

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。

19	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74986	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
20	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74735	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
21	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74740	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
22	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74781	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
23	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74067	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
24	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74041	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
25	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74719	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
26	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74935	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
27	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74935	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
28	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.74939	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
29	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.75042	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
30	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	120	3.75097	802.11	Probe Req	FE+.....,SN=550,FW=0,SSID=nduril
31	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.11085	802.11	Ack	FE+.....
32	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.11781	802.11	Ack	FE+.....,SN=677,FW=0,Algorithm= (Open System),ATIM=1,Status=0
33	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.11755	802.11	Ack	FE+.....
34	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	152	4.12121	802.11	Assoc Req	FE+.....,SN=551,FW=0,Listen1,SSID=nduril
35	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	155	4.12039	802.11	Assoc Req	FE+.....,SN=670,FW=0,Status=0,AID=1
36	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	89%	6.0	14	4.12242	802.11	Ack	FE+.....
37	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	159	4.12902	EAPOL-Key	FE+.....,SN=0,FW=0	
38	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	159	4.15696	EAPOL-Key	FE+.....,SN=0,FW=0	
39	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.15726	802.11	Ack	FE+.....
40	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	217	4.15813	EAPOL-Key	FE+.....,SN=1,FW=0	
41	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.15852	802.11	Ack	FE+.....
42	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	137	4.16049	EAPOL-Key	FE+.....,SN=1,FW=0	
43	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.16032	802.11	Ack	FE+.....
44	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	37	4.23070	802.11	Action	FE+.....,SN=349,FW=0
45	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	90%	6.0	14	4.23074	802.11	Ack	FE+.....
46	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	488.0	190	4.23128	802.11	Encrypted...	FE+.....,SN=0,FW=0
47	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	300	4.24728	802.11	Encrypted...	FE+.....,SN=64,FW=0
48	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	488.0	110	4.31074	802.11	Encrypted...	FE+.....,SN=1,FW=0
49	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	31	4.310570	802.11	BA	FE+.....
50	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	120	4.31057	802.11	Encrypted...	FE+.....,SN=66,FW=0
51	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	31	4.61194	802.11	BA	FE+.....
52	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	192	4.61208	802.11	Encrypted...	FE+.....,SN=67,FW=0
53	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	112	4.61395	802.11	Encrypted...	FE+.....,SN=68,FW=0
54	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	488.0	190	4.64901	802.11	Encrypted...	FE+.....,SN=5,FW=0
55	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	192	4.65195	802.11	Encrypted...	FE+.....,SN=69,FW=0
56	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	300	4.70354	802.11	Encrypted...	FE+.....,SN=0,FW=0
57	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	14	4.70370	802.11	Ack	FE+.....
58	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	390	4.70425	802.11	Encrypted...	FE+.....,SN=6,FW=0
59	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	89%	6.0	14	4.70416	802.11	Ack	FE+.....
60	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	390	4.70167	802.11	Encrypted...	FE+.....,SN=6,FW=0
61	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	300	4.70270	802.11	Encrypted...	FE+.....,SN=1,FW=0
62	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	24.0	400	4.70279	802.11	Encrypted...	FE+.....,SN=70,FW=0
63	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	36	100%	6.0	300	4.80007	802.11	Encrypted...	FE+.....,SN=1,FW=0

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