高校校园宽带防私接的研究

易 铭
（中国联通武汉分公司，湖北 武汉 430040）

摘要：校园宽带市场作为宽带业务最优质的市场，是各家运营商重点争夺的热点。在校园市场的争夺中除了资费的竞争，最有效的手段就是推出满足用户需求的资费套餐同时可实现收益的不断增长。目前各运营商在发展校园宽带中遇到主要的问题是学生用户私接上网的问题，该问题严重影响了运营商的宽带收入，导致投入回报比低。校园网学生私接行为主要有两种：一是利用硬件，即使用宽带路由器共享上网；二是利用专门的一台服务器安装代理软件共享上网。面对用户的私接行为，在总结与分析目前市场上各种防私接的解决方案的基础上，加上对校园市场中用户、校方、运营商三方的深层次需求分析基础上，创新的提出了宽带防私接解决方案，既提高了用户的满足度，满足了校方安全监管要求，同时能为运营商增加收入，是一个实现三方共赢的创新解决方案。

关键词：校园；防私接；运营商；共赢创新
中图分类号：TP393.18 **文献标识码：**A **文章编号：**1673-1131（2019）05-0241-04

Abstract:The campus broadband market, as the best market for broadband business, is the hot spot of various operators.In addition to the competition of fees, the most effective way to compete in the campus market is to introduce a set of fees to meet the needs of users, and at the same time to achieve the continuous growth of revenue. At present, the main problem that operators encounter in the development of campus broadband is the problem of students'private access to the Internet. This problem seriously affects the broadband income of operators, resulting in low input-return ratio. There are two main types of private student behavior in campus network: The first is to share the Internet by using hardware, that is, using broadband routers. The two is to use a special server to install proxy software to share Internet.。Faced with the user's private connection behavior, on the basis of summarizing and analyzing various solutions to prevent private connection in the current market, and on the basis of analyzing the deep-seated needs of users, schools and operators in the campus market, this paper innovatively puts forward a broadband anti-private connection solution, which not only improves the user's satisfaction, but also satisfies the school's side. Safety regulatory requirements, while increasing revenue for operators, is a tripartite win-win innovative solution。

0 引言

在对目前市场上各种防私接的解决方案进行了系统的分析与总结，武汉联通通过对用户、校园的需求进行了分析整理，认为不能简单照搬或套用目前的防私接解决方案解决武汉联通的问题，而应以为用户提供更好上网体验的基础上提高经济效益为校园宽带业务的改造目标，并提出了武汉联通校园宽带改造目标如下。

1 防私接改造的必要性

1.1 宽带上网用户

通过提供差异化的资费套餐疏导用户私接问题：对于用户私接上网行为，既不能简单一刀切的方式进行禁止，也不能放任自流影响收益，因此武汉联通创新的提出通过差异化的资费套餐疏导用户私接上网上网。即推出账号不可共享、账号可共享 2 个或 4 个不同用户使用等不同的资费套餐，学生可根据自己的需求选择满足适合的资费套餐，同时又解决了收入流失的问题，可实现双赢的局面。

1.2 校园管理者

上网日志留存及关键字过滤：公安部 82 号令即《互联网安全保护技术措施规定》要求记录并留存用户访问的互联网地址或域名，在公共信息服务中发现、停止传输违法信息，并保留相关记录，能够记录并留存发布的信息内容及发布时间，应当具有至少保存六十天记录备份的功能。在进行校园网络改造时，校方为规避法律风险，往往强制要求运营商网络具备上网日志留存及关键字过滤功能。

1.3 运营商

（1）基于应用价值优化带宽，提升资源利用率：校园是典型的高带宽消耗用户，学生用户大量长时间使用 P2P、视频等高带宽应用，造成高峰时间网络拥塞，用户投诉增加，用户上网体验较差，影响了武汉联通的品牌形象。基于应用价值优化带宽方法可根据不同应用的价值实施流量保障或流量限制策略，如对于低价值 P2P 应用可在高峰时段进行限制，对于网页、IM 等高价值应用可进行流量保障预留带宽，可极大程度优化带宽资源，提升资源利用率。

（2）分析用户行为助力市场营销：通过对学生上网流量的应用层面分析，可了解学生上网偏好，如喜欢的游戏、热门网站、视频等等，有助于后续开展针对校园用户的精准营销。

2 私接上网技术原理

目前，从技术上来说，学生通过代理、共享方式上网主要为两种技术：NAT 和 PROXY。

NAT：基于网络层的包重组技术。此项技术本来是为了解决 IPV4 地址资源严重不足而产生的。可以实现多个私有 IP 共用一个公网 IP 地址实现网络访问的目的。但在国内这个技术被大量的应用到代理和共享上网上。NAT 一般情况下是通过出口设备（如路由器、服务器）上的多个网络接口，其中一个接口设置为公网地址，另外的接口设置为内部地址。通过特定的地址转换软件，通过修改数据包的源 IP 和目的 IP，端口等，从而实现共享上网的目的。常见的路由器一般都具备 NAT 功能，WINDOWS 下的 Winroute、连接共享、sygate 等均是此原理的实现。（包括各种路由器如无线路由器、宽带路由器等）。

PROXY：即应用代理，和 NAT 的主要区别在于 NAT 实现的是整个三层协议的转换。对被私接的客户端用户透明。而 PROXY 则是基于应用层，只能实现特定的协议代理。目前主要有两种代理形式：HTTP 代理和 SOCKS 代理。HTTP 主要应用于 HTTP 协议，而 SOCKS 代理则可以支持多种协议。

2.1 客户端防私接技术

该技术需要强制用户使用专用登陆 PPPoE 客户端，在客户端包含防代理的程序，如果用户没有使用防代理客户端，系统会在用户登录后，退出警告页面，同时阻止用户上网上网。正常的合法用户要上网，必须使用客户端认证登录。客户端运行后，是作为一个服务程序来运行的。客户端程序对本机网卡上所有收发数据报文会进行监听。针对不用的代理行使，客户端会做出不同的处理，以防止被代理的机器上网。包括如下情况：

⑴ 使用双网卡做 NAT：可禁止用户使用双网卡，包括虚拟网卡设备

⑵ 单网卡做独臂 NAT：路由被代理的数据包和本机正常的数据包有一个很明显的区别，就是源地址或者目的地址均不是本机 IP。

所以客户端对源地址或目的地址均不是本机 IP 的数据包会进行阻隔。从而被代理的机器无法上网。；

⑶ 使用路由器，一个人拨号后大家共用：客户端会提取本机的真实 IP 并提交给认证服务器，认证服务器会比较这个提取的 IP 和认证报文所用的 IP 是否一致，不一致则拒绝认证。故这种情况主机根本无法拨上号；

⑷ 使用 CCPROXY 等 HTTP，SOCKS 代理：客户端会监听本机的端口，发觉请求的报文中来自临近的局域网，则拒绝连接本机端口，以此来限制使用应用代理。

主要缺陷：由于需要强制学生用户安装客户端，在推广过程中会遇到来自学生的较大阻力，严重时甚至导致学生转网。

2.2 非客户端防私接技术

由于客户端防私接技术需要强制学生用户安装客户端，易引起学生的反感而遇到较大推行阻力，由此产生了非客户端的防私接技术，在不要求学生安装任何客户端的情况，通过对学生上网的数据进行应用特征的分析从而发现用户的私接行为。

目前的非客户端防私接技术主要技术原理如下：

⑴ 基于 Cookie 监测的非客户端防私接技术

①技术原理：通过给 PC 种 Cookie 的方式检测用户的上网私接行为。

②主要缺陷：但由于某些浏览器如 360、搜狗等为解决同时打开多个 QQ 空间问题，不同页面的 Cookie 可以分离开，这样种 Cookie 的方式存在误判的风险。

⑵ 基于单应用的行为特征检测

①技术原理：在给 PC 种 Cookie 的方式检测用户的上网私接行为的基础上，通过对 QQ 应用指纹特征进行识别，从而共同进行检测。

②主要缺陷：解决了通过单一的 Cookie 检测方式产生的误判可能，但是由于通过 QQ 应用的特征检测依赖于用户是否使用 QQ 应用行为，有一定漏判的可能。

3 校园宽带防私接的主要思想

在分析了武汉联通需求基础上，武汉联通创新的提出了校园宽带防私接整体方案，经过前期的试运营效果良好，目前已经在武汉进行分阶段的全面推广。

3.1 基于多应用的行为特征检测非客户端防私接技术

在传统非客户端防私接技术存在漏判、误判的缺陷下，为了进一步提高防私接识别率，对互联网主流应用的特征进行了分析，提取了主流应用的“特征指纹”，应用的“特征指纹”是指通过对应用的 DPI 分析，在数据包中发现包含多个用户的特征关键字，从而准确的识别用户私接行为以及私接的用户数，目前已经建立了包含 QQ、360、PPS、迅雷、搜狗输入法等多种应用的完整特这指纹库，通过对多种应用的组合检测可以很大程度的提高识别的准确性。主要采取的技术如下：

⑴ 用户全应用分析：通过现网数据分析学生用户的应用偏好及常用的应用类别；

⑵ 应用指纹特征库：在用户的全应用分析的基础上，通过 DPI/DFI、弱特征识别、智能识别等技术，提取用户主流应用的指纹特征库，并通过应用指纹特征库匹配用户的上网行为，通过多种应用指纹特征的加权来判断用户的私接行为；

⑶ 行为关联分析：在对用户进行分析时，完整分析用户的上网行为，并通过行为间的关联特征提升识别的精确度。

3.2 准确识别上网私接的用户数量

在提高识别用户私接上网行为检测的准确度基础上，能够精确定位出上网私接的用户数量。主要采取的技术如下：

通过用户的全应用分析、应用指纹特征库及行为关联分析的基础上获取用户数。

3.2.1 降低防私接技术的维护管理难度

目前使用的上网私接功能由于主要通过定制来实现，在学生用户的使用体验及电信设备维护管理上略有不便，并过多依赖厂商的维护与管理，为提升学生用户及电信管理员对设备的使用体验，将实现上网私接用户检测功能在主设备的模块化，并提供友好的人机界面，方便的设备升级。主要采取的技术如下：

⑴ 设备配置模块化：将上网私接用户检测功能在主设备的配置模块化，成为主设备的标准功能；

⑵ 设备升级简化：将通过提供在线与离线的升级方式，并支持更新应用特征指纹库；

⑶ 提醒友好化：对于检测到有上网私接行为的学生能够友好提醒，同时提醒界面可以在线定制。

⑷ 报表例行化：定时提供分析报表，并按照指定的格式发送到管理员邮箱。

3.2.2 10G 万兆高性能处理能力

随着网络流量的增加，检测设备同样需要满足流量增加的需求。目前可实现在 10G 万兆设备上实现防私接技术。满足校园不断增长的流量扩容要求。

3.2.3 用户上网行为管控

管控用户的互联网访问行为。包括过滤色情、反动网站，尤其非法论坛、BBS 等；过滤用户向公网 BBS、论坛发布的言论；对用户使用 QQ、MSN、等聊天软件进行限制；用户收发的 Email 要全面管理和过滤，避免用户与非法组织通过 Email 联

系给单位造成影响；向公网上传的文件同样需要控制；以及用户发生的其他各种网络行为进行全面管控。

3.2.3 用户上网日志留存

记录用户访问的 URL 地址、网页标题、甚至是网页内容，向公网论坛、BBS 发布的言论、包括向公网 Email 站点张贴的 WebMail 内容，用户使用 QQ、MSN、飞信等 IM 的聊天内容，全面记录用户收发的所有 Email 邮件，以及其他各种网络访问行为。全面的日志记录既满足公安部 82 号令要求，同时为日后的网络行为审计提供基础。

4 防私接项目方案实例

武汉联通校园宽带防私接改造目前已经部署了三个学校：武汉理工大学（升升公寓）、华夏学院、汉口学院，三个学校中除了升升公寓使用 PON 接入，其他均采用 LAN 方式接入。

设备均串行部署在园区网上行到联通机房的链路上，根据上行链路情况配备相应 bypass 设备，配置独立的管理网口连接互联网。设备故障或者调试重启均可以自动 bypass，有效避免发生网络中断故障。串接方式上三个学校大致相似，均为链路聚合方式。

升升公寓园区为 PON 方式接入，园区网接入到华为 5680T PON 设备上后，两条 10GE 上联至联通主机房华为 9312 上。防私接设备 AC9680 双网桥串接在该链路上，配合部署了双路 bypass 设备。

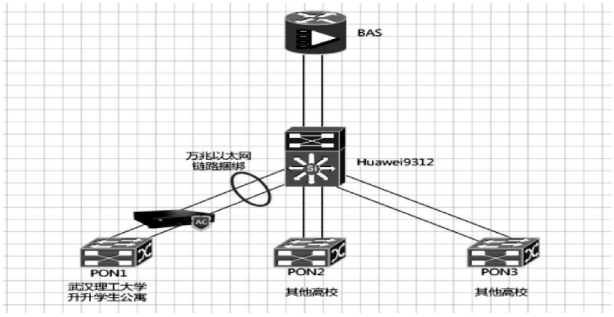

图 1

华夏学院园区为 LAN 方式接入，园区网接入到华为汇聚交换设备上后，四条 GE 上联至联通主机房。防私接设备 AC9600 四网桥串接在该链路上，配合部署了四路 bypass 设备。

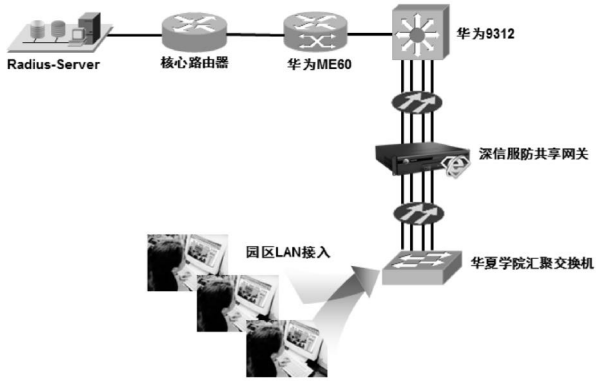

图 2

汉口学院园区为 LAN 方式接入，基本情况和华夏学院一样。防私接 AC9600 四网桥串接在该链路上，配合部署了四路 bypass 设备。

设备配置了 PPPOE 单点登录，实现了以拨号账号方式识别出在线用户：

图 3

图 4

图 5

设备设定了防私接检测阀值和冻结时间，实现了对私接用户的识别和冻结并且可以根据效果进行灵活的修改：

图 6

图 7

5 结语

防私接设备上线后，伴随着持续地观察调整，目前各校区防私接效果良好，私接用户开始下降，新增开通入网用户数开始上升。

以汉口学院为例，私接用户数目从每天 300-400 个，下降到每天 100-200 个，使用私接方式上网的数量的用户有了明显

的下降，同时，该校区的入网用户数，从去年三千多人上升到今年的接近一万人，有了很明显的效果。

下图中显示，开学附近 9 月 10 日，当天检测到统计私接行为共计发生了 347 次。

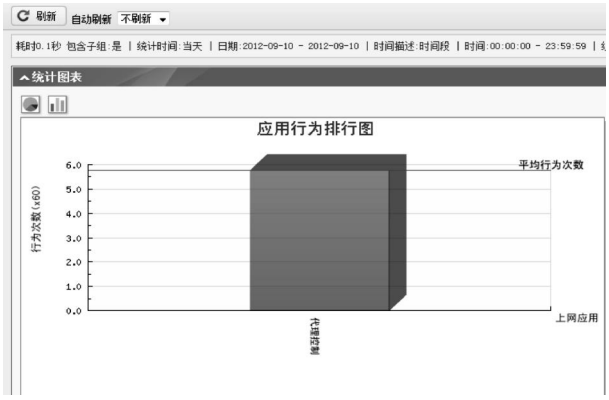

图 8

图 9

下图中显示，截至 10 月 28 日，当天当天检测到统计私接行为共计发生了 144 次。

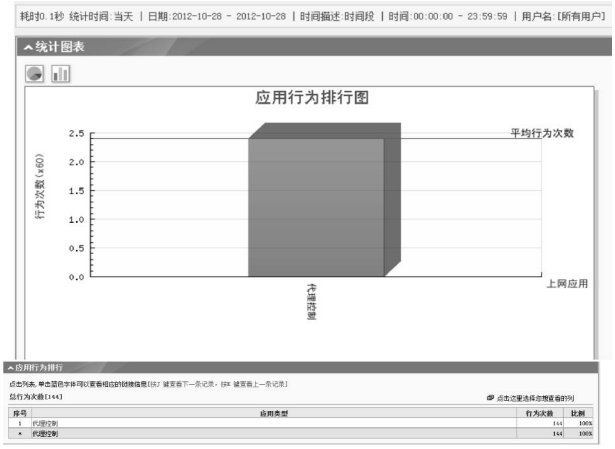

图 10

从开学到现在，整个学校出口的流量从当初的最高峰 1.5Gbps 上升到目前的 3Gbps，流量和用户数都有了明显的提升。但是从私接行为发生的趋势来看，目前私接行为趋势各个峰值的次数比才开学时有了明显的下降。说明了私接用户数量的下降和总流量的上升成反比，防私接的效果明显。

下图显示了近期一周出口总流量趋势。

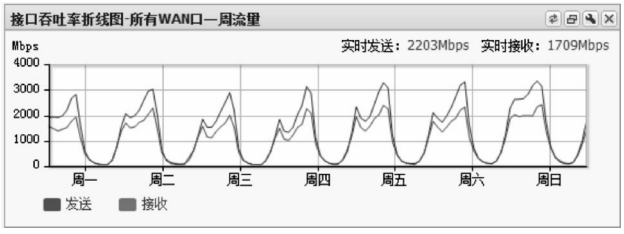

图 11

下图显示了才开学 9 月某天私接行为趋势。

图 12

下图显示了 10 月某天私接行为趋势。

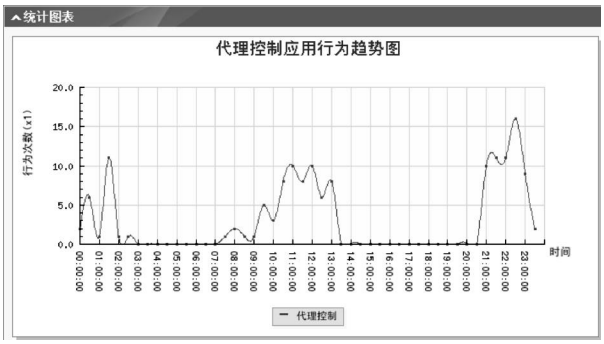

图 13

设备上线后已经持续平稳运行两个月以上，没有出现过故障停机现象。通过不断的总结和完善，目前各个校区设备均正常运行并发挥出了重要的作用，有效减少了私接上网的用户数，提升了新入网人数。

作者简介：易铭，湖北武汉人，硕士，湖北武汉联通计划建设部项目经理。

（上接第 240 页）损耗+建筑物、树木遮挡产生的损耗+大气吸收损耗。自由空间对电磁波损耗可根据式(1)算出 建筑物对电磁波损耗可参考图 4 算出；小片树林对电磁波的损耗可参考表 1 算出。当建筑物、树木遮挡导致信号传输路径上的损耗较大时，可提高通信塔的高度来满足损耗的要求。

当终端和基站天线所接收的信号大小适中时，此时的信号是正常传输的，此时通信塔的高度才是合理的。

3 结语

根据无线通信设备的无线发射功率、无线灵敏度计算出传输路径上最大可接收的损耗，传输路径上的实际损耗以及基站天线覆盖范围，计算出所需通信塔的最低高度，可有效减少建设设计失误以便减少不必要的损失。

参考文献：

[1] 李宗谦,佘京兆,高葆新.微波工程基础[M].清华大学出版社.

[2] 刘立国,王海松,史晓新,盖轶冰,丁国文.树冠中电波传播路径损耗的研究及模型的建立[J].电波科学学报,第 21 卷第 6 期 2006 年 12 月.

[3] 王海松.树林中电波传播路径损耗的研究[D].山东大学硕士学位论文,2005 年 5 月.