Wireshark软件缓存大量报文优化方式

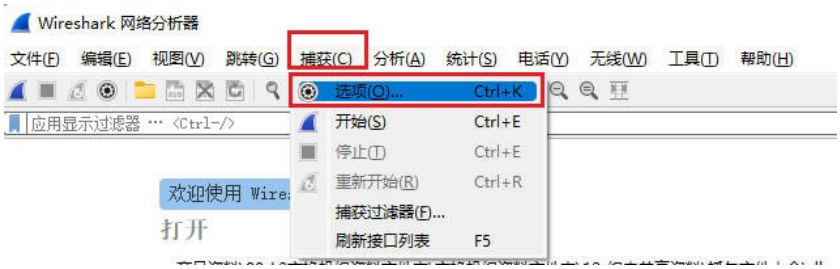
配置优化 镜像 丁犁 2022-07-27 发表

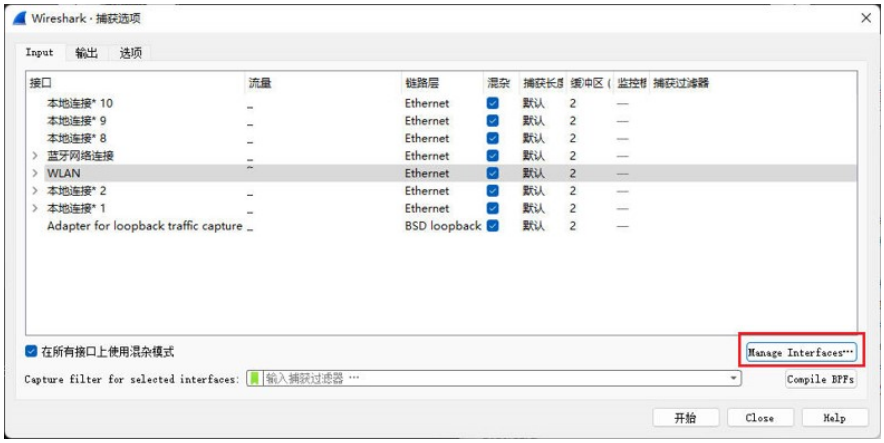
组网及说明

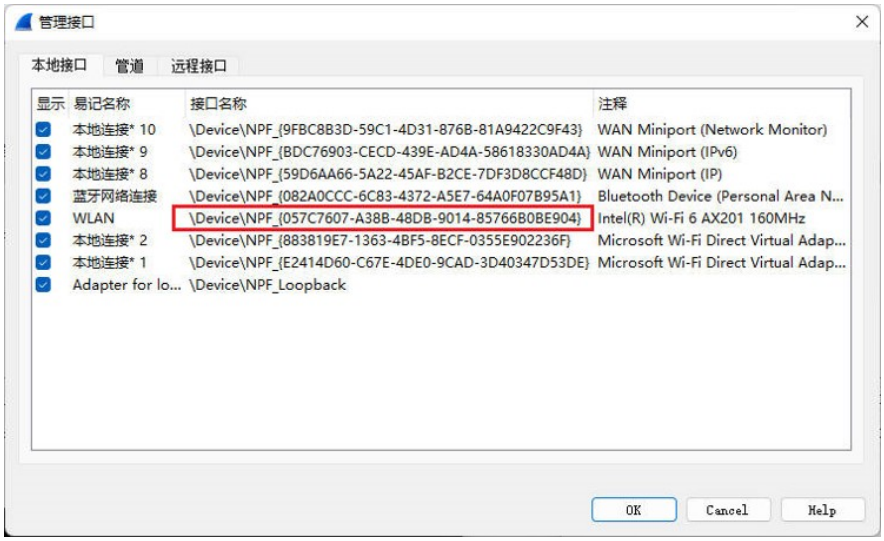
当需要使用Wireshark长时间抓包或抓取的数据流量过大时，可以使用Wireshark命令行抓包方法，将报文直接缓存到本地硬盘中。

配置步骤

① 在Wireshark图形化界面查找到网卡信息：







② 在命令提示符下切 换 到 Wireshark 安装目录， 使用命令 dumpcap.exe -i \Device\NPF_{70F4F310-5321-40D2-93A9- DFD0D1ED319D} -w d:test.pcap -b filesize:500 可直接进行抓包并保持 到本地D盘中，其中：

-i: 后面接的是网卡信息。

-w: 后面接的是保存的数据包路径和文件名。

-b: 后面接的是每个文件的大小，500单位是KB，即5M，每5M保 存为一个文件，多个文件命名方式是“指定的文件名_序号_日期时间.扩展名”。

举例如下：


名称
dfilters
dftest.exe
dumpcap.exe 属性
常规
兼容性
数字签名
安全
详细信息
以前的版本