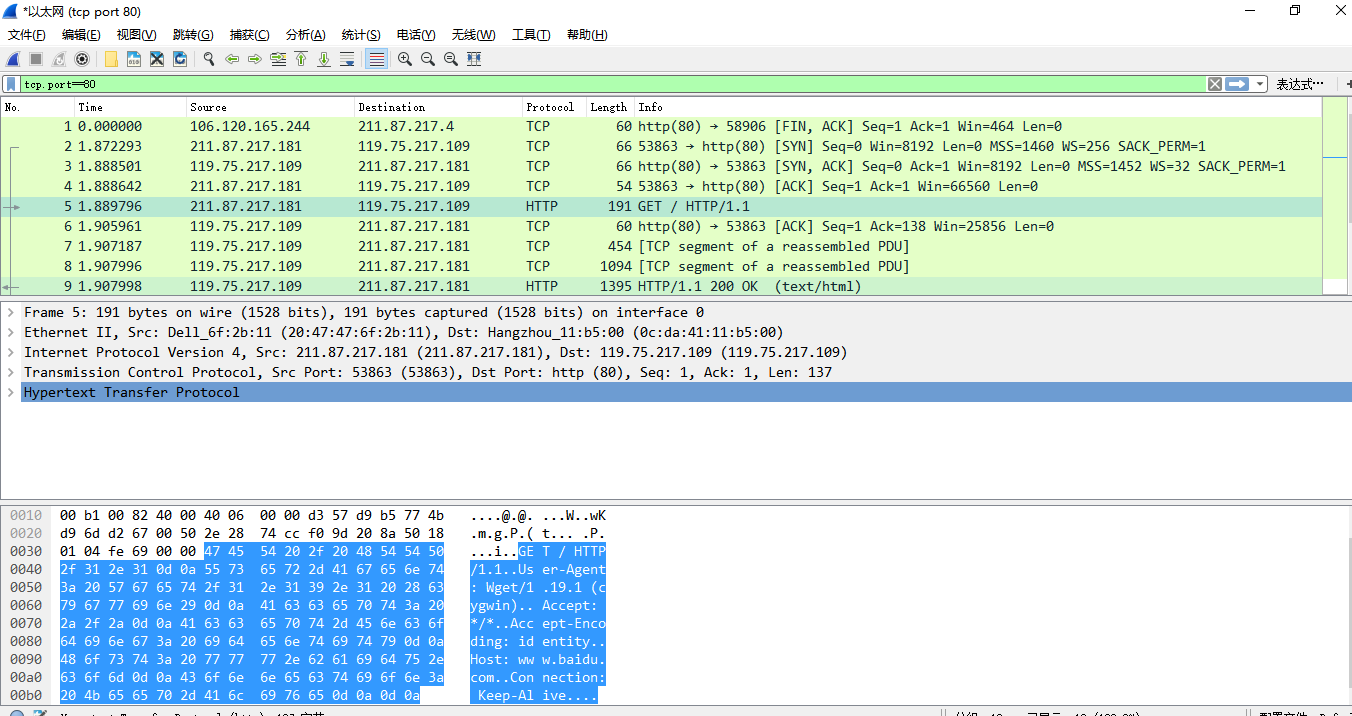
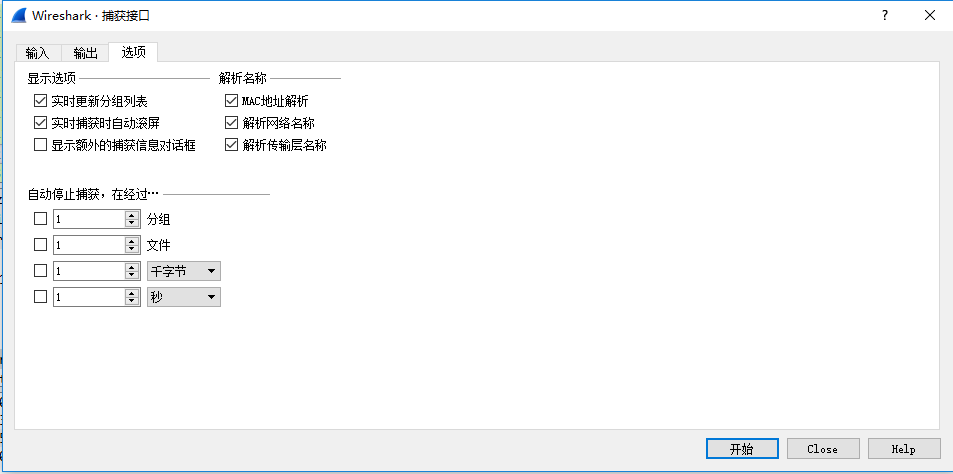
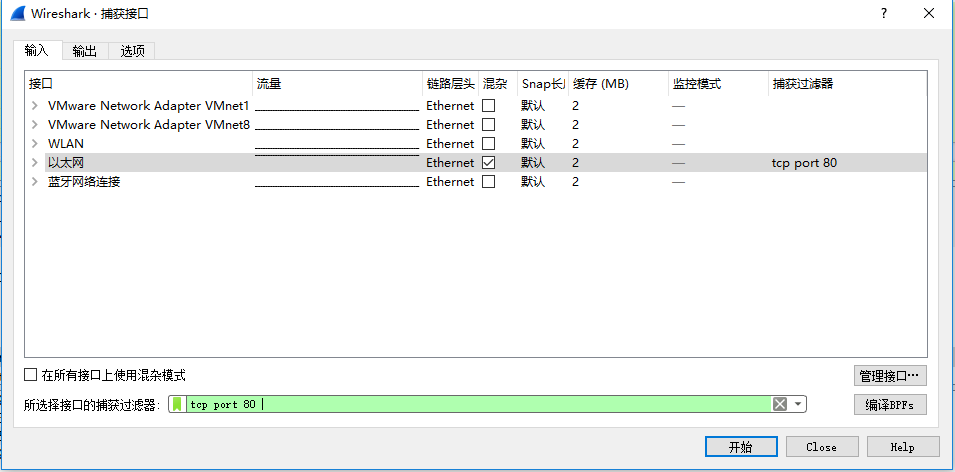
# Lab Exercise – Protocol Layer

## Step 1.



## Step 2.



## Step 3

|  |  |  |  |
| --- | --- | --- | --- |
| Ethernet | IP | TCP | HTTP |

0 14 34 54 192

Ethernet header Ethernet payload

IP header IP payload

## Step 4

Protocol overhead:

Packet2:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 32 bytes

Packet3:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 32 bytes

Packet4:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Packet5:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Http: 137 bytes

Packet6:

Ethernet: 20 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Packet7:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Data: 400 bytes

Packet8:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Data: 1040

Packet9:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Data: 1341 bytes

Packet10:

Ethernet: 20 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Packet11:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Packet12:

Ethernet: 14 bytes  
IP header: 20 bytes

TCP header: 20 bytes

Packet13:

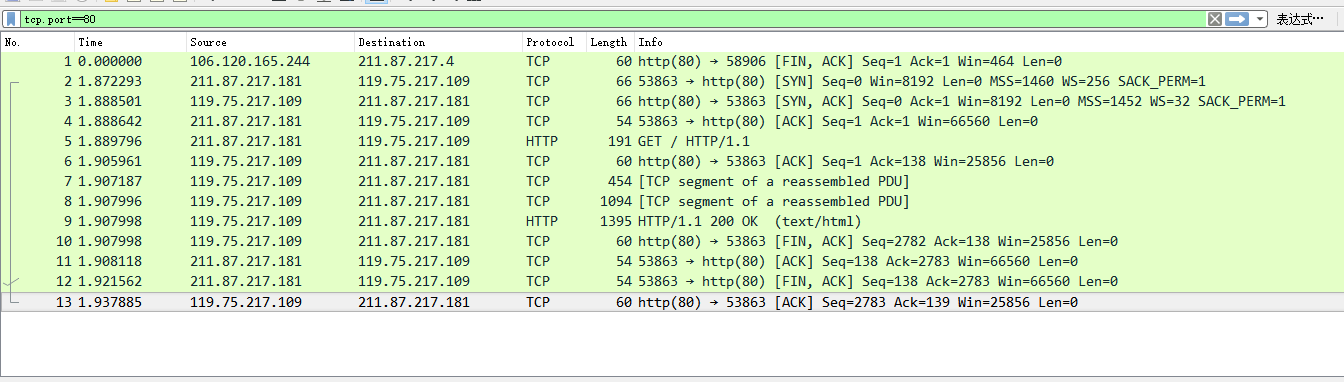
Ethernet: 20 bytes  
IP header: 20 bytes

TCP header: 20 bytes

其中 packet7 和packet8 是将一个网页分两部分传送的,packet9是将两部分合起来的结果.

传输的packet的Ethernet, IP, and TCP header 的总的字节数是9\*54+60\*3=666 bytes,传输的有效数据是137+400+1040=1577 bytes

有效数据所占的比重是1577/(1577+666)=0.73, overhead 所占的比重0.27, 所以可以看出头确实占了很大的比重。



Step5:

1. Which Ethernet header field is the demultiplexing key that tells it the next higher layer is IP? What value is used in this field to indicate “IP”?

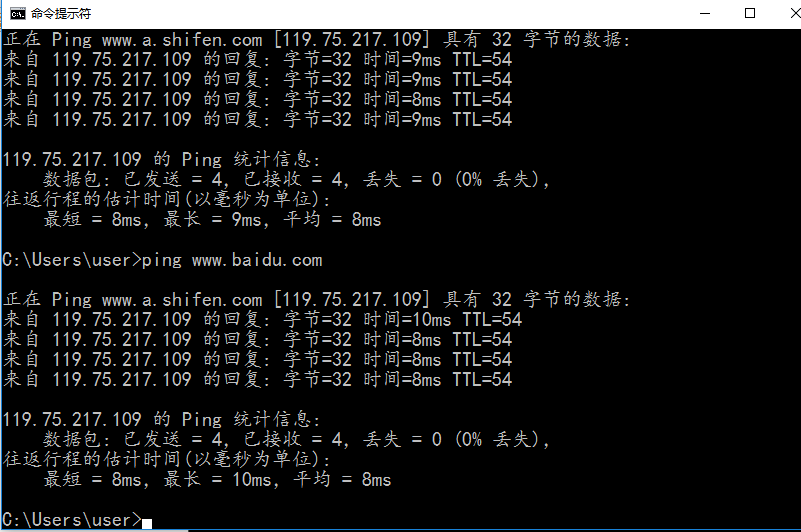
Answer. The demultiplexing key for Ethernet is the Type field. It holds 0x800 when the higher layer is IP and the key is the last two bytes.

2. Which IP header field is the demultiplexing key that tells it the next higher layer is TCP? What value is used in this field to indicate “TCP”?

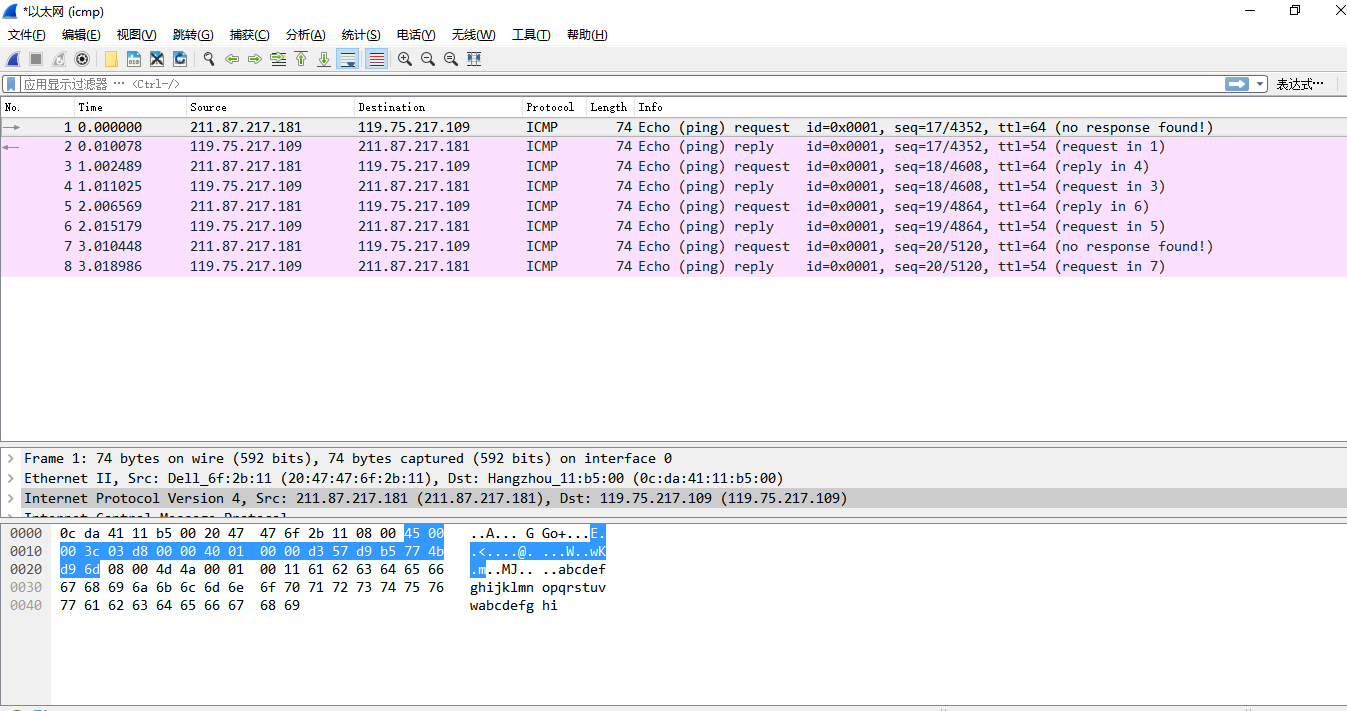
Answer: The demultiplexing key for IP is the Protocol field. It has value 0x06 when the higher layer is TCP and it is in the tenth byte of the header.

# Lab Exercise – Ethernet

## Step1



## Step 2



## Step 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Destination Address | Source  Address | Type | Payload | Checksum |

6 bytes 6 bytes 2 bytes 56 bytes 4 bytes

## Step 4

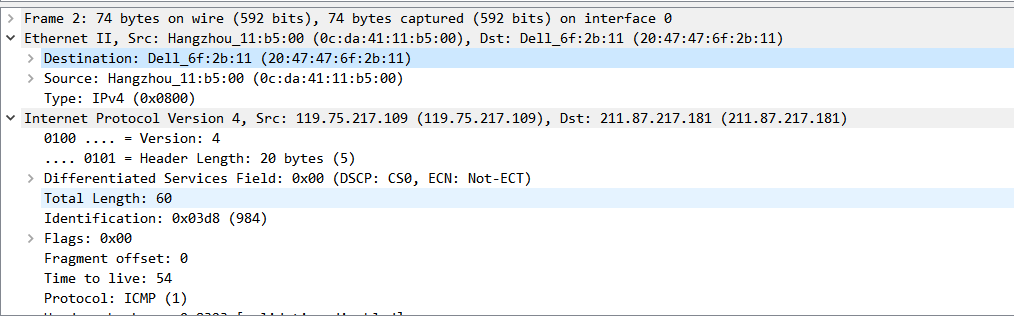
IP: 211.87.217.181 IP:未知 IP:119.75.217.109

Eth Addr=20:47:47:6f:2b:11 Eth Addr:0c:da:41:11:b5:00 Eth Addr:未知

My computer

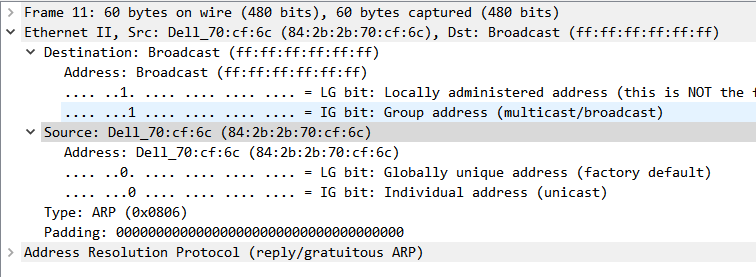
Remote Server

Router



## Step 5

1. broadcast address 是 ff:ff:ff:ff:ff:ff.,也就是全是1.
2. The broadcast/multicast or “group” bit is shown by Wireshark as “.... ...1 .... .... .... ....” or a one in the low-order bit of the first address byte. We could also write this 01:00:00:00:00:00. This bit is actually the  
   bit that is transmitted on the wire first because Ethernet defines the transmission order to be the “least significant bit of each byte first”.



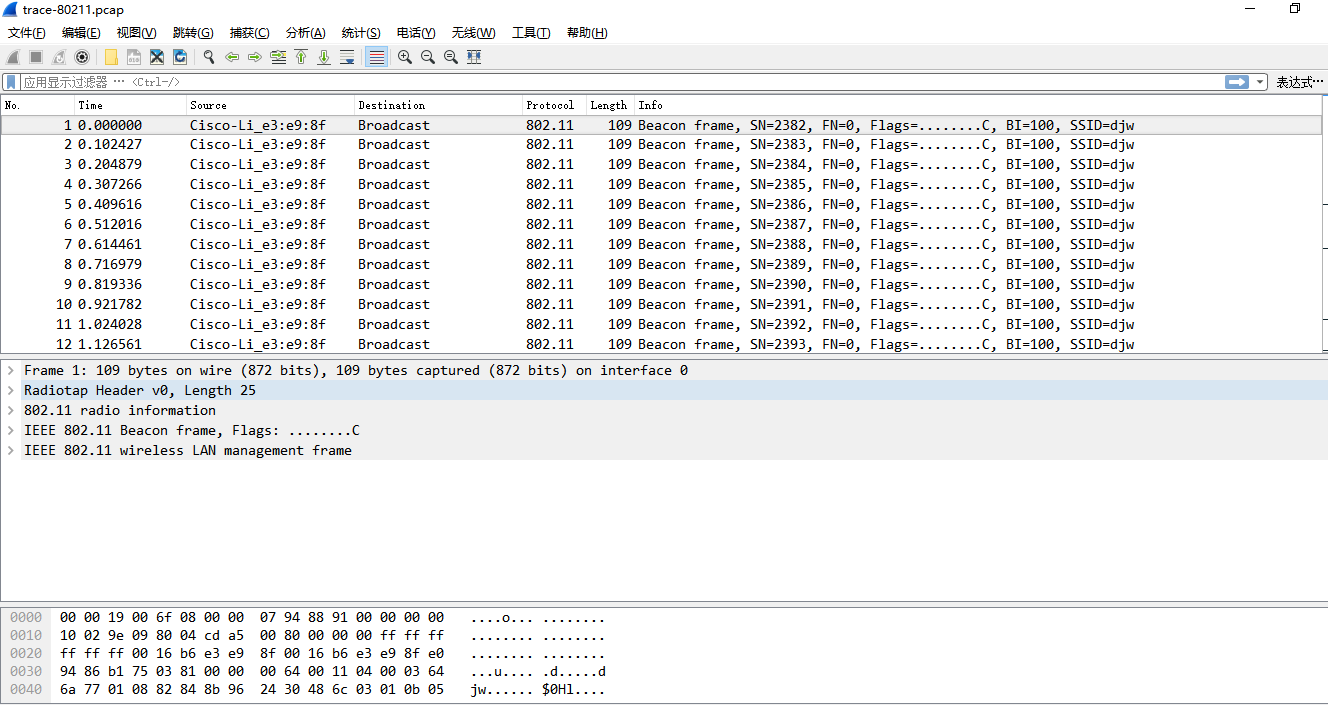
## Step6

1．802.3 and DIX Ethernet header is 14 bytes, LLC has 17 bytes.

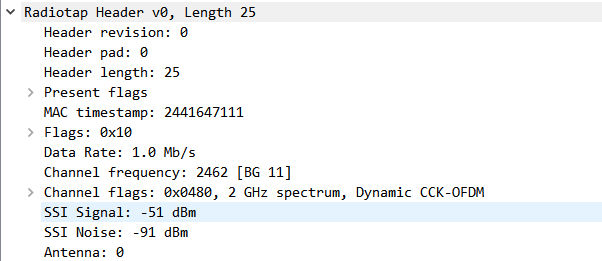
2. The DIX Ethernet Type field and IEEE 802.3 Length field are in the same position. If the value is less than 0x600 (1536) then it is interpreted as a frame length. If the value is larger than 0x600 (1536) then it is interpreted as a Type value.

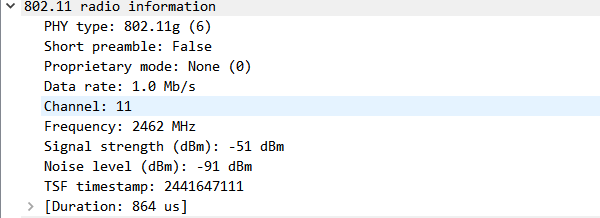
3. IEEE 802.3 uses LLC headers to present.

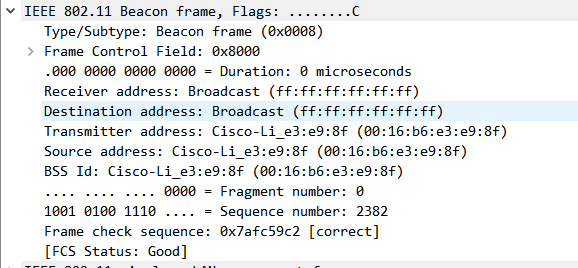
# Lab Exercise – 802.11

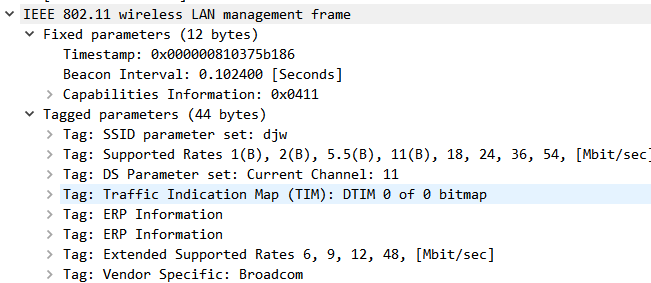
Step1 

## Step 2



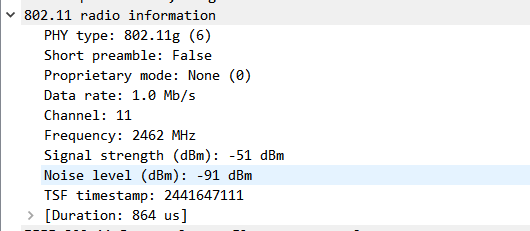






## Step 3

1.What is the channel frequency? To find the frequency, expand the Radiotap header of any frame and look for the Channel frequency.  
Answer: The Channel frequency is 2462 MHz

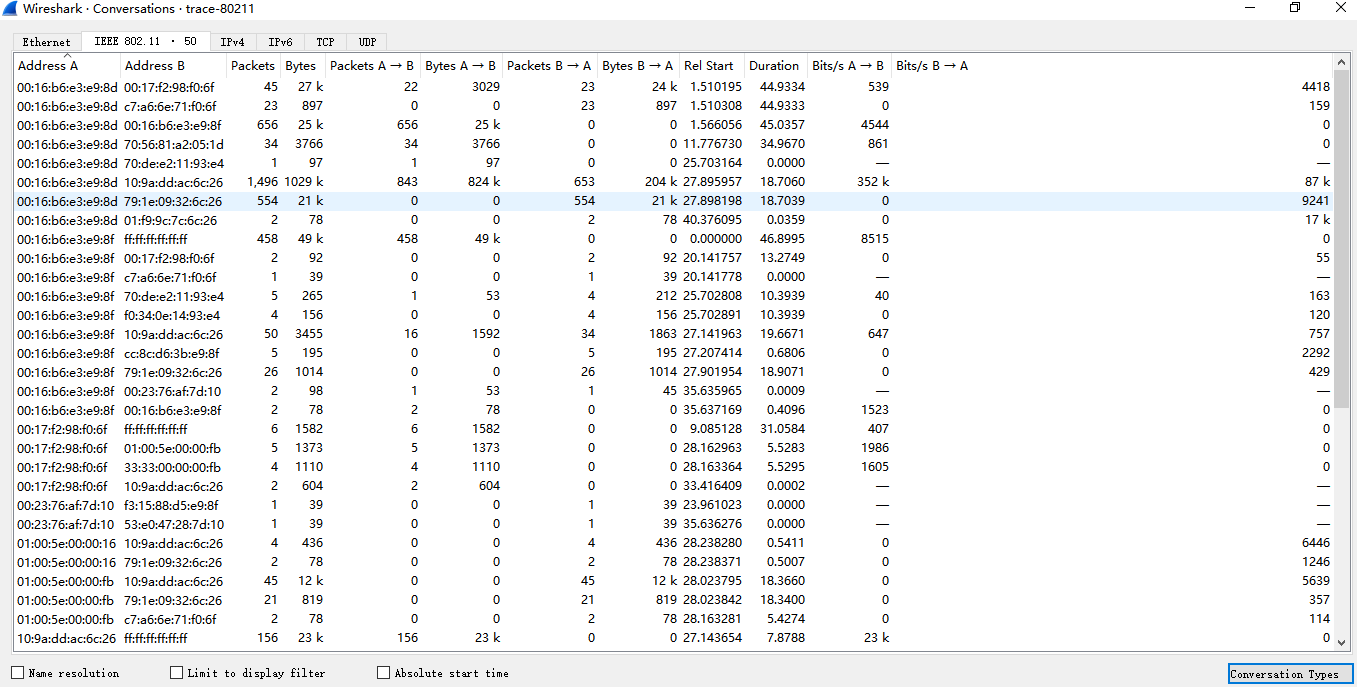


2.What rates are used? Give an ordered list of rates from lowest to highest. Hint: you can click the Rate column to sort by that value.

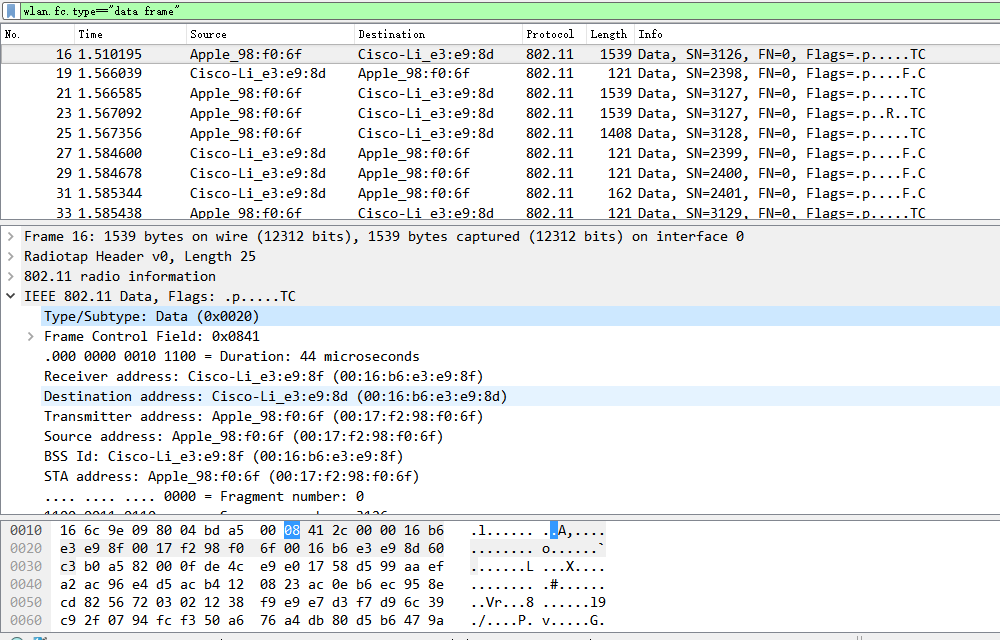
Answer: The rates are 1, 6, 12, 18, 24, 38, 48, and 54 Mbps.

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.

Answer: The RSSIs range from -44 dBm (strongest) to -69 dBm (weakest signal). This is a variation of 25 dB or around a factor of 300 in the SNR

Step4 4 

1. the AP has a BSS ID of 00:16:b6:e3:e9:8f



1. There are totally 1783 data frames in the trace.

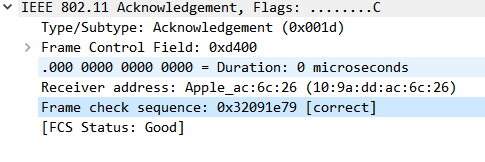
The most common Data frame is  
simply called “Data” with subtype 0. The fraction of Data frames will depend heavily on whether there are active data transfers during the trace; there is a small transfer during this trace.

1. There are 1391 Control frames. The most common Control frame is the Acknowledgement frame with subtype 13.
2. There are 557 Management frames. The most common Management frame is the Beacon frame with subtype 8
3. Frame Control: 2 bytes

Receiver Address: 6 bytes

Duration: 2 bytes

Frame Check Sequence: 4 bytes



1. 353 Data frames have their Retry bit set in the Frame Control field, while  
   the number of their unset counterparts is 1430, so that the retransmission  
   rate is about 24.69%.
2. 16 out of 822 or 2% of the frames sent to the AP have their power management bit set, indicating that they are about to sleep

## Step 5

1. The SSID is “djw”.
2. beacon frames are sent by the “djw” AP every 102.4 milliseconds, or a rate of roughly  
   10/second.
3. The AP supports 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps.
4. The Beacon frames for this AP are all transmitted at a rate of 1 Mbps.
5. Request is Type 0 (Management) and Subtype 0. Response is Type 0  
   (Management) and Subtype 1
6. Probe Request is Type 0 (Management) and Subtype 4. Probe Response is Type 0 (Management) and Subtype 5.

