路由器频繁掉线怎么办？ PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/293/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E9_c101_293913.htm 伴随着局域网规模的逐步扩大，以及用户上网需求的不断提高，局域网中有限的带宽资源正变得越来越紧张，而路由器频繁掉线现象也就会随之变得象家常便饭一样平常了。很显然，路由器频繁掉线会严重影响局域网上网效率，为了有效提高上网效率，我们除了要更换高档次的路由器设备来提高网络处理能力和速度外，还需要从路由器设置出发，来增强路由器的工作稳定性！ 巧用ACL功能，远离病毒攻击 现在的网络病毒可谓随处可见，它们的攻击力之强、破坏力之大，足以让任何人对它敬而远之。不过，任何一种网络病毒都是借助网络通道进行传输、扩散的，它的数据报文也是按照TCP/IP协议标准进行通信传输的，因此每一个病毒数据包都包含目的IP地址、源IP地址，同时包含目的传输端口、源传输端口，类型相同的网络病毒所使用的目的传输端口一般都是相同的，比方说震荡波病毒全部使用445端口、冲击波病毒全部使用135端口等.如果我们想办法在路由器的后台管理界面中对这些病毒通信端口进行适当的限制，那么来自Internet网络的一些病毒就不会通过路由器，进入到单位局域网网络了，如此一来局域网中的所有工作站包括路由器设备遭受到病毒攻击的可能性就大大降低了。 要让路由器远离病毒攻击，我们可以巧妙地利用路由器设备自带的ACL功能，来对特定网络端口的数据网络报文进行限制，我们既可以对局域网内部通信接口的数据报文进行过滤，也可以对外部通信接口的数据报文进行过

滤，这么一来就能确保网络病毒的数据报文不会消耗路由器设备的系统资源，同时也不会消耗有限的网络带宽资源，那样的话路由器设备出现掉线的机率就会大大降低。 限制NAT链接，谨防资源耗尽 一般来说，单位局域网中包含的工作站数量少则几十台，多则几百台，而本地ISP服务商由于手头的IP地址资源本就非常有限，他们通常只会给单位局域网分配一到两个公网IP地址，这么少的IP地址显然是不够分配的，那么我们如何利用这一到两个公网IP地址让局域网中的所有工作站都能接入到Internet网络中呢?其实很简单，我们只要善于使用路由器设备的NAT功能就可以了。当局域网中的内部工作站要访问Internet网络中的资源时，我们可以在路由器设备的后台管理界面创建一个对应列表，这个列表中包含的信息有内部工作站的IP地址、外部目标网站IP地址、内部网络通信端口、外部网站的通信端口等，局域网用户每一次的网络访问操作都会自动在路由器设备的后台创建对应关系列表，要是列表中的网络链接记录有数据在传输，那么这些列表记录将会一直存储在路由器设备中，一旦某个网络链接项目没有数据在传输时，那么要不了多长时间该链接记录就会自动消失。 倘若局域网中的某台工作站不幸感染了某种特殊网络病毒，该病毒可能在短暂的时间内，向路由器设备同时连续发出成千上万个针对不同目标工作站的网络链接请求，如此一来路由器设备就必须腾出适当的系统资源来为这些成千上万个链接请求创建对应列表。而路由器设备本身能够支持的NAT网络链接数量是十分有限的，要是这些链接资源全部被网络病毒给占用的话，那么局域网中的其他用户再尝试通过路由器设备访问外部网络时，路由器设备就无法腾出有

效的NAT链接资源给其他工作站了，那么其他工作站自然就会发生无法访问网络的故障，这种上网掉线故障事实上就是由于网络病毒耗尽NAT资源引起的。 为了避免由NAT资源耗尽引起的路由器掉线故障，我们可以进入到路由器设备的后台管理界面，将其中的NAT网络链接数量设置到最大数值(当然这需要路由器设备在自身性能方面能够承受)，如果路由器设备自身性能有限的话，我们必须对NAT网络链接数量进行适当限制，采取的限制措施既可以针对局域网中的所有工作站，也可以只针对其中的某一台工作站。当然，要是我们从路由器设备的后台管理界面中，看到来自内网某台工作站的NAT网络链接数量比较多时，我们不妨尝试断开那台内网工作站，然后再进行网络访问测试，看看路由器设备是否还会继续发生频繁掉线故障，要是掉线故障现象立即就消失了的话，那就说明那台内网工作站感染了病毒，此时我们只要对那台特定的内网工作站执行病毒查杀操作就可以了。 预防ping攻击，避免系统拖跨 为了测试某个网站的连通性，相信多数朋友都会使用Ping命令，来对目标网站执行Ping测试操作，而目标网站接受到工作站的Ping连接请求后，往往需要腾出一定的系统资源来应答这个请求.同样地，如果目标网站同时接收到大量的Ping测试请求，那么目标工作站就需要耗费更多的系统资源进行应答，而在此刻如果有用户在尝试访问该目标网站时，那么该网站系统可能就腾不出系统资源进行及时应答这个用户的上网请求了，所以该用户也就会遇到上网掉线故障了。 而网络病毒或黑客在对目标网络或设备发动攻击之前，往往要对目标网络中的各个工作站地址进行依次Ping扫描，如果某个网络设备或工作站进行了应答，那说

明该网络设备或主机是可以攻击的，于是病毒或木马就会对目标主机发动Ping攻击，直到把目标主机系统拖跨为止。 为了避免路由器设备遭受ping攻击，从而导致路由器无法正常处理上网请求，我们可以对路由器设备的WAN端口进行设置，启用防Ping功能，以便阻止来自外部网络的数据包对路由器执行ping攻击，这么一来路由器设备日后对所有来自外部网络的ping数据请求都作弃权处理，那样的话路由器设备不但不会暴露自己，而且还能预防ping攻击，从而保证路由器设备能够安全、稳定地工作。 合适分配带宽，有效限制速度我们知道，现在的局域网出口带宽多数都是2MB或10MB标准，每一台工作站所能享受到的带宽资源平均为100KB左右，在这种上网环境中，要是有几台工作站同时进行BT下载，那么局域网中有限的出口带宽资源很快就会被挥霍一空，那么其他人再尝试上网时，就会明显感觉到网络访问速度缓慢，甚至会频繁发生掉线故障。 为了让路由器设备远离由带宽没有限制引起的掉线现象，我们可以进入到路由器设备的后台管理界面，对所有工作站的出口带宽速度进行合适限制，以避免某几台工作站过度消耗局域网的有限带宽资源。当然，我们也可以在局域网工作站中，对信息上传速度和信息下载速度进行限制，确保网络带宽资源不会被非法使用。 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