

利用 IfferPro 彻底解决 IP 被盗用问题 PDF 转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/264/2021_2022__E5_88_A9_E7_94_A8_iff_c67_264850.htm 在公司中，经常有一些事情令网管很头痛，IP 地址被非法用户盗用更是头痛。为了找到是哪台机器盗用了 IP 地址，一般可以采用如下方法：

1. 首先登记所有机器的网卡物理地址，即网卡的 MAC 地址。
2. 以后如果发现 IP 地址被盗用，先使用 Ping 命令 Ping 相应的 IP 地址。
3. 然后用 Arp -a 命令查看当前的 Arp 解析表，从中获得对方网卡的 MAC 地址。
4. 检查网卡 MAC 地址列表，确定机器位置。

但随着网络蠕虫病毒的流行和网络攻击的增多，许多计算机上都安装了防火墙软件，从而使得单纯的 Ping 命令失效。如果盗用 IP 的这台机器安装了防火墙软件并且把所有端口都关闭的话，这台机器就仿佛从网络上消失了一样，你无法用正常的方法去访问到它，从而也就无法知道它的具体位置。解决问题的思路：用户使用网络，访问网络上的资源，就势必会在网络上传输数据。如果我们能够监听到这些数据并对它进行分析的话，就有可能找出特定用户的位置。解决方案：经过对各种方法的测试，笔者发现有一种方法可以在机器安装了防火墙的情况下依然可以探测到它的存在并且查到它的网卡 MAC 地址，从而确定它的物理位置。首先安装 Sniffer Pro，它是一个网络监测软件，可以监测到网络上流动的数据，安装好后运行该软件，单击工具条最左边的“开始”按钮，启动探测功能。此时屏幕上会出现一个窗口，显示当前发现的机器列表和相应的参数，其中有一项“DLC Station”指的就是机器网卡的 MAC 地址，如图所示：Sniffer Pro 的 Expert

对话框 找到被盗用的IP地址所对应的网卡MAC地址，就可以顺藤摸瓜查到这台机器究竟是哪台了。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com