如何增强VLAN的安全性 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/250/2021_2022__E5_A6_82_E4_BD_95_E5_A2_9E_E5_c101_250985.htm 千兆以太网技术作为当前的主流局域网技术，已经得到广泛应用。千兆以太网对QoS的保证来源于两个方面：一是标准和协议的制定，如IEEE802.1Q/P、RSVP等；二是第三层交换技术的应用。在QoS的实现策略方面，千兆以太网与ATM一样，也分为4种，即业务分类、排队机制、带宽管理和拥塞控制。 在LAN交换技术中，虚拟局域网（VLAN／L3交换）是一种迅速发展的技术。VLAN／L3交换技术的引入给网络设计、管理和维护带来某些根本性的改变，使得计算机设备的互联和管理不再受地理环境和位置的制约；使网络结构变得灵活、方便、随心所欲。随着VLAN / L3技术的广泛应用，技术人员提出了新的要求： 是否可以基于LAN环境提供某些服务质量（QoS）特性，以实现对VLAN用户流量控制方面的管理呢？ 针对不同网络设备生产厂家的不同产品，具体可以实现的QoS特性会有较大区别。以3Com公司的企业级千兆交换机Switch4007为例，简单讨论基于该型千兆交换机的QoS特性来增强VLAN安全性的实现方法。 制定VLAN之间的访问控制策略 一个典型的校园网环境，一般可以根据不同的业务部门来划分VLAN.我们把所有的外来人员、流动用户或是学生，划到一个独立的VLAN9.出于保护内部网络安全的考虑，我们要限制VLAN9用户对校园网内部其他VLAN的访问，同时允许 VLAN9用户向外的合法访问。基于此，我们制定了如下过滤规则： ● 允许VLAN9用户访问DHCP服务器； ● 允

许VLAN9用户访问FireWall服务器；● 允许VLAN9用户访问校园网内部的一些应用服务器，如VOD视频点播服务器；● 不允许VLAN9用户访问其他VLAN用户；● 允许VLAN9用户访问Internet. 访问控制策略在3Com 4007上的实现 （1）创建classfier Classfier用于实现源网络／源端口到目的网络／目的端口的流量定义。在本文中，不允许9网段访问其他网段，只能上网，定义规则如表1所示。 具体实现步骤可以参考有关技术手册。 基本思路是实现VLAN9→VLAN1、VLAN1→VLAN9、VLAN9→ VLAN2、VLAN2→VLAN9的流量定义，如果网络中存在其他VLAN，可以用相同方法实现。完成了对所有VLAN的流量定义后，就定义完了Classfier 9-to-otherlan，序号为99. 在创建classfier的过程中，序号非常重要，它决定了控制策略执行的顺序。其他Classfier的定义方法可以参见9-to-otherlan的定义步骤。 （2）创建Control实现对Classfier的控制 创建Control来控制各个Classfier，包括允许、拒绝、速率等级等，最重要的是允许／拒绝操作。Control的序列号有顺序要求，先执行低级别的Control.其定义规则如表2所示。 具体实现步骤可以参考有关技术手册。 基本思路是首先完成对Control 15到 Internet及Control 14到otherlan的定义，其他Control的定义方法可以参考上述步骤完成。
在3Com 4007上完成了设计的过滤规则后，还需要在实际的网络环境中做必要的测试，以保证所做的设置是成功的、有效的。 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