Configuration of BBBW for WiFi sniffer:

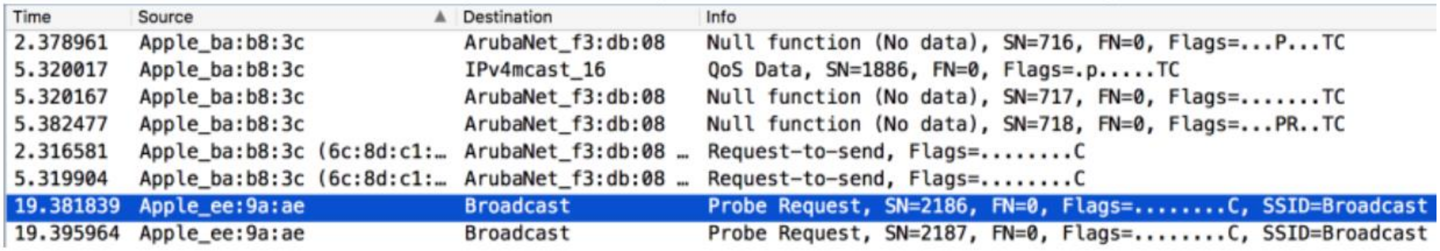
1. Embedded Wi-Fi Module Setting:

1) Connect BBBW with laptop via USB cable.
2) Open the 'BeagleBone Getting Started' file in 'Computer'.
   Choose the driver file in corresponding OS file.
3) If Windows system, use 'putty' and input '192.168.7.2' to login system.
   If Linux system, use 'terminal' and input 'ssh root@192.168.7.2' to login system
4)
```
root@beaglebone->sudo connmanctl
Connmanctl >      tether wifi disable
Connmanctl >      enable wifi
Connmanctl >      scan wifi
Connmanctl >      services
......  all available wifi information will be shown on screen        .....
Connmanctl >      agent on
Connmanctl >      connect <Wi-Fi information>
Passphrase? <input Wi-Fi passaword>
Connmanctl >      quit
```
5) Input 'ifconfig –a' OR 'iwconfig wlan0' to check the IP address
6) The setting is finished. The BBBW can be logged in by 'ssh root@<IP address>'

2. Check the WIFI Packet Format:

In Linux system, use WireShark and TP_LINK Wi-Fi adapter.

1) Connect laptop with Ethernet via wired cable. Insert TP-Link Wi-Fi Adapter into laptop.
2) Set the Wlan0 as 'managed' mode:
   a. -> sudo ifconfig wlan0 down
   b. -> sudo iwconfig wlan0 mode managed
   c. -> sudo ifconfig wlan0 up
3) Use 'iwconfig' to know the title of TP-Link Wi-Fi adapter, then set it as 'monitor' mode:
   a. -> sudo ifconfig wlan'x' down
   b. -> sudo iwconfig wlan'x' mode monitor
   c. -> sudo ifconfig wlan'x' up
4) Open WireShark, choose the "wlan'x'" as interface to check the wifi packets information.
5) Choose the item with information "probe request" and then analyze its detailed information including "**RadioTap Header**" and **Binary Information**.



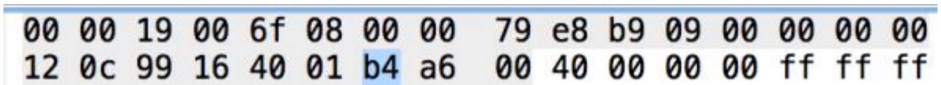
Time	Source	Destination	Info
2.378961	Apple_ba:b8:3c	ArubaNet_f3:db:08	Null function (No data), SN=716, FN=0, Flags=...P...TC
5.320017	Apple_ba:b8:3c	IPv4mcast_16	QoS Data, SN=1886, FN=0, Flags=.p.....TC
5.320167	Apple_ba:b8:3c	ArubaNet_f3:db:08	Null function (No data), SN=717, FN=0, Flags=.......TC
5.382477	Apple_ba:b8:3c	ArubaNet_f3:db:08	Null function (No data), SN=718, FN=0, Flags=...PR..TC
2.316581	Apple_ba:b8:3c (6c:8d:c1:…	ArubaNet_f3:db:08 …	Request-to-send, Flags=........C
5.319904	Apple_ba:b8:3c (6c:8d:c1:…	ArubaNet_f3:db:08 …	Request-to-send, Flags=........C
19.381839	Apple_ee:9a:ae	Broadcast	Probe Request, SN=2186, FN=0, Flags=........C, SSID=Broadcast
19.395964	Apple_ee:9a:ae	Broadcast	Probe Request, SN=2187, FN=0, Flags=........C, SSID=Broadcast

6) Check each item in 'RadioTap Header' and its **BYTES NUMBER & POSITION** in 'binary information'.

3. Modify RadioTap Header Structure in head.h File:

Two examples:

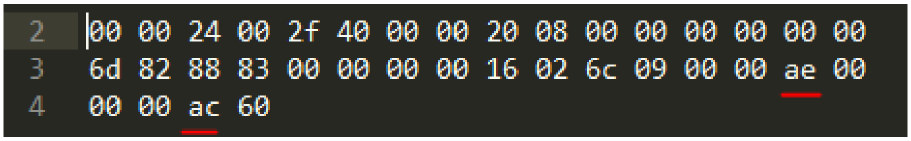
1.



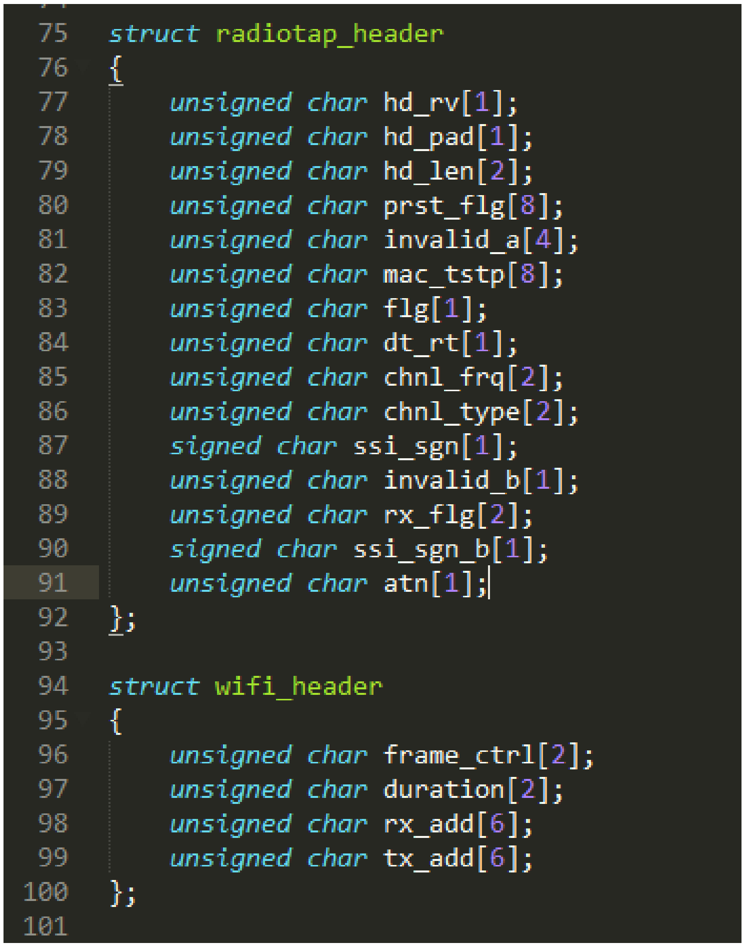
```
00 00 19 00 6f 08 00 00  79 e8 b9 09 00 00 00 00
12 0c 99 16 40 01 b4 a6  00 40 00 00 00 ff ff ff
```

```
struct radiotap_header
{
    unsigned char hd_rv[1];
    unsigned char hd_pad[1];
    unsigned char hd_len[2];
    unsigned char prst_flg[4];
    unsigned char mac_tstp[8];
    unsigned char flg[1];
    unsigned char dt_rt[1];
    unsigned char chnl_frq[2];
    unsigned char chnl_type[2];
    signed char ssi_sgn[1];
    unsigned char atn[1];
    unsigned char rx_flg[2];
};
```

2.



```
00 00 24 00 2f 40 00 00 20 08 00 00 00 00 00 00
6d 82 88 83 00 00 00 00 16 02 6c 09 00 00 ae 00
00 00 ac 60
```



```
struct radiotap_header
{
    unsigned char hd_rv[1];
    unsigned char hd_pad[1];
    unsigned char hd_len[2];
    unsigned char prst_flg[8];
    unsigned char invalid_a[4];
    unsigned char mac_tstp[8];
    unsigned char flg[1];
    unsigned char dt_rt[1];
    unsigned char chnl_frq[2];
    unsigned char chnl_type[2];
    signed char ssi_sgn[1];
    unsigned char invalid_b[1];
    unsigned char rx_flg[2];
    signed char ssi_sgn_b[1];
    unsigned char atn[1];
};

struct wifi_header
{
    unsigned char frame_ctrl[2];
    unsigned char duration[2];
    unsigned char rx_add[6];
    unsigned char tx_add[6];
};
```