怎么抓取数据包

一、在话机上抓取话机收发的数据包

步骤如下：

1、 在浏览器中输入话机的 IP 地址，登陆话机的 web 界面，

2、找到对应的抓包功能界面：

C 系列、Android 系列：管理设置 -- 系统日志 -- 网页抓包。

X 系列的话：系统 -- 辅助工具 -- 网络报文撷取。

3、点击**“开始”**按钮，提示保存“xxx.pcap”文件，请保存文件。

4、重新执行问题出现的动作，直到问题出现。

备注：网页操作中，有的浏览器在步骤 3 就无法操作了，可以按 F5 刷新页面再操作，不会影响抓包。不过在步骤 5 前要再按下“开始”按钮，然后开始步骤 5 的操作

5、问题重现完成之后，点击网页上的**“停止”**按钮，抓取数据包结束。

提示：标准使用的浏览器是 chrome，老的话机版本可能没有兼容 chrome 最新版本，导致不能下载数据包，这种情况下建议切换火狐以及其他浏览器另获取抓包

说明：在步骤 3 或步骤 5 中保存的“xxx.pcap”文件就是抓到的数据包，这里含有问题发生的信息。整理好抓包和说明后，发给技术去分析确认。有对应交接的技术时，直接发给对应的技术人员，若没有的话，可以发送到 support@fanvil.com

二、通过 PC 端的 wireshark 抓包

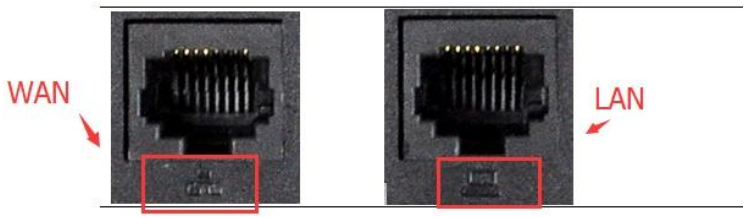
在特殊的情况下，话机端 web 不方便抓包的情况，可以使用 PC 端的软件 wireshark 抓包。

提示：Wireshark 软件可以直接在百度中搜索下载，以下简单介绍如何使用安装在 PC 端的 Wireshark 2.2.1.0 来抓取话机的网络数据，

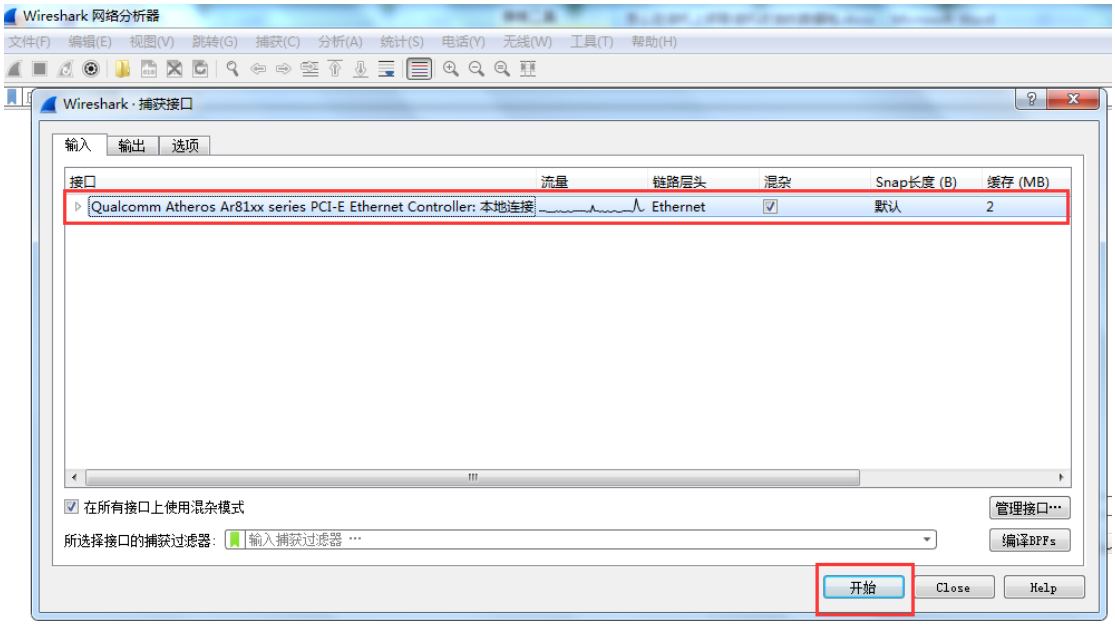
网络连接方式有 2 种，选择其中一种：

1、若是有 hub 的话，将话机的 wan 口、PC 网口都接在 hub 下就可以了。

2、PC 网口接在话机的 LAN 口，话机的 WAN 口接交换机或是路由器下



打开 Wireshark 抓包工具，选择本地的端口，键盘上按下 Ctrl+K，打开【wireshark-捕获接口】页面，选择抓包网卡，点击【开始】按钮开始抓包。



(2)　　键盘上按下 Ctrl+E 选择终止抓包，按下 Ctrl+S 保存刚才抓取到的数据报文到本地。若确认可以正常抓包并保存后，再次再按 Ctrl+E 正式开始抓包。
(3)重现故障的现象。比如说无法获取到 IP，从话机上电前就可以开始抓包了，直到启动 2 分钟后
（4）键盘上按下 Ctrl+E 选择终止抓包，按下 Ctrl+S 保存刚才抓取到的数据报文到本地，重命名为方便标示的文件名，命名规则建议为型号+故障问题，例如“X4-注册不上.pcap”。

提示：
1、抓包技巧：关键是要将异常现象的整个过程抓捕下来。如网页打不开，先打开抓包软件开始抓包，再尝试访问某个固定的网页两次，复现故障现象，然后再终止抓包，并将获取到的数据报文保存或提供技术工程师分析。
2、抓包命名：最好将抓包进行重命名，命名规则建议为型号+故障问题，例如“X3S-DHCP 获取不到 IP.pcap”，这样方便分析更快判断问题
3、备注说明:抓包发给技术人员时，最好能另备注说明下如下情况
（1）设备的型号、版本、IP，是否是定制版本
（2）网络环境结构：服务器在哪里？什么设备？IP 是什么？是在内网还是外网？
（3）是否可以重现现象，怎么样操作会出现？
（4）是否有测试账号，若是有，请一并提供给我们验证
（5）其他需要说明和备注的情况

发送技术分析：整理好抓包和说明后，就可以发给技术去分析确认。有对应交接的技术时，直接发给对应的技术人员，若没有的话，可以发送到 support@fanvil.com