文章编号:1674 - 2869(2011)04 - 0097 - 03

# 中小型校园网流量的控制方法

林维锵

(广东广播电视大学信息网络中心,广东 广州 510091)

**摘 要**:分析了目前流量控制的主要方法,并提出一种非常适合中小型校园网部署的具有上网管理功能的流量控制方案,进一步以实例说明了流控设备的部署、管理策略和实施效果,提供了一个解决流量问题的思路.

**关键词**:校园网;P2P;流量控制设备;网络管理

**中图分类号**:TP393 **文献标识码**:A **doi**:10.3969/j.issn.1674-2869.2011.04.025

## 0 引 言

随着互联网技术的快速发展,学校信息化建设发展迅速,校园网作为数字化信息的最重要载体,在学校的信息化建设中发挥着非常重要的作用,维护校园网络正常运行则是学校信息化建设的基础.近年来,随着各种新网络应用对带宽需求的快速提高及 P2P 应用对校园网出口带宽的严重影响,很多校园网经常出现出口流量超负荷,导致网络拥塞、性能降低,对其它应用的服务质量形成威胁,影响了校园网的正常运行[1].特别是数量众多的中小型校园网,由于设备投入及技术人员的不足,缺乏对流量的有效控制,网络常处于拥塞状况,使得校园网未能发挥应有的作用.为了使校园网用户能合理地使用网络资源和带宽,使基于网络的教学办公工作正常开展,应采取有效的技术手段对耗费大量带宽的 P2P 应用进行合理的监测和控制.笔者通过对目前主要流量控制技术及多所电大系统中市县级电大的中小型校园网进行研究分析,提出了一种非常适合中小型校园网部署的具有上网管理功能的流量控制方案,并在多所校园网中进行了实践.

## 1 流量控制常用解决方法

目前校园网中以迅雷、快车、电驴和各种在线音频视频为代表的 P2P 应用,占用了大量的出口带宽资源.校园网中流量管理的主要工作就是对 P2P 应用协议和用户进行带宽控制管理,目前采用的流量控制方法主要有以下几种:

### 1.1 封禁 P2P 应用端口及限制并发连接数

目前校园网出口均部署有防火墙或路由器,可通过在防火墙或路由器上封堵 P2P 应用的常用端口,如:BT 的 6881-6890,迅雷的 3076-3078 等,这种办法在 P2P 应用开始普及的早期或实施的初段有一定效果,但现在大部分 P2P 软件可自动协商通信端口,若发现某端口无法通信,通讯双方将自动更换端口,且允许设置为 80 等正常端口,所以封禁端口的效果并不理想.

P2P 软件寻找资源时,需发起大量的网络连接,高达几百或上千,通过限制主机的并发连接数及新建连接数,如设置在 50 和 10 条以下,将有效地抑制 P2P 软件寻找到可用下载资源的几率,从而减少对带宽的占用.该方法可有效限制 P2P 软件对带宽滥用,但同时也会对部分正常的网络应用造成影响,如访问新浪等大型网站时,所需并发数高达上百,将导致访问变得缓慢,且 P2P 软件通过长时间运行后,可能会找到有效下载资源进行高速下载,所以控制并发数的办法有一定的作用,但效果不显著,也存在副作用.

### 1.2 限制用户的上网流量或带宽

使用防火墙或城市热点等可管理主机带宽的设备,对用户进行流量限制的策略,对每个用户的互联网出口流量进行严格的控制,使之每天可用的流量限制在指定范围内.在实际使用中发现,该方法虽可使用户在使用 P2P 软件时有所节制,但在实施中也经常出现部分正常用户在使用某些对流量要求高的应用时,因为限制而无法完成,或者因为计算机中病毒导致发生突发流量将其可用流量耗尽,导致其无法正常上网.除了限制用户的总流量外,也可采取限制用户的可使用带宽,给每个用户只分配较小的带宽,但该方法使得正常网络应用无法得到所需带宽,导致运行缓慢,存在用户体验差等问题.

**收稿日期**:2011 - 03 - 02

**作者简介**:林维锵(1975 -),男,广东揭阳人,实验师,硕士.研究方向:网络管理和安全.

### 1.3 使用专业流控设备

为了对网络流量进行管理控制，需识别流量的应用类型.目前较成熟的技术有DPI(深度报文检测)和DFI(深度流行为检测)等技术，国内外很多厂商在基于这些技术基础上推出了不少的专业流量控制设备，其产品应用效果良好且应用较广泛的厂商有思科、Allot、Packeteer和华三等[2].这些厂商的专业流控产品可实现对深层次协议的识别，且对可识别的应用流量进行最大、最小带宽保障或阻断等控制效果，实现对流量良好控制效果.这些专业流控产品具有性能高、效果好等特点，适合在较大规模的网络部署，其价格较为昂贵，性价比不高，且其协议更新较慢，对迅雷等更新快的软件控制效果较差.另外，还有一些和流控产品功能相近的流控服务器，是通过在服务器上安装Panabit、RouterOS和海蜘蛛等流控软件来实现的，投入较少，效果也较好，但性能相对较差，且维护难度较高，对管理人员有一定技术要求.

以上流量控制方法，有的投入少但效果较差，有的效果好但性价比低，或者对管理人员技术要求较高.目前大多数中小型校园网普遍存在设备投入不足、管理人员不足或技术水平不高等问题，所以对网络设备一般要求具备性价比较高、功能完善、使用方便等特性，前面介绍的流量控制方法不是很适合在这类校园网使用.根据这类网络的需求，具有上网管理功能的流控控制设备目前开始得到较多部署应用，这种流控设备除了有完善的流量管理控制功能外，还具备上网行为管理功能，可实现对用户的分级分组管理，实施不同的流量控制管理及上网权限策略，以及网络行为的审核、上网日志记录、接入控制和安全性检查等管理策略.这种类型的流量控制设备大多基于X86结构，具有对深层次协议检测实现容易、功能完善、升级快等特性，虽性能相对较弱，但可完全满足中小型网络的性能需求，非常适合在中小型校园网中使用.中小型校园网可利用这类设备作为核心来构建一个具有较完善上网管理功能和出口流量可控的高可用性网络.

## 2 中小型校园网流控控制实施案例

### 2.1 某市级电大校园网现况

某市级电大校园网主要为远程开放教学提供服务，有2条10兆互联网出口分别接入当地电信网和教科网，校园网内办公及教学信息点共约有1 000个，根据各种用途划分为多个VLAN，并有多台部署在DMZ区的服务器提供教学、教务、视频点播等网络服务.该校园网因编制限制只配备两三个技术人员进行网络管理，同时这些管理人员还有授课任务.因设备及管理人员不足，校园网虽部署有路由器、三层交换机和防病毒软件等，但P2P应用引起上网缓慢、接入控制不到位、客户端安全性差等问题导致该校园网经常出现拥塞、断网等问题，无法为数字化校园网应用提供良好网络支撑，该校园网的现状具有一定普遍性.

### 2.2 流控设备选型

中小型校园网的拓扑结构应简单实用、便于管理，出口设备应首选多功能应用网关，除了应具备防火墙、流量管理功能外，最好还具备接入控制、客户端安全性检测、上网审计、入侵检测等功能.网关进行网络流量控制时，由于需对经过设备的每个数据包进行分析、处理等消耗资源的操作，所以应具备一定数据处理能力及吞吐量，以免成为网络瓶颈.目前应用较广的具有上网管理功能流控网关厂商主要有深信服、网康、锐捷、飞鱼星等，笔者通过对多种主流产品的性能、功能、稳定性等进行对比研究、试用后，选用了深信服的M5400－AC对该校园网进行改造.

### 2.3 网络流量控制设备部署

通过对该校园网原有拓扑结构进行分析后，采用保持原有网络架构的原则，将原性能老化的路由器替换为流控网关，不需做大幅更改，保证了网络平稳升级[3].改造后的网络拓扑结构如图1所示，两条互联网出口线路直连到网关，服务器集中在DMZ区中保证安全性，网关设备与核心三层交换机通过高速千兆链路互联.

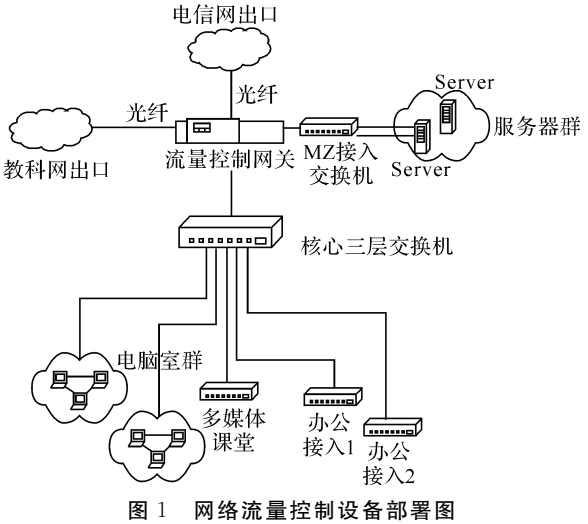


**图1 网络流量控制设备部署图**

Fig.1 Control equipment deploying of network flows

### 2.4 网络流量控制网关的实施策略

为保证充分发挥设备效用，出口带宽高效合理使用，提升校园网服务质量，应根据校园网的实

际情况,进行规划、设计、测试,方能达到较理想效果.通过详细调研分析、设计多种方案并测试对比,根据网络流量控制网关功能制定并实施了以下管理策略:

2.4.1　限制 P2P 应用、保证正常应用带宽　　建立 P2P 应用的流量通道,将迅雷等 P2P 类应用软件可使用的校园网出口带宽限制在 40%左右,并根据时段进行动态调整,在网络使用高峰期减低,低谷时适当调高,以充分使用网络,同时限制单用户最高带宽,保证通道公平使用;建立 HTTP、E-Mail 等正常网络应用的优先保障通道,保证网络繁忙时正常应用的服务质量.

2.4.2　对不同用户部署相应管理策略　　根据校园网中办公用户、机房用户、学生用户等各种不同网络使用需求,采用分组结构对不同类型用户进行管理,并实施不同管理策略.对办公用户采取较为宽松的管理策略,只适当限制 P2P 应用;对主要用于教学的机房用户,则采取严格管理策略,禁止使用 P2P、流媒体、下载工具、IM 等与教学无关应用,减少带宽占用,同时提高教学效果;对学生用户则采取适中措施,限制其 P2P 类软件的可用带宽及并发连接数,将其对出口带宽占用控制在一定范围内.

2.4.3　实施详细上网审计、日志记录　　对校园网所有用户实行详细的上网行为审计,记录所使用协议、应用、流量、时长、访问的 IP 地址等,并可根据需要选择对访问网址、收发邮件、论坛发帖、聊天记录等进行监控;定时通过数据中心的详尽统计功能,分析校园网的应用使用情况,做出相应管理措施调整,优化网络性能;实施超过 60 天上网日志记录,满足公安部门的安全规定.

2.4.4　启用客户端接入控制及安全性检测　　中小型校园网大多因缺乏管理设备及技术措施,对接入用户无法做到严格控制,导致用户可随意接入校园网,影响了校园网安全性,可在网关上实施 IP/MAC 地址绑定及认证措施,保证只有合法用户方能接入网络;启用接入客户端的安全性检测,只有安装了符合要求的安全软件及措施的客户端才能接入网络,否则只能访问指定服务器进行升级,有效提升校园网安全性.

### 2.5　实施效果

使用流量控制设备之前,P2P 类应用软件占用了该校园网出口带宽的 70%～80%,严重影响了校园网正常使用,用户上网体验很差.通过部署流控设备并采取以上管理策略后,校园网的 P2P 应用得到了有效限制,对带宽占用在 30%以下,各类应用都能够得到较为合理的带宽和保证,出口带宽资源得到了高效的利用,如图 2 所示.

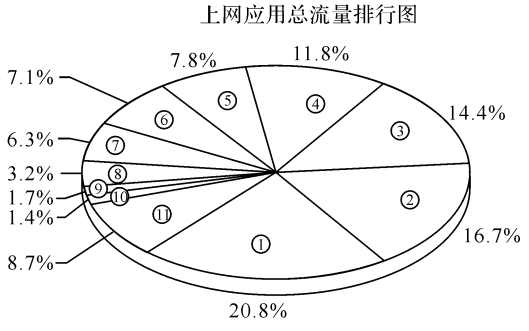


**图 2　网络流量分布图**

Fig. 2　Distribution of network flows

**注**:①访问网站　②P2P　③HTTP 文件下载　④网络流媒体　⑤下载工具　⑥P2P 流媒体　⑦FTP　⑧IM　⑨软件更新　⑩IM 传文件　⑪其他

校园网的核心业务系统所需的网络带宽得到保障,保证了基于校园网的教学、办公工作能高效进行;校园网的接入得到有效控制,客户端的安全性得到有效检测,较大提升了该校园网安全性、稳定性,使其更好为远程开放教育服务.

## 3　结　语

校园网中,P2P 应用丰富了校园网应用的同时也占用了大量出口带宽,笔者通过较全面分析流量控制技术,给出了适合中小型校园网的流量控制管理策略并给出实施案例,该方案在多所校园网中进行实施后均取得良好应用效果,为目前中小型校园网普遍存在的流量控制及安全问题提出一种具有较高借鉴价值的解决思路.对 P2P 类应用控制将使部分用户无法快速下载资源,导致其满意度的下降,管理者应丰富校内资源,合理进行网络使用引导.网络应用不断更新发展,流量控制策略也应不断更新,方能不断提升网络应用水平.

**参考文献:**

[1]　周文莉,吴晓非.P2P 技术综述[J].计算机工程与设计,2006(1):76-79.

[2]　胡俊,程瑾.网络流量管理控制技术在校园网的应用研究[J].中国教育信息化,2009(21):29-30.

[3]　郑林江.基于交换机流量和网络线路的监控系统[J].计算机应用,2009(12):8-10.

(下转第 110 页)