计网实验三

姓名：岳宇轩　　学号：19020011038

专业：19 计算机　　指导教师：洪峰

STEP1：fetch a trace

在这里我是用的是助教提供的 trace

STEP2：inspect the trace

一：

用 wireshark 打开 trace 文件

No.	Time	Source	Destination	Protocol	Length	Info
10	0.921782	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2391, FN=0, Flags=........C, BI=100, SSID=djw
11	1.024028	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2392, FN=0, Flags=........C, BI=100, SSID=djw
12	1.126561	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2393, FN=0, Flags=........C, BI=100, SSID=djw
13	1.228923	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2394, FN=0, Flags=........C, BI=100, SSID=djw
14	1.331358	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2395, FN=0, Flags=........C, BI=100, SSID=djw
15	1.433666	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2396, FN=0, Flags=........C, BI=100, SSID=djw
16	1.510195	Apple_98:f0:6f	Cisco-Li_e3:e9:8d	802.11	1539	Data, SN=3126, FN=0, Flags=.p.....TC
17	1.510308		Apple_98:f0:6f (00:…	802.11	39	Acknowledgement, Flags=........C
18	1.536030	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2397, FN=0, Flags=........C, BI=100, SSID=djw
19	1.566039	Cisco-Li_e3:e9:8d	Apple_98:f0:6f	802.11	121	Data, SN=2398, FN=0, Flags=.p....F.C
20	1.566056		Cisco-Li_e3:e9:8f (…	802.11	39	Acknowledgement, Flags=........C

根据 info 字段选择一个 Data 类型的帧，在下方可以看到这个帧的信息：

```
> Frame 16: 1539 bytes on wire (12312 bits), 1539 bytes captured (12312 bits) on interface unknown, id 0
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Data, Flags: .p.....TC
> Data (1478 bytes)
```

- Frame 是 wireshark 添加时间、长度等信息后的记录。

• Ratdiotap 是 wireshark 用来捕获物理层参数的记录。

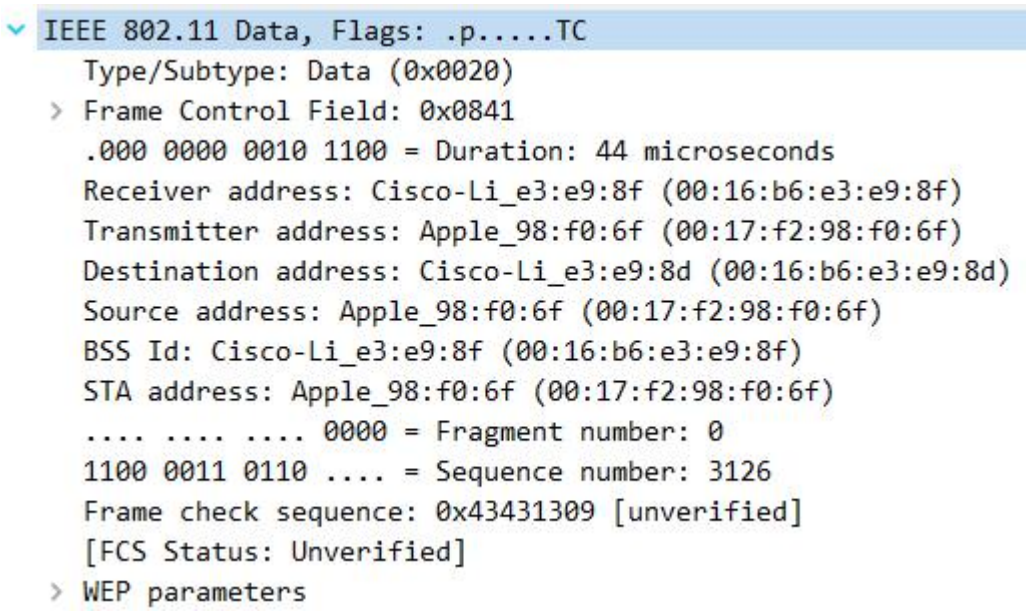
• IEEE 802.11 是 802.11 数据帧的位。

• Data 是一条含有有效荷载数据的记录，有像 LLP,IP 包这样的高层协议。

在很多无线网的设置中，有效荷载数据只对外表现为一条记录，被视作 802.11 协议。

二：

点开 IEEE 802.11 记录可以看到以下信息



• Frame control：编码了帧的类型和子类型，例如数据和各种标志位.

• Duration：这个字段告诉计算机在无限媒体上在此次交换之外额外的分组需要花费多少时间.

• BSS identifier：源地址和目的地址，视帧具体情况决定排列顺序，表示帧的发出者和接受者。它表示接入点的地址。

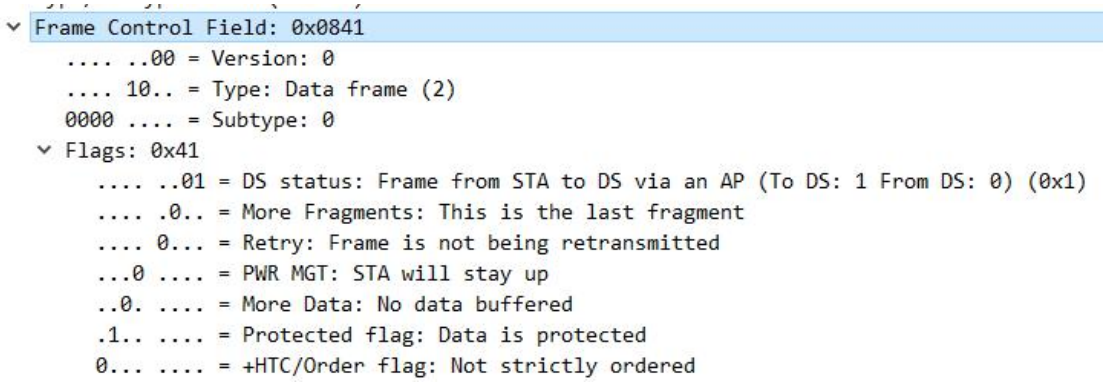
• Frame and sequence number：如果需要的话，这个字段用来表示这个帧的重组次数和重传次数，数字随着每次重传而增大。

• Frame check sequence：CRC 校验码。

• WEP：该字段携带安全参数。

三.

点开 Frame Control Field 字段，看到如下信息：



• Version：0，表示当前版本

• Type 和 Subtype：标明这个帧的类型，比如说明它是 Data 还是 Ack

• To DS：当这个帧是从一个主机通过接入点 AP 发向无线网时，置该标志位，可以看到这个帧就是从主机通过接入点 AP 发向无线网络的，因此它的 To DS 是 1.

• From DS：当这个帧是通过接入点 AP 从无线网发向主机时，置该标志位，可以看到这个帧不是从无线网络通过接入点 AP 发向主机的，因此它的 From DS 是 0.

• More Fragments：标志是否有后续帧，0 表示没有

• Retry：表示该帧是否是重传，0 表示这个帧不是重传的帧

• PWR MGT：表示发送者在发送该帧后为了省电要进入睡眠，这里这个帧的该字段值为 0，表示发送后不进入睡眠。

• Protected：表示是否有 WEP 或 WPA2 加密

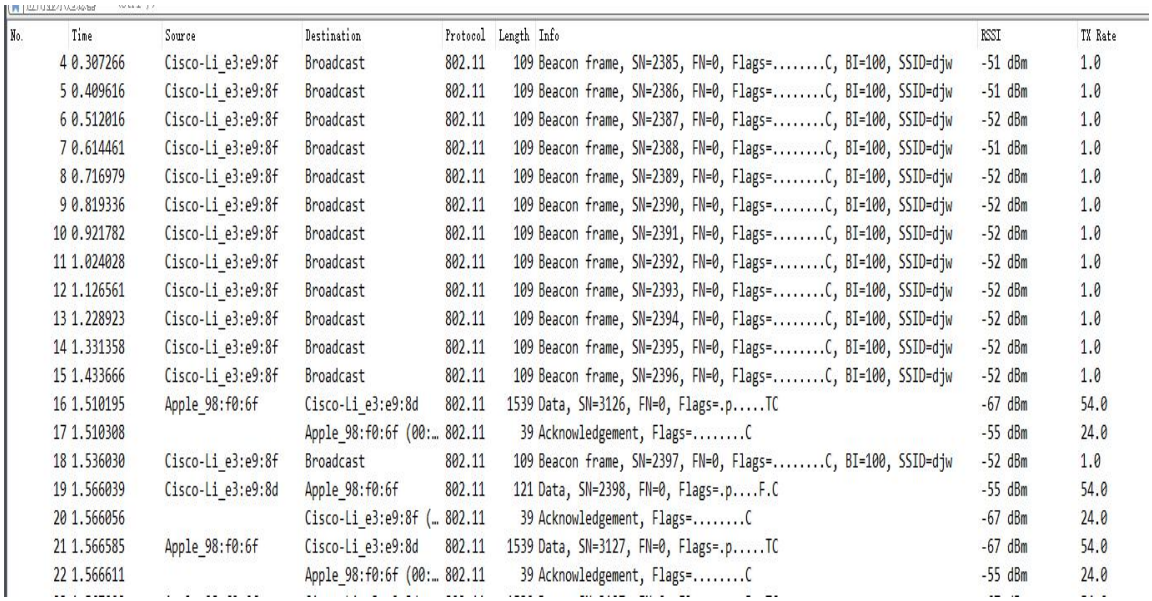
• Order：表示接收方是否必须按顺序接受一系列的帧

STEP3：802.11 物理层

1.1What is the channel frequency?

首先在展示界面添加新列 TX Rate 和 RSSI

结果如下：



No.	Time	Source	Destination	Protocol	Length	Info	RSSI	TX Rate
4	0.307266	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2385, FN=0, Flags=.....C, BI=100, SSID=djw	-51 dBm	1.0
5	0.409616	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2386, FN=0, Flags=.....C, BI=100, SSID=djw	-51 dBm	1.0
6	0.512016	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2387, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
7	0.614461	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2388, FN=0, Flags=.....C, BI=100, SSID=djw	-51 dBm	1.0
8	0.716979	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2389, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
9	0.819336	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2390, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
10	0.921782	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2391, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
11	1.024028	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2392, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
12	1.126561	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2393, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
13	1.228923	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2394, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
14	1.331358	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2395, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
15	1.433666	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2396, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
16	1.510195	Apple_98:f0:6f	Cisco-Li_e3:e9:8d	802.11	1539	Data, SN=3126, FN=0, Flags=.p.....TC	-67 dBm	54.0
17	1.510308		Apple_98:f0:6f (00:...	802.11	39	Acknowledgement, Flags=.....C	-55 dBm	24.0
18	1.536030	Cisco-Li_e3:e9:8f	Broadcast	802.11	109	Beacon frame, SN=2397, FN=0, Flags=.....C, BI=100, SSID=djw	-52 dBm	1.0
19	1.566039	Cisco-Li_e3:e9:8d	Apple_98:f0:6f	802.11	121	Data, SN=2398, FN=0, Flags=.p....F.C	-55 dBm	54.0
20	1.566056		Cisco-Li_e3:e9:8f (...	802.11	39	Acknowledgement, Flags=.....C	-67 dBm	24.0
21	1.566585	Apple_98:f0:6f	Cisco-Li_e3:e9:8d	802.11	1539	Data, SN=3127, FN=0, Flags=.p.....TC	-67 dBm	54.0
22	1.566611		Apple_98:f0:6f (00:...	802.11	39	Acknowledgement, Flags=.....C	-55 dBm	24.0

点开每一个帧查看，发现 channel frequency 都是

```
Channel frequency: 2462 [BG 11]
```

故：信道频率是 2462MHz

1.2 What rates are used? Give an ordered list of rates from lowest

to highest. Hint:you can click the Rate column to sort by that value.

点击 TX Rate 表头，可以排序，排序后结果为：

1,6,12,18,24,36,48,54

1.3 What is the range of RSSI and hence variation in SNRs in the trace? Give this as the strongest and weakest RSSI and the dB difference between them.

RSSI 范围：-44dBm(strongest) 到 -69dBm(weakest)

SNRs: 300

dB differences: 25dBm

STEP4 链路层

打开 Conversations 页面，显示如下

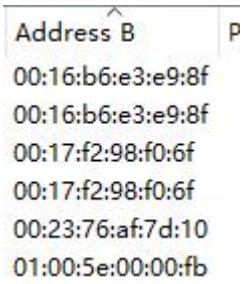
Wireshark · Conversations · trace-80211.pcap

Ethernet | IEEE 802.11 · 50 | IPv4 | IPv6 | TCP | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/
00:16:b6:e3:e9:8d	10:9a:dd:ac:6c:26	1,496	1029k	843	824k	653	204k	27.895957	18.7060	352k	
00:16:b6:e3:e9:8d	00:16:b6:e3:e9:8f	656	25k	656	25k	0	0	1.566056	45.0357	4544	
00:16:b6:e3:e9:8d	79:1e:09:32:6c:26	554	21k	0	0	554	21k	27.898198	18.7039	0	
00:16:b6:e3:e9:8f	ff:ff:ff:ff:ff:ff	458	49k	458	49k	0	0	0.000000	46.8995	8515	
10:9a:dd:ac:6c:26	ff:ff:ff:ff:ff:ff	156	23k	156	23k	0	0	27.143654	7.8788	23k	
00:16:b6:e3:e9:8f	10:9a:dd:ac:6c:26	50	3455	16	1592	34	1863	27.141963	19.6671	647	
00:16:b6:e3:e9:8d	00:17:f2:98:f0:6f	45	27k	22	3029	23	24k	1.510195	44.9334	539	
01:00:5e:00:00:fb	10:9a:dd:ac:6c:26	45	12k	0	0	45	12k	28.023795	18.3660	0	
00:16:b6:e3:e9:8d	70:56:81:a2:05:1d	34	3766	34	3766	0	0	11.776730	34.9670	861	
79:1e:09:32:6c:26	ff:ff:ff:ff:ff:ff	28	1092	28	1092	0	0	27.907063	7.0369	1241	
10:9a:dd:ac:6c:26	33:33:00:00:00:fb	27	8808	27	8808	0	0	33.333958	13.0583	5396	
00:16:b6:e3:e9:8f	79:1e:09:32:6c:26	26	1014	0	0	26	1014	27.901954	18.9071	0	
00:16:b6:e3:e9:8d	c7:a6:6e:71:f0:6f	23	897	0	0	23	897	1.510308	44.9333	0	
01:00:5e:00:00:fb	79:1e:09:32:6c:26	21	819	0	0	21	819	28.023842	18.3400	0	
23:b0:69:98:e9:8f	70:56:81:a2:05:1d	16	624	16	624	0	0	11.776581	35.1729	141	

2.1 What is the BSS ID used by the most active wireless conversations?

点击 Address B 进行排序，得到以下结果



从排序结果图中可以看出，最活跃的无限会话使用的 BSS ID 是 00:16:b6:e3:e9:8f

2.2 How many Data frames are in the trace, and what is the most common subtype ofData frame?

有 1783 个 Data Frame，最常见的 Subtype 是 Data，标号为 0

2.3 How many Control frames are in the trace, and what is the most common subtype?

有 1391 个 Control Frame，最常见的 Subtype 是 Acknowledgement Frame，标号为 13

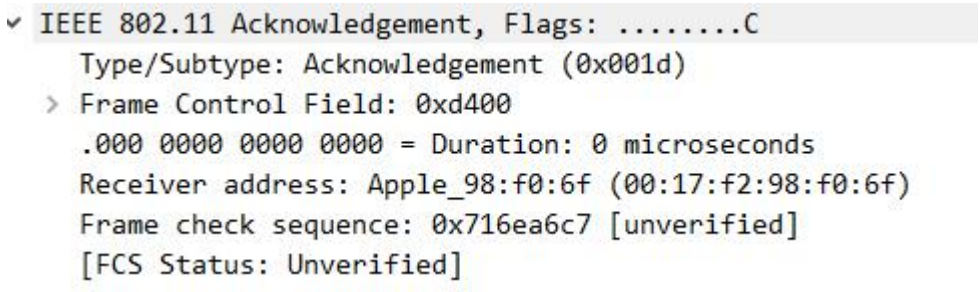
2.4 How many Management frames are in the trace, and what is the most common subtype?

有 557 个 Management Frame，最常见的 Subtype 是 Beacon Frame，标号为 8

2.5 List in the order they are sent the IEEE 802.11 fields in an

Acknowledgement frame and their lengths in bytes.

打开一个 Acknowledgement frame 的 IEEE802.11 域，显示结果如图



Type/Subtype 4bytes

Frame Control Field 2bytes

Duration 2bytes

Receiver address 6bytes

Frame check sequence 4bytes

2.6 Give an estimate of the retransmission rate as the number of retransmissions overthe number of original transmissions.

这个可以根据帧中的 Frame Control Field 中的 Retry 字段来确定，Retry 为 1 表示重传，Retry 为 0 表示非重传

original transmissions number = 1430

retransmissions number =353

retransmission rate

= 353 / 1430

= 24.69%

2.7 What fraction of the frames sent to the AP signal that the client is poweringdown?

这个可以根据帧中的 Frame Control Field 中的 PWR MGT 字段来确定，PWR MGT 为 1 表示断电，PWR MGT 为 0 表示没有断电

poweringdown number = 16

not poweringdown number = 822

rate = 16 / 822 = 1.95%

STEP5: 802.11 Management

3.1 What is the SSID of the main AP?

打开一个 Beacon Frame 后如图

```
    BSS Id: Cisco-Li_e3:e9:8f (00:16:b6:e3:e9:8f)
    .... .... .... 0000 = Fragment number: 0
    1001 1101 0001 .... = Sequence number: 2513
    Frame check sequence: 0x7d869666 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (44 bytes)
    v Tag: SSID parameter set: djw
        Tag Number: SSID parameter set (0)
        Tag length: 3
        SSID: djw
```

可以看到 SSID 是 djw

3.2 How often are Beacon frames sent for the main AP?

在 wireshark 里选择视图->时间显示格式->自上一个捕获分组经过的秒数

```
160 0.101767
161 0.102555
162 0.102345
163 0.102463
164 0.102324
165 0.102343
166 0.102528
167 0.102406
```

从图中可以看出 Beacon Frame 的发送频率大概在 0.1023s 发送一帧

3.3 What data rates does the main AP support?

从 Beacon Frame 的参数中可以直接读到如下结果：

```
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
Supported Rates: 18 (0x24)
Supported Rates: 24 (0x30)
Supported Rates: 36 (0x48)
Supported Rates: 54 (0x6c)
```

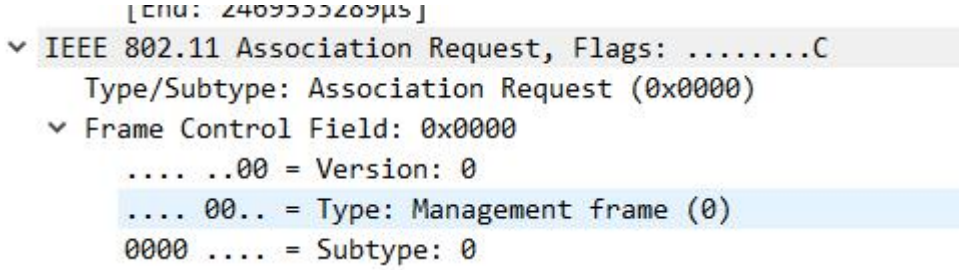
3.4 What rate is the Beacon frame transmission?

```
Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  Present flags
    Present flags word: 0x0000086f
    MAC timestamp: 2454037403
  Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2462 [BG 11]
  Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
```

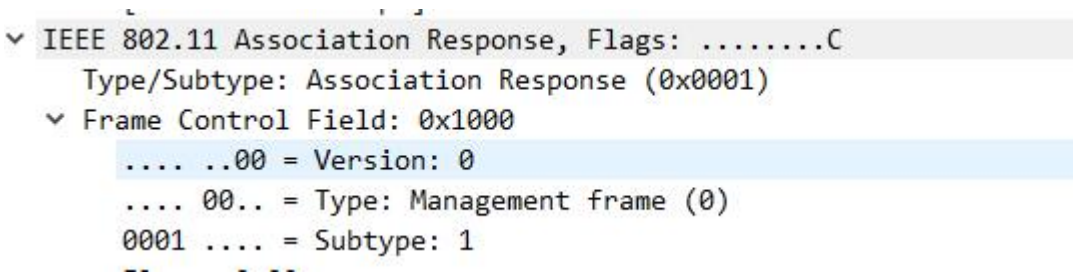
在 Radiotap Header 中可以看到 Data Rate 是 1.0Mb/s

3.5 What are the Type and Subtype values of Association Request / Association Response frames?

Association Request:



Association Response:



根据图可知，Association Request:的 Type 是 0(Management frame)，Subtype 是 0; Association Response 的 Type 是 0(Management frame)，Subtype 是 1

3.6 What are the Type and Subtype values for the Probe Request / Probe Responseframes?

Probe Request:

```
    [End: 2468912247µs]
▾ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▾ Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    ▾ Flags: 0x00
```

Probe Response:

```
      [End: 24688/5025µs]
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▾ Frame Control Field: 0x5000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
    ▾ Flags: 0x00
```

由上图可知， Probe Request 的 Type 是 0(Management frame), Subtype 是 4; Probe Response 的 Type 是 0(Management frame)，Subtype 是 5.