基于 ACL 控制校园网 P2SP 下载流量的研究与实现①

周迪民 段国云 (湖南科技学院 现代教育技术中心 湖南 永州 425100)

摘 要： P2P (Peer-to-Peer，点对点)下载技术是校园网带宽控制的技术热点，此技术的应用占用了校园网大量的出口带宽，80%的出口资源被 20%的用户所占用，造成了校园网带宽的瓶颈。分析 P2SP (Peer-to-Sever&Peer)技术原理，结合校园网络的设计及使用的特点，提出了利用基于时间的 ACL (Access Control Lists,访问控制列表)来控制用户访问 P2SP 资源索引服务器以控制下载流量的具体实现方法。校园网出口实际测试结果显示，本方法能准确控制 P2SP 流量。

关键词： P2P；访问控制列表；流量控制；资源索引服务器

Research and Implementation of Controlling P2SP Download Traffic of the Campus Network Based on ACL

ZHOU Di-Min, DUAN Guo-Yun

(Dept. of Modern Education Technology Center, Hunan University of Science and Engineering, Yongzhou 425100, China)

Abstract: P2P is used frequently in campus network technology. The application of this technology takes up a large number of bandwidth in a campus network. 80% of resources are occupied by 20% of users, which results in a bottleneck of a campus network bandwidth. According to the principle of P2SP technique and the characteristics of a campus networks design and use, this paper proposes concrete approaches to limit the number of P2SP resource server users based on ACL，which is used to control the net traffic.

Keywords: P2P; ACL; traffic control; index server

基于 P2P、P2S (Peer-to-server，点对服务器)技术的下载应用在方便了用户下载的同时，严重占用出口资源，80%的出口带宽被 20%的用户所占用，对校园网流量产生了巨大的影响[1]。在带宽资源有限的校园网络中，为满足教学和科研的需要，合理规划带宽，对部分网络应用进行控制将成为网络管理人员必须面对的课题。控制 P2P 流量的方法中，多数是采用封端口的技术[2]，但仅能控制部分 P2P 流量，针对动态端口技术所开发的 P2P 下载工具将失控。文中分析 P2SP 技术的工作过程，结合网络出口设备，采用 ACL 技术控制下载主机与资源索引服务器地址之间的连接，截断用户获取资源服务器地址。这种方法可减轻网络压力，进行深入研究对加强校园网带宽管理具有现实意义。

1 校园网P2P存在的问题

1.1 安全隐患

P2P 的核心技术与当前流行的攻击技术的核心非常相似，它使用成千上万台被控制的计算机对被攻击目标(如：Web 服务器)发起分布式的拒绝服务攻击

① 基金项目:湖南省教育厅课题(09C449);湖南省自然科学基金(08JJ6043)
收稿时间:2010-04-05;收到修改稿时间:2010-04-22

(DDOS)。迅雷、电驴等一些基于 P2P 应用的软件穿透现有的防火墙，利用虚拟网络技术组建成一张虚拟的逻辑网络供用户高速传递数据，缺少必要的安全机制；因此，从局域网内部打开网络安全防护漏洞，在为用户提供高速文件传输的同时，为各类病毒、恶意代码的传递创造了有利条件。

1.2 关键业务无保障

P2P 类应用软件在工作时，试图建立尽可能多的链接来占用带宽以达到最高的下载速度。随因特网的快速发展，P2P 应用越来越广泛,音频、高清视频等大型文件对于单个网络节点的计算机来说，要完成一个下载周期需要一定的时间。在 P2P 虚拟网络中，各逻辑相邻节点的地理位置可视为无穷远，而参与 P2P 网络的节点数量很多，从而导致校园网出口的上行带宽明显高于下行带宽，消耗了大量的出口带宽。

在我校校园网环境中，使用基于 FreeBSD 平台的 Panabit 网络应用分析系统对校园网出口流量进行统计(如图 1)，已有 72.4%的带宽被 P2P 所占用，严重影响了我校正常教学、科研等关键业务的开展。

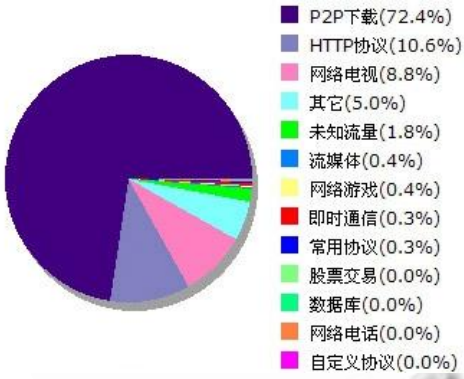

图 1　校园网出口流量统计

2　P2SP工作原理

P2SP 技术是 P2S 技术和 P2P 技术的结合体，是 P2P 技术的进一步延伸，它不需要文件资源服务器，充分利用了用户网络的“上行带宽”，实现用户间数据的传输。通过多媒体检索数据库这个桥梁把原本孤立的服务器资源和 P2P 用户资源整合到了一起，利用服务器性能资源优势和用户上行带宽的优势，以达到下载速度更快、资源丰富、稳定性更强的目的[3,4]。传输过程原理如图 2 所示。

以迅雷为代表的 P2P 下载工具是采用 P2SP 技术开发，支持多协议、多资源超线程技术下载的下载工具。网络中任一用户使用基于 P2SP 原理的工具下载资源，需经历以下步骤：

图 2　P2SP 工作原理

(1)客户端向索引服务器发出下载资源请求；

(2)进行相同资源的检索，并将结果返回给用户端；

(3)连接服务器所传递的资源地址，所有资源服务器或个人电脑同时向客户端传输下载内容的不同部分，以加速下载；记录当前下载用户的资源信息，存入资源服务器待下一用户使用。

通过 P2SP 工具下载的过程进行分析，每个下载用户均需要连接 P2SP 资源索引服务器，以获得下载地址；因此，我们只需控制用户连接资源索引服务器地址成功与否来控制基于 P2SP 技术的下载。

3　流量控制

3.1 抓包位置的部署

网络协议分析软件以嗅探方式工作，它必须要采集到网络中的原始数据包，才能准确分析网络故障。如安装的位置不当，采集到的数据包将存在较大的差别，从而影响分析的结果，无法反映网络真正存在的问题。

校园网应用是网络应用中最活跃的分支，网络管理和维护也比较有代表性。在设计时，如图 3 所示，常采用经典的三层网络结构，对出口数据进行分析时，在核心交换机中将出口数据镜像到核心交换机的某一端口，此时协议分析软件可以捕获整个网络中转发的数据。

3.2 索引服务器地址收集

收集迅雷服务器地址可通过 DNS 解析、出口镜像抓包等方法来获取。如果使用 DNS 解析的方法来获取地址，将无法得出新增加或未进行域名绑定的资源索

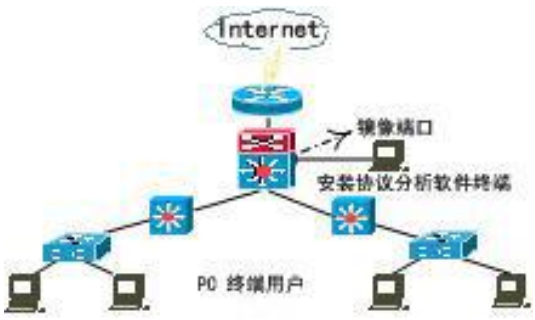

图 3 捕获网络数据

引服务器地址。出口镜像的方法是在 linux 系统环境下安装 Tcpdump,置于出口分析所经过的数据包。可以通过图 4 所示脚本来过滤数据包，并将服务器地址写入到文本文件中。

```
#!/bin/sh
# create new chains
/sbin/iptables -F thunder_fw 2>> /dev/null
/sbin/iptables -F thunder_in 2> /dev/null
/sbin/iptables -N thunder_fw 2> /dev/null
/sbin/iptables -N thunder_in 2> /dev/null
# anchor to main chains
/sbin/iptables -d input -j thunder_in
2>/dev/null
/sbin/iptables -d forward -j thunder_fw
2>/dev/null
/sbin/iptables -I input -j thunder_in
/sbin/iptables -I forward -j thunder_fw
echo "Building deny rules for Thunder
begin"
while read i;do
        /sbin/iptables -i thunder_fw -s $i -j drop
        /sbin/iptables -i thunder_fw -d $i -j drop
        /sbin/iptables -i thunder_in -s $i -j drop
        /sbin/iptables -i thunder_in -d $i -j drop
```

图 4 数据包过滤脚本

经过上述分析，得出近百个服务器 IP 地址。由于地址不连续，造成部分地址无法进行汇聚，不能进行汇聚的地址在写 ACL 时，需要一条一条加入。对于部分连续的地址段进行汇聚，得出地址段以方便编写 ACL。

3.3 ACL 的组成

ACL 是应用在路由器、交换机、网关等网络设备接口的指令列表[5]。它读取数据包第三及第四层包头中的信息，如源地址、目的地址、源端口、目的端口等；根据预先设定好的规则，设备接口对包进行过滤，从而达到访问控制的目的。

交换机路由器中的 ACL 有标准 ACL 和扩展 ACL，区别主要体现在匹配和过滤流量的条件上[6]。标准 ACL 可检查 IP 包头的源 IP 地址，并以此为匹配条件对流量允许或拒绝；而扩展的 ACL 可基于包的目标地址、源地址和网络协议及其端口来匹配和过滤流量。随着网络的发展和用户要求的变化，各类网络设备支持基于时间的访问列表(Time Access Control Lists,T-ACL)，它可以根据一天中的不同时间或者根据一周中的不同日期来控制对应类型数据包的转发，为网络的流量管理工作带来更大的便捷和灵活性。

3.4 创建 ACL 策略

基于 P2P 资源的下载方式是用户从网上获取资料的主要手段。根据图 1 中，P2P 流量占据了近 80%的出口带宽，利用 ACL 封迅雷资源索引服务器的方法将无条件地禁止了迅雷的下载。这种“一刀切”的流量管理策略不能满足用户的需求，我们应该结合实际应用及时间变化规律来制定校园网带宽管理策略。

根据我校对带宽使用的具体情况，为保障教学及各项关键性应用的进行，规定在每周的星期一到五工作时间内，限制迅雷的下载；在周末以及其它休息时间开放 P2P 的应用带宽，这样以达到人性化的管理。

4 出口迅雷流量测试

校园网出口网关采用两台基于 Linux 操作系统的 Router OS 软件路由器对校内数据进行转发。在核心交换机上将整个网络出口数据的端口镜像到监控服务器所接的端口，采用 Panabit 对出口数据进行分析统计。基于时间的 ACL 可以在核心交换机上启用，也可以在出口网关启用，所达到的结果完全一至。下面实验是在网关上启用 T-ACL 来控制迅雷的资源服务器地址，图 5 为 T-ACL 的部分关键代码。

```
/ ip firewall address-list
.....    //省略的部分代码
add      list="Kunlei"      address=58.61.39.206
disabled=no
add  list="  Kunlei  "  address=58.61.39.209
disabled=no
add  list="  Kunlei  "  address=58.61.39.211
disabled=no
add  list="  Kunlei  "  address=58.61.39.212
disabled=no
add  list="  Kunlei  "  address=58.61.39.214
disabled=no
add  list="  Kunlei  "  address=123.129.242.168
disabled=no
```

图 5 T-ACL 核心代码

图 5 中的配置，限制了每周周一到周五中的上班

时间内(9:00 到 17:30)，不允许校园网内用户用迅雷下载 P2P 资源。图 6 是未执行 T-ACL 前，校园网出口迅雷流量监控图。根据图 6 分析，用户在 9:00 到 14:30 时的迅雷流量在 100M 左右，下午 14:30 到 17:30 间，迅雷流量峰值 200M，最高值达到 240M 浪费了巨额带宽资源。图 7 是执行了 T-ACL 后出口的流量监控情况，发生了明显的变化；在 ACL 控制的时间范围内，流量明显下降，因为只控制了迅雷流量，其它 P2P 类下载依然存在，流量不会下降到零。与图 6 相比，同一时刻的流量已明显下降，峰值时间已推移到 19:30 的 260M。保证了在办公、教学及科研的时间内网络能通畅的运行。通过两个图的对比可以看出，通过这种方式来控制校园网流量，取得了很好的效果。

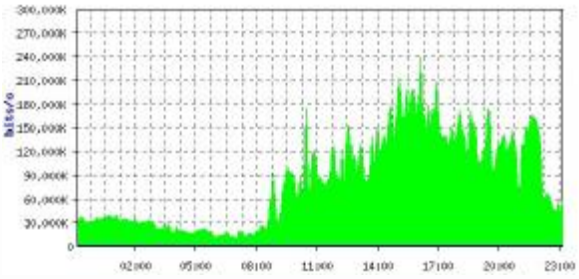

图 6　执行 T-ACL 前流量监控图

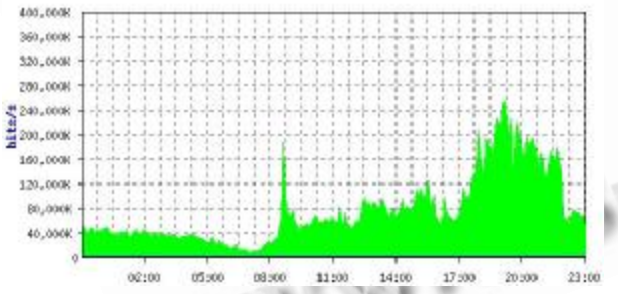

图 7　执行 T-ACL 后流量监控图

5　结论

文中针对现有校园网中 P2P 流量占用大量出口带宽和现状和 P2P 流量难控制的现像，结合已有的 P2P 的控制方法，分析了 P2SP 协议的工作机制，提出了在核心交换或出口防火墙上使用 T-ACL 控制用户获取 P2SP 资源服务器地址的方法来控制以迅雷为代表的 P2SP 下载流量。经校园网出口实验证明，将 T-ACL 应用到出口来控制 P2SP 的流量是一种较好的策略；但 P2P 技术的发展日新月异，要将此技术推广应用到其它 P2P 类工具下载流量的控制以达到更好的效果和更高的可信度，还需要进一步分析采用更加全面的综合性策略。

参考文献

1 马淑文.基于 P2P 应用的校园网带宽管理研究.计算机工程与设计,2007,28(12):5736－5738.
2 邢小良.P2P 技术及其应用.北京:人民邮电出版社,2008.
3 刘贵宝.基于 P2SP 的流媒体技术在远程教育中的应用探索.软件导刊(教育技术), 2008,1(6):90－91.
4 陈巍.迅雷软件在网格技术中的商业应用.电子元器件应用, 2009,11(3):77－79.
5 诸晔.用 ACL 实现系统的安全访问控制.计算机应用与软件, 2005,12(3):111－114.