Doctors of Intelligence &Technology(DOIT)

Doit 探宝

(V1.0)

2016-06-30

Catalogue

This document demonstrates the principles of the wifi Sniffer.

1, IEEE802.11 介绍

IEEE 802.11 是现今无线局域网通用的标准，它是由国际电机电子工程学会(IEEE)所定义的无线网络通信的标准。其中定义了媒体访问控制层(MAC 层)和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种扩频作调制方式和一种红外传输的方式，总数据传输速率设计为 2Mbit/s。两个设备可以自行构建临时网络，也可以在基站(Base Station, BS)或者接入点(Access Point，AP)的协调下通信。为了在不同的通讯环境下取得良好的通讯质量，采用 CSMA/CA(Carrier Sense Multiple Access／Collision Avoidance)硬件沟通方式。在 802.11 协议的发展过程中，衍生出了一系列的和安全、加密相关的技术。

1. WEP，Wired Equivalent Privacy: 802.11 中最早期的加密标准
2. CCMP(CTR with CBC-MAC Protocol): 基于 AES 的全新加密协议，在 IEEE 802.11i 中提出
3. WPA(Wi-Fi Protected Access)
4. TKIP(Temporal Key Integrity Protocol)
5. WPA2(Wi-Fi Protected Access 2)

802.11 标准将所有的数据包分为 3 种:

1. 数据: 数据数据包的作用是用来携带更高层次的数据(如 IP 数据包，ISO7 层协议)。它负责在工作站之间传输数据
2. 管理: 管理数据包控制网络的管理功能
    1) 信标帧(Beacons): 在无线设备中，定时依次按指定间隔发送的有规律的无线信号(类似心跳包)，主要用于定位和同步使用
    2) 解除认证(Deauthentication)数据包
    3) Probe(request and response)
    4) Authenticate(request and response)
    5) Associate(request and response)
    6) Reassociate(request and response)

7) Dissassociate(notify)

管理帧负责监督，主要用来加入或退出无线网络，以及处理接入点之间连接的转移事宜

3. 控制：控制数据包得名于术语"媒体接入控制(Media Access Control, MAC)"，是用来控制对共享媒体(即物理媒介，如光缆)的访问

1) 请求发送(Request To Send，RTS)数据包

2) 清除发送(Clear To Send，CTS)数据包

3) ACK 确认(RTS/CTS)

4) PS-Poll：当一部移动工作站从省电模式中苏醒，便会发送一个 PS-Poll 帧给基站，以取得任何暂存帧

控制帧通常与数据帧搭配使用，负责区域的清空、信道的取得以及载波监听的维护，并于收到数据时予以正面的应答，借此促进工作站间数据传输的可靠性

2, IEEE Frame 格式

我们知道数据链路层是一个很靠近底层的通信协议，它使用 Bit 来表示信息(也使用 Bit 来标识数据包的开始和结束)，所以数据链路层的协议格式并没有强制 要求一个固定的长度，即 802.11 协议长度是可变的。不同功能的数据帧长度会不一样。这一特性说明 mac802.11 数据帧显得更加灵活，然而，也会更 加复杂。

下图展示示的是一一个完整的 IEEE802.11 数据包的格式

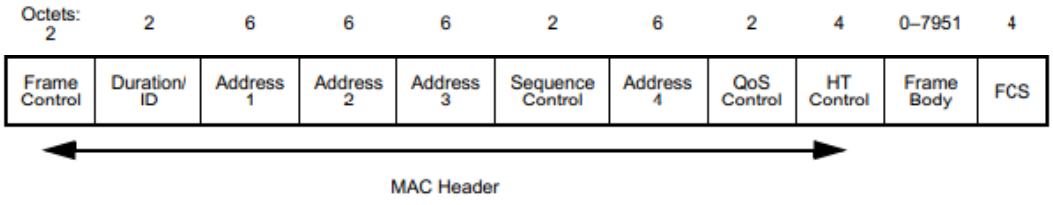


Figure 8-30—Data frame

控制帧 Frame Control 字段 2 个字节：

4bit(Subtype)+2bit(Type)+2bit(Protocol Version，默认为 00)，针对 Frame Control 的各 bit 位的说明如下：

控制帧Frame Control字段		
名称	功能描述	字段位数(位)
Protocol	该位设置为0.	2
Type	该位设置为01，表示控制帧	2
Subtype	设置此位，标志不同的子类型	4
To DS	该位设置为0	1
From DS	该位设置为0	1
More Fragments	该位设置为0	1
Retry	该位设置为0	1
Power Management	该位设置为0	1
More Data	该位设置为0	1
Protected Frame	该位设置为0	1

1） 管理帧：type 为 00 时，代表管理帧，

负责监督，用来加入或退出无线网络以及处理接入点之间关联的转移事宜。为了限制广播或组播管理帧所造成的副作用，收到管理帧后，必须加以查验。只有广播或者组播帧来自工作站当前所关联的 BSSID 时，它们才会被送至 MAC 管理层。唯一例外是 beacon 帧

此时各 Subtype 的值如下：

0000 Association request（连接要求）
0001 Association response（连接应答）
0010 Reassociation request（重新连接要求）

0011	Reassociation response（重新连接应答）
0100	Probe request（探查要求）
0101	Probe response（探查应答）
1000	Beacon（导引信号）
1001	Announcement traffic indication message (ATIM)
1010	Disassociation（解除连接）
1011	Authentication（身份验证）
1100	Deauthentication（解除认证）

2) 控制帧：type 为 01 时，代表控制帧

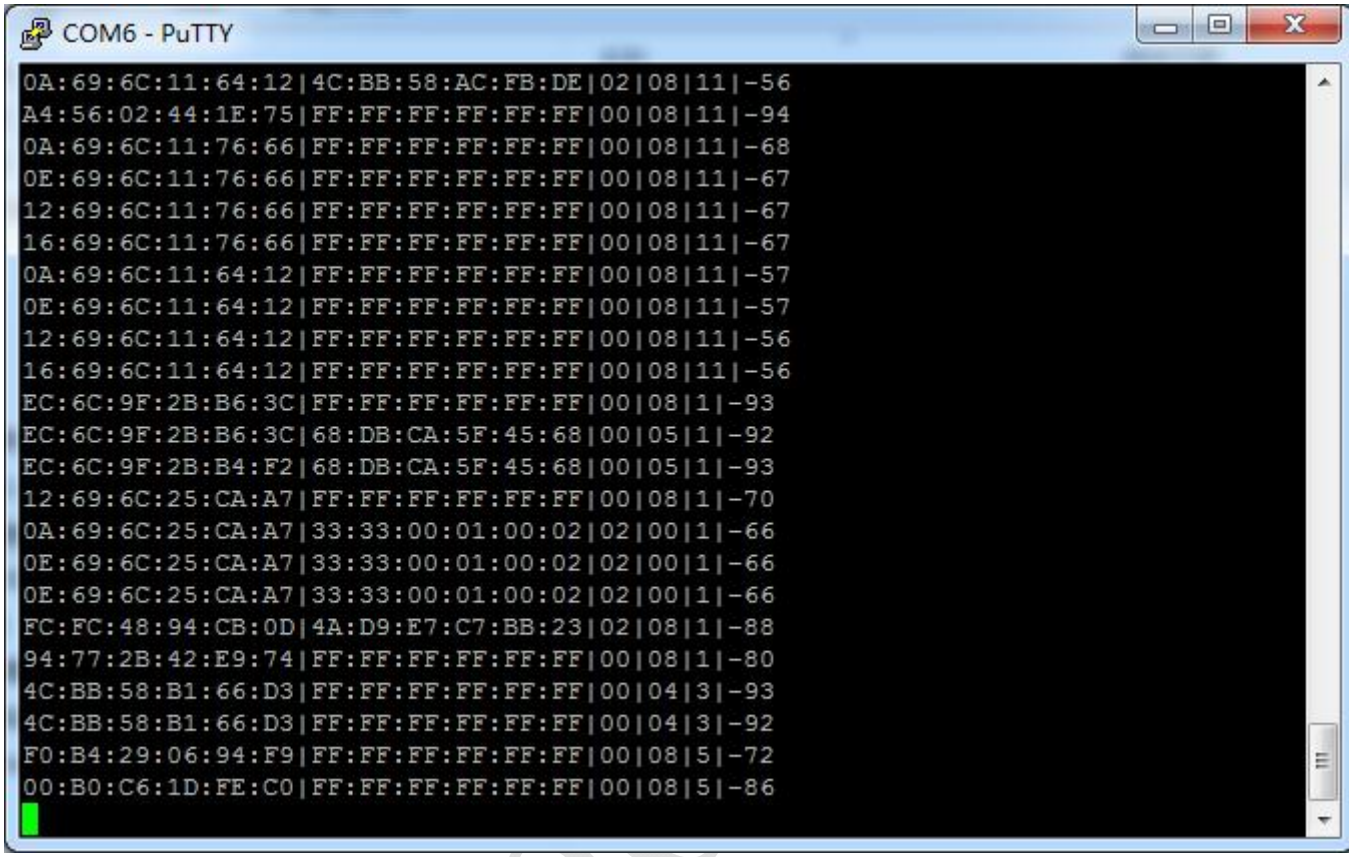
subType	含义
1010	Power Save-Poll（省电模式一轮询）
1011	RTS（请求发送）
1100	CTS（允许发送）
1101	ACK（应答）
1110	CF-End（免竞争期间结束）
1111	CF-End（免竞争期间结束）+CF-Ack（免竞争期间回应）

3) **数据帧：type 为 10 时，代表数据帧**

subType	含义
0000	Data（数据）(0x08)
0001	Data+CF-Ack
0010	Data+CF-Poll (0x28)
0011	Data+CF-Ack+CF-Poll
0100	Null data (无数据：未发送数据)(0x48)
0101	CF-Ack (未发送数据)
0110	CF-Poll (未发送数据)
0111	Data＋CF-Ack+CF-Poll
1000	QoS Data【注 c】 (0x88)
1001	QoS Data + CF-Ack
1010	QoS Data + CF-Poll
1011	QoS Data + CF-Ack + CF-Pol
1100	QoS Null (未发送数据)
1101	QoS CF-Ack (未发送数据)
1110	QoS CF-Poll (未发送数据)
1111	QoS CF-Ack+CF-Poll （未发送数据)

3，探宝抓取格式

格式如下： Frmae 源 MAC||Frmae 目的 MAC | Frame 大类|Frame 小类| RSSI 信号强度



4 如何解析出手机 mac

通常一个 WiFi 的连接过程如下（**说明下面的截图是在 PC 的进行的，因为大小头的原因，在 PC 的类型是 type 在前，subtype 在后，比如同样是 Beacon，PC 上是 0x08,探宝为 大类为 0x00, 小类为二进制 1000， 也就是 0x08**）：

1) AP 发送 Beacon 广播管理帧

```
+ Frame 7: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface 0
+ Radiotap Header v0, Length 18
- IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  - Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
    - Flags: 0x0
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: 74:25:8a:47:3b:70 (74:25:8a:47:3b:70)
    BSS Id: 74:25:8a:47:3b:70 (74:25:8a:47:3b:70)
```

在第 2 节中，已经给出，Beacon 属于管理帧一种， subtype 为 0x0001，其 type 值为 0x0000, 两值加一起为 0x08. 因为 AP 发送的这个 Beacon 管理帧数据包是广播地址，所以我们的 PCMIA 内置网卡、或者 USB 外界网卡会接收到这个数据包，然后在我们的"无线连接列表"中显示出来

2) 客户端向承载指定 SSID 的 AP 发送 Probe Request(探测请求)帧

在第 2 节中，已经给出，Beacon 属于管理帧一种，其 subtype 为 0x1000，type 值为 0x0000, 两者合在一起为 0x40

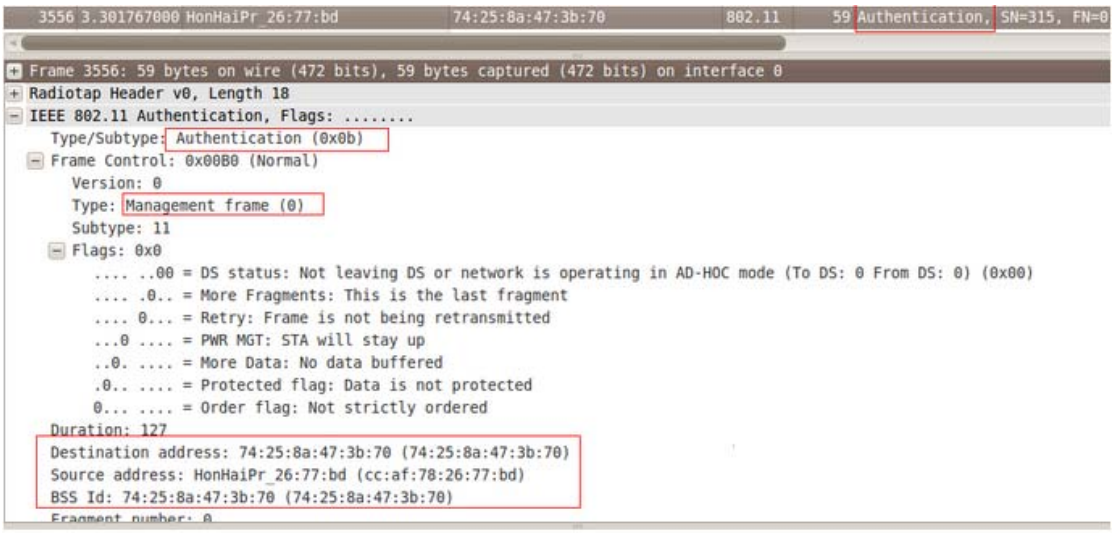
```
Frame 3512: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Radiotap Header v0, Length 18
IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x04)
  Frame Control: 0x0040 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 4
    Flags: 0x0
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: HonHaiPr_26:77:bd (cc:af:78:26:77:bd)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
```

当我们点击"连接"的时候，无线网卡就会发送一个 Prob 数据帧，用来向 AP 请求连接

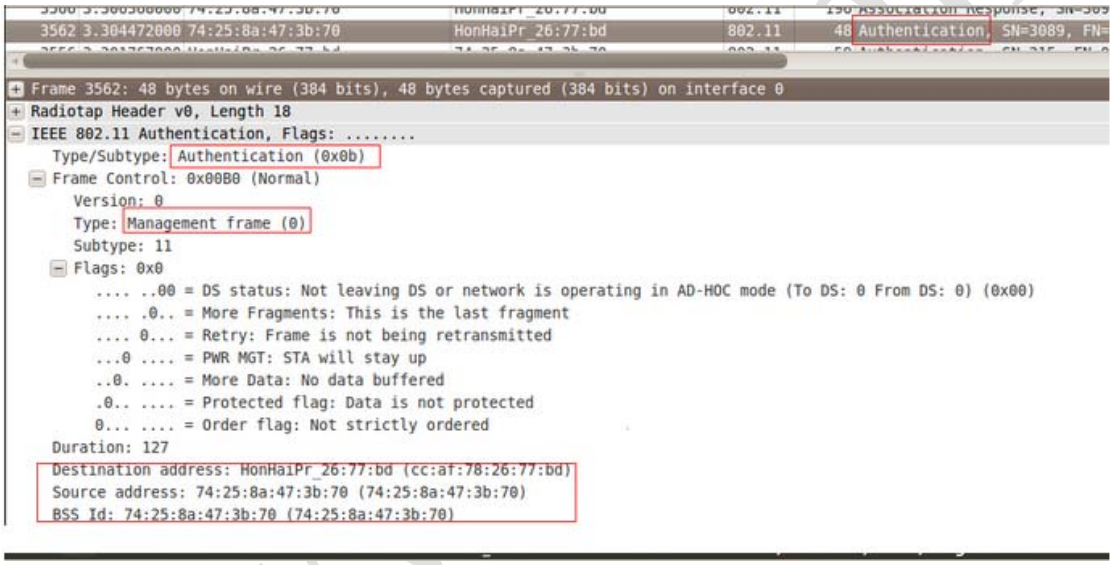
3) AP 接入点对客户端的 SSID 连接请求进行应答

```
3542 3.286598000 74:25:8a:47:3b:70          HonHaiPr_26:77:bd          802.11     222 Probe Response, SN=3083, FN=
Frame 3542: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0
Radiotap Header v0, Length 18
IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x05)
  Frame Control: 0x0050 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 5
    Flags: 0x0
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 127
    Destination address: HonHaiPr_26:77:bd (cc:af:78:26:77:bd)
    Source address: 74:25:8a:47:3b:70 (74:25:8a:47:3b:70)
    BSS Id: 74:25:8a:47:3b:70 (74:25:8a:47:3b:70)
```

4）客户端对目标 AP 请求进行身份认证(Authentication)

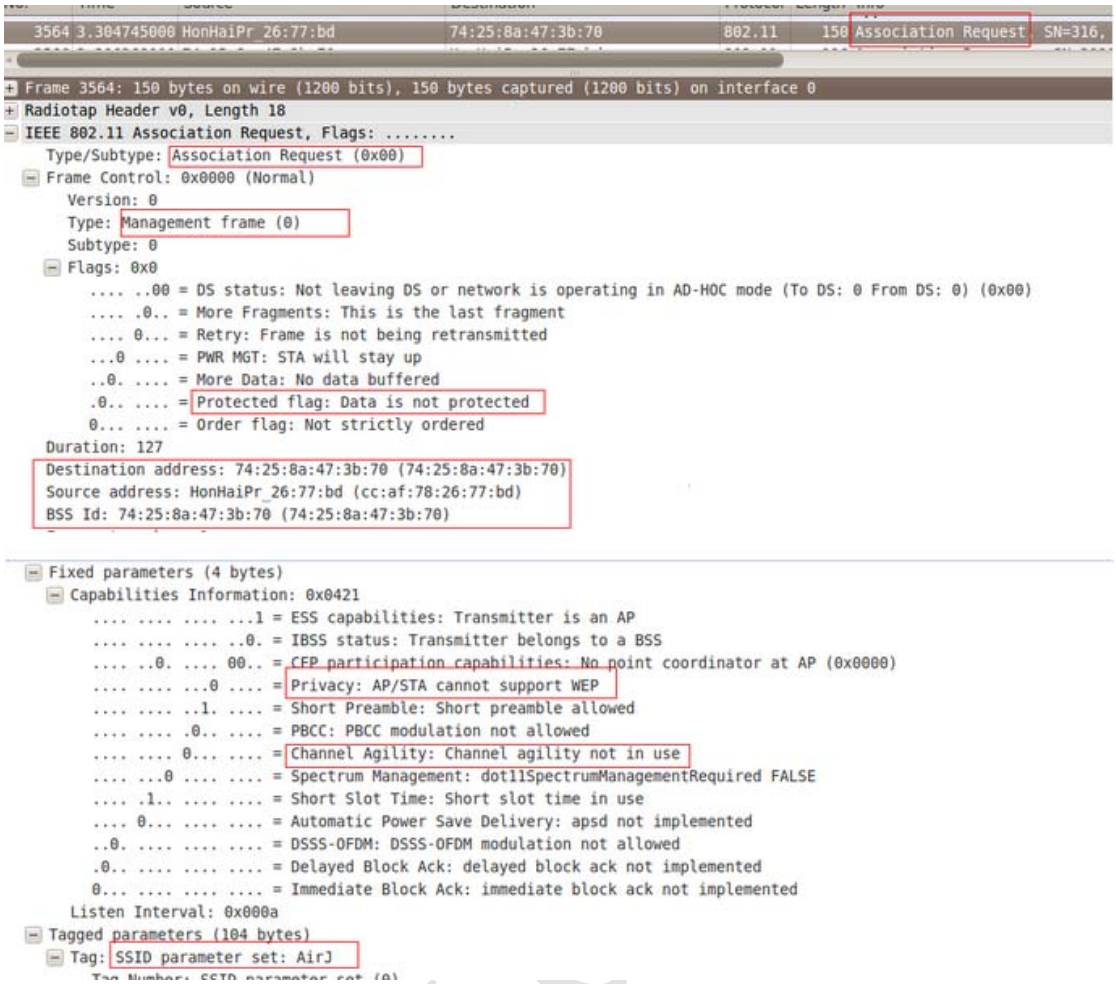


5) AP 对客户端的身份认证(Authentication)请求作出回应

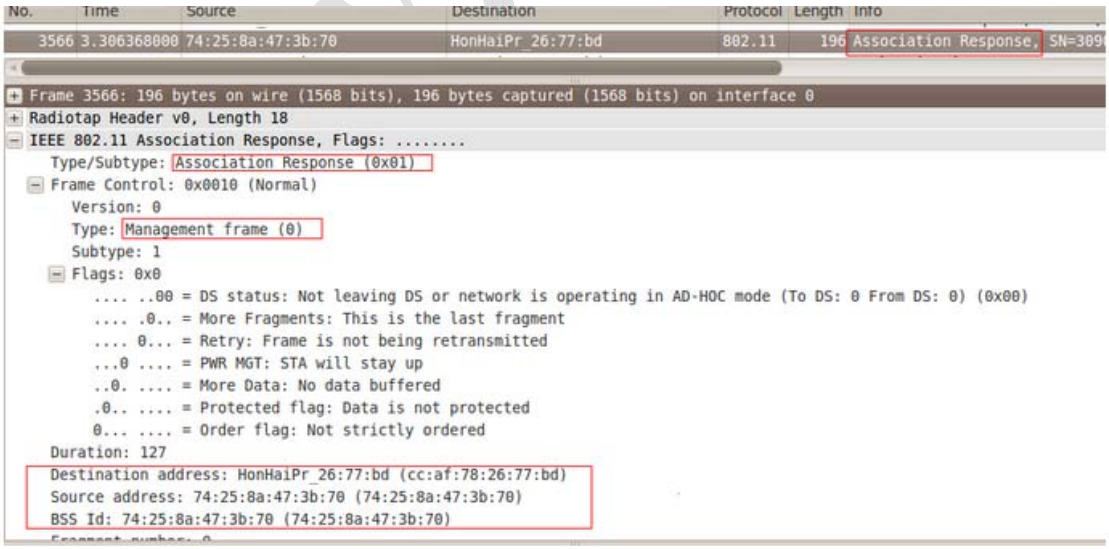


6)客户端向 AP 发送连接(Association)请求

身份认证通过之后，所有的准备工作都做完了，客户端这个时候可以向 WLAN AP 发起正式的连接请求，请求接入 WLAN

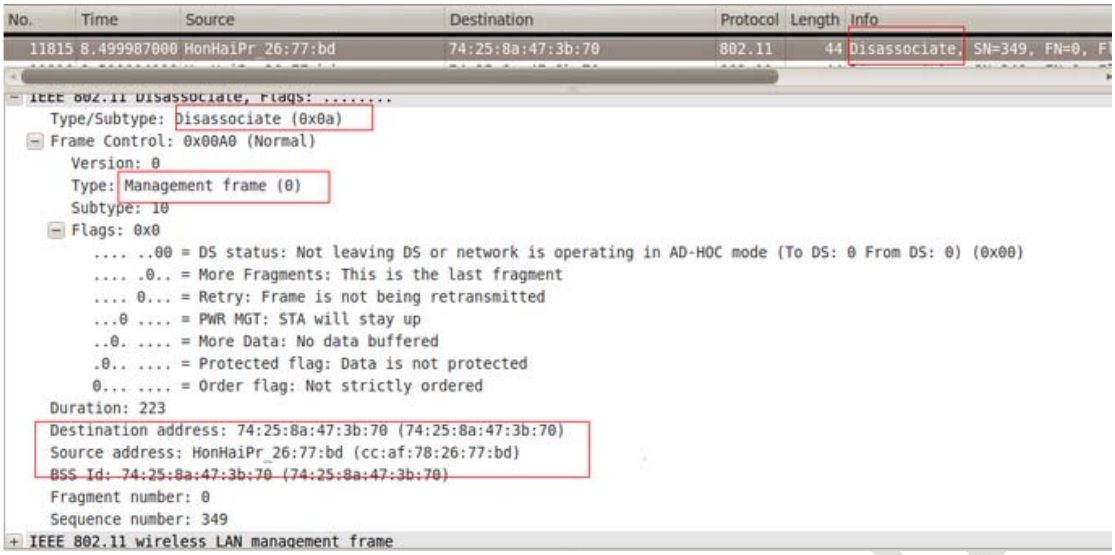


7). AP 对连接(Association)请求进行回应



8). 客户端向 AP 请求断开连接(Disassociation)

当我们点击"断开连接"的时候，网卡会向 AP 发送一个断开连接的管理数据帧，请求进行断开连接



那如何解析出一个手机的 MAC 呢，从上面的分析我们知道，手机会不断的发的探测针(0x04)，在连接上后会发数据帧具体来讲，如果仅仅是分析手机 mac，可以

1.当 type 为 0 时，subtype 为 4.

2.当 type 为 2 时，subtype 为 0、2、4、8、10

当然了，作为一个专业的抓包工具，您也可以从里面分析出整个的过程。

如果专业一点，您可以分析出探宝周边的 AP，每个 AP 下面连接的手机，周边总共有多少手机，如下图：

```
##########################################
Doit                                    BSSID: bc:d1:77:32:e7:2e        Channel: 3
        Client MAC: 90:67:1c:1e:86:db   RSSI: -74dbm
        Client MAC: 8c:70:5a:66:da:60   RSSI: -56dbm
        Client MAC: 08:11:96:7b:c9:40   RSSI: -71dbm
        Client MAC: 10:0b:a9:6b:3e:f4   RSSI: -42dbm
        Client MAC: 38:bc:1a:bb:ed:68   RSSI: -69dbm
        Client MAC: 00:cd:fe:51:e3:f5   RSSI: -61dbm
newifi_doit3305                         BSSID: 20:76:93:36:b7:60        Channel: 10
        Client MAC: 70:72:0d:cb:df:f3   RSSI: -42dbm
        Client MAC: 00:1e:65:2f:5b:46   RSSI: -59dbm
        Client MAC: c4:6a:b7:77:79:3b   RSSI: -58dbm
        Client MAC: b0:d5:9d:00:e2:f4   RSSI: -34dbm
        Client MAC: c0:f2:fb:de:db:0f   RSSI: -59dbm
MWIFI-ILCK                              BSSID: 00:0c:43:d0:08:b2        Channel: 3
        Client MAC: a8:7c:01:47:ee:d1   RSSI: -56dbm
dlink                                   BSSID: 00:22:b0:f7:35:ca        Channel: 6
        Client MAC: 38:bc:1a:e0:80:2e   RSSI: -78dbm
wanyuwangcheng                          BSSID: 1c:fa:68:44:10:e6        Channel: 6
        Client MAC: 20:82:c0:e4:0c:df   RSSI: -88dbm
        Client MAC: 58:44:98:c8:9d:c1   RSSI: -92dbm
feifei                                  BSSID: bc:46:99:cb:4e:10        Channel: 6
familynet                               BSSID: 00:22:3f:6a:77:40        Channel: 11
ChinaNet-dLhL                           BSSID: d0:0f:6d:31:4b:ad        Channel: 8

Total APs: 8
--------------------------
Orphan Clients
        Client MAC: e8:8d:28:a7:6d:b9 BSSID: bc:d1:77:de:46:ec RSSI: -93dbm
##########################################
```

5 如何根据 RSSI 计算距离

RSSI 信号和距离有一定关系，我们推导出了一个公式，因为如果要准确找出两者的关系，需要根据环境设置相应的参数，此外仅给出一个简单的对应关系：

Distance	RSSI
10	-63
20	-72.030899869919
30	-77.31363764159
40	-81.061799739839
50	-83.969100130081
60	-86.344537511509
70	-88.352941200428
80	-90.092699609758
90	-91.62727528318
100	-93

如果您需要更好的对应，请联系 QQ 1971152432（需要付费购买）

Doit 技术支持群 453053759

官网：http://www.doit.am

技术支持：
QQ：114209716
邮箱:lihonggang@doit.am