基于 DPI 技术的校园网络带宽管理

聂瑞华，黄伟强，吴仕毅，罗辉琼
（华南师范大学 网络中心，广东 广州 510631）

摘 要：面对校园网用户和业务流量的不断增长，对网络带宽资源需求也越来越大，但是各种网络应用无序地抢占有限的带宽，必然导致网络运行效率的降低。文中为了提高网络运行效率，比较三种主流带宽管理技术，结合学校实际，在校园网出口部署带宽管理设备，通过分析校园网络出口流量，对出口网络流量带宽进行有效的管理，实施网络带宽管理策略，保证关键的科研教学网络需求，控制非关键应用对带宽的耗费，节约出口带宽资源，提高网络使用性能，保障了网络安全运行。

关键词：带宽管理；深度包检测法；深度流检测法；带宽策略
中图分类号：TP393.02 文献标识码：A 文章编号：1673－629X(2009)04－0250－04

Bandwidth Management in Campus Network Based on DPI Technology

NIE Rui-hua, HUANG Wei-qiang, WU Shi-yi, LUO Hui-qiong
(Center of Network, South China Normal University, Guangzhou 510631, China)

Abstract: With the development of campus network consumer and business rate of flow, the demand of network bandwidth is becoming greater and greater. Whereas, various network applications have occupied the limited bandwidth disorderedly, leading to low efficiency of network operation. Aims at improving the network operation by a comparison of three current techniques of bandwidth management. Combine the reality of school, and deploy bandwidth managing equipment at the outlet of campus network. Thus is able to analyze and well administrate the rate of flow at the outlet. By this means, can carry out the supervision strategy of bandwidth, ensuring the demand of key studying and teaching, as well as controlling the waste of unimportant use of network resource. All in all, the supervision management is able to improve the capacity of the network and guarantee the network safety.

Key words: bandwidth management; DPI; DFI; stagegy of bandwidth

0 引 言

随着我国信息化的发展，信息化已经深入到教育行业方方面面。教育行业也借助信息化的动力，在对现有教育资源合理配置、有效利用的基础上，实现了从传统教学方式向现代教育方式的转变。教育行业借助校园网的建设，各项主要教育活动越来越依赖于网络，在教务管理、网络教学、学生学习、行政管理、图书资料管理以及信息交流、资源共享等方面得到了很大的发展。校园网主干网虽然年年升级，但是由于教育网的规模庞大，学生数量众多，网络应用环境非常复杂，包括 P2P 下载、网络游戏、网络视频、网络炒股、网络病毒等应用占用了巨大的网络带宽，使得校园网内网和外网的带宽面临严峻的挑战，甚至严重影响教务行政以及教学工作的正常开展。因此如果没有有效的带宽规划和管理策略，网络带宽拥堵将成为校园网运行的最为迫切的问题。

1 主流带宽管理技术介绍

目前常用的流量带宽管理技术有：常用端口检测法、深度流检测法(DFI)、深度包检测法(DPI)。

常用端口检测法是通过四层处理完成检测，由于基于开放端口、随机端口甚至采用加密方式进行传输的应用类型在目前网络中广泛使用，通过常用端口方式能够识别的协议类型非常有限。

深度流检测法即是基于流量行为的应用识别技术[1]，根据各种应用的连接数、单 IP 地址的连接模式、上下行流量比例关系、数据包发送频率等数据流的行

收稿日期：2008－07－07
基金项目：国家 211 工程重点支持项目；中国下一代互联网示范工程 CNGI 示范网络高校驻地网建设项目(CNGI－CERNET2－CPN－2007－060)
作者简介：聂瑞华(1963－)，男，江西樟树人，教授，研究方向为计算机网络与应用、多媒体发展。

为特征指标的不同与 DFI 检测模型进行匹配, 进而从中区分出流量应用类型。由于粒度较粗, 只能对应用类型进行笼统分类。

深度包检测法(DPI), DPI 全称为"Deep Packet Inspect", 称为"深度包检测"[2]。所谓"深度"是和普通的报文分析层次相比较而言的, "普通报文检测"仅分析 IP 包的层 4 以下的内容, 包括源地址、目的地址、源端口、目的端口以及协议类型, 而 DPI 除了对前面的层次分析外, 还增加了应用层分析, 识别各种应用及其内容, 基本概念如图 1 所示。

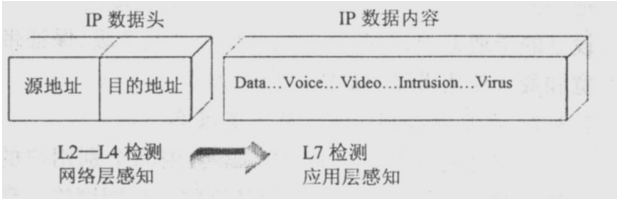

图 1　DPI 基本概念

DPI 的技术关键是高效的识别出网络上的各种应用, 其基本原理如图 2 所示。

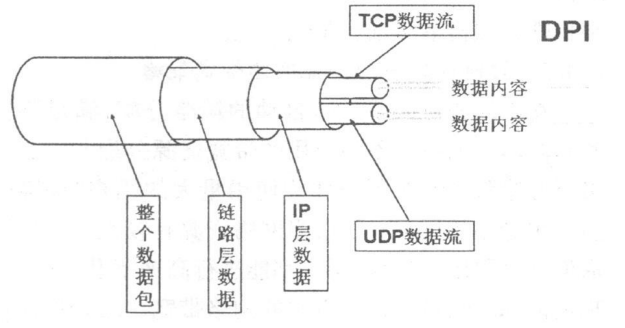

图 2　DPI 基本原理

当 IP 数据包、TCP 或 UDP 数据流经过基于 DPI 技术的带宽管理系统时, 该系统通过深入读取 IP 包载荷的内容来对 OSI7 层协议中的应用层信息进行重组, 从而得到整个应用程序的内容, 对流量中的具体应用类型和协议做到比较准确的识别, 然后按照系统定义的管理策略对流量进行整形操作, 从而有效管理网络带宽。

DPI 的识别技术可以分为以下几大类:

(1)基于"特征字"的识别技术。

不同的应用通常依赖于不同的协议, 而不同的协议都有其特殊的指纹, 这些指纹可能是特定的端口、特定的字符串或者特定的 Bit 序列。基于"特征字"的识别技术通过对业务流中特定数据报文中的"指纹"信息的检测以确定业务流承载的应用。

根据具体检测方式的不同, 基于"特征字"的识别技术又可以被分为固定位置特征字匹配、变动位置的特征匹配以及状态特征匹配三种技术。

通过对"指纹"信息的升级, 基于特征的识别技术可以很方便地进行功能扩展, 实现对新协议的检测。

如: Bittorrent 协议的识别, 通过反向工程的方法对其对等协议进行分析, 所谓对等协议指的是 peer 与 peer 之间交换信息的协议。对等协议由一个握手开始, 后面是循环的消息流, 每个消息的前面, 都有一个数字来表示消息的长度。在其握手过程中, 首先是先发送 19, 跟着是字符串"BitTorrent protocol"。那么"19BitTorrent Protocol"就是 Bittorrent 的"特征字"。

(2)应用层网关识别技术。

某些业务的控制流和业务流是分离的, 业务流没有任何特征。这种情况下, 就需要采用应用层网关识别技术。

应用层网关需要先识别出控制流, 并根据控制流的协议通过特定的应用层网关对其进行解析, 从协议内容中识别出相应的业务流。

对于每一个协议, 需要有不同的应用层网关对其进行分析, 如 SIP、H323 协议都属于这种类型。SIP/H323 通过信令交互过程, 协商得到其数据通道, 一般是 RTP 格式封装的语音流。也就是说, 纯粹检测 RTP 流并不能得出这条 RTP 流是通过哪种协议建立的。只有通过检测 SIP/H323 的协议交互, 才能得到其完整的分析。

(3)行为模式识别技术。

行为模式识别技术基于对终端已经实施的行为的分析, 判断出用户正在进行的动作或者即将实施的动作。行为模式识别技术通常用于无法根据协议判断的业务的识别。例如: SPAM(垃圾邮件)业务流和普通的 Email 业务流从 Email 的内容上看是完全一致的, 只有通过对用户行为的分析, 才能够准确地识别出 SPAM 业务。

由于 DPI 应用识别的准确度、控制力度等方面优势, 华南师范大学校园网采用基于 DPI 技术的流量带宽设备来对流量带宽进行管理, 并综合运用了以上三种识别技术, 在检测效率和灵活性方面均达到最优。

2　校园网带宽管理的实现

2.1　校园网带宽管理网络结构

对于广域网的带宽管理, 可在局域网与广域网交界处配备一台带宽管理器来实现[3]。对于互联网出口的带宽管理, 可在网络出口防火墙和核心交换机之间配备一台带宽管理设备, 如图 3 所示。

由于我们学校使用双核心交换机, 需要两条链路冗余, 基于端口的考虑, 将带宽管理设备前移到防火墙与路由器之间来实现带宽流量管理, 对于所有经过网

络出口的数据包进行了特征码分析，从而实现 Internet 出口带宽的优化。如图 4 所示。

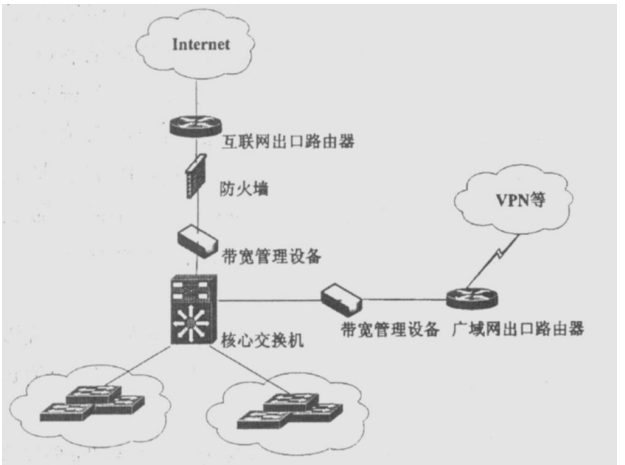

图 3 带宽管理网络结构

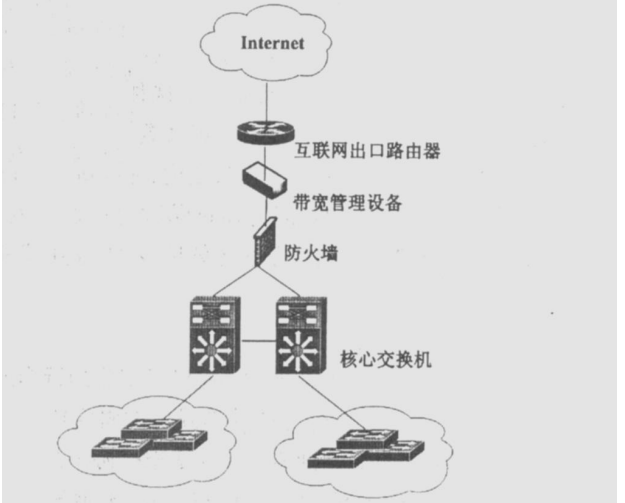

图 4 本校带宽管理网络结构

2.2 校园网带宽监控与分析

对所有流经带宽设备的流量实时产生各种统计分析报表，包括对网络流向的监控，对网络协议的监控和对用户的监控。通过一定时间内的历史数据报表统计，获取网络总体流量水平、流量波动、流量跳变等参数，分析异常流量与正常流量的偏差，可以有效防止异常流量对运行网络的影响。同时，网络管理员可以更准确、详细地了解各类带宽的占用情况，及时作出合理的网络资源分配决策。

我校校园网络出口中基于协议和应用进行的带宽使用情况统计，PPLive、HTTP 以及 BT 等应用占用了近 60％的带宽。分析发现 P2P 软件、网络电视、网络游戏这些应用毫无节制地加速吞噬着宝贵的带宽资源，严重影响校园网的其他应用。

2.3 校园网带宽管理策略

带宽管理策略需要以用户或应用为对象，以时间为纬度，以带宽值为杠杆，制定精细的管理分配策略，真正帮助学校提升带宽价值。

2.3.1 保障关键应用的网络带宽及优先权策略

在校园网中，教务管理、网络教学、行政管理、图书资料管理、视频会议和资源共享是学校的关键应用。利用分级管理功能[4]，指定校园网络为 WEB 应用和财务及教学应用为关键应用，把这些关键应用分配在一个较大的逻辑通道中，从而确保这些应用能高效运作，提高服务质量。例如，在带宽管理设备 Outband 和 INtbound 设立 HTTP，RSTP，POP3，SMTP 的子通道，把办公网络、图书馆网络、会议厅、教学大楼网络划到设立的子通道中，服务优先级设到最高的 7 级，保证带宽和最大使用带宽根据需要设置大小。

2.3.2 按区域合理分配网络带宽策略

固定分配每个子网的带宽，不会因为个别用户的过量下载而导致某个网段内部甚至整个校园网络出现重大问题，对用户相对密集和网络使用率高的子网适当加大分配的带宽。例如，按教学区域、办公区域、无线区域、教工宿舍区域、学生宿舍区域等子网分类，个别特殊区域再继续细分子网带宽。

2.3.3 按时间段合理分配网络带宽策略

在不同的时间段进行自动的策略分配，满足不同时间段内不同用户不同应用的带宽资源分配[5]。当网络资源紧张的时候限制那些使用量大的用户，保障那些使用量小的用户，反之，当网络资源有较大空闲时则取消这些限制，让每个用户都能进行高速下载，从而实现灵活、高效、可靠使用有限的网络带宽。结合按区域合理分配网络带宽策略，例如，在上班时间段，对学生宿舍区域网络进行适当的限制，从而保证正常的教学区域网络使用需求，在下班时间段，则取消对办公区域网络的优先策略。

2.3.4 限制或禁止非学习工作网络流量带宽策略

非学习工作的流量主要是与教学工作无关的非业务流量。对于那些 P2P 软件的使用者来说，下载一个文件花 5 个小时或者 10 个小时差别并不大，但是对于其他浏览网页的用户，访问一个网页需要 5 秒钟还是 10 秒钟还是有很大区别的。同样，如果某个用户急需下载一个几兆大小的文件或者电子邮件，他也会很关注当前的网络速度，而此时的网络带宽也许正在被某些 P2P 软件或者其他一些网络资源消耗较多的用户占用。因此，对 P2P 下载、网络游戏等影响学生学习和生活的各种网络应用，采取限制或禁止这类流量带宽的策略。

2.3.5 控制异常网络流量带宽策略

异常流量包括：DoS（拒绝服务攻击）/DDoS（分布

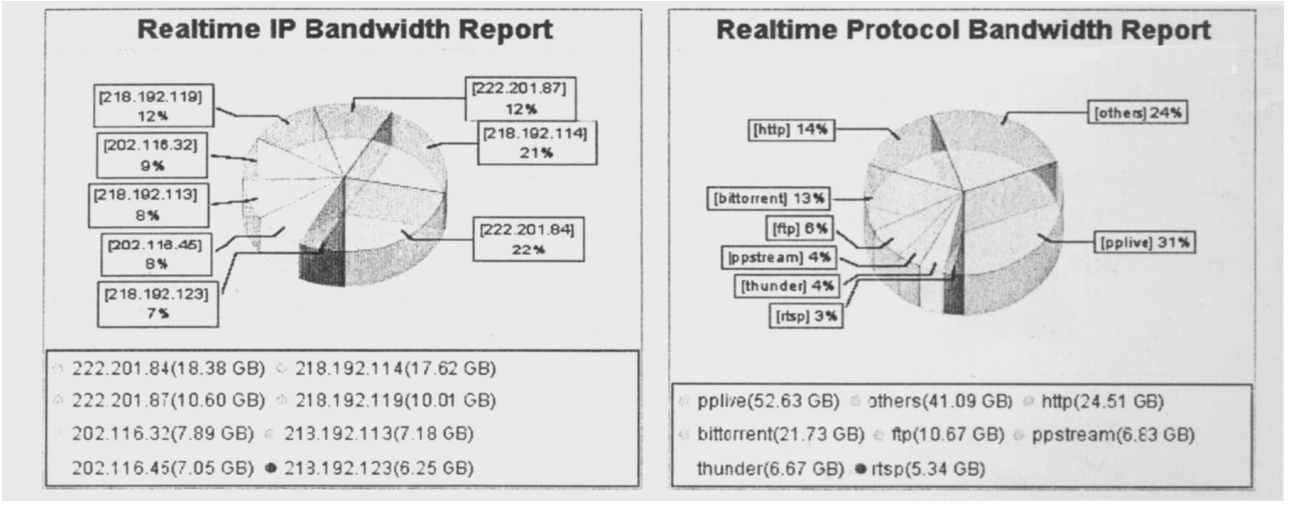

图 5　流量实时报告

式拒绝服务攻击)、蠕虫/病毒、垃圾邮件、P2P 应用、非法 VoIP 等等[6~8]。根据异常流量呈现的各种特征,深度检测应用业务区别异常流量,结合协议、端口、IP 地址、蠕虫、攻击报文等模式的统计报表,通过控制会话数、源地址端口、目标地址端口、应用协议等参数制定策略,控制和预防异常流量。

采取相应流量带宽策略后,我校校园网络应用有了显著的改善,如图 5 为流量实时报告。

HTTP 等主要应用比例占据流量的大部分,而 bt,pplive 等应用比例明显减少。

3　结束语

文中根据我校校园网的现状,结合实际对校园网出口应用及带宽使用情况的分析后,针对性地给出对我校校园网出口带宽的控制和优化;根据带宽和应用使用现状的详细评估,找到当前网络带宽使用和应用性能方面存在的问题和隐患;对特定的、非关键的应用流量(特别是 P2P 流量),通过设置带宽使用上限,降低对总体链路的负载影响,保障关键应用,提高带宽使用效率;对需要保障的关键应用和重点客户,根据应用优先级的不同专门为其设定相应的保证带宽,确保其获得有保障的带宽通道和使用感受,提高用户的服务质量(QoS);对诸如蠕虫病毒、DDoS 等非正常应用流量,通过实时流量分析器,结合历史记录分析,找到问题源头进行及时处置,保障网络安全可靠运行。

参考文献:

[1] 王　超,赵文杰. IP 网络带宽管理技术及应用分析[J]. 电信技术, 2007(5): 101—103.

[2] MAXNET 应用优化系统(AOS)技术白皮书[EB/OL]. 2007—09—01. http://www.maxnetsys.com.cn/download/MaxNet%20whitepaper.pdf.

[3] 黄小波. 企业网络带宽管理[J]. 计算机与网络, 2004(19): 46—47.

[4] 严伟荣,赖谭海. 宽带 IP 城域网的流量管理策略研究[J]. 电信网技术, 2002(2): 18—20.

[5] 黄　蕊,凌　东. 宽带互联网的带宽管理[J]. 中国新通信, 2006(11): 84—87.

[6] 邢长明,刘方爱. 基于 P2P 的网格资源发现机制研究[J]. 计算机技术与发展, 2006, 16(8): 21—23.

[7] Tang Chunqiang. PeerSearch: Efficient Information Retrieval in Peer—to—Peer Networks[M]. [s. l.]: [s. n.], 2002.

[8] Karagiannis T. Transport layer identification of p2p traffic [C]//Internet Measurement Conference (IMC). Taormina, Sicily, Italy: [s. n.], 2004.

(上接第 249 页)

on Operating Systems Principles. Bolton Landing. NY, USA: Virtual Machine Monitors, 2003: 164—177.

[3] 董耀祖,周正伟. 基于 X86 架构的系统虚拟机技术与应用[J]. 计算机工程, 2006(7): 71—73.

[4] Sugerman J, Venkitachalam G. Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor [C]//Proc. Usenix Annual Technical Conference. [s. l.]: [s. n.], 2001.

[5] 王春海. 虚拟机技术与应用[M]. 北京: 清华大学出版社, 2006.

[6] Waldspurger C A. Memory Resource Management in VMware ESX Server[C]// Proceedings of the 5th Symposium on Operating Systems Design and Implementation. [s. l.]: [s. n.], 2002.

[7] 刘　武,吴建平,段海新,等. 用 VMware 构建高效的网络安全实验床[J]. 计算机应用研究, 2005(2): 212—214.

[8] 王经坤,艾　兴,张进生,等. 虚拟产品开发技术的理论体系研究[J]. 计算机工程, 2003(3): 11—13.

[9] 杨少春. 采用 VMware 构建虚拟并行计算网[J]. 计算机工程与设计, 2006(7): 2546—2547.