一个片段的编号为0，其后每个片段依序累加1；重传的片段会保有原来的 sequence number 协助重组。

Beacon Timestamp: Beacon时间戳

用来同步 AP 和 STA 的 TBTT (信标预定传送时间) 窗口, AP 的主计时器会定期发送目前已经工作的微秒数。当计数器到达最大值 (64bit) 时, 便会从头开始计数。

Beacon Interval: Beacon间隔

周期性按照Beacon时间间隔发送, 时间单位通常缩写为TU, 代表1024微秒(microsecond), 相当于1毫秒(millisecond), 这里是100ms。

Capability Info: 性能信息

```
Capability Info: %0000010000110001 [34-35]
0..... Immediate Block Ack Not Allowed
.0..... Delayed Block Ack Not Allowed
..0..... DSSS-OFDM is Not Allowed
...0..... No Radio Measurement
....0.... APSD is not supported
.....1.. G Mode Short Slot Time [9 microseconds]
.....0.. QoS is Not supported
.....0... Spectrum Mgmt Disabled
.....0... Channel Agility Not Used
.....0... PBCC Not Allowed
.....1... Short Preamble
.....1... Privacy Enabled
.....0... CF Poll Not Requested
.....0... CF Not Pollable
.....0... Not an IBSS Type Network
.....1... ESS Type Network
```

发送 Beacon 信号的时候, 它被用来通知各方, 该网络具备哪种性能。

发送 Beacon 信号的时候, 它被用来通知各方, 该网络具备哪种性能。

bit_15 & bit_14: 10 -立即应答block ack、01 - 延迟应答block ack

bit_13: **bit = 1**代表使用 802.11g 的 DSSS-OFDM 帧构建 (frame construction) 选项。

bit_12: **bit = 1**为支持无线电测量

bit_11: **bit = 1**为支持自动省电

bit_10: **bit = 1**为 802.11g 支持的较短的时槽

bit_9: **bit = 1**为支持Qos (服务质量保证), 目前好像都是以WMM字段来判断支不支持Qos的, 可能是为了兼容不支持Qos的设备吧

bit_8: **bit = 1**为支持频谱管理

bit_7: 802.11b 独有, 是为了支持高速直接序列扩频物理层(high-rate DSSS PHY), **bit = 1**为此网络使用机动信道转换 (Channel Agility) 选项; 2016-802.11协议已经将此bit更新为保留

bit_6: 802.11b 独有, 是为了支持高速直接序列扩频物理层(high-rate DSSS PHY), **bit = 1**为此网络目前使用分组二进制卷积编码 (packet binary convolution coding)调变机制, 或是 802.11g PBCC 调变机制; 2016-802.11协议已经将此bit更新为保留

bit_5: 802.11b 独有, 是为了支持高速直接序列扩频物理层(high-rate DSSS PHY), **bit = 1**为此网络目前使用短同步信号 (short preamble)

bit_4: **bit = 1**为需要使用 WEP 以维持机密性

bit_3 & bit_2:

STA: 00 - sta不支持轮询、01 - sta支持轮询, 且要求将之置于轮询表、10 - sta支持轮询, 但并没有要求置于轮询表 (polling list)、11 - 工作站虽然支持轮询, 但要求不要对其轮询 (结果是该工作站会被视为不支持免竞争工作)

AP: 00 - ap不支持中枢协调功能 (point coordination function)、01 - ap使用 PCF 来传递与轮询、10 - ap使用 PCF 来传递, 但并不支持轮询、11 - 保留

bit_1 & bit_0: 10 - IBSS、01 - ESS (AP一般都是ESS)

SSID: 服务集标识

```
SSID
  Element ID: 0 SSID [36]
  Length: 14 [37]
  SSID: .....lu... [38-51]
```

通俗来讲，就是我们平时所说的无线网络名称

Element ID: 元素识别码

每个元素识别码对应信息元素，0就代表SSID

Length: SSID长度

因为我的AP包含4个汉字，一个汉字是3个byte，再加2个字符，一共14个byte。

SSID: SSID名称

汉字没有解析出来，Wi-Fi名称是“你是小lu吗”，一个汉字正好对应一组“...”。

Rates: 支持速率

```
Supported Rates
  Element ID: 1 Supported Rates [52]
  Length: 8 [53]
  Supported Rate: 1.0 Mbps (BSS Basic Rate) [54]
  Supported Rate: 2.0 Mbps (BSS Basic Rate) [55]
  Supported Rate: 5.5 Mbps (BSS Basic Rate) [56]
  Supported Rate: 11.0 Mbps (BSS Basic Rate) [57]
  Supported Rate: 9.0 Mbps (Not BSS Basic Rate) [58]
  Supported Rate: 18.0 Mbps (Not BSS Basic Rate) [59]
  Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [60]
  Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [61]
```

AP所支持的速率，每个速率占一个byte，最高位为1代表必须支持该速率，比如上图的1.0Mbps、2.0Mbps、5.5Mbps、11.0Mbps；要接入该网络的STA必须要支持的速率，而最高位为0代表AP支持该速率，但STA可以不支持。

3. 实验结果展示与分析

(1) 30 Munroe St 和 linksys12

33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame
----	----------	-------------------	-----------	--------	------------------

- > Fixed parameters (12 bytes)
- ▼ Tagged parameters (119 bytes)
 - > Tag: SSID parameter set: 30 Munroe St
 - > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - > Tag: DS Parameter set: Current Channel: 6
 - > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
 - > Tag: Country Information: Country Code US, Environment Indoor
 - > Tag: EDCA Parameter Set
 - > Tag: ERP Information
 - > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - > Tag: Vendor Specific: Airgo Networks, Inc.
 - > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

(2) 均为 Beacon Interval: 0.102400 [Seconds]

(3) Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

源地址是发送无线信号站点本身的地址，目的地址是接收无线信号站点的地址，基本服务集地址是指基本服务集基础设施的地址（AP的地址）。

▼ IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x0008)

► Frame Control Field: 0x8000

.000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

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

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

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

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

.... 0000 = Fragment number: 0

1011 0010 1010 = Sequence number: 2858

Frame check sequence: 0x13d68f47 [unverified]

[FCS Status: Unverified]

(4) Destination address: Broadcast (ff:ff:ff:ff:ff:ff) 表示广播地址

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

(6) 如下图

▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]

Tag Number: Supported Rates (1)

Tag length: 4

Supported Rates: 1(B) (0x82)

Supported Rates: 2(B) (0x84)

Supported Rates: 5.5(B) (0x8b)

Supported Rates: 11(B) (0x96)

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

Tag Number: Extended Supported Rates (50)

Tag length: 8

Extended Supported Rates: 6(B) (0x8c)

Extended Supported Rates: 9 (0x12)

Extended Supported Rates: 12(B) (0x98)

Extended Supported Rates: 18 (0x24)

Extended Supported Rates: 24(B) (0xb0)

Extended Supported Rates: 36 (0x48)

Extended Supported Rates: 48 (0x60)

Extended Supported Rates: 54 (0x6c)

(7) 接收、发送、目的 MAC 地址如下图所示。

无线主机 MAC 地址: Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

接入点 MAC 地址: BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

第 1 跳路由的 MAC 地址: Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

无线主机 IP 地址: Source Address: 192.168.1.109

目的 IP 地址: Destination Address: 128.119.245.12

不与任何当前 MAC 地址对应, 因为不在同一“子网”中。

468	24.795431	Cisco-Li_f7:1d:51	Cisco-Li_f4:eb:...	802.11	90	Fragmented IEEE 802.11 frame
469	24.795573		Cisco-Li_f7:1d:...	802.11	38	Acknowledgement, Flags=.....
470	24.795673	192.168.1.109	68.87.71.226	DNS	125	Standard query 0x7892 A gaia.c
471	24.795769		IntelCor_d1:b6:...	802.11	38	Acknowledgement, Flags=.....
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892
473	24.809513		Cisco-Li_f7:1d:...	802.11	38	Acknowledgement, Flags=.....
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	2538 → 80 [SYN] Seq=0 Win=1638
475	24.811231		IntelCor_d1:b6:...	802.11	38	Acknowledgement, Flags=.....
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack
477	24.827922		Cisco-Li_f7:1d:...	802.11	38	Acknowledgement, Flags=.....
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Wi

Type/Subtype: QoS Data (0x0028)

› Frame Control Field: 0x8801

.000 0000 0010 1100 = Duration: 44 microseconds

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

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

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

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

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

STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

.... 0000 = Fragment number: 0

(8)

无线主机 MAC 地址: Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

接入点 MAC 地址: BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

第 1 跳路由的 MAC 地址: Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

不对应, 不在同一子网中。

▼ IEEE 802.11 QoS Data, Flags: ..mP..F.C

Type/Subtype: QoS Data (0x0028)

› Frame Control Field: 0x8832

Duration/ID: 11560 (reserved)

Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

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

Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

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

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

STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

.... 0000 = Fragment number: 0

1100 0011 0100 = Sequence number: 3124

(9) 发送 DHCP Release 报文以及 802.11 Deauthentication 类型报文。

49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=
49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:...	802.11	54	QoS Null function (No data), SN=166
49.440243		IntelCor_d1:b6:...	802.11	38	Acknowledgement, Flags=.....C
49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=
49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea
49.583771		IntelCor_d1:b6:...	802.11	38	Acknowledgement, Flags=.....C
49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:...	802.11	54	Deauthentication, SN=1605, FN=0, F1
49.609770		IntelCor_d1:b6:...	802.11	38	Acknowledgement, Flags=.....C
49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags

(10) 通过过滤器我们发现主机只接受到一次 linksys AP 的 Beacon 帧, 其余报文均是同 30 Munroe St. AP 来往, 可能是由于实验材料的版本问题, 这些问题不能得到很好的细究。

wlan.addr == 50:2b:25:67:22:94						
No.	Time	Source	Destination	Protocol	Length	Info
	14 0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, F

(11) 观察字段 Authentication Algorithm: Open System (0) 表示主机希望开放系统的认证算法。

▼ IEEE 802.11 Wireless Management

▼ Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0001

Status code: Successful (0x0000)

(12) 无

(13) 由下图可见，于 63.168087 时刻及之前主机不断发送请求帧，于 63.169071 时刻 AP 回复。

wlan.fc.subtype == 11 and wlan.fc.type == 0						
Time	Source	Destination	Protocol	Length	Info	
1744 49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1606, FN	
1746 49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1606, FN	
1749 49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1606, FN	
1821 53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1612, FN	
1822 53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1612, FN	
1921 57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1619, FN	
1922 57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1619, FN	
1923 57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1619, FN	
1924 57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1619, FN	
2122 62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1644, FN	
2123 62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1644, FN	
2124 62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	58	Authentication, SN=1644, FN	
2156 63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:...	802.11	58	Authentication, SN=1647, FN	
2158 63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:...	802.11	58	Authentication, SN=3726, FN	
2160 63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:...	802.11	58	Authentication, SN=1647, FN	
2164 63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:...	802.11	58	Authentication, SN=3727, FN	

(14) 使用过滤器 wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == 00:13:02:d1:b6:4f (要使用 MAC 地址而不是别名) 筛选得

wlan.fc.subtype < 2 and wlan.fc.type == 0						
Time	Source	Destination	Protocol	Length	Info	
53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1613, FN=0,	
53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1613, FN=0,	
57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1620, FN=0,	
52.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1645, FN=0,	
52.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:...	802.11	107	Association Request, SN=1645, FN=0,	
53.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:...	802.11	89	Association Request, SN=1648, FN=0,	
53.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:...	802.11	94	Association Response, SN=3728, FN=0	
70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:...	802.11	132	Fragmented IEEE 802.11 frame	

(15)

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

(16) Request 帧中:

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
Type/Subtype: Probe Request (0x0004)
‣ Frame Control Field: 0x4000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

Response 帧中:

Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Type/Subtype: Probe Response (0x0005)
‣ Frame Control Field: 0x5000
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... 0000 = Fragment number: 0
1011 1100 0110 = Sequence number: 3014
Frame check sequence: 0x555cc5c6 [unverified]
[FCS Status: Unverified]

用于主机主动扫描周围的 AP 信号。

结论分析与体会:

这次实验学习了 802.11 协议, 与之前的协议不同, 这个协议是无线的, 因而 Wireshark 也收集了许多通信时物理数据如信号强度、噪声强度等等。之前做过蓝牙相关的安卓开发, 在学习了 802.11 之后对无线通信的许多概念 (例如 Beacon 帧, 最初接触, 我以为这是一种虚拟路标呢, 不过确实也可以这么干哈哈, 可以展示一些信息比如图片, 现在才知道它本质是 AP 的广播帧) 有了深入的体会。