

安全第一 第三层交换机预防病毒能力思科认证 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\\_AE\\_89\\_E5\\_85\\_A8\\_E7\\_AC\\_AC\\_E4\\_c101\\_644423.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E5_AE_89_E5_85_A8_E7_AC_AC_E4_c101_644423.htm) 第三层交换机的预防病毒能力也是很强大的，特别是在网络攻击泛滥的今天，保证安全是网络设备最重要的一点。目前计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁.二是对网络中设备的威胁。影响计算机网络的因素很多，主要是网络软件的漏洞和“后门”，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。一些黑客攻入网络内部的事件，这些事件的大部分就是因为安全措施不完善所招致的苦果。软件的“后门”都是软件公司的设计编程人员为了自己方便而设置的，一旦“后门”打开，造成的后果将不堪设想。其实，第三层交换机的安全策略也具备预防病毒的功能。下面我们详细介绍一下如何利用第三层交换机的安全策略预防病毒，计算机网络的安全策略又分为物理安全策略和访问控制策略。

- 1、物理安全策略 物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击.验证用户的身份和使用权限、防止用户越权操作.确保计算机系统有一个良好的电磁兼容工作环境。
- 2、访问控制策略 访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。安全策略分为入网访问控制、网络的权限控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和节点的安全控制等。为各种安全策略必须相互

配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。病毒入侵的主要来源通过软件的“后门”。包过滤设置在网络层，首先应建立一定数量的信息过滤表，信息过滤表是以前收到的数据包头信息为基础而建成的。信息包头含有数据包源IP地址、目的IP地址、传输协议类型(TCP、UDP、ICMP等)、协议源端口号、协议目的端口号、连接请求方向、ICMP报文类型等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问，也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包，无法实施对应用级协议的处理，也无法处理UDP、RPC或动态的协议。根据每个局域网的防病毒要求，建立局域网防病毒控制系统，分别设置有针对性的防病毒策略。划分VLAN 1、基于第三层交换机的虚拟局域网能够为局域网解决冲突域、广播域、带宽问题。可以基于网络层来划分VLAN，有两种方案，一种按协议(如果网络中存在多协议)来划分.另一种是按网络层地址(最常见的是TCP/IP中的子网段地址)来划分。建立VLAN也可使用与管理路由相同的策略。根据IP子网、IPX网络号及其他协议划分VLAN。同一协议的工作站划分为一个VLAN，第三层交换机检查广播帧的以太帧标题域，查看其协议类型，若已存在该协议的VLAN，则加入源端口，否则，创建个新的VLAN。这种方式构成的VLAN，不但大大减少了人工配置VLAN的工作量，同时保证了用户自由地增加、移动和修改。不同VLAN网段上的站点可属于同一VLAN，在不同VLAN上的站点也可在同一物理网段上。利用网络层定义VLAN缺点也是有的。与利用MAC

地址的形式相比，基于网络层的VLAN需要分析各种协议的地址格式并进行相应的转换。因此，使用网络层信息来定义VLAN的第三层交换机要比使用数据链路层信息的第三层交换机在速度上占劣势。

## 2、增强网络的安全性

共享式LAN上的广播必然会产生安全性问题，因为网络上的所有用户都能监测到流经的业务，用户只要插入任一活动端口就可访问网段上的广播包。采用VLAN提供的安全机制，可以限制特定用户的访问，控制广播组的大小和位置，甚至锁定网络成员的MAC地址，这样，就限制了未经安全许可的用户和网络成员对网络的使用。

### 设置访问控制列表

首先根据各单位的需求，制定不同的策略，比如文件的传输、游戏等。在制定策略之前，我们首先要了解什么样的文件依靠计算机上哪个端口来传输。端口大约分为三类：

- 公认端口(01023)：它们紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如：80端口实际上总是HTTP通讯，110端口实际上是pop3通讯。
- 注册端口(102449151)：它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其它目的。例如：许多系统处理动态端口从1024左右开始。
- 动态和/或私有端口(4915265535)：理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外：SUN的RPC端口从32768开始。

编辑特别推荐: IPv6正把互联网拖入更加混乱的时代 IETF认错：不向下兼容是IPv6致命伤 成本速度成关键解析 四种宽带接入技术 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](http://www.100test.com)