无线空口抓包小知识

wlan接入 **谭奇伟** 2024-10-01 发表

问题描述

1. 空口抓包的方法有哪些?
2. 使用例如omnipeek + A6210网卡（802.11ac）或者Macbook（支持802.11ax的款型）能否抓取到Wi-Fi 7（802.11be）终端和AP之间交互的无线空口报文?

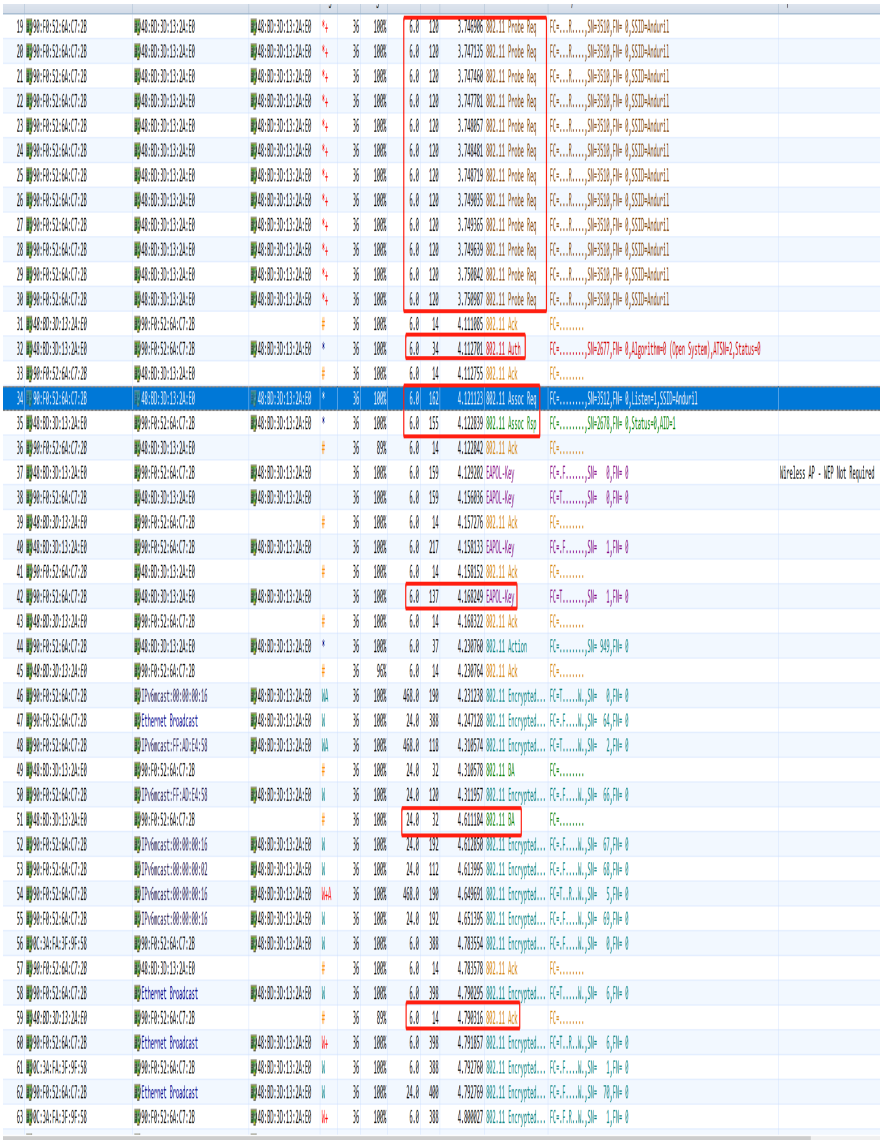
解决方法

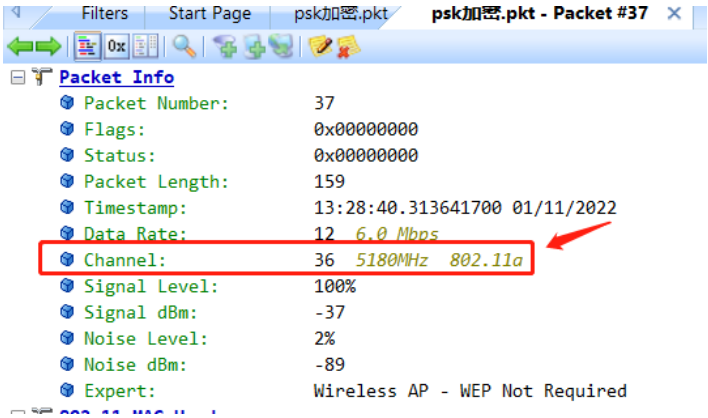
问题一，答:

① 使用windows系统下omnipeek + A6210网卡进行抓包，可参考:
https://zhiliao.h3c.com/TechDoc/details/829
② 使用Macbook进行抓包，可参考:
https://zhiliao.h3c.com/Theme/details/17019
https://zhiliao.h3c.com/Theme/details/212205
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html#anc8

问题二，答:

答：Wi-Fi 7（802.11be）终端和AP之间交互的无线数据报文如果是采用802.11be协议标准传输的则无法抓取到，但802.11管理报文由于采用较低的协议标准传输，使用支持802.11ac或者802.11ax协议的网卡也是可以捕获到的。
例如下图中红框标注的beacon，probe，auth，association，deauth，disassociation，802.11action，BA，Ack等，以及PSK密钥交互的EAPOL key等均以802.11a协议较低速率（6 Mbps）发送，因此是可以使用老网卡捕获到的，但是终端上线后的数据报文（DHCP，DNS，ICMP，TCP，UDP，ARP，IPv6）等如果使用802.11be协议发送，则老网卡是无法抓到的，如果此时需要捕获这些数据报文，则只能强制Wi-Fi 7 AP的radio为802.11ac或者802.11ax的协议来捕获。




Filters
Start Page
psk加密.pkt
psk加密.pkt - Packet #37
Packet Info
Packet Number: 37
Flags: 0x00000000
Status: 0x00000000
Packet Length: 159
Timestamp: 13:28:40.313641700 01/11/2022
Data Rate: 12 6.0 Mbps
Channel: 36 5180MHz 802.11a
Signal Level: 100%
Signal dBm: -37
Noise Level: 2%
Noise dBm: -89
Expert: Wireless AP - WEP Not Required