网管经验：从sniffer下手揪出ARP病毒 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_AE_A1_E7_BB_8F_E9_c101_644684.htm ARP欺骗病毒是目前最让企业网络管理员头疼的病毒，他的特点就是隐蔽性强，一台机器感染后全网段机器都受影响，故障一样。所以很难找出真正的病毒来源。在实际维护过程中笔者发现即使ARP病毒发作后我们也可以通过sniffer工具这个放大镜来找出真凶。下面笔者就以一次个人查杀arp病毒的经历为例向各位IT168的读者介绍如何从sniffer下手揪出ARP病毒。 一，ARP欺骗病毒发作迹象： 一般来说ARP欺骗病毒发作主要有以下几个特点，首先网络速度变得非常缓慢，部分计算机能够正常上网，但是会出现偶尔丢包的现象。例如ping网关丢包。而其他大部分计算机是不能够正常上网的，掉包现象严重。但是这些不能上网的计算机过一段时间又能够自动连上。ping网关地址会发现延迟波动比较大。另外即使可以正常上网，象诸如邮箱，论坛等功能的使用依然出现无法正常登录的问题。 二，确认ARP欺骗病毒发作： 当我们企业网络中出现了和上面描述类似的现象时就需要我们在本机通过arp显示指令来确认病毒的发作了。 第一步：通过“ 开始- 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