# 基于 3Com 4007 QOS 特性增强 VLAN 安全性

宋博强 （北京军医学院网络管理中心 100071）
陈岩 （北京深思软件股份有限公司系统集成部 100005）
陈洪涛 张晟 刘畅 （北京军医学院网络管理中心 100071）

**摘要**：本文讨论了在典型校园网环境中利用3Com 4007的QOS特性，实现各VLAN用户之间访问控制的方法。通过VLAN用户之间访问控制的设置，可以有效增强校园网内网的安全，使之成为网络稳定运行的一道安全屏障。

**关键词**：校园网 3Com 4007 QOS特性 VLAN网络安全

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？本文以3com 4007交换机为例，就这方面问题作一讨论。

## 1 VLAN和三层交换（L3）技术

### 1.1 二层交换

传统共享型以太网的和新技术集线器位于OSI参考模型的第1层（物理层），在同一时间，集线器上只能有一个端口进行数据的发送，以共享介质的形式工作。传统共享型以太网处于同一个碰撞（冲突）域中，传输效率低下。交换型以太网的核心设备机位于OSI参考模型的第2层（数据链路层），它的每个端口都可以划分为一个网段，多网段位于不同的碰撞域，使得网络各站点间可独享带宽，改变了传统以太网的共享模式，消除了无谓的碰撞检测和出错重发，提高了传输效率，这就是所说的二层交换技术。二层交换技术的操作对象是数据帧，根据Mac地址进行数据交换和过滤。它在实现上采用专用集成电路ASCI技术，以硬件实现协议解析和包转发以达到线速交换。二层交换技术在物理上进行了网段划分，整个以太网仍然处于同一个广播域中，并不能解决诸如广播风暴、安全性控制等问题。

### 1.2 VLAN技术

VLAN的出现解决了二层交换技术存在的问题，它使子网的划分不再受物理位置的限制。整个以太网可以基于不同的策略划分为多个VLAN子。一个VLAN在逻辑上等于一个广播域。在一个VLAN子网中，一个站点发出的广播数据只能发送到同一VLAN的其他站点，其他VLAN中的站点则收不到这些广播信息。VLAN的划分有效地控制了网络上的广播风暴，并以一种集中化的方式使网络管理更为有效。VLAN之间的通信如何实现，是否可以在VLAN之间增加访问控制以增强网络的安全性成了技术人员需要解决的新问题。

### 1.3 三层交换

VLAN之间的通信必须借助第三层路由功能才能实现。将路由功能与第二层线速交换结合，即所谓的三层交换技术。支持三层交换技术的交换机同时工作在OSI参考模型的第二层（数据链路层）和第三层（网络层）上，可以实现同一种子网内的线速交换和不同子网间的路由通信。与专用路由器相比，三层交换机具有以下优点：

(1) 由于采用ASCI技术通过硬件实现交换路由功能，数据转发效率提高。

(2) 在同一工作组内交换，在不同工作组间路由，除了必要的路由决定过程外，大部分数据流量由第二层交换处理。

(3) 多个子网互连只是与第2层交换模块的逻辑连接，不需要增加专用端口。

## 2 基于3com 4007的QOS特性增强VLAN安全性

### 2.1 千兆位以太网的QOS特性

千兆位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。千兆位以太网对QOS的保证来源于2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，千兆位以太网与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。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。本文以3com公司推出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。

### 2.2 制定VLAN之间的访问控制策略

一个典型的校园网环境中，一般可以根据不同的业务部门来划分VLAN（详见图1）。在图1所示的网络环境中，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，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：

# Enhanced VLAN Security Based on 3Com 4007 QOS

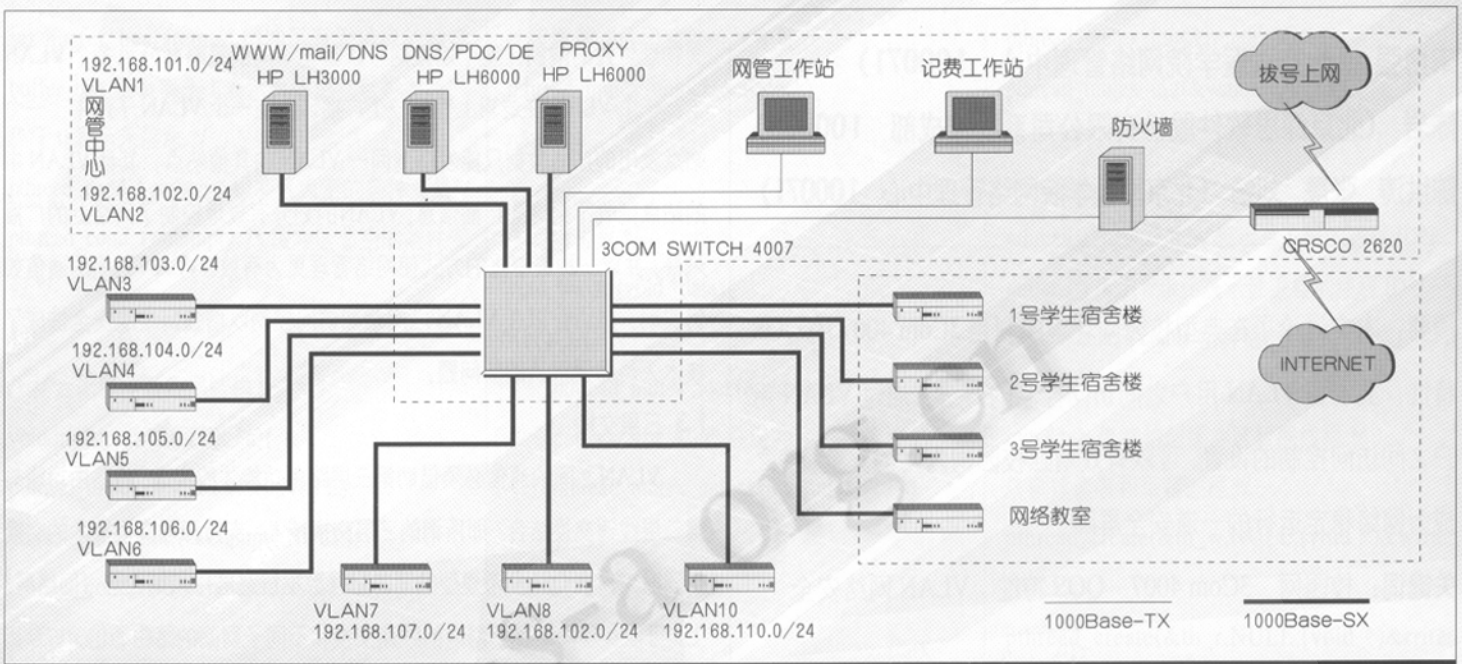



图1

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。

### 2.3 访问控制策略在 3Com 4007 上的实现

2.3.1 首先创建 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：

具体实现步骤如下所示：

```
CB9000@slot6.1 [4-GEN-GBIC-L3] (qos/classifier): def
Enter classifier number (1-498): 99
Enter classifier name {?}: 9-to-otherlan
Select cast type (unicast,multicastlalll?): a
Select IP protocol type (TCP,UDPlalll?): a
Enter source IP address [0.0.0.0]: 192.168.109.0
Enter source IP address mask [255.255.255.0]:
Enter destination IP address [0.0.0.0]: 192.168.101.0
Enter destination IP address mask [255.255.255.0]:
Enter start of TCP/UDP source port range (0-65535) [0]:
Enter end of TCP/UDP source port range (0-65535) [65535]: 1023
Enter start of TCP/UDP destination port range (0-65535) [0]:
Enter end of TCP/UDP destination port range (0-65535) [65535]: 1023
Enter another filter (yes,no) [no]: y
Enter source IP address [0.0.0.0]: 192.168.101.0
Enter source IP address mask [255.255.255.0]:
Enter destination IP address [0.0.0.0]: 192.168.109.0
Enter destination IP address mask [255.255.255.0]:
Enter start of TCP/UDP source port range (0-65535) [0]:
Enter end of TCP/UDP source port range (0-65535) [65535]: 1023
Enter start of TCP/UDP destination port range (0-65535) [0]:
```

表 1

| | | | | | | |
|---|---|---|---|---|---|---|
| 96 | 9-to-dhcp | 11 | Unicast or Multicast | TCP or UDP | – | Yes |
| 97 | 9-to-firewall | 12 | Unicast or Multicast | TCP or UDP | – | Yes |
| 98 | 9-to-vod | 13 | Unicast or Multicast | TCP or UDP | – | Yes |
| 99 | 9-to-otherlan | 14 | Unicast or Multicast | TCP or UDP | – | Yes |
| 100 | 9-to-internet | 15 | Unicast or Multicast | TCP or UDP | – | Yes |

Enter end of TCP/UDP destination port range (0-65535) [65535]: 1023

Enter another filter (yes,no) [no]: y

Enter source IP address [0.0.0.0]: 192.168.109.0

Enter source IP address mask [255.255.255.0]:

Enter destination IP address [0.0.0.0]: 192.168.102.0

Enter destination IP address mask [255.255.255.0]:

Enter start of TCP/UDP source port range (0-65535) [0]:

Enter end of TCP/UDP source port range (0-65535) [65535]: 1023

Enter start of TCP/UDP destination port range (0-65535) [0]:

Enter end of TCP/UDP destination port range (0-65535) [65535]: 1023

Enter another filter (yes,no) [no]: y

Enter source IP address [0.0.0.0]: 192.168.102.0

Enter source IP address mask [255.255.255.0]:

Enter destination IP address [0.0.0.0]: 192.168.109.0

Enter destination IP address mask [255.255.255.0]:

Enter start of TCP/UDP source port range (0-65535) [0]:

Enter end of TCP/UDP source port range (0-65535) [65535]: 1023

Enter start of TCP/UDP destination port range (0-65535) [0]:

Enter end of TCP/UDP destination port range (0-65535) [65535]: 1023

以上步骤实现 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。

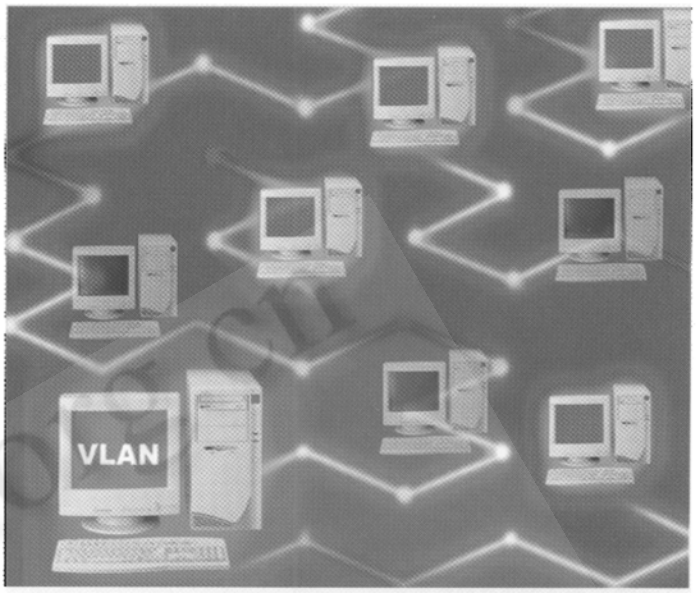
在创建 classfier 的过程中，序号非常重要，他决定了控制策略执行的顺序。其他 Classfier 的定义方法可以参见 9-to-otherlan 的定义步骤。

2.3.2 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，先执行低的 Control。

表2

| | | | | | |
|---|---|---|---|---|---|
| 11 | dhcp/dns | 96 | Best Effort | No | None |
| 12 | firewall | 97 | Best Effort | No | None |
| 13 | vod | 98 | Best Effort | No | None |
| 14 | otherlan | 99 | Drop | No | None |
| 15 | internet | 100 | Best Effort | No | None |




具体实现步骤略。

### 2.4 验证过滤规则

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。具体步骤如下：

(1) VLAN9 用户 PING dhcp 服务器，结果应为通；

(2) VLAN9 用户 PING firewall 服务器，结果应为通；

(3) VLAN9 用户 PING 视频点播服务器，结果应为通；

(4) VLAN9 用户 PING 其他 VLAN 用户，结果应为不通；

(5) VLAN9 用户 PING internet 用户，结果应为通；

(6) 其他 VLAN 用户 PING VLAN9 用户，结果应为不通。

做的测试结果显示符合设计要求，这充分说明设计是成功、可行的。

## 3 结束语

利用3Com 4007的QOS特性，还可以完成许多其他有关流量控制、带宽限制、业务分类、排队机制方面的业务，笔者在这里仅介绍了一个典型环境中的应用，希望能够起到抛砖引玉的作用。大家可以结合各单位的实际情况，充分利用3Com 4007优越的性能，来实现不同的业务需求。

## 参考文献

1 Chris Brenton, Andrew Hamilton, Gary Kessler,Mastering Cisco Routers [M], 美国 SYBEX Inc, 1999。

2 Cisco system, cisco internetwork design [M], 美国 CISCO 公司，1998。

3 Chris lewis, Cisco Tcp/Ip Routing Professional Reference [M], 机械工业出版社，1999。