

校园网络流量控制的应用

徐 维,李兴军

(湖北工程学院现代教育技术中心,湖北 孝感 432000)

摘 要:从流量特性、建模复杂性、预测精度及应用场景等多角度进行分析比较,选用流量控制设备将网络带宽的管理提升为主动的、有效的、智能化的带宽管理服务,根据流量控制设备生成的日志总结了校园网络流量的规律,采取措施控制流量的分配,从而提升网络的利用率,结果证明,这种方法简便易行,性能指标较好地满足校园网络流量实时控制的需求。

关键词:网络管理;网络流量;流量控制

中图分类号:TP393

文献标识码:A

doi:10.3969/j.issn.1674-2869.2012.04.018

0 引 言

随着信息化和计算机技术的不断发展,用户对网络的要求越来越高,而网络带宽资源日益紧张.若干不可预知的、突发的性能瓶颈会影响关键应用的运作效率,会出现网络拥塞或者短暂性的网络断开.校园网具有用户比较集中,访问峰值高以及网络中承载的内容较为复杂多样的特点,因此,如何高效地管理校园网,保证网络带宽资源的有效使用是校园网络管理面临的一个严峻问题.在高等院校的网络管理中,用户数量庞大,网络应用环境复杂,特别是点对点技术的出现与发展,不同种类的点对点应用占用了大量网络带宽(例如比特流、迅雷等),消耗了网络中的大量带宽,高峰期可以耗尽整个网络带宽.由网络链路拥塞引发的应用性能下降问题也日益严重,极大地影响了校内正常业务的使用以及师生员工正常网络应用的服务质量.

网络的正常运行,不仅仅需要设备先进,运行稳定,更加需要管理精细.如果网络运行缺乏管理,核心业务应用、时延敏感的应用、即时通讯、点对点、网络游戏等应用将同时抢用相对固定的带宽资源,随之,网络带宽的使用没有保障业务应用的优先级以及重要程度,最终导致网络带宽被抢占资源比较厉害的诸如点对点应用耗尽.

由于点对点的使用占用了至少50%的网络带宽资源,并且毫无节制地吞噬着宝贵的带宽资源,将严重影响网络中关键应用的正常运行和使用.

带宽的容量是有限的,带宽的价值是不菲的.

当没有对应用进行优先级划分的时候,非关键性应用总是占据上风.巨大的电子邮件附件或大容量文件传输所消耗的带宽远远超过它们所应享有的,而校园网络中的关键性应用之间又在相互竞争仅有的少量的带宽,特别是域名系统服务、网站服务、办公自动化等关键性应用.

网络安全方面的隐忧很多,病毒是大部分高等院校网络管理面临的一大挑战.网络病毒的入侵无处不在,可以通过用户电子邮件、网页浏览等途径进入到网络中,然后发起破坏性攻击.当攻击发生的时候,可能的情况是网络内的若干台中毒计算机同时往服务器发送大量攻击包,严重阻塞网络骨干和校园网出口通道.

1 流量控制的技术及设备选型

为了减少上述问题带来的负面影响,管理员可以在校园网的核心交换机和防火墙之间部署流量控制硬件设备来解决.

流量控制,首先需要一定的检测手段,主要的检测技术包括深度包检测(Deep Packet Inspection,下文简称为DPI)、深度流检测(Deep/Dynamic Flow Inspection,下文简称为DFI)等.

DPI技术是一种基于应用层的流量检测和控制技术,当数据包、数据流通过带宽管理系统时,该系统通过深入读取数据包载荷的内容来对开放式系统互联七层协议中的应用层信息进行分析与重组,从而得到原始内容,然后按照系统定义的管理策略对流量进行整形操作^[1].

DFI是相对于DPI技术提出的一种业务识别

技术,即不同的应用类型体现在会话连接或数据流上的状态各有不同,能够保证正确识别加密传输的应用流量。DFI 关注于网络流量特征的通用性,它不对不需进行深度报文检测和使用协议还原技术,仅仅通过获取点对点流量的各项统计参数,分析点对点流量的空间特性和时间特性,构建相应的点对点流量模型,探寻有效的点对点流量控制策略^[2]。

基于应用层的网络流量控制采用的设备需要兼具有 DPI 技术(深度报文检测技术)与 DFI(深度流检测)技术;经过查阅各种资料及试用设备,选用了 TTNET1000(the traffic control facility)。

2 流量控制的策略

通过特有的带宽管理和分配算法,流量控制设备可以将网络带宽的管理从被动的、消极的、无效的传统模式提升到主动的、有效的、智能化的带宽管理服务,保证关键应用正常运行,提高网络管理水平。

2.1 应用优先级的划分

流量控制设备可基于业务应用的重要程度,将校园内部的应用划分为若干个优先级,并在后续的带宽管理过程中将核心业务应用的应用配置为高优先级,同时将占用带宽资源较高的应用配置为低等级,从而可以实现优先保证高等级的应用。将所有需要保障和抑制的应用进行合理分组,校园网络基本上应以保证网站访问应用为前提,在工作时间内抑制点对点等应用。

2.2 强大的带宽控制与管理功能

流量控制设备结合应用优先级、共享通道、权重、自定义虚拟带宽通道等,提供了多层多级带宽通道、最大带宽限制、带宽保障、带宽预留、带宽租借、微带宽控制、虚拟局域网带宽控制等一系列强大的流量整形和带宽管理功能。可对特定的用户组进行带宽总通道划分,例如 500 MB 带宽,点对点下载限速最多 100 MB,网络视频最多 200 MB,网页浏览及传统应用保障 100 MB 等。

2.3 基于应用层防火墙的应用优化策略

流量控制设备可以内置灵活、高效的应用层防火墙^[3],通过参考传统防火墙的访问控制策略,将其深化至应用层面,管理员可以基于应用优先级、源 IP(Internet Protocol,下文简称 IP)地址、目标 IP 地址、用户、虚拟局域网、时间段、协议和应用组、动作(允许或阻断)、会话数以及带宽通道等进行自由的带宽控制和应用优化,确保方案有效,功能合理。

2.4 安全保护措施

采用主动预防和设备拦截等技术,安装监视、日志或者其他流量分析系统,启用客户接入控制及安全性检测^[4],攻击发生时,就可很快地诊断出攻击的类型以及攻击源,要尽可能地修正已发现的问题和系统漏洞,识别、跟踪或禁止这些机器或网络对校园网的访问,如对异常流量的端口流量进行限制;把网络分为多个子网,并改变 IP 地址和主机名,在拒绝服务攻击中,这种方法是一种较为有效的方法;应用包过滤的技术,配置正确的路由器和防火墙,采用防火墙或网关等设备进行拦截;从保障主要业务不受影响方面考虑可采用异常流量的清洗与回注技术。

3 流量控制的应用

流量控制设备正常运行后,系统管理员可以通过日志分析校园网络的流量,一般高峰期在上午的 10 点 30 分和下午的 4 点 30 分,晚上 10 点左右又是一个小高峰,晚上 10 点半之后,流量逐渐下降,直到次日的上午 8 点。

鉴于这个结果,管理员可以按照时间制定策略,白天可以控制点对点的流量,限制小一点,夜间放大点对点的流量,按照规律合理地使用带宽资源。

通过日志,管理员观测到部分终端计算机在完成下载功能后,继续供其他用户下载。管理员可以相应的限制其上传的速度和通道带宽,可以有效保护网络带宽的资源。

根据网络带宽管理和用户的不同需求,管理员合理安排不同规则的控制策略,使得有限的带宽资源得到合理的利用,满足高等院校师生员工的需要。保障了包括网页浏览、电子邮件、SQL(Structured Query Language)数据库等核心业务,而对于点对点类下载、视频流量进行了有效的限速处理,对网络中各用户的上网行为进行有效管理,提高内部教职工的工作效率,为学校网络规划和带宽扩容提供科学的依据。

当然,流量控制设备也有不足之处。流量控制设备的关键技术指标是特征码,对新的网络协议、应用类型应该在流量控制设备上及时更新特征码库,用以满足用户新的需要。而一般特征码库的更新都在新的网络协议、应用类型出现之后,所以存在暂时网络流量不受管控的现象。管理员还可以自定义特征码,为不同的环境定制相应的特征码库,使师生员工有一个良好的网络环境。

4 结 语

通过上述所采取的控制策略,解决了校园网网络拥塞等问题,对校园网的流量进行控制后,基本上能保证学校的正常教学、办公及科研等网络的应用。

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] 崔燕,汪斌强,陈庶樵,等. 基于行为特征加权的 P2P 流识别方法的研究[J]. 计算机工程与设计,2009,30(20):4805-4807.

[3] 刘瞳红,纪越嶂. 下一代应用层防火墙性能及其测试[J]. 计算机工程,2006,32(11):169-171.

[4] 林维镭. 中小型校园网流量的控制方法[J]. 武汉工程大学学报,2011,33(4):97-99.

Application of traffic control of campus networks

XU Wei, LI Xing-jun

(Technique Center of Modern Education, Hubei Engineering University, Xiaogan 432000, China)

Abstract: Different kinds of classic traffic prediction methods were reviewed. By comparison of their suitable data, prediction precision and suitable scene were presented. Using TTNET1000 to improve network bandwidth management services actively, effectively and intelligently, and some methods were taken according to the regularity drawn from the daily records of the traffic control facility, so as to raise the rate of campus networks utilization. Experimental results prove that this method is simple, and can meet the needs of real-time monitoring campus network traffic due to the better performance indicators.

Key words: network management; network traffic; traffic control

本文编辑:邹礼平



(上接第 75 页)

Control and principle of islanding effect of photovoltaic grid-connected

GAN Jia-liang, LI Zhi-min, TAN Huai-jiang

(School of Computer and Information Science, Hubei Engineering University, Xiaogan 432100, China)

Abstract: The islanding problem in grid-connected photovoltaics system was analyzed and several methods of detecting islanding effect were compared. There was non-detecting zone problem in the conventional methods of islanding detection, and the islanding detection method based on the power balance of small changes frequency was proposed. This method has the advantages of no undetected zone, high response speed and no influence on the output active power of the system. The simulation results by Matlab/Simulink show the method is effective.

Key words: grid-connected photovoltaics; islanding detection; grid-connected inverter; Simulink

本文编辑:苗 变