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

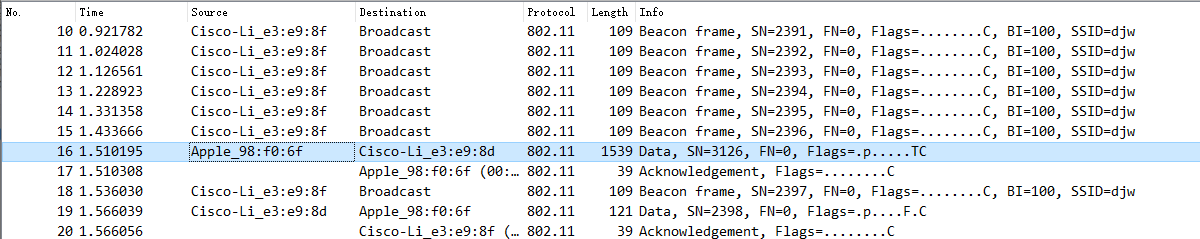
STEP1：fetch a trace

在这里我是用的是助教提供的trace

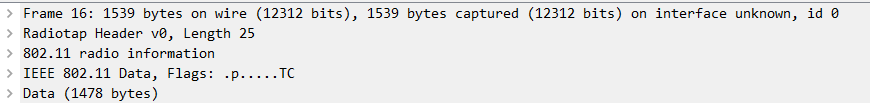
STEP2：inspect the trace

一：

用wireshark打开trace文件



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。

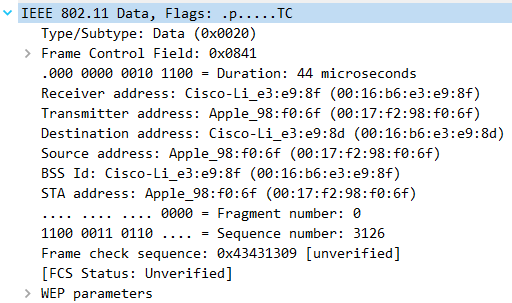
·IEEE 802.11是802.11数据帧的位。

·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。

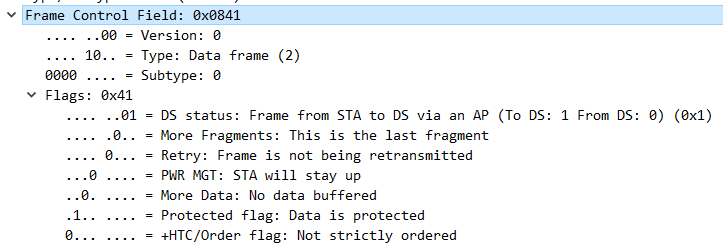
·Frame and sequence number：如果需要的话，这个字段用来表示这个帧的重组次数和重传次数，数字随着每次重传而增大。

·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

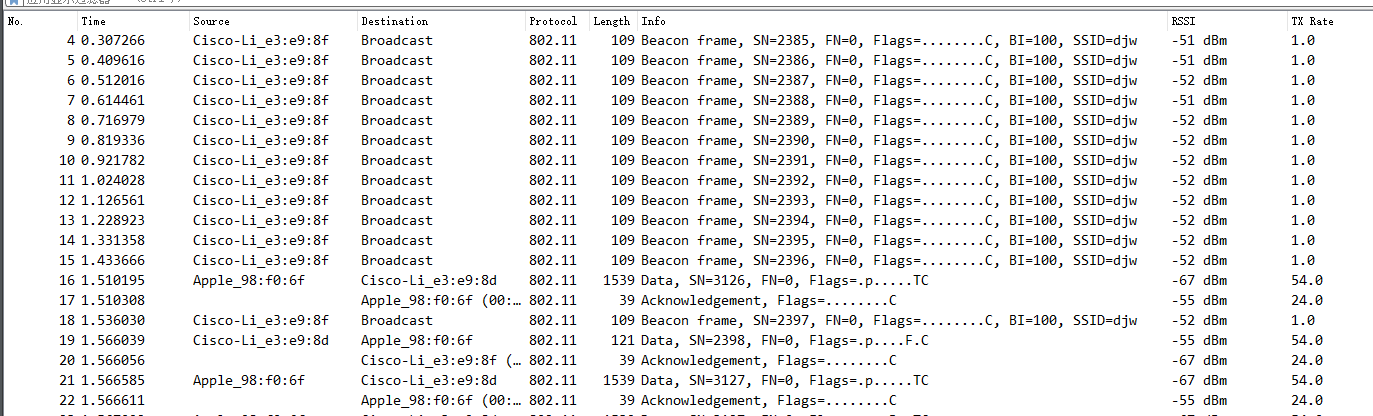
·Order：表示接收方是否必须按顺序接受一系列的帧

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：



点开每一个帧查看，发现channel frequency都是



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 RSSl and hence variation in SNRs in the trace? Give this as the strongest and weakest RSSI and the dB difference between them.

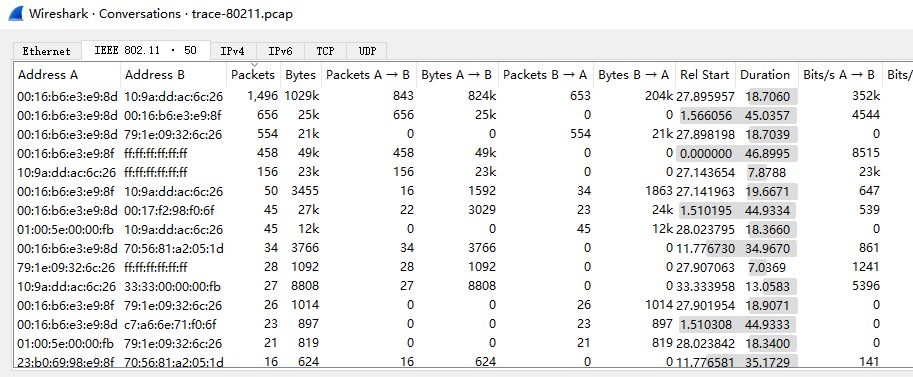
RSSI范围：-44dBm(strongest) 到 -69dBm(weakest)

SNRs: 300

dB differences: 25dBm

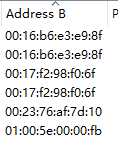
STEP4 链路层

打开Conversations页面，显示如下



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?

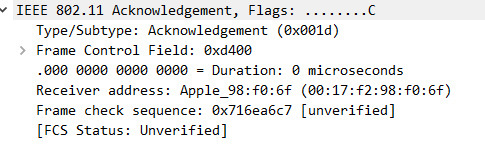
有1391个Control Frame，最常见的Subtype是Acknowledgement Frame，标号为13

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

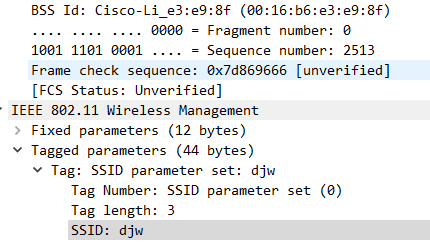
not poweringdown number = 822

rate = 16 / 822 = 1.95%

STEP5: 802.11 Management

3.1 What is the SSID of the main AP?

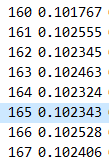
打开一个Beacon Frame后如图



可以看到SSID是djw

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

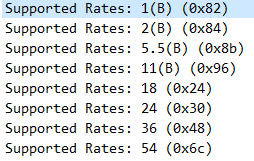
在wireshark里选择视图->时间显示格式->自上一个捕获分组经过的秒数



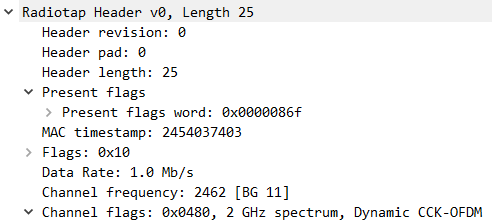
从图中可以看出Beacon Frame的发送频率大概在0.1023s发送一帧

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：



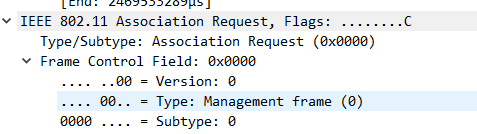
3.4 What rate is the Beacon frame transmission?



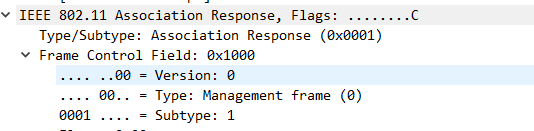
在Radiotap Header中可以看到Data Rate是1.0Mb/s

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

Association Request:



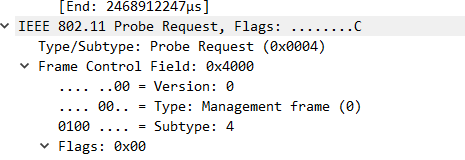
Association Response:



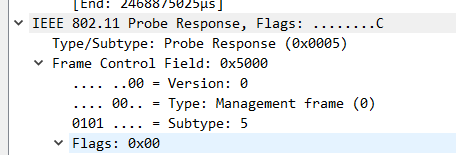
根据图可知，Association Request:的Type是0(Management frame)，Subtype是0; Association Response的Type是0(Management frame)，Subtype是1

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

Probe Request:



Probe Response:



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.