局域网交换机能够避免病毒高发区吗？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_ti2020/644/2021_2022__E5_B1_80_E5_9F_9F_E7_BD_91_E4_c101_644527.htm 要解决局域网交换机的安全问题，交换机就不能再纯粹完成转发工作了事，如果这些功能转移到交换机上，简化了网络节点的增加、移动和网络变化的操作。 有一定网龄的朋友大概都知道，早期的网络攻击和恶意入侵主要来自外网，而且是少部分学习黑客技术的人所为，因此当时哪怕只是通过一个防火墙简单的封堵一些端口，检测一些特征数据包就能实现内网的安全。 然而，自冲击波病毒开始，病毒在局域网交换机疯狂传播所造成的强大杀伤力开始让用户心惊胆战，之后计算机病毒更是控制住大量的“ 僵尸 ”电脑对特定网站或者服务器发动洪水攻击。 进入2006年，在网吧行业影响最严重的安全问题变成了ARP和DDOS，这些恶意程序不仅巧妙伪装而且无处不在，更严重的是一旦局域网交换机某台计算机感染了病毒，就会造成大量的计算机掉线甚至整个网络陷入瘫痪，令网吧业主和网吧玩家万般无奈，在公司企业内部网络也几乎存在同样的问题，而此时传统的防火墙却显得毫无办法。 局域网也成病毒高发地区 如果是在4年前，局域网还是非常安全的，很多公司也习惯了直接在局域网共享各种常用软件和资料，但是现在为了获得一些非正当的利益，很多病毒开发者打起了局域网交换机的主意：先是由于网游的热火而产生了ARP病毒。 这是一种欺骗性质的病毒，虽然它的目的并不是破坏局域网，但为了达到它盗号盗宝的目的，会严重影响其它局域网用户的正常上网活动。所谓ARP攻击其实就是内网某台主

机伪装成网关，欺骗内网其他主机将所有发往网关的信息发到这台主机上。 但是由于此台主机的数据处理转发能力远远低于网关，所以就会导致大量信息堵塞，网速越来越慢，甚至造成网络瘫痪，而且ARP病毒这样做的目的就是为了截取用户的信息，盗取诸如网络游戏帐号、QQ密码等用户信息，因此它不仅会造成局域网堵塞，也会威胁到局域网交换机用户的信息安全。 接着很多针对特殊服务器或是网游私服的DDOS攻击也开始大举利用网吧或企业网络中的客户机作为“ 僵尸 ”电脑，对指定的服务器IP发送大量的数据包，“ 僵尸 ”电脑越多，服务器被消耗的带宽也越多。 利用这个原理耗尽服务器的带宽，就可以达到让对方服务器掉线以便对服务器运营者进行恶意勒索的目的。这种攻击方式虽然是针对外网服务器，但是它在攻击过程中需要向路由器发送大量的数据包，会直接导致路由器仅有的100M LAN口被“ 堵满 ”，因此其他局域网的计算机的请求无法提交到路由器进行处理，结果就产生局域网计算机全部“ 掉线 ”的现象。 还有一种针对服务器的SYN攻击也会令局域网电脑全体“ 掉线 ”：SYN攻击属于DOS攻击的一种，它利用TCP协议三次握手的等待确认缺陷，通过发送大量的半连接请求，耗费CPU和内存资源。 SYN攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上SYN攻击并不管目标是什么系统，只要这些系统打开TCP服务就可以实施。配合IP欺骗，SYN攻击能达到很好的效果。 通常，感染SYN病毒的客户端在短时间内伪造大量不存在的IP地址，向服务器不断地发送SYN包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造

的SYN包将长时间占用未连接队列，正常的SYN请求被丢弃，目标系统和路由器运行缓慢，严重的时候就直接引起整个局域网交换机的网络堵塞甚至系统瘫痪。 面对日益严重的内网攻击和整网掉线问题，很多路由器和防火墙开发商也在产品中加入了相关技术，例如加入IP-MAC绑定功能可以防止局域网的ARP欺骗，但是这些设备由于以太网工作原理的关系，其实还是无法全面解决内网安全问题。 例如DDOS攻击，虽然路由器和防火墙可以利用一些设定好的规则判断出哪些数据包带有DDOS攻击的特征，但是它必须在收到这些数据包之后才能对数据包进行分析，而这些数据包在收过来的时候其实就已经占用了LAN口的带宽资源。 由于路由器和防火墙都在局域网的最外端，这样的网络结构已经决定了它们无法在攻击数据包产生的时候就进行封堵，而且这些设备大部分还是采用100Mb的带宽与LAN交换机相连。 加上大部分的局域网交换机都是线速转发的二层交换机，受感染客户端发送的大量数据包可以很快用完这些带宽，因此网络数据传输的压力都加载在路由器的LAN端口，这时候很多正常的请求都无法顺利通过LAN口提交过去，因此即使路由器知道哪些是正常的请求也无济于事。 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