案例分析－江苏省某中学网络故障诊断 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E6_A1_88_E4_BE_8B_E5_88_86_E6_c101_142896.htm 一、故障描述故障地点：江苏省某中学校园网故障现象：严重网络阻塞，客户机之间相互ping时严重丢包，校园网用户访问互联网的速度非常慢，甚至不能访问。故障详细描述：整个校园网突然出现网络通讯中断，内部用户均不能正常访问互联网，在机房中进行ping包测试时发现，中心机房客户机对中心交换机管理地址的ping包响应时间较长且出现随机性丢包，主机房客户机对二级交换机通讯的通讯丢包情况更加严重。二、故障详细分析1.前期分析初步判断引起问题的原因可能是：交换机ARP表更新问题 广播或路由环路故障 &#61548. 病毒攻击需要进一步获取的信息：ARP信息 交换机负载 网络中传输的原始数据包2.故障具体分析排查开始实际具体排查工作：1.在主机房的客户机和以下的客户机上分别使用“ arp a ”命令查看ARP缓存信息，结果正常；2.登录中心交换机查看各端口的流量，由于交换机反应速度较慢，操作超时，无法获得负载的实际流量；3.使用科来网络分析系统5.0捕获并分析网络中传输的数据包，具体过程如下。 在中心交换机上做好端口镜像配置操作，并将分析用笔记本接到此端口上，启动科来网络分析系统5.0捕获分析网络的数据通讯，约2.5分钟后停止捕获并分析捕获到的数据包。 XX中学校园网的主机约为1000台，一般情况下，同时在线的有600台左右。在停止捕获后，我们在科来网络分析系统5.0主界面左边的节点浏览器中发现，内部网络（Private-Use Networks）同时在线的IP主机达到

了6515台，如图1，这表示网络存在许多伪造的IP主机，网络中可能存在伪造IP地址攻击或自动扫描攻击。选择连接视图，发现在约2.5分钟的时间内网络中共发起了3027个连接，且状态大多都是客户端请求同步，即三次握手的第一步，
由TCP工作原理可知， TCP工作时首先通过三次握手发起连接，如果请求端向不存在的目的端发起了同步请求，由于不会收到目的端主机的确认回复，其状态将会一直处于请求同步直到超时断开，据此，我们现在更加断定校园网中存在自动扫描攻击。 详细查看图1的连接信息，发现这些连接大多都是由192.168.5.119主机发起，即连接的源地址
是192.168.5.119。选中源地址是 192.168.5.119的任意一个连接，单击鼠标右键，在弹出的右键菜单中选择“ 定位浏览器节点>>端点1 IP ”，这时节点浏览器将自动定位到192.168.5.119主机。screen.width*0.7) {this.resized=true.
this.width=screen.width*0.7. this.alt=点击在新窗口查看全图\nCTRL 鼠标滚轮放大或缩小.}" border=0> （图1 网络中的TCP连接信息） 选择图表视图，并选中TCP连接子视图项，查看192.168.5.119主机的TCP连接情况，如图2所示。查看图2可知，192.168.5.119 这台主机在约2.5分钟的时间内发起了2800个连接，且其中有2793个连接都是初始化连接，即同步连接，这表示192.168.5.119主机肯定存在自动扫描攻击。screen.width*0.7) {this.resized=true. this.width=screen.width*0.7. this.alt=点击在新窗口查看全图\nCTRL 鼠标滚轮放大或缩小.}" border=0> （图2 192.168.2.119主机的TCP连接信息） 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