

知 在升级MacOS Big Sur软件版本之后，使用wireshark尝试无线捕获将无法正 常进行

wlan接入 朱楷 2022-05-20 发表

问题描述

Macbook 在升级MacOS Big Sur软件版本之后，使用wireshark尝试无线捕获将无法正常进行。
尤其一些新款的Macbook M1芯片版本尤其如此。

主要表现为，

- 1、wireshark尝试使用wifi网卡使用monitor模式无法捕获无线报文
- 2、无法通过无线诊断工具尝试让macbook去嗅探指定信道，即使你已经在页面上调整了channel 频宽参数。

解决方法

这个问题的原因是Macos Big Sur的改动带来的，看起来现在Apple还没有改动的迹象。

我找到了一些规避手段。

1、历史上使用macos系统下的wireshark抓取无线报文，可以先连接wifi然后抓取；这个在Big Sur操作系统下不行了，取代的方法是先把wifi断开，保证macbook不连接wifi的情况下（但是wifi网卡是up的）开启wireshark 无线monitor模式就可以抓包了。

2、但是这个操作会无法指定想要的信道和频宽，对抓包来说不是很友好。因此我又找到了命令行修改信道频宽的手法。具体为：

```
sudo /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport  
--channel=149,20 (149信道, 20Mhz频宽的意思, 其他组合请举一反三)
```

当然这个路径看起来藏得比较深 复杂，你可以先做个文件的替身去访问（修改到usr/local/bin路径下）

:

```
sudo ln -s
```

```
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport /usr/  
ocal/bin/airport 当然这个airport还有更多硬核的玩法就靠你自己去挖掘了。
```

