无线AP远程抓包（报文捕获）方法

wlan接入 AP管理 朱鹏飞 2023-02-13 发表

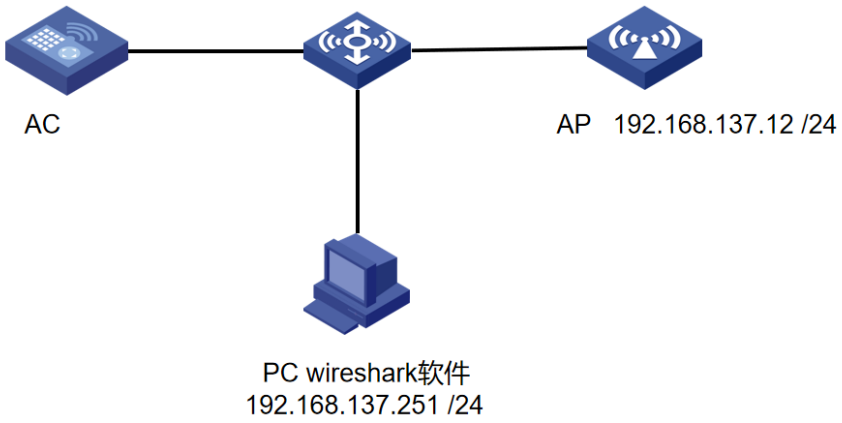
组网及说明

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。

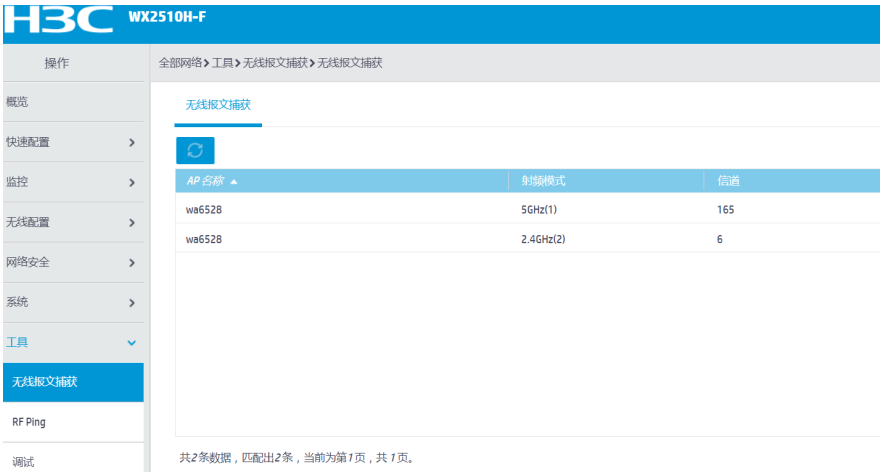
2.组网说明

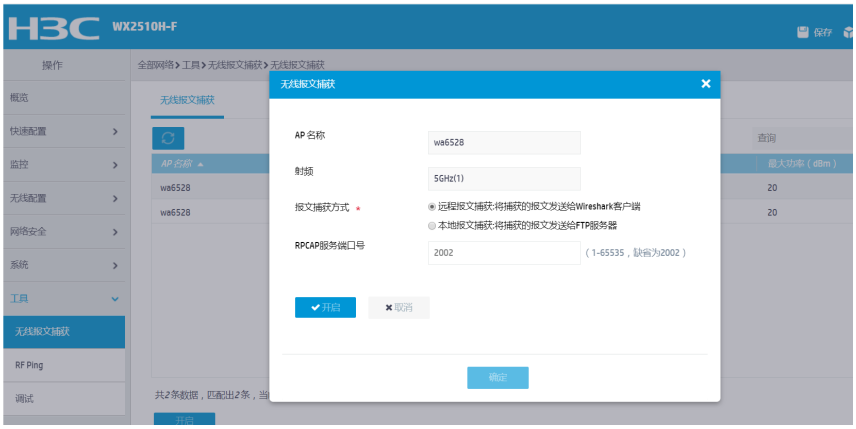


配置步骤

1. 打开AP报文捕获功能

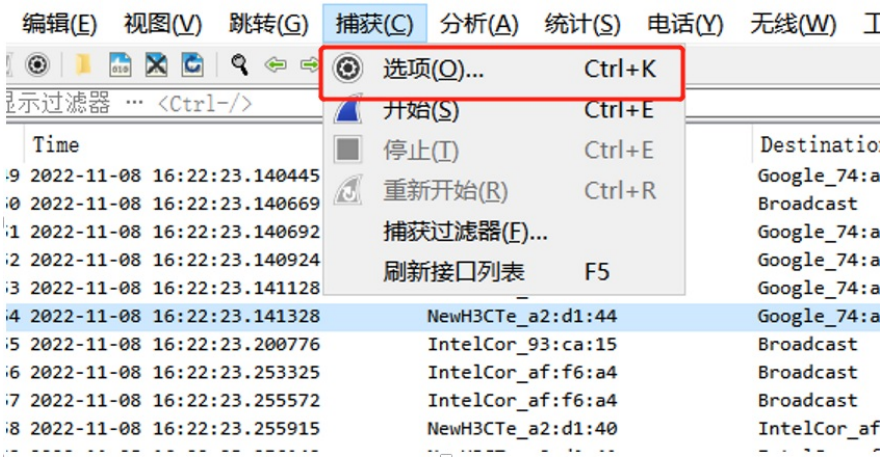
打开AC的web界面，选择“工具 > 无线报文捕获”，选择指定的ap的指定信道，点击开启。报文捕获方式选择“远程报文捕获”，RPCAP服务端口号选择默认。设置好以后选择开启，抓包不需要时选择停止捕获。



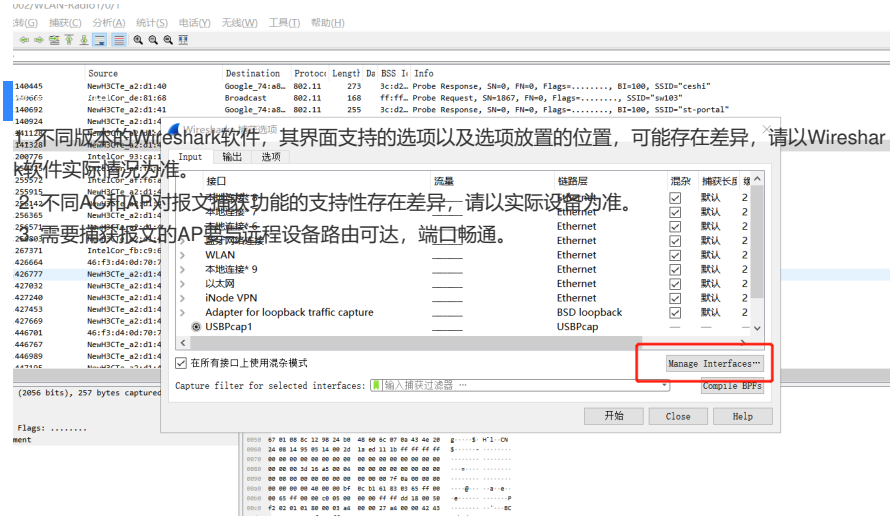


2. 配置Wireshark

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



2) 选择“管理接口（Manage Interface）> 远程接口”。

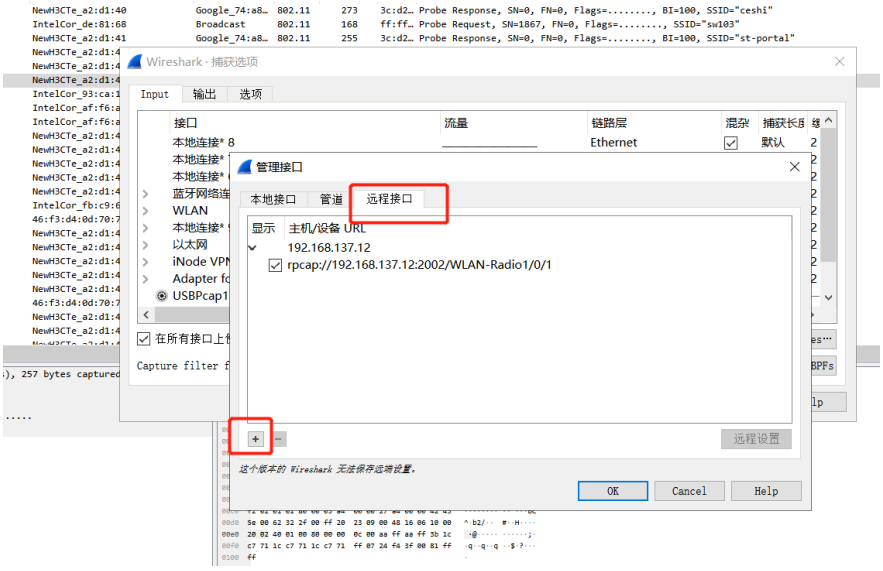


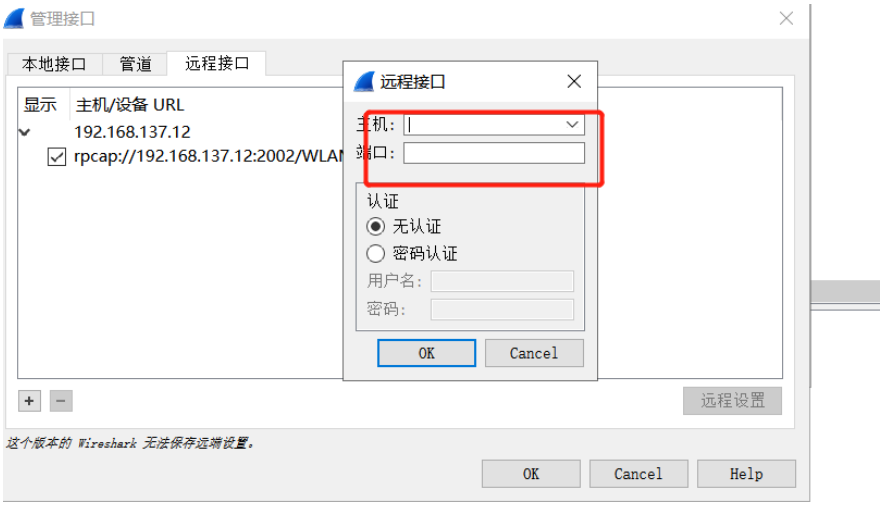
1.不同版本的Wireshark软件，其界面支持的选项以及选项放置的位置，可能存在差异，请以Wireshark软件实际情况为准。

2.不同AC和AP对报文捕获功能的支持性存在差异，请以实际设备为准。

3.需要捕获报文的AP要与远程设备路由可达，端口畅通。

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





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。