

基于 802.1X 的可管理、可运营宽带校园网技术研究

李兴国 蒋玉明

(四川大学信息中心 成都 610065)

摘要 目前,高校校园网的应用越来越重要、规模也越来越大、功能也越来越强。但是,校园网也存在不少问题,诸如,缺乏合理的管理模式、灵活的计费策略,网络的安全及稳定得不到保障,急需一个合理的、细致的管理限制和收费手段来完善校园网,因此可管理、可运营宽带校园网成为当前高校网络建设的热点。本文对宽带 IP 网建设与发展过程中产生的多种认证与计费的前沿技术进行分析、比较和研究,重点介绍了 802.1x 协议体系结构,分析了协议的工作原理及认证机制,提出了基于 802.1x 协议的校园网认证计费解决方案。

关键词 校园网, 802.1x 协议, 认证, 授权, 计费

1 引言

高校经过近 10 年校园网的建设,已经建成覆盖学生宿舍、大部分家属区的庞大校园网络系统,为学校的教学、科研、行政、医疗提供了信息化平台。但建网初期只考虑了能尽快上网,只强调规模,随着越来越多的师生上网,网络管理、网络安全、用户控制方面的难题逐渐暴露出来,尤其学生还处于网络的探索阶段,对网络尤其感兴趣,存在着对网络的有意或无意攻击现象,因此存在网络性能低、网络盗用滥用的现象非常严重。

学校为了加快信息化建设的步伐,给师生创造一个一流的上网环境,使全体师生能方便自如地上网学习、交流信息、查询资料,保证网络运营有效畅通,要求把校园网建设成一个安全可靠、可运营、可管理的网络。为了避免滥用网络给学校和社会带来不必要的损失和危害,学校要求校园网要具有认证、计费的功能,实现灵活收费的策略。随着校园网络的迅猛发展,采用宽带接入、认证和计费系统,建立一个可运营、可管理的校园网络,已成为各高校网络运营的迫切要求。

随着用户数的急剧增加和对业务多样性要求的提高,网络的安全性问题也日益突出。由于传统认证方式对校园网中用户数据包繁琐的处理造成了网络传输瓶颈,而通过增加其他网络设备来解决传输瓶颈势必造成网络成本的提升,因此无法满足用户对网络安全性、高效性和低成本的要求。IEEE 802.1x 通过对认证方式和认证体系结构进行优化,有效地解决了传统 PPPoE 和 Web/Portal 认证方式带来的问题,消除了网络瓶颈,减轻了网络封装开销,降低了建网成本,从而成为当前校园网选型的一

个重要趋势。

2 校园网现状分析

校园网从结构上,可以分成核心、汇聚和接入这三个层次。从网络类型划分成教学子网、办公子网、宿舍子网等类型。与企业网相比,校园网独具特色:

1) 规模非常大,接入用户类型非常多,管理复杂性很强;

2) 具有双出口甚至多出口的结构,既通过 CERNET 中心,也有通过电信或其它的出口接入公众网;

3) 在接入层,更有高校网络最大的特色,学生密度非常高,思维活跃,接入类型非常多,有学生区、教学科研区、行政办公网、家属区、商用办公区等用户接入。

校园网目前存在的如下亟需解决的问题有:

(1) 缺乏合理的管理模式

校园网用户数量多,而且分散、流动性强,很难在虚拟的网络世界中实现统一的管理。学校中的用户身份不同:管理人员、教师、学生(留学生、研究生、本科生、进修生等),他们对网络的需求是不同的,对他们的管理也应该区别对待,这就使管理的难度又增加了一个深度。

局域网带来的弊端,被部分校园网用户利用。他们恶性下载占用带宽,当正常办公人员上网时,得不到足够带宽,使更多的用户无法体验到一流网络环境带来的速度,网络利用率不足 40%,校园网无法发挥它真正的价值。

(2) 缺乏灵活的计费策略

学校为网络支付的高额通讯费用,已成为学校沉重的财务负担。国家或学校拨专款对校园网进行

改造,希望建成“可管理、可运营的宽带校园网”。而建成后校园网的维护、升级、设备更新等经费问题都需要学校自行解决。网络建好了,成本怎么回收,“以网养网”被提上日程。利用有限的投资并在保证网络先进性的前提下,选用性价比最好的网络管理和计费系统,成为学校关心的重要问题。校园网用户多,要求计费策略非常灵活,需要计费策略不但要适应不同消费层次的要求,同时还需要该系统具有运营产品的领导性和前瞻性技术。也就是说学校可以通过强大的管理功能、灵活的计费策略来保障校园网的高效运营。

(3) 网络的安全性及稳定性得不到保障

网络安全包括两个方面。其一是网络内容的安全,目前 Internet 上网络资源良莠不齐,反动网站、黄色网站不断的腐蚀着校园这方净土,如何防止用户访问这类网站,跟踪并记录每个用户的上网记录,这已经成为校园网中必备的功能;其二是网络内容及设备的安全,目前针对校园网用户而言,学生网络使用技能较高,好奇心强,网络病毒防不胜防,都会对网站及其设备造成恶性攻击,导致网络无法正常运行甚至瘫痪。

综上所述,校园网急需一个合理的、细致的管理机制和收费手段来完善,达到可管理、可运营的要求。

3 宽带用户认证管理技术分析

总结以往校园网建设中的经验,探索出学生宿舍网与教工宿舍网差异化的需求,并结合学校对认证计费的需求,对所选用的认证计费系统提出了具体要求:系统能够有效地对用户进行接入控制,做到入网即认证,保证只有申请开通的合法用户才可能使用网络。对于接入用户进行账号/密码、IP 地址、MAC 地址、交换机 IP、交换机端口、VLAN ID 等多元素绑定,以确定用户身份。从功能上来说,学校希望在实现用户管理、灵活计费等基本功能基础上,还能够为用户提供自助查询服务,并且能够对管理员账号进行分级管理,支持远程登录的管理方式。对于系统的安全性,要求系统能够有效地解决 IP 地址冲突及盗用问题,有效地控制用户私自架设代理服务器。

根据学校对认证计费应用的需求,目前业界有三种主流认证方式可供选择:PPPoE、Web Portal 和 802.1x 技术。为了保证能够实现最优化的应用,在制定方案时对这三种技术分别进行了比较分析。实践证明,PPPoE 认证技术、VLAN+Web 认证技术、802.1x 认证技术均可很好地支撑宽带网络的计费、安全、运营和管理要求,但它们各自有自己的优缺点。

首先,PPPoE (PPP over Ethernet) 由传统的 PSTN (公共电话网) 窄带拨号接入技术发展而来,其优点是原有的窄带网络用户接入认证体系一致,操作简单且用户较容易接受。但 PPPoE 也有不可避免的缺点,PPP 协议与以太网技术存在本质的差异,需要被再次封装到以太网的帧里,存在封装效率问题,而且无法支持组播业务。

其次,Web Portal 认证最初是一种业务类型的认证,通过启动一个 Web 页面输入用户名/密码,实现身份认证。Web 认证目前已经成为小区或酒店网络平台的认证计费方式,通过 Web 页面,实现对用户是否有使用网络权限的认证。Web 认证方式有以下优点:无需特殊的客户端软件,降低网络维护工程量;无需多层数据封装,保证效率。但 Web 认证也有明显的缺点,Web 承载在应用层协议上,对设备的要求较高,建网成本高;易用性不够好,用户访问网络前,不管是 Telnet、FTP,还是其他业务,都必须使用浏览器进行 Web 认证;开放性不够好,Web Portal 认证方式均为各厂商私有,没有国际标准。

第三,IEEE 802.1x 称为基于端口的访问控制协议,其实质上是交换机基于端口对用户接入的合法性进行认证,进而决定允许或拒绝用户进入网络。在 802.1x 的认证体系结构中,引入了受控端口与非受控端口两个概念,即将交换机的一个物理端口分为两个逻辑端口,同时也首次将用户的认证报文流与业务报文流区分开来。其中,非受控端口一直处于常开状态,但只能传送用户的认证、计费报文流。受控端口则可以传送用户的业务报文流。当用户尚未进行认证时,受控端口处于关闭状态,即用户无法使用网络资源;只有用户在进行合法身份认证后,交换机打开受控端口,用户开始进行正常的业务流传输。用户通过认证后,业务流和认证流分开,对后续的数据包处理没有特殊要求,所有业务很灵活,都不受认证方式限制,易于实现多业务运行,去除冗余昂贵的多业务网关设备。IEEE 802.1x 协议为二层协议,不需要到达三层,对设备的整体性能要求不高,因此可以有效降低建网成本。

4 基于 802.1x 的认证计费技术

在分析比较了各种认证计费技术之后可以看出:由于 PPPoE 是传统 PSTN 窄带拨号接入技术在以太网接入技术的延伸,适合目前电信运营商对原有窄带网络用户进行接入认证及运行维护,不能很好地满足学校网络发展需要。Web Portal 的认证方式需要由应用层协议承载,无法实现用户接入认证的需求;如果采用此认证方式,还需要购买昂贵的网关设备,将增加建网的成本。802.1x 认证计费

技术以其独特的优势已成为目前校园网建设的最佳选择。

4.1 802.1x 的体系结构

使用 802.1x 的系统为典型的 C/S (Client/

Server) 体系结构, 包括三个实体, 分别为: Suppliment System (接入系统)、Authenticator System (认证系统) 以及 Authentication Server System (认证服务器系统), 三者之间的关系如图 1 所示。

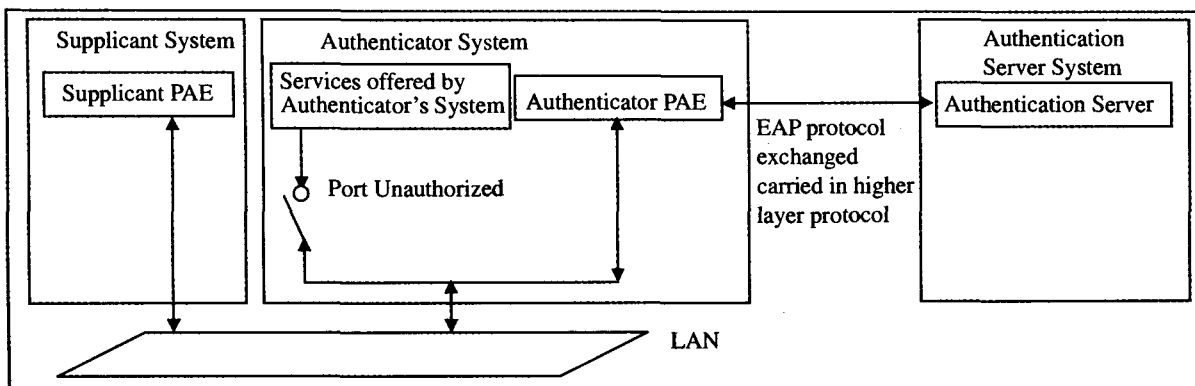


图 1 802.1x 协议的体系结构

局域网接入控制设备需要提供 802.1x 的认证系统 (Authenticator System) 部分; 用户侧的设备如计算机等需要安装 802.1x 的客户端 (Suppliment) 软件, 或用 Windows XP 自带的 802.1x 客户端; 802.1x 的认证服务器系统 (Authentication Server System) 则一般驻留在运营商的 AAA 中心。

4.2 802.1x 的认证过程

802.1x 的端口具有三种控制状态:

1) Force Authorized: 强开, 端口一直维持授权状态;

2) Force Unauthorized: 强关, 端口一直维持未授权状态;

3) Auto: 激活 802.1x, 设置端口为未授权状态, 并通知设备管理模块需要进行端口认证, 端口的控制状态决定了客户端是否能接入网络: 启用 802.1x 认证端口 (Auto) 的初始状态一般为非授权 (unauthorized), 在该状态下, 除了 802.1x 报文外不允许任何业务输入、输出。当客户通过认证后, 端口状态切换到授权状态 (authorized), 允许客户端通过端口进行正常通信。

由此可见, 802.1x 的认证过程, 就是控制系统的 802.1x 逻辑端口认证状态的过程。

在认证通过之前, 逻辑端口的状态为 unauthorized, 此时只能通过 EAPOL 的 802.1x 认证报文; 认证通过时, 逻辑状态切换为 authorized, 此时远端认证服务器可以下发用户的属性信息, 如 VLAN、CAR 参数、优先级、用户访问控制列表等; 在认证通过后, 用户的流量将接受上述参数的监管, 此时逻辑端口可以通过任何报文, 注意只有认证通过后才会有 DHCP 等过程。802.1x 的认证过程如图 2 所示。

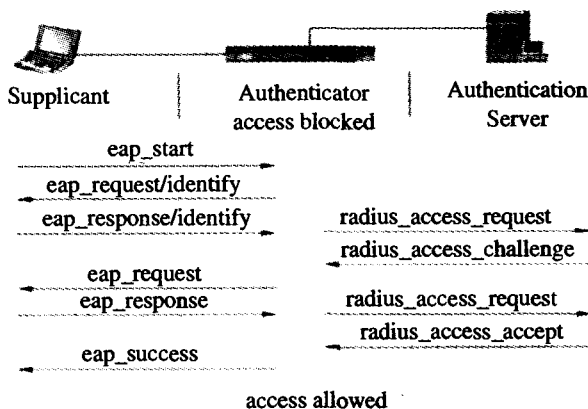


图 2 802.1x 协议的认证过程

4.3 802.1x 宽带网认证计费方式的特点

802.1x 协议仅仅关注端口的打开与关闭, 对于合法用户 (根据帐号和密码) 接入时, 该端口打开, 而对于非法用户接入或没有用户接入时, 则该端口处于关闭状态。认证的结果在于端口状态的改变, 而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题, 是各种认证技术中最简化的实现方案。

这种认证方式有如下几个特点:

1) 简洁高效: 纯以太网技术内核, 保持 IP 网络无连接特性, 去除冗余昂贵的多业务网关设备, 消除网络认证计费瓶颈和单点故障, 易于支持多业务。

2) 容易实现: 可在普通 L3、L2、IP DSLAM 上实现, 网络综合造价成本低。

3) 安全可靠: 在二层网络上实现用户认证, 结合 IP 地址、MAC、端口、账户和密码绑定技术, 使网络具有很高的安全性。

4) 行业标准: IEEE 标准, 微软操作系统内置支持。

(下转第 88 页)

分布式存储系统的实现是基于 Web 应用框架 Struts 进行开发的。Struts 是一个开放源码项目,具有高可配置性,有一个前端控制组件,一系列动作类,动作映射,处理 XML 的实用工具类,服务器端 Java Bean 的自动填充,支持验证的 Web 表单,国际化支持,生成 HTML,实现表现逻辑和模板等^[3]。Struts 底层是基于 MVC 设计模式的。本系统的实现基于 Struts1.1 版本。

系统的实现共分为 4 大部分:介质管理的相关实现,介质调用接口的实现,介质存储类的实现,介质预警的相关实现。介质管理主要实现介质管理的界面以及数据库服务器中 Media Server 记录信息的维护与管理;介质调用接口主要实现介质调用接口的定义(即从 Media Server 读写电子文档的方法定义),以及目前系统支持的三种 Media Server 的调用接口的实现;介质存储类相关实现包括实际介质目录的创建与移除,以及介质目录合法性的校验等;介质预警的实现主要依赖于文档管理系统中的消息管理模块和系统守护进程管理模块,系统通过一个介质预警检查的守护进程(该进程已注册到系统守护进程队列中,定期执行,且时间周期在系统内可配置),获得需要发送预警信息的 Media Server 后,组织好预警信息,将预警信息提交给消息管理模块即可。

结论 据 Jupiter Research 的报告显示,企业所产生的文档数量每 6~8 个月便以双倍或更快的速率急增,如此大的文档量对电子文档管理系统的

存储能力提出了新的挑战。这个分布式海量存储设计方案与其他存储方案相比较有很多优势^[4,5]。

(1)同时支持多种类型存储介质,包括本地文件系统、远程 FTP 服务器、本地或远程数据库服务器以及其他;

(2)存储介质调用接口与系统松耦合,更易于扩展;

(3)采用多种方式压缩存储,更节省存储介质空间;

(4)采用文档加密技术,使文档数据更安全;

(5)易于同其他大型信息软件系统,如 HIS, PACS, ERP 等集成。

目前这种分布式海量存储方案已成功应用于基于 J2EE 的文档管理系统中,系统运行一段时间以来状态良好,完全能够满足企业、政府等的文档管理和存储要求。

参考文献

- 1 付铮. 内容管理峰回路转市场需求日益攀高[J]. 电信工程技术与标准化, 2004(5): 73~75
- 2 邵志举. 海量数据高效存储与管理研究: 一种高效海量数据存储、管理与实时发布方案[J]. 现代软科学, 2006(3): 127~129
- 3 陈志凌, 程耀东, 刘爱贵等. 海量存储文件系统 CastorFS 的设计与实现[J]. 计算机工程与应用, 2006, 42(4): 108~110
- 4 周志华, 何萍, 尹建伟等. 基于 Web 的海量存储柔性分布式文件服务器设计[J]. 计算机应用研究, 2002(11): 14~16
- 5 杨本杰. 企业电子文档的安全存储和访问问题的研究[J]. 工业控制计算机, 2003, 16(11): 3~7

(上接第 32 页)

5)易于运营:控制流和业务流完全分离,易于实现多业务运营,少量改造传统网络即可升级成运营级网络。

结论 建设可管理、可运营的高校网络正成为 IT 业的热点之一,是互联网进一步发展的潜在市场。校园网络要做到学校要求的可运营、可管理和用网公平性,身份验证、授权和计费是必不可少的。利用 802.1X 认证方式,为高校运营提供了一个认证、授权和计费的整体解决方案。

802.1X 认证计费管理方案特色体现:与安全交换机结合,可以实现对用户账号、IP、MAC、交换机 IP、交换机端口、VLAN ID 六元素任意绑定的严格认证,实现包月、预付款、计时长、计流量、实时扣费等计费原型,更支持用户自定义的计费策略,并且支

持限制用户固定 IP 地址,或限制用户只能是 DHCP 动态获取 IP,或限制用户只能是静态设备 IP 地址功能,完全可以满足学校对认证计费的综合要求。

参考文献

- 1 Mamakos L, Lidl K, Evarts J, Carrel D, Simone D, Wheeler R. A Method for Transmitting PPP over Ethernet (PPPoE), February 1999
- 2 罗娟. 网络计费系统的关键技术. 网络世界, 2001(7)
- 3 钟健松. 宽带网认证计费方式比较. 北京朗新信息系统有限公司, 2002(10)
- 4 杜宾. 宽带城域网的建设与以太网的发展. 网络世界, 2002(3)
- 5 周卫东, 等. RADIUS 协议安全分析. 计算机应用与软件[J], 2002(11)
- 6 易正强, 王耀军. 基于 Proxy 的网络计费系统的设计与实现[J]. 计算机工程, 2001, 27(2): 166~168