网管经验：从sniffer下手揪出ARP病毒思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/629/2021_2022__E7_BD_91_E7_AE_A1_E7_BB_8F_E9_c101_629036.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-&gt.运行 ”，输入CMD指令后回车。这样我们将进入命令提示窗口。第二步：在命令提示窗口中我们输入ARP -A命令来查询本地计算机的ARP缓存信息。在显示列表中的physical address列就是某IP对应的MAC地址了。如果企业没有进行任何MAC与IP地址绑定工作的话，ARP模式列显示的都是dynamic动态获得。当我们发现arp -a指令执行后显示信息网关地址对应的MAC

地址和正确的不同时就可以百分之百的确定ARP欺骗病毒已经在网络内发作了。例如正常情况下笔者网络内网关地址192.168.2.1对应的MAC地址是00-10-5C-AC-3D-0A，然而执行后却发现192.168.2.1对应的MAC地址为00-10-5c-ac-31-b6。网关地址MAC信息错误或变化确认是ARP病毒造成的。（如图1） 第三步：我们用笔将错误的MAC地址记录下来，为日后通过sniffer排查做准备。 接下来我们就应该利用sniffer这个强大的工具来找出病毒根源了。 