

# 校园无线局域网部署及接入认证方式的探讨

严世强, 肖 众

(石家庄铁道大学 现代教育技术中心 河北 石家庄 050043)

**摘要:** 针对校园无线局域网建设中,面临的校园无线局域网部署的方式和接入认证方式的问题,探讨了无线局域网的部署中常见的几种方式,分析了各自的优缺点。提出了校园无线局域网应以本地转发模式进行建设的观点。给出了校园网无线局域网接入应该采用 802.1x 的方法,以及如何与现有有线网络实现统一用户身份认证。通过这种方案进行校园网无线局域网建设,就能够保障校园无线局域网的高效、便捷和安全,实现有线网和无线局域网的统一管理。

**关键词:** 校园网; WLAN; 802.1x; 认证方式

**中图分类号:** TP393.1 **文献标识码:** A **文章编号:** 2095-0373(2013)04-0102-04

## 0 引言

自20世纪90年代起,经过几轮的校园网建设,至今各个高校都通过有线方式建立了自己的校园网络。随着互联网技术的进步,信息化程度的提高,用户的需求也进一步增加。伴随着数字化校园工程的推进,学校的传统互联网应用也逐渐向移动互联的方向靠拢。更多的用户希望在校内,通过笔记本电脑、平板电脑、智能手机等各种无线上网工作,随时随地使用各种网络资源。因此,各个高校的校园网无线局域网建设方兴未艾,蓬勃发展,成为新一轮校园网建设的热点。

校园网无线局域网一般是依托现有的有线网络而建立,是有线网络的扩展和补充。通过无线局域网,校园网用户可以更便捷、更灵活地使用校园网各种信息资源,而这种便捷性和灵活性,对校园网的管理工作提出挑战。同时,如何依靠现有的有线网络,提高无线局域网的运行性能,规范化管理无线局域网接入用户也是建设校园网无线局域网需要认真考虑的问题。

## 1 无线局域网部署方式

传统上,对于无线点数较少,覆盖范围不广的区域,一般会采用胖无线接入点 AP(Access Point),如图1所示。这种方式需要对逐台设备进行配置和管理,无法形成一个整体,无法实现无线网络中的漫游服务功能。这种方式在校内无线点数比较密集,用户移动性比较频繁的情况下,是不适合的。

针对胖 AP 存在的问题,无线局域网厂商提供了瘦 AP 架构的产品解决方案。瘦 AP 将原先胖 AP 的绝大部分功能移到无线交换机 AC(Access Controller)。通过 AC 完成所管辖的无线局域网的所有 AP 的配置、管理和控制,实现了对瘦 AP 的零配置。AC 和 AP 间通过 CAPWAP(Control And Provisioning of Wireless Access Point)协议交互控制信息<sup>[1]</sup>。瘦 AP 架构能够

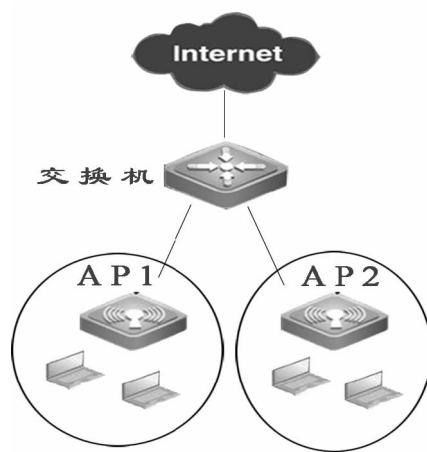


图1 胖 AP 部署示意

收稿日期: 2013-02-16

作者简介: 严世强 男 1973 年出生 高级工程师

对无线用户数据进行统一管理,并能实现无线射频资源的智能管理,简化了无线局域网的部署难度,降低了无线局域网的建设和维护成本。这种架构是目前进行无线局域网建设的主流技术方案。

瘦 AP 架构对于数据转发有两种实现模式,集中转发和本地转发<sup>[2]</sup>。

在集中转发模式下,如图2所示,AP和AC会构建一个数据隧道,这个数据隧道中传输的是二层数据,所有用户业务数据由数据隧道传送到AC处,再由AC转发。集中转发方式下,AC能对报文进行全面控制。由于AC处于无线数据交换的核心位置,无线加解密由AC完成,AC性能压力较大,在AC处易形成AC处产生单点故障和瓶颈。如果采用双AC热备的方式,又会增加建设费用。如果校园无线局域网建设着重于通过无线局域网本身即可以进行完成针对无线局域网用户的细节管理,如限制单个用户速率、加密管理等工作,集中转发模式才是一个恰当的选择。

在本地转发模式下,如图3所示,AC和AP间仅建立控制通道,但不建立数据隧道。用户数据不经过AC,直接由AP负责本地转发,等同于胖AP对用户数据流量的处理方式,在AP上直接转化为有线格式的报文,实现无线报文的宽带接入。在本地转发模式下,可以实现基于业务的最优化路由,提高网络服务的响应速度,而且避免了在大数据流量情况下,AC成为网络性能的瓶颈的问题。相对于集中转发模式,本地转发模式的网络结构较复杂,网络安全性较弱。但是,本地转发可以充分利用现有网络资源,如报文转发、端到端QoS、用户接入控制等提高无线局域网的安全性和可控性。校园网作为一个相对封闭的区域,移动用户较为密集,提高无线网络的访问速度应该是首要考虑的问题。经实践证明,本地转发模式的时延、丢包率和下载速率等表征网络性能的指标均优于集中转发模式<sup>[3]</sup>。所以,在校园无线局域网部署中,应优先考虑本地转发模式。

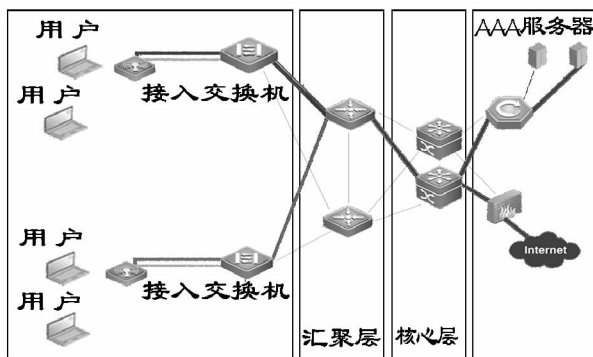


图2 集中转发模式

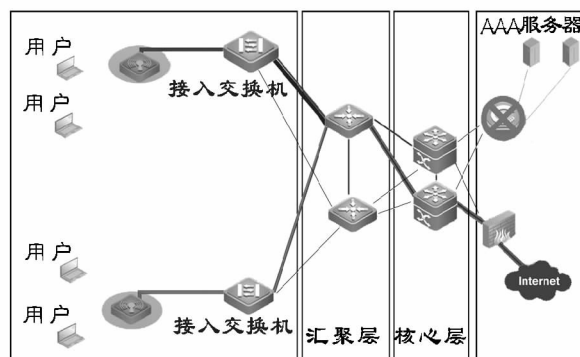


图3 本地转发模式

## 2 无线局域网接入认证方式

从网络安全角度考虑,一般需要无线局域网用户在认证后,方可使用校园网资源。为了方便管理,更为了方便用户使用,就需要通过现有的有线用户管理策略,实现对无线局域网用户的接入管理工作,即实现有线和无线局域网用户统一的身份认证。

当前,校园内提供接入的交换机一般都是可管理的智能交换机,在校园网出口处部署BAS(Broadband Access Server)系统,采用802.1x方式进行校园网准入管理方式,如图4所示。无线局域网本地转发模式下,无线准入一般使用Web Portal的方式,完成无线局域网用户的准入管理。为了实现用户的统一管理,AC作为BAS系统中Raidus Server的客户端,将用户通过web页面传递过来的用户名及密码信息,发送至Raidus Server进行校验,如果信息与Raidus Server信息一致,即认证成功,AC将控制AP,允许该用户通过该AP访问校园网。因为无线用户的准入信息和有线用户的准入信息共享同一个数据库,所以,就能够实现了有线和无线用户统一的身份认证。

无线局域网准入的Web Portal的方式,属于应用层的认证,用户事先要先通过DHCP服务,获取IP地址,然后才能发起认证工作。这样,往往会产生不进行认证的用户占用IP地址的现象。在校园这种用户较为密集的环境下,这种IP地址分配策略,较容易地产生单个AP的可用IP地址耗尽的情况,从而影响正

常用用户的使用。另外,被用户认证信息要通过 HTTP 协议的明文方式传递,存在一定的网络信息安全问题隐患。

如果无线局域网采用本地转发模式,就比较容易地实现同有线用户一样的 802.1x 认证方式,解决 Web Portal 方式的不利因素。无线局域网 802.1x 准入认证方式,在具体的部署上有两种方案可以选择:一种是与 AP 直接连接的交换机端口启用 802.1x 模式,由接入交换机完成 802.1x。这样,就可以将无线用户当成有线用户一样管理,无线用户使用的 802.1x 的 supplicant 与有线用户一致。为了保证 AC 对 AP 的管理,这种方式下,需要对连接 AP 的交换机端口进行相关配置,使得该端口透传 AC 与 AP 的管理数据传输。这种方式,淡化了 AC 的作用,无法实现无线用户的漫游服务,用户切换不同的 AP 时需要重新认证。

另一种是在 AP 上启用 802.1x 准入认证,认证信息经 AP 和 AC 的控制通道,传送至 AC,再有 AC 向 Radius Server 发起 802.1x 的校验认证工作,认证成功后,用户将获得相应的 IP 地址,AC 控制 AP 允许该用户访问校园网。对于 Windows 系统、IOS 系统、安卓系统自带的 802.1x 的 supplicant,即可完成无线局域网的 802.1x 认证过程。

一般地,有线网络的 802.1x 的认证过程中的加密协议一般是 EAP 或 CHAP<sup>[4]</sup>,而无线网络的 802.1x 的采用的加密协议为 PEAP<sup>[5]</sup>。对于前期部署支持 802.1x 认证的有线网络的 Radius Server 往往不支持 PEAP 协议。在这种情况下,可以升级现有的 Radius Server 来满足无线网络 802.1x 接入认证的需求。另外一个方法是,再部署一台支持无线 802.1x 认证的 Radius Server,AC 向该台服务器发起认证请求。这台 Radius Server 服务器使用有线网络 Radius Server 服务器的用户管理数据库,从而实现有线和无线用户统一的身份认证。实践证明,开源的 FreeRadius 以其丰富的协议支持能力,开放的系统接口,可以兼容现存的大部分商业 Radius Server,在校园网无线局域网建设过程中,是一个不错的无线局域网 Radius Server 的选择<sup>[6]</sup>。

### 3 结束语

在校园这个特殊的环境下,校园无线局域网建设的需求和方式具有自己鲜明的特点。结合目前无线局域网的主流技术,通过实践对比,校园无线局域网采用无线网络本地转发模式,有线与无线统一的 802.1x 身份认证,就能做到兼顾性能、安全、便捷、经济因素下,实现无线网络与现有有线网络的无缝对接。统一的无线和有线用户管理,也有助于无线局域网的后期运行维护和相关管理策略的制定。按上述方案设计和建设的石家庄铁道大学无线局域网,在实际运行过程中,产生了良好的效果。

### 参 考 文 献

- [1] 孟一飞. 基于 CAPWAP 协议的集中式无线局域网架构[J]. 网络安全技术与应用 2009(9): 29-31.
- [2] 史扬, 蔡自彬, 蔡贤森. 基于瘦 AP 架构实现 WAPI[J]. 信息通信技术 2009(3): 61-65.
- [3] 雒明世, 魏二虎, 柳建勇. WLAN 本地转发和集中转发应用模式分析[J]. 山东科技大学学报: 自然科学版 2010 29(6): 74-79.
- [4] IEEE Standard. RFC 3748. Extensible Authentication Protocol (EAP) [S/OL]. [2004-06-15]. <http://tools.ietf.org/html/rfc3748>.
- [5] IEEE Standard. RFC 4017. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs [S/OL]. [2005-03-20]. <http://tools.ietf.org/html/rfc4017>.
- [6] Gavinzhm. FreeRadius + OpenLDAP + PEAP 认证 [EB/OL]. [2009-01-21]. [http://www.chinaunix.netld\\_jh/49/1214563.html](http://www.chinaunix.netld_jh/49/1214563.html).

(下转第 108 页)

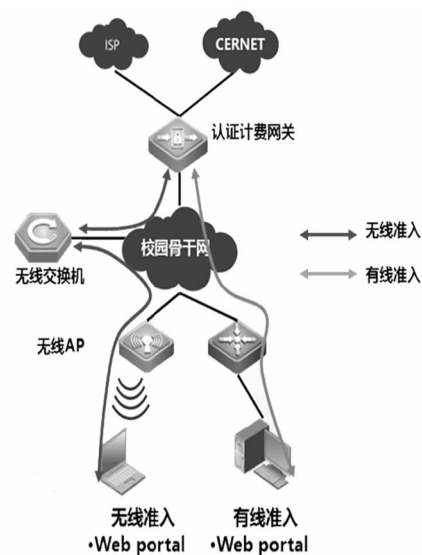


图 4 无线网认证方式

- [4]朱川曲. 采煤工作面瓦斯涌出量预测的神经网络模型[J]. 中国安全科学学报, 1999, 9(2): 42-45.
- [5]史峰, 王小川, 郝磊, 等. MATLAB 神经网络 30 个案例分析[M]. 北京: 中国航空航天大学出版社, 2010.
- [6]韩玉芳, 谢士宏, 杨龙. 马家坡瓦斯隧道设计等级的判定研究[J]. 石家庄铁道大学学报: 自然科学版, 2011, 24(4): 74-77.

## Gas Emission Forecast Based on GRNN

Ge Jiang

( School of Transportation and Logistics , Southwest Jiaotong University , Chengdu 610031 , China )

**Abstract:** This paper introduces the characteristics of the gas emission forecast and the GRNN , and points out the rationality of using GRNN to forecast the gas emission and its advantage over the BP. The forecast is carried out based on a case , proving that GRNN can solve the problem of gas emission.

**Key words:** neural ; gas emission; forecast; GRNN

( 责任编辑 车轩玉)

( 上接第 101 页)

## A Web Services Selection Method Based on QoS Comprehensive Matching

Zhang Cuixiao , Xu Li , Chong Li

( Major Computer Science and Technology , Shijiazhuang Tiedao University , Shijiazhuang 050043 , China)

**Abstract:** Currently , many selection methods of Web Services based on QoS don't have a comprehensive consideration of the QoS semantics , numerical processing and service requestors' personality needs on service quality. The method presented in this paper is to apply multi-attribute decision-making theory to the QoS value pretreatment and QoS comprehensive matching and to design comprehensive matching method of QoS parameter. The efficiency and feasibility of the method is verified.

**Key words:** semantic Web service; semantic similarity; QoS value similarity ( 责任编辑 车轩玉)

( 上接第 104 页)

## Campus WLAN Deployment and Access Authentication

Yan Shiqiang , Xiao Zhong

( Educational Technology of Center Shijiazhuang Tiedao University , Shijiazhuang 050043 , China )

**Abstract:** In view of campus WLAN deployment and access authentication method for the construction of the campus WLAN , the advantages and disadvantages of several common ways of WLAN deployment are analyzed , pointing out the campus WLAN should be constructed by a local forwarding mode. Campus WLAN access method using 802.1x is given , as well as how to achieve a unified user authentication with an existing wired network. WLAN construction of the campus network through this program will be able to safeguard the campus WLAN efficiency , convenience and security , and achieve unified management of wired and WLAN.

**Key words:** campus network; WLAN; 802.1x; authentication method

( 责任编辑 车轩玉)