实例剖析：网络环路轻视不得 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_AE_9E_E4_BE_8B_E5_89_96_E6_c101_461678.htm 以太网中的交换机之间存在不恰当的端口相连会造成网络环路，如果相关的交换机没有打开STP功能，这种环路会引发数据包的无休止重复转发，形成广播风暴，从而造成网络故障。我们在校园网的维护过程中多次遇到过这种故障，其中有一次排除故障的过程令我们印象深刻。 故障描述 一天，我们在校园网的网络运行性能监控平台上发现某栋楼的VLAN有问题其接入交换机与校园网的连接中断。检查放置在网络中心的汇聚交换机，测得与之相连的100BASE-FX端口有大量的入流量，而出流量却非常小，显得很不正常。然而这台汇聚交换机的性能似乎还行，感觉不到有什么问题。于是，我们在这台汇聚交换机上镜像这个异常端口，用协议分析工具Sniffer来抓包，最多时每秒钟居然能抓到10万多个。对这些数据包进行简单分析，我们发现其中一些共同特征(如图1所示)。 图1 抓包数据 绝大部分的包长为62字节(加上4字节的差错检测FCS域即为66字节)，TCP状态为SYN。 源IP为其他网段的IP、目的IP均为该楼网段的IP。 尽管源IP地址不同，但源MAC地址却是一样的。 目的IP地址和目的MAC地址与在这台汇聚交换机上绑定该楼VLAN的IP-MAC参数一致。 实际的数据流向(流入)与这些数据包中的源IP地址和目的IP地址所确定的流向(流出)相反。当时，我们急于尽快抢修网络，没去深究这些数据包的特征，只看到第1点就以为网络受到不明来历的Syn Flood攻击，估计是由一种新网络病毒引起，马上把这台汇聚交换机上的该

端口禁用掉，以免造成网络性能的下降。