

# 计费网关系统在多出口多核心校园网的部署研究

田小萍, 孙建刚, 陈金焘, 陈 平  
(北京师范大学 信息网络中心, 北京 100875)

**摘 要:**随着网络日新月异的变化, 为了进一步保障校园网的安全, 规范和审计师生的上网行为, 保证学校对上网人员的可控性, 文中研究了计费网关系统及目前计费网关系统在校园网出口的实现方式, 分析了高校校园网的出口现状, 设计了在多出口多核心校园网的计费网关系统部署方案, 分析了该方案中的计费网关在网络正常运行模式下的数据流转发机制和链路异常模式的无中断转发机制。针对以上计费网关系统的部署方案进行了综合分析和比较, 最终减少了对用户上网的影响, 保障了校园网出口链路的稳定性。

**关键词:**计费网关; 多出口; 多核心; 校园网; Srun3000

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1673-629X(2011)02-0022-04

## Deployment Solution Research of Authentication and Accounting System Based on Multi-exit and Multi-core Campus Network

TIAN Xiao-ping, SUN Jian-gang, CHEN Jin-tao, CHEN Ping  
(Center of Information & Network Technology, Beijing Normal University, Beijing 100875, China)

**Abstract:** In order to further protect the campus network security and regulate and audit online behavior of teachers and students with the rapid development of the network, in the paper studied the realization methods of authentication and accounting system of campus network, analyzed current situation of campus network in many colleges. Proposed a deployment solution of authentication and accounting system based on multi-exit and multi-core network. Then analyzed the forwarding mechanism of data stream in normal mode and abnormal mode in detail, conducted a comprehensive analysis and comparison for the proposed deployment scenario of authentication and accounting system.

**Key words:** authentication and accounting system; multi-exit; multi-core; campus network; Srun3000

### 0 引 言

随着师生对网络需求的日益增大, 校园网在高校的教学、科研、学习、生活中发挥了越来越多的支撑作用, 同时也推动了教育信息化的发展。为了节约学校的网络资源, 为了防止非法人员使用校园网, 为了规范师生的上网行为, 保证学校对上网人员及上网行为具有可控性, 在校园网出口处部署了认证计费系统。校园网认证计费系统一般为一个透明网关, 部署在校园网的出口处, 直连校园内部网络和外部网络, 该网关可以为硬件设备, 也可部署在服务器上的软件系统。认证计费网关易于升级和移植, 和 802.1x 认证<sup>[1]</sup>相比, 不关心网络设备的厂家和型号, 和 PPPoE 认证<sup>[2]</sup>

相比, 可以轻而易举的跨越三层网络设备。

### 1 计费网关系统的概述

认证计费系统的关键在于认证计费网关, 实现了基于用户 IP 地址和账号的认证和计费<sup>[3]</sup>, 系统将网络服务划分为不同的层次, 使得用户可以免费访问校园网资源, 比如学校主页、电子邮件、院系主页、学校公共服务器等资源, 也可以缴费访问外网资源。从内网访问外网的所有数据包都流经计费网关, 它处理所有的数据包。通常, 计费网关禁止校园网内部网络和外部网络之间的通信, 当用户申请登录以后, 计费网关将检查其 IP 地址和账号信息, 如匹配将授权和外部网络的通信, 网关并记录该用户的网络流量和访问记录, 一旦用户注销认证信息, 计费网关将终止授权, 禁止通信<sup>[4]</sup>。

很多高校在校园网的出口处部署了计费网关系统, 通常情况下有良好的性能支撑, 可靠的安全设置,

收稿日期: 2010-06-03; 修回日期: 2010-09-25

基金项目: 北京师范大学校园网核心层改造资金

作者简介: 田小萍(1980-), 女, 山西昔阳人, 工程师, 研究方向为网络基础及应用。

完善的用户管理,灵活的计费模式,个性化的IP管理,系统的报表功能,详细的日志记录,多样化的认证模式。我校校园网出口处也部署了计费认证网关 Srun3000,以透明网桥的形式工作在数据链路层,是网桥模式;而不是路由模式,对于外界无法察觉认证网关的存在,这样有效防止了外界的攻击性,而且不影响原有网络的拓扑结构。

计费网关系统一般分为几个功能模块<sup>[5]</sup>:用户管理、后台管理、计费系统、流量采集、财务管理、统计报表等。用户管理实现了对用户资料、信息的增加删除修改等操作,甚至可以对用户进行带宽限制,监控用户流量、访问记录等上网行为,可以对在线用户实施灵活、有效的控制与管理。后台管理是管理员操作的核心部分,可以按照流量、时间、行为等制定各种灵活的计费策略,针对不同的用户使用不同的资费,用户也可根据需求自己选定策略;可以对IP地址进行各种权限的操作,比如IP漫游<sup>[6]</sup>:不同身份用户只能在各自的活动范围登录,也可以使得某些IP地址无须认证,直接和外界通信,计费网关系统灵活的后台管理大大减轻了网络管理员的负担。

## 2 校园网多出口多核心的网络拓扑结构

近年来,广大师生不仅满足于可以访问网络,而且对网络访问的速度及质量也有了更大的需求,应对这样的需求,校园网的出口从建网初期教育网的10M扩展到100M、1000M,但单纯的千兆教育网已逐渐无法满足师生访问国际网络资源的需求,随之又增加了电信、联通等多元化的网络出口<sup>[7]</sup>。由于计费网关服务器配置的网卡一般为千兆,所以出口也仅仅能达到千兆,但出口线路总带宽已超过千兆,在一定程度上限制了网络的迅速发展。

利用端口链路聚合双千兆的模式可解决以上矛盾,即核心出口双千兆聚合,同时要求计费系统支持双千兆,且必须运行在桥接模式下,不能为路由模式,出口路由器也采用双千兆聚合的模式,实际聚合的两端为核心交换机和路由器,所以中间的计费网关系统要求在桥接模式。但该模式下,出口的每一台核心设备和服务器都承载了校园网的全部流量,长时间处于高负荷状态,不利于设备的长期运行,且仍无法避免单点故障,单链路的模式无法保证校园网的高质量运行。

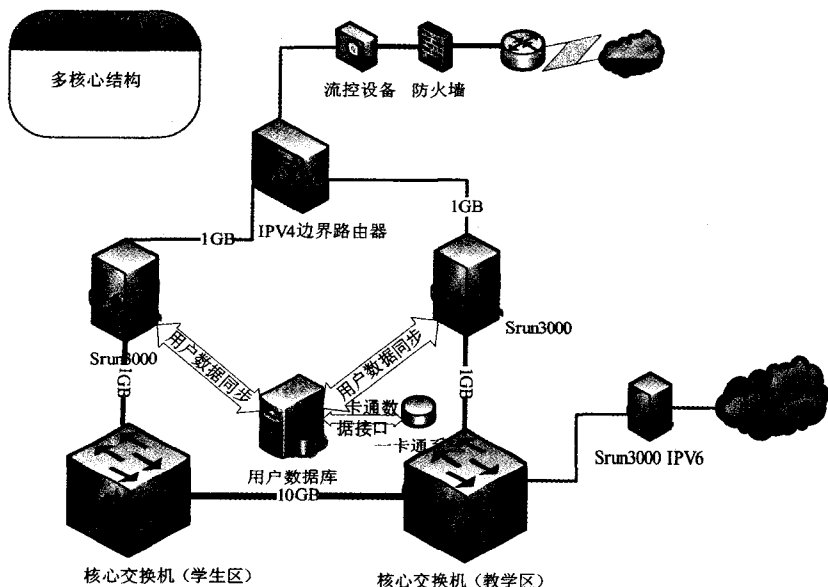


图1 多出口多核心的校园网拓扑图

针对以上的问题,文中设计了一个多出口多核心的校园网络拓扑图,如图1所示。校园网出口处教学区核心交换机和学生区核心交换机之间互联,采用OSPF动态路由协议即可以实现链路的相互备份冗余性,且学生区和教学区可分别划分在不同的区域<sup>[8]</sup>,避免路由收敛时间太长,影响网络性能,如果一个设备出现故障,可根据路由的优先级自动启用冗余备份线路,大大提高了网络的稳定性。边界路由器可以为一台,也可以为两台或多台,也可以直接为防火墙,减少了出口的设备,也相对减少了出口的成本和故障。交换机的冗余性、扩充性技术非常成熟,防火墙一般也支持硬件级心跳检测,然而适合高校校园网计费的软硬件系统和交换机、防火墙相比,可选择性比较小,因此出口认证计费网关的部署实现将成为一个重点、难点。

## 3 多计费网关的部署探讨

### 3.1 计费网关正常运行模式

如图2所示,校园网中的每一个用户,在链路正常的情况下,数据包转发的链路是确定的,比如用户A,经过的链路就是 学生区核心交换机→计费网关A→出口路由器→出口;用户B,经过的链路就是 教学区核心交换机→计费网关B→出口路由器→出口。认证网关A和B有各自的认证地址,用户A会弹出认证网关A的计费地址,用户B会弹出认证网关B的计费地址,用户认证通过后沿着各自的网关链路访问网络,两条链路相互独立、互不影响。

Srun3000认证网关系统运行在Linux平台上,采用Netfilter架构<sup>[9]</sup>,在内核对数据报文进行高效的处理,内核中存放着一张巨大的多维数据表。当数据报

文到达的时候,仅需对 IP 地址做分离处理,将 IP 地址分为三段,在多维数组中作一次对比即可实现对数据报文的验证,判断是否需要对该数据报文进行控制。这种对比办法的效率比较高,仅对比一次即可实现,同时在对比后可以对数据报文进行计费处理。

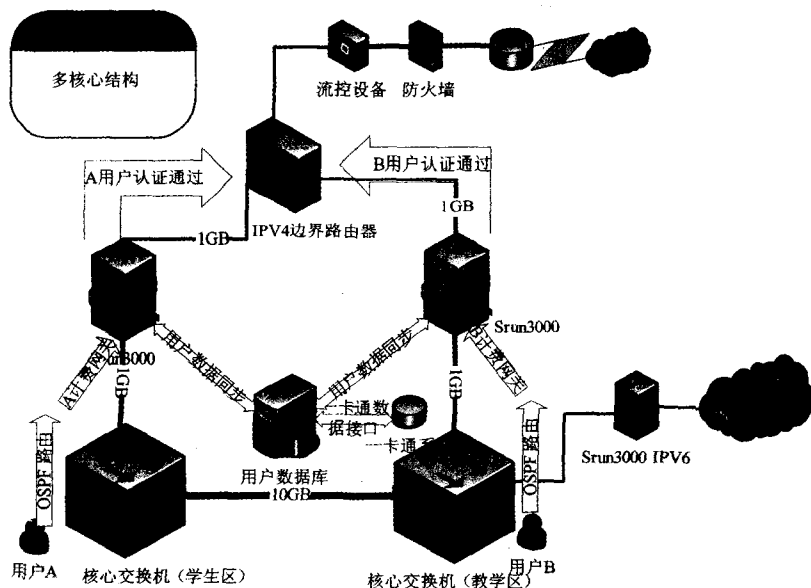


图2 计费网关系统正常运行模式

### 3.2 用户认证过程(以学生区的用户为例)

用户发起认证信息(见图3),经过校园网中的各节点网络设备到达学生区核心交换机,核心交换机将该认证信息转发至认证网关 GW1, GW1 按照预先设定的规则进行验证,验证通过后返回验证成功信息。用户的认证请求经过任何一个网关都将被重定向返回认证页面,认证通过后,用户的信息将被同步到两个网关上,用户的数据可以从任意的网关通过。每个计费网

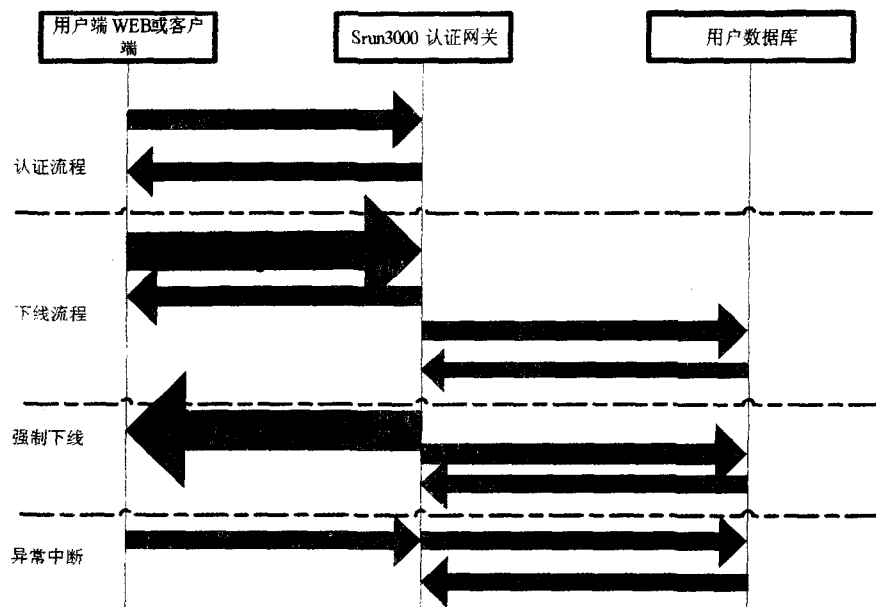


图3 用户认证流程

关都有自己独立的用户信息表和用户信息同步程序,在计费网关服务器启动时,自动和数据库进行连接,从中读取数据,保存在计费网关的内存表中。每隔一分钟,同步程序和数据库进行一次数据交换,同步用户数据。

当用户上网结束正常离线时,向 GW1 发起下线请求 Logoff-Request, GW1 将返回用户下线成功 Logoff-ACK, GW1 向用户数据库写入下线明细,写入完成后 DB 会返回写入成功信息。如果数据库服务器出现故障,网关无法连接数据库时,将数据保存在本地,其中用户数据可保存 5 万,明细数据可达到 10 万条。

当用户被迫下线时(同时在线人数达到最大,或登录后未离线,在校园内其他地方再次接入或者被系统管理员强制离线),向 GW1 发起被迫下线的指令

Force-Off,同时 GW1 向数据库写入信息。

当发生异常中断时,用户向 GW1 发送 Keep-live 信号消失, GW1 收到信息号向数据库写入异常中断记录。

当其中的计费网关 A 宕机或出现故障时, A 线路出现中断的情况下(即一个认证网关,两个核心交换机的模式),学生区核心交换机会通过 OSPF 协议路由自动将 A 用户的数据包路由到教学区核心交换机,用

户的认证数据会通过右边的计费网关 B 得以顺利转发,保证用户认证的畅通性。因在 A 线路原来认证通过的用户,认证通过信息已经被同步到用户数据库,由于链路的中断,数据会自动选择 B 链路通过,用户也无需再次认证。

计费网关系统异常运行模式如图 4 所示。

若其中一个核心交换机宕机,该种情况和目前学校的运行模式相同,一个核心,一个网关,另外一个网关处于空闲状态。

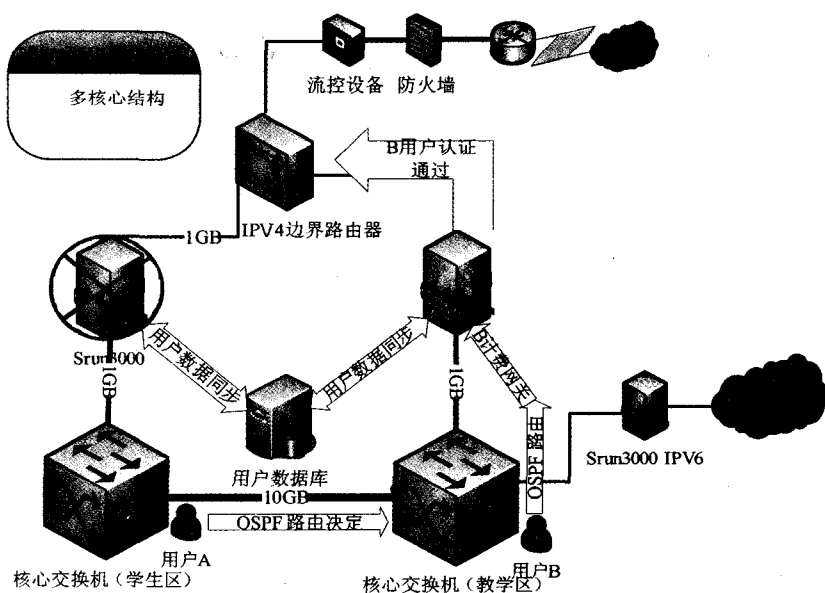


图4 计费网关系统异常运行模式

#### 4 结束语

文中提出的架构和目前的运行方案相比,出口核心交换机从一台增加为两台,甚至可以为多台,减小了出口核心交换机的负载;计费网关从一个扩展为两个,或者多个,实现了计费网关的冗余性和互为备份能力,使得任一核心交换机或者计费网关出现故障时,将不影响用户的上网,保障了校园网出口链路的稳定性。

在未来校园网的规模不断扩大,带宽增加到几个千兆,或是万兆的时候,整个校园网会呈现多种接入模式并存,学生区会呈现类似运营商的认证模式(PP-PoE),教学区采用 Portal 认证(网关),涉密区域包含无线网<sup>[10]</sup>采用 802.1x 认证,整个网络统一采用 Radius<sup>[11]</sup>+网关的计费<sup>[12]</sup>,迎合不同用户的需要。

#### 参考文献:

- [1] RFC3580. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)[S]. 2003.
- [2] RFC2516. A Method for Transmitting PPP Over Ethernet (PPPoE) [S]. 1999.
- [3] RFC3539. Authentication, Authorization and Accounting (AAA) Transport Profile[S]. 2003.
- [4] 张涛. 校园网部署集中式身份认证的利弊探讨[J]. 科技资讯, 2009(21):18-21.
- [5] 谭跃生, 张晓琳, 陶格图, 等. 基于 linux 的网关计费系统关键技术研究[J]. 内蒙古大学学报, 2003, 34(4):458-461.
- [6] 苏红军. 基于 WEB 方式的网络接入认证技术实现研究[D]. 昆明:昆明理工大学, 2004.
- [7] 罗伟雄, 时东晓, 刘 岚. 校园网多出口路由优化方案[J]. 计算机应用, 2009, 29(6):41-43.
- [8] 白丽媛, 金培莉, 岳江红. 分布式认证与计费系统在校园网中的研究与应用[J]. 中山大学报(自然科学版), 2009, 48(增刊):75-77.
- [9] 邹宗惠, 唐学文, 肖书成, 等. 校园网计费系统的研究与实现[J]. 计算机工程与设计, 2005, 26(1):132-134.
- [10] Tseng Yuh-Min, Yang Chou-Chen, Su Jiann-Haur. Authentication and Billing Protocols for the Integration of WLAN and 3G Networks[J]. Wireless Personal Communications, 2004, 29(3-4):351-366.
- [11] RFC2866. RADIUS Accounting[S]. 2000.
- [12] 田志英, 廖晓群, 赵安新. 校园网认证计费系统的研究与实现[J]. 计算机技术与发展, 2010, 20(5):202-206.

(上接第 21 页)

- [6] Chang N B, Chen W C, Shieh W K. Optimal control of wastewater treatment plants via integrated neural network and genetic algorithms[J]. Civ Eng Environ Syst, 2001(18):1-17.
- [7] Pai T Y, Tsai Y P, Loh H M, et al. Grey and neural network prediction of suspended solids and chemical oxygen demand in hospital wastewater treatment plant effluent[J]. Computers and Chemical Engineering, 2007, 31:1272-1281.
- [8] 田 奕, 乔俊飞. 基于遗传算法的 BOD 神经网络软测量[J]. 计算机技术与发展, 2009, 19(3):127-133.
- [9] 张烈平, 牛秦洲, 敖茂尧. 基于 OPC 的 MATLAB 与 MCGS

实时通讯的实现[J]. 微计算机信息, 2007, 23(21):54-55.

- [10] 胡剑杭, 陈 冲. 基于 OPC 技术的 MATLAB 实时过程控制系统[J]. 福州大学学报(自然科学版), 2008, 36:105-109.
- [11] 李安伏, 崔亚量. 基于 OPC 的 Matlab 与组态王的数据通信[J]. 电力自动化设备, 2007, 27(7):113-115.
- [12] The Math Works Inc. OPC Toolbox User's Guide [EB/OL]. 2004-10[2010-07-17]. [http://www.mathworks.com/access/helpdesk/help/pdf\\_doc/opc/opc.pdf](http://www.mathworks.com/access/helpdesk/help/pdf_doc/opc/opc.pdf).