wlan接入 AP管理 **朱鹏飞** 2023-02-13 发表

组网及说明

1.需求

(1) 空口抓包是定位无线终端问题最有效的手段,但是很多情况下现场并不具备无线空口抓包所需要的外置网卡或者其他抓包工具,问题定位受到很大的限制。

(2) 在AP的Radio接口上开启远程报文捕获功能,将捕获的报文上送到Wireshark软件上解析是一个可选的空口抓包替代办法。

2.组网说明



配置步骤

1. 打开AP报文捕获功能

打开AC的web界面,选择"工具 > 无线报文捕获",选择指定的ap的指定信道,点击开启。报文捕获方式选择"远程报文捕获",RPCAP服务端口号选择默认。设置好以后选择开启,抓包不需要时选择停止捕获。

H3C	WX	2510H-F								
操作		全部网络》工具》无线报文捕获》无线报文捕获								
概览		无线报文捕获								
快速配置	>	Ø								
监控	>	<i>AP </i>	射频模式	信道						
工化和学		wa6528	5GHz(1)	165						
	<i>_</i>	wa6528	2.4GHz(2)	6						
网络安全	>									
系统	>									
工具	•									
无线报文捕获										
RF Ping										
调试		共2条数据,匹配出2条,当前为第1页,共1页	ξ.							

H ₃ C	w	2510H-F				💾 保存 🗳
操作		全部网络〉工具〉无线报文捕获〉	无线报文捕获			
概览		无线报文捕获	无线报文捕获		×	
快速配置	>	C	AP名称	wa6528		查询
监控	>	<i>AP 合称</i> ▲ wa6528	射频	5GHz(1)		最大功率(dBm) 20
无线配置	>	wa6528	报文播获方式 \star	● 远程版文捕获:将捕获的报文发送给Wireshark客户端		20
网络安全	>		RPCAP服务端口号	2002 (1-65535,款省为2	002)	
	~		✓开启 ×取消			
无线报文捕获					- 1	
RF Ping				确定	- 1	
调试		共2条数据,匹配出2条,当			_	

2. 配置Wireshark

1) 在PC上打开Wireshark软件,选择"Capture > Options" (捕获>选项)。

	编辑(<u>E</u>)	视图(⊻)	跳转(<u>G</u>)	捕	夹(<u>C</u>)	分析(<u>A</u>)	统计(<u>S</u>)	电话((<u>Y</u>)	无线(<u>W</u>)	I
Ĩ	۱	à 🗙 🖸	۹ 🗢 🖻	۲	选项	ī(<u>O</u>)	Ctrl	+K			
Ŀ	示过滤器	··· <ctrl< th=""><th>/></th><th>Δ</th><th>开始</th><th>i(<u>S)</u></th><th>Ctrl-</th><th>+E</th><th></th><th></th><th></th></ctrl<>	/>	Δ	开始	i(<u>S)</u>	Ctrl-	+E			
	Time				停止	(T)	Ctrl-	+E		Destinat	tio
.9	2022-11-0	08 16:22: 08 16:22:	:23.140445 :23.140669	6	重新	开始(<u>R</u>)	Ctrl-	⊦R		Google_7 Broadcas	4:a t
1	2022-11-0	8 16:22	:23.140692		捕获	过滤器(<u>F</u>)				Google_7	4:a
i2	2022-11-0	08 16:22: 08 16:22:	:23.140924 :23.141128		刷新	接口列表	F5			Google_7 Google_7	4:a 4:a
4	2022-11-0	8 16:22	:23.141328			NewH3CTe_	a2:d1:44			Google_7	4:a
5	2022-11-0	08 16:22	:23.200776			IntelCor_	93:ca:15			Broadcas	t
6	2022-11-0	08 16:22	:23.253325			IntelCor_	af:f6:a4			Broadcas	t
7	2022-11-0	8 16:22	:23.255572			IntelCor_	af:f6:a4			Broadcas	t
8	2022-11-0	08 16:22	23.255915			NewH3CTe_	a2:d1:40			IntelCor	_af

2) 选择"管理接口 (Manage Interface) > 远程接口"。

002/112/11110	401017071											
) 分析(<u>A</u>) 统计(<u>S</u>)	电话(Y)	无线(W) 工具	(T) 帮助(H)								
** * *	🔬 📃 📃 🔍 🔍 🤄	A III										
140445 140665 140692 140924	Source NewH3CTe_a2:d1:40 intelCor_de:81:68 NewH3CTe_a2:d1:41 NewH3CTe_a2:d1:41		Destination Google_74:a8 Broadcast Google_74:a8	Protoc: Ler 802.11 802.11 802.11	ngti Da BSS 273 3c:d 168 ff:f 255 3c:d	I: Info 2 Probe Resp 4 Probe Requ 2 Probe Resp	onse, SN=0, FN=0 est, SN=1867, FN onse, SN=0, FN=0	, Flags=, BI =0, Flags=, S , Flags=, BI	=100, SSID="ce SSID="sw103" =100, SSID="st	shi" -portal"		
**112不同 141328下同	版本的Wite	shark	软件, 其	「界面」	支持的	先项以	及选项放	置的位置,	可能存	在差异,	`请	以Wireshar
繁化实	际情况为	input 佳。 接	输出 选项 □			流量		链路层	混杂	捕获长盾螺へ		
255915 22142不同 256365	AGADAPX NewH3CTe_a2:d1:4	报文	設力能	的支持	性存在	差异,	请以实际	示设 篇为准。	V	默认 2 默认 2		
2000mm要 2000mm要	捕获报文白	匀AP畫	為這程	殳备路	由可达	,端口	畅通。	Ethernet	V	默认 2 默认 2		
426664	46:f3:d4:0d:70:7	> WI	.AN teiteiteiteiteiteiteiteiteiteiteiteiteit				-	Ethernet		新込 2		
426777 427932	NewH3CTe_a2:d1:4 NewH3CTe_a2:d1:4	> U	た网				_	Ethernet		默认 2		
427240	NewH3CTe_a2:d1:4	> iNe	ode VPN				-	Ethernet		默认 2		
427453 427669 446701	NewH3CTe_a2:d1:4 NewH3CTe_a2:d1:4 46:f3:d4:0d:70:7	> Ad	apter for loopb BPcap1	ack traffic ca	apture		-	BSD loopback USBPcap	\checkmark	默认 2 ─ ─ ─ >		
446767	NewH3CTe_a2:d1:4	<								,	-	
446989	NewH3CTe_a2:d1:4	🗹 在所有	接口上使用混杂	横式					Manag	e Interfaces…		
(2056 bits),	257 bytes captured	Capture f	ilter for sele	cted interfa	ices: 📕 输/	、捕获过滤器				Compile BPFs		
Flags:								开始	Close	Help		
ment			0050 67 81 0050 24 86 0070 00 00 0050 00 00 0050 00 00 0050 00 00 0050 00 00 0050 00 00 0050 00 00 0050 00 00 0050 00 00	88 8c 12 98 24 1 14 95 85 14 89 2 80 80 80 80 80 80 80 54 16 45 86 8 80 80 80 80 80 8 4f 90 90 c0 85 8 81 81 88 80 80 81	48 60 6C 07 11 10 00 00 00 00 10 00 00 00 00 00 00 10 00 <td>83 43 40 28 g ## ## ## ## ## ## 80 00 00 00 ## ## 80 00 00 00 ##<td></td><td></td><td></td><td></td><td></td><td></td></td>	83 43 40 28 g ## ## ## ## ## ## 80 00 00 00 ## ## 80 00 00 00 ## <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						

3) 选择目标远程接口,如果没有,选择新增,输入AP的IP地址(该地址必须和Wireshark路由可达) 和绑定的RPCAP服务端口号2002



▲ 管理接口		×	
本地接口 管道 远程接口 显示 主机/设备 URL ▼ 192.168.137.12 ✓ rpcap://192.168.137.12:2002/WLA	 远程接口 × 机: 		
+ -		远程设置	
这个版本的 Wireshark 无法保存远端设置。	OK	Cancel Help	

4) 设置好接口以后,可以选择捕获报文。此时在报文捕获窗口可看到捕获到的报文。