网吧频繁掉线（ARP）与快速解决方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E7_BD_91_E5_90_A7_E9_A2_91_E7_c101_181842.htm 现在频繁掉线的网吧很多。但为何掉线。许多网管朋友。不是很清楚。网吧掉线的原因很多。现在我给大家讲一下现在很流行的一种木马。.基本上东北地区的网吧都被这一木马弄的身心疲惫。但是现在有解决的方法了。 中病毒特征 网吧不定时的掉线。（重启路由后正常），网吧局域网内有个别机器掉线。 木马分析：传奇杀手木马，是通过ARP欺骗，来或取局域网内发往外网的数据。从而截获局域内一些网游的用户名和密码。 木马解析 中木马的机器能虚拟出一个路由器的MAC地址和路由器的IP.当病毒发作时，局域网内就会多出一个路由器的MAC地址。内网在发往外网的数据时，误认为中木马的机器是路由器，从而把这些数据发给了虚拟的路由器。真正路由器的MAC地址被占用。内网的数据发出不去。所以就掉线了。 解决办法 首先你下载一个网络执法官，他可以监控局域网内所有机器的MAC地址和局域网内的IP地址。在设置网络执法官时。你必须将网络执法官的IP段设置和你内网的IP段一样。比如说：你的内网IP是192.168.1.1192.168.1.254你的设置时也要设置192.168.1.1192.168.1.254.设置完后，你就会看到你的内网中的MAC地址和IP地址。从而可以看出哪台机器中了木马。（在多出的路由器MAC地址和IP地址和内网机器的IP地址，MAC地址一样的说明中了传奇网吧杀手）要是不知道路由器的MAC地址，在路由器的设置界面可以看到。发现木马后。你还要下载瑞星2006最新版的杀病毒软件（3月15日之后的

病毒库）。在下载完之后必须在安全模式下查杀（这是瑞星反病毒专家的见意）反复查杀（一般在四次就可以了）注意查完后杀病毒软件不要卸载掉。观查几天（这是我个人的经验。在卸后第三天病毒还会死灰复燃，我想可能是注册表里还有他的隐藏文件。在观查几天后正常就可以卸载掉了。 注：还原精灵和冰点对网吧传奇杀手木马不起做用。（传奇杀手木马不会感染局域网。不要用硬盘对克，对克跟本不起任何做用。而且还会感染到母盘上。切记！） 最好主机安装上网络执法官，这样可以时时监控局域网内的动态，发现木马后可以及时做出对策） 面是传奇网吧杀手木马的文件： 文件名： 文件路径： 病毒名： a.exe>>b.exe c：\windows\system32 Trojan.psw.lmir.jbg 235780.dll c：\windows\ Trojan.psw.lmir.aji kb2357801.log c：\windows\ Trojan.psw.lmir.jhe Q98882.log c：\windows\ Trojan.psw.lmir.jhe kb2357802.log c：\windows\ Trojan.psw.lmir.jbg Q90979.log c：\windows\ Trojan.psw.lmir.jhe Q99418.log c：\windows\ Trojan.psw.lmir.jbg ZT.exe c：\windows\program Files\浩方对战平台 病毒名：Trojan.dL.agent.eqv a[1].exe>>b.exec：\documents and sttings\sicent\local settings\Temporary Internet Files\content.IE5\Q5g5g3uj 病毒名：Trojan.psw.lmir.jbg 有需要瑞星2006 18.18.22（3月15日的版本）和网络执法官2.75注册版的软件请把邮箱留下。 （各位朋友。瑞星杀毒软件文件过大邮箱发送不了。请大家下载瑞星个人18.18.20版杀毒软件我现在给大家提供注册码。希望大家原谅。） SN=P5V6EH-61FHJK-9G0SS7-C4D200 ID=5B3C5BJ4Y125 （网络执法官可以批量MAC捆绑，到执法官的局域网MAC界面，

全选后单击右键会出现批量MAC捆绑。做完捆绑以后，ARP要是在次攻击时他会报警，出现的假MAC是为非法。网络执法官会终止他的一切操作。）这样可以解决ARP在次攻击。