wlan射频 **股俊** 2017-03-27 发表

在处理无线网络问题时,一般会有一个初步排查的过程,判断具体出问题的节点。由于无线网络是电磁波,传输介质是在空气,没有实际存在的物理链路。经过初步排查后,如果怀疑问题出在AP到无线终端这一端,常常无法判断具体问题是出在无线客户端上还是在AP上。此时就需要采集到报文在空间传输过程中的交互,再定位具体问题出在哪个节点。

此类问题一般涉及无线空口丢包,无线终端接入,无线终端异常掉线等接入层问题。 因此本章内容主要分享第三方抓包网卡Netgear A6210的安装方式以及采集无线空口抓包软件omnipee

k的操作方法。



无线终端与AP之间复现问题时,插有无线抓包网卡Netgear A6210的PC使用omnipeek空口抓包软件抓包

1. Netgear A6210的安装方式

1.1 Netgear A6210及驱动 Netgear A6210网卡:



随着无线网络的发展,目前支持802.11ac协议的AP和无线终端已经普及,在处理无线问题涉及到802. 11ac时,相应的抓包网卡也需要支持802.11ac协议才能采集到空口的报文交互。 该款网卡支持802.11ac协议,因此该款网卡嗅探模式时,支持抓取802.11ac协议报文交互过程。 驱动下载: DMP上下载网卡sniffer模式驱动,网卡直接插上电脑时为普通无线网卡接入模式,安装sniffer嗅探模式 驱动才可用来抓包。驱动下载见附件或下方链接: 技术支持中心→01-IP网络产品→20-无线产品→19-相关软件 →Ralink_Wireless_USB_Driver_v5.1.12.48.zip 1.2 Netgear A6210驱动安装指导: PC上插上USB无线网卡,打开设备管理器中A2610,右键选择"更新驱动程序软件",选择"浏览计算机 以查找驱动程序软件",浏览到响应的驱动程序安装即可。





安装完成后,点击无线网卡可以看到一个新添加的网卡显示为"sniffer mode"即为驱动安装成功,某些系统安装完成后未显示"sniffer mode"可以尝试重启电脑。

当前连接到:	47
h3croot.huawei-3co 无 Internet 访问	om.com
拨号和 VPN	^
宽带连接	
无线网络连接 4	•
无线网络连接 7	~
~Sniffer Mode~	×
打开网络和共享	中心

2. omnipeek抓包软件操作方法

1.1 omnipeek下载安装:

以前11n时代使用的omnipeek抓包软件版本为75,需要抓取11ac协议的报文交互不仅需要网卡的支持,同样需要抓包软件支持。目前支持抓取11ac协议的omnipeek抓包软件版本为81。

软件下载路径以及安装方法参考DMP上: 技术支持中心→01-IP网络产品→20-无线产品→19-相关软件 1.2 omnipeek空口抓包方法:

打开omnipeek 81版本,选择"New Capture"弹出对话框,选择左侧"Adapter"查看抓包网卡是否已识别

,有红色标记的网卡即为已识别的抓包网卡。



选择左侧"802.11"设置抓包的信道,在空口抓包过程中,网卡只能抓取指定信道的报文,因此需预先查看AP的信道,然后设置需要抓包的信道。

General	802.11			
Adapter 802.11 Hardware Profiles Triggers Filters Statistics Output Analysis Options	Select channel wumber: Scan: Encryptic Key	$ \begin{bmatrix} 1 & - 2412 & MHz & (bgn) \\ 1 & - 2412 & MHz & (n40h) \\ 2 & - 2411' & MHz & (bgn) \\ 2 & - 241' & MHz & (bgn) \\ 2 & - 242' & MHz & (n40h) \\ 3 & - 2432' & MHz & (n40h) \\ 4 & - 243'' & MHz & (n40h) \\ 4 & - 243'' & MHz & (n40h) \\ 5 & - 2432' & MHz & (n40h) \\ 5 & - 2442' & MHz & (n40h) \\ 6 & - 2443'' & MHz & (n40h) \\ 6 & - 2443'' & MHz & (n40h) \\ 6 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2443'' & MHz & (n40h) \\ 8 & - 2444'' & MHz & (n40h) \\ 9 & - 2445'' & MHz & (n40h) \\ 9 & - 2445'' & MHz & (n40h) \\ 9 & - 2445'' & MHz & (n40h) \\ 10 & - 2445'' & MHz & (n40h) \\ 10 & - 2445'' & MHz & (n40h) \\ 10 & - 2445'' & MHz & (n40h) \\ 10 & - 2452'' & MHz & (n40h) \\ 10 & - 2452'' & MHz & (n40h) \\ 10 & - 2452'' & MHz & (n40h) \\ 10 & - 2452''' & MHz & (n40h) \\ 10 & - 2452'''''''''''''''''''''''''''''''''''$	<u>N</u>	

设置完成后,点击"确认",即跳转到抓包界面,点击"Start Capture"按钮即开始抓包。

Packets received: Packets filtered:	0 0	Buffer usage: 0% Filter state: 🖛	Accept all packets				Start	Capture
🕈 🌱 🕶 Enter a f	ilter expression	here (use F1 for hel	.p)					
Dashboards 🔺		0x 🔄 🔍 🗞	9-183	9 🖉 🖉				
Voice & Video Apdex	Packet	Relative Tim	e Source		Destination	BSSID	Flags	Channel
Compass Capture			The	ere are no iter	ns to show in this	view.		
Packets Log Filters								
Expert Clients/Server								
Flows Applications								
Web								
Servers Clients								
Pequeste								
Voice & Video Calls								
Visuals Peer Map								
Graphs								
Statistics								
Summary					_			
Protocols	((III						+
Wireless								
WLAN Channels Signal								
Idle	1				一 无线网络连接 7	Packets: 0	Duration: 0):00:00

复现问题后,停止抓包,点击"Stop Capture"停止抓包,再进一步对抓取报文进行分析。

Dashboards						_	10
Network			7 • \$ \$ \$ \$ ¥ \$			-	
Voice & Video	Packet	Relative Time	Source	Destination	BSSID	Flags	Chann
Apdex	1	0.000000	TE:50:49:21:15:D8	80:19:34:27:41:92		#	
Compass	2	0.001091				C	
apture	3	0.003532	DC:53:60:DE:48:DD	Mcast IP IANA802	HangzhouH3:A9:4B:D0	CW	
 Packets 	4	0.003793	DC:53:60:DE:48:DD	Mcast IP IANA802	HangzhouH3:A9:5B:D0	W	
Log	5	0.005609	HangzhouH3:A9:4B:70	Ethernet Broadcast	HangzhouH3:A9:48:70	*р	
Filters	6	0.006110	HangzhouH3:A9:4B:71	Ethernet Broadcast	HangzhouH3:A9:4B:71	*р	
Expert	7	0.006414	Xerox:00:00:00	BC:62:C9:01:F9:F1	80:86:F2:A3:B3:49	CW+	
Clients/Server	8	0.009905	TE:50:49:21:15:D8	80:19:34:27:41:92		#	
Flows	9	0.009959	B0:19:34:27:41:92	7E:50:49:21:15:D8		#	
Applications	10	0.010058	80:19:34:27:41:92	## 7E:50:49:21:15:D8		#	
Neb	11	0.013504	6A:6E:BA:A9:60:10	Ethernet Broadcast	HangzhouH3:A9:60:10	*PC	
Servers	≡ 12	0.014319	80:19:34:27:41:92	CC:68:85:28:DB:BD	TE:50:49:21:15:D8	CW	
Clients	13	0.014382		80:19:34:27:41:92		#	
Pages	14	0.015087	AC:FD:CE:6C:79:4C	Mcast IP IANA802	HangzhouH3:A9:5B:D0	W	
Requests	15	0.015948	# 70:14:A6:C8:D5:BE	HangzhouH3:A9:61:F1		#1	
/oice & Video	16	0.016227	70:14:A6:C8:D5:BE	HangzhouH3:A9:61:F1		#	
Calls	17	0.016352				CWA	
Media	18	0.016415	AA:10:2A:27:B0:F6	C0:C5:D8:83:BF:6E	80:52:F6:51:BF:C1	CWA	
/isuals	19	0.016831	D3:7F:25:91:EC:D1	EB:5B:D7:F3:D9:A0	EXerox:00:00:00	*C	
Peer Map	20	0.017017	TE:50:49:21:15:D8	80:19:34:27:41:92	100.00	#	
Graphs	21	0.017287	TE:E1:88:76:5E:12	HangzhouH3:A9:61:02		#C	
statistics	22	0.017351	TE:50:49:21:15:D8	80:19:34:27:41:92		#1	
Summary	23	0.017726	TE:50:49:21:15:D8	80:19:34:27:41:92		#1	
Nodes							
Protocols							
Vireless							
WLAN							
-							

1. 抓包网卡需安装指定的sniffer嗅探模式驱动,才可以作为抓包网卡使用,但不是所有网卡都可以安装sniffer驱动来抓包,目前Netgear A6210可以作为抓包网卡使用。

2. 需要抓取802.11ac协议的报文交互,必须使用支持802.11ac的抓包网卡才可抓取, Netgear A6210 支持802.11ac。

3. 需要抓取802.11ac协议的报文交互, 空口抓包软件omnipeek必须安装81版本。

4. 空口抓包时只能抓取指定信道的报文交互,所以抓包前必须设置需要抓包的信道。

附件下载: Ralink_Wireless_USB_Driver_v5.1.12.48.zip