

有线无线一体化的扁平校园网设计

谢胜军¹, 殷锋¹, 周绪川²

(1. 西南民族大学 校园网络管理中心, 四川 成都 610041; 2. 西南民族大学 计算机科学与技术学院, 四川 成都 610041)

摘要: 分析了高校校园网拓扑结构现存的问题, 依据扁平化的大二层网络设计思路, 提出了一种以 BRAS 设备为网络核心的有线无线一体化网络拓扑结构。该拓扑结构能够最大限度地保护现有投资, 只需在核心层增加 BRAS 设备, 将原有交换机全部作为二层设备上联至 BRAS 即可。利用 BRAS 设备的性能和特性完成了内外网用户的隧道建立、隔离、流控、故障定位等精细化管理; 利用大二层结构特性实现网内 IPv4/IPv6 双栈及多播业务, 各种品牌有线无线设备的统一管理。该拓扑结构应用在实际网络环境中时 BRAS 设备必须进行热备, 无线 AC 需要支持本地转发。

关键词: 校园网; 一体化; 扁平化

中图分类号: TP393

文献标识码: A

文章编号: 1000-436X(2013)Z2-0079-05

Cable and wireless integrated flat campus network design

XIE Sheng-jun¹, YIN Feng¹, ZHOU Xu-chuan²

(1. Campus Network Management Center, Southwest University for Nationalities, Chengdu 610041, China;

2. College of Computer Science and Technology, Southwest University for Nationalities, Chengdu 610041, China)

Abstract: The campus network topology of the existing problems was analyzed, and according to a large flat layer 2 network design ideas, a device for the network core BRAS wired and wireless integrated network topology was proposed. The topology can maximize the protection of existing investments, simply increasing the core layer BRAS device, and all of the original switches can be linked to the BRAS as a layer 2 device. BRAS equipment performance and characteristics were used to finish tunnel network users inside and outside the establishment, isolation, flow control, fault location and other fine management; large two-story structure features were used to achieve net IPv4/IPv6 dual and multicast services, various brands the unified management of wired and wireless devices. The topology used in the actual network environment BRAS equipment must be hot standby, wireless AC needs to support local forwarding.

Key words: campus network; integration; flat structure

1 引言

伴随 Wi-Fi 及云技术的不断发展、Cernet2 项目的快速推进, 高校针对校园网络应用需求正在不断更新, 传统校园网结构与管理模式正逐步呈现出许多难以应对的难题: 内部攻击与 ARP 类病毒的困扰、IPv4 地址紧缺、无法实现用户的精细化管理、原有相当数量网络设备无法支持 IPv6 协议、无法实现校园网络 IPv6 的多播, 有线无线不能统一管理。因此, 探索一个全新的校园网络结构体系以及相应的管理模式是目前高校网络管理者必须面对的一个紧迫课题。

2 传统校园网结构分析

目前, 绝大多数高校校园网有线部分采用的仍是以交换技术为主的经典 3 层组网结构, 分为核心、汇聚和接入 3 层结构形式^[1], 各层次的业务功能也有所区分。如图 1 所示, 接入层一般为二层交换机, 设备数量庞大, 但性能一般。它负责用户的接入、相互间隔离、带宽的限制、802.1X 认证、DHCP 侦听和 ARP 动态检测, 广播报文抑制双栈多播控制与分发等; 汇聚层一般为性能较好的 3 层交换机, 负责用户的 3 层终结及路由、ACL、QoS 功能实现^[2]、双栈多播控制与分发; 核心层负责数据的高速交换、ACL、QoS 功

能实现、与 Radius 的对接、双栈多播控制与分发等；核心层一般为性能较强的三层交换机，主要是一些对内交换及对外路由功能，还有部分对外的 ACL 和 QoS 控制，性能虽然强悍，但功能却相对弱化。

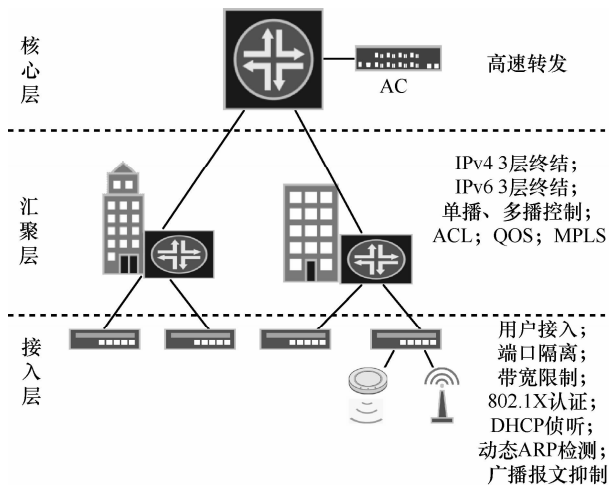


图1 传统3层校园网结构

在传统的3层校园网络结构中，越靠近用户接入边缘的交换机数量越多，虽然性能弱，但功能要求却多；逐年的建设投入导致接入层设备品牌不一，版本混乱，管理配置复杂多变。而且部分老旧接入设备不支持 IPv6 及 IPv6 多播控制，新建 Wi-Fi 网络无法和有线网络融合，不能实现流量的分布式转发，用户认证请求和高峰期流量对 AC 的压力过大。有线无线无法统一用户认证和精细化控制，校园网内有线无线设备分开管理，不能统一网管平台。用户使用有线和无线网络需要多次切换、多次认证，用户间及应用间不能有效隔离，相互干扰较大，安全无法保障。

在实际校园网环境中故障最多、维护量最大的一定是接入层和汇聚层的设备，在这样的网络结构中，处理一个简单故障往往涉及多个层面的多台设备，出现故障后，定位难、恢复时间长。而且校园网内的新功能新应用无法快速部署和实施，难以实现网络的精细化管理和控制。

3 一体化的扁平校园网设计

参考现在国内各运营商大规模网络发展的经验，网络结构正从复杂化的多层结构向简单的扁平化结构发展。扁平化的结构模式并不是网络结构物理连接层次上的简单减少，而是逻辑层次上的集中和简化。扁平化的网络结构不仅更有利于用户及设备的管理，也有着更高的效率。

3.1 一体化的扁平网络拓扑

如图2所示，在一体化的扁平校园网结构中，将传统的3层结构按照校内业务模式划分成业务控制和业务接入2个层面，也就是俗说大二层结构。核心部分变成了业务控制层，将3层路由交换机换成了 BRAS（broadband remote access server，宽带接入服务器）设备，汇聚和接入层不用改变，全部作为校内业务的接入层。

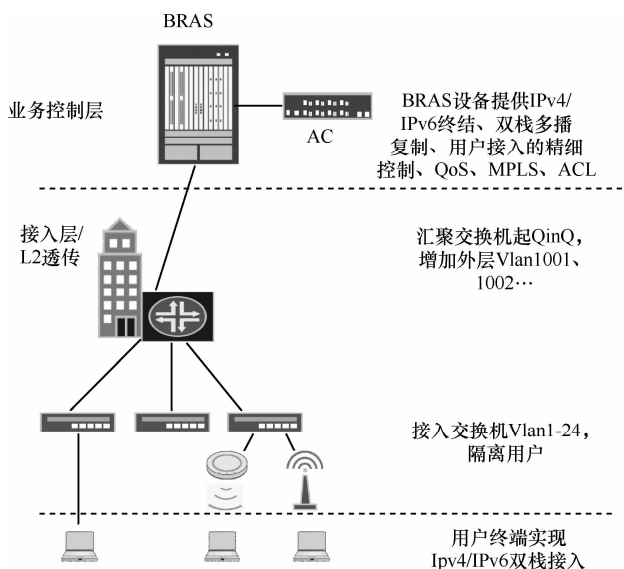


图2 一体化的扁平校园网结构

此结构按照网络业务分层，将原先校园网模糊的功能清晰化，整个网络更具开放性和扩展性，非常有利于校园网私有云的快速部署，也为校内的三网融合提供了可能^[3]。由性能最强、功能最丰富的 BRAS 设备配合新建或原有的 Radius，发挥核心设备的高性能、稳定性、可靠性等优势，提供集中的业务控制和有线无线用户的统一管理。汇聚和接入设备一般只需提供最基本的二层 VLAN 隔离功能，不涉及任何业务功能，因此在校园网内部署新的业务和功能时，不用考虑其是否支持，也无需考虑原有设备品牌型号等，有利于降低和保护数量众多的汇聚和接入层设备投资。

目前，部分高校校园网已经采用了以 BRAS 为核心的两层结构模式，选用了 Juniper 或华为公司的 BRAS 设备，利用 QinQ 技术实现了校园网的扁平化结构^[1]。用户终端采用 DHCP 模式接入校园网，自动获取 IPv4/IPv6 双栈地址，然后通过 BRAS 拨号访问校外网络。通过 BRAS 进行 IPv6 协议及 IPv6 多播信号的硬件复制和下发，在不更换原有接入交换机的情况下实现了全网的双栈和多播功能，前期

的投入得以保护，后期的投入也相对较低。

3.2 用户管理精细化

3.2.1 有线无线一体化认证

在该结构下，无线网络可以和有线网络同时使用“BRAS+Radius”的方式形成用户接入网络的统一入口^[4]，用户无需进行有线无线认证的切换，实现了用户的一体化认证。具体实现过程如图 3 所示。用户终端开机以 DHCP 的方式获取 IPv4/IPv6 双栈地址，根据自己的需要，发起 PPPOE 或 Portal 认证请求访问网络。

如果用户在使用有线网络的过程中还要使用移动终端连接无线网络，可以使用同一帐号再次发起无线网络的认证请求，BRAS 设备在接到请求后会根据设定好的策略，在断开或者保持有线网络连接的同时，通过用户无线终端发起认证请求。

该结构中 BRAS 设备可以为每个用户的接入提供一个虚拟子接口，在用户端和 BRAS 间建立专门的通道，用户之间以及业务之间能够被有效隔离，既可以避免用户之间的相互干扰，又实现了用户的精细化管理。

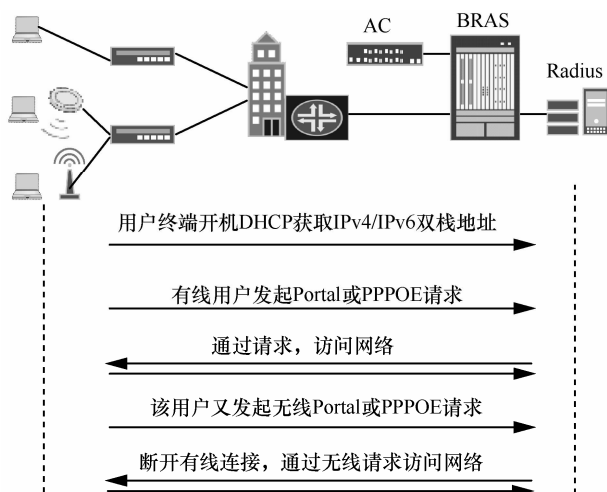


图 3 直线无线认证一体化

3.2.2 用户信息及状态可查可控

通过入网认证机制，用户通过 DHCP 获取地址的过程中，BRAS 就提供了用户接入校园网的各种信息，包括用户终端的接入时间、所处的交换机端口或 AP 位置，用户终端的 MAC 地址、IPv4/IPv6 地址等，这些信息可以准确地定位网内某台终端在何处、从何时、有线或无线方式连接进网络，上线/下线的的时间等，配合 Radius 和日志分析系统完全做到网内用户行为的可查可控。以华为 ME60 为例，查看离线帐号为“31100013”的用户信息：

```
[ME60]display aaa offline-record username
31100013
```

```
-----
User name: 31100013
Domain name: pppoe
User MAC : 8c2d-aa46-7ad4
注：用户终端的 MAC 地址
User access type: PPPoE
注：使用了 PPPOE 认证方式
User access interface: Eth-Trunk4.22
User access PeVlan/CeVlan: 23/1001
注：用户的内外层 Vlan
User IP address: 211.83.241.169
注：用户的 IPv4 地址
User IPv6 address:
fe80::8c1a:f535:bce9:c09c%12
注：用户的 IPv6 地址
User ID: 34526
User authen state: Authened
User acct state: AcctStopWait
User author state: AuthorIdle
User login time: 2013-07-14 09:26:34
注：用户上线时间
User offline time: 2013-07-14 12:35:57
注：用户下线时间
User offline reason: PPP with echo fail
```

3.2.3 用户端故障维护简单

由于全网采用了 2 层的扁平结构，校园网络管理人员可以远程针对网内任意一个接入层交换机端口实施端口镜像（接入交换机需支持远程镜像功能），可以在机房内模拟一个故障现场环境，如图 4 所示。针对现在高校多校区的普遍现象，无需管理员奔赴现场排查，不仅极大地方便了管理，而且提高了工作效率和服务质量。

3.2.4 用户速率及权限控制精细化

BRAS+QinQ+Radius 可以实现多样化多层次的用户速率及权限控制。在任意一个逻辑子接口（等同一个物理接口）上实现速率限制、访问权限控制，因此可以提供针对全校任意区域或用户实现单独的策略管理。在普遍采用多 ISP 接入的校园网环境中，配合类似于华为 ME60 的 DAA 功能（根据不同的目的地址进行带宽限制和计费），让用户自主地选择多样的网络服务和计费策略。

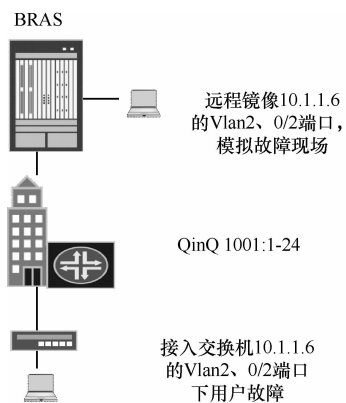


图 4 用户故障远程模拟

在无线网络中每个 AP 只能划分在一个 VLAN 中，而 AP 下同时存在数个用户，由于此网络结构下控制策略是针对每个用户的，所以即便有用户使用了 P2P 类高带宽的应用，仍然可以确保此 AP 能为其他用户提供稳定的服务。

3.3 统一设备管理

此网络结构相对传统的 3 层网络结构更易将校园网内多种品牌及型号的交换机（可网管）、路由器、信息安全、无线 AC/AP 等设备纳入统一的网络管理平台。定时轮巡采集数据，收集设备的工作状态、端口状况、链路流量等，并自动记录网内设备的中断、恢复时间，方便故障回溯。采集完数据后，可以自动地分析 IP、MAC、端口对应情况，并纳入数据库备查。还可以针对网内设备的电源、CPU、端口流量等指标设置阈值，进行实时告警，实现全网设备的统一管理。

3.4 出口管理精细化

现在高校校园网普遍存在有多条出口链路，此网络结构下，BRAS+Radius+出口流量控制设备可以针对不同的用户群制定不同的策略。用户可以根据自己的需要和经济能力自由地选择不同的带宽、不同的出口。校园网管理部门可以根据不同出口的经营记录，统计用户对网络的喜好和需求，为校园网的营运和发展提供可靠依据。

4 注意事项

1) BRAS 设备需热备

此结构下 BRAS 处于整个网络的核心部位，负责校内有线与无线网络各种业务的控制，一旦出现故障，整个校园网将面临瘫痪，必须进行冗余设计。

且多个校区需要多台 BRAS 进行热备，BRAS

的单台成本会比传统 3 层结构的核心交换机稍高。如果进行校园网结构的调整，核心更换需要较大的投入，但却可长期保留以前的汇聚和接入交换机，总体成本相对较低，其中一种多校区 BRAS 热备结构如图 5 所示。

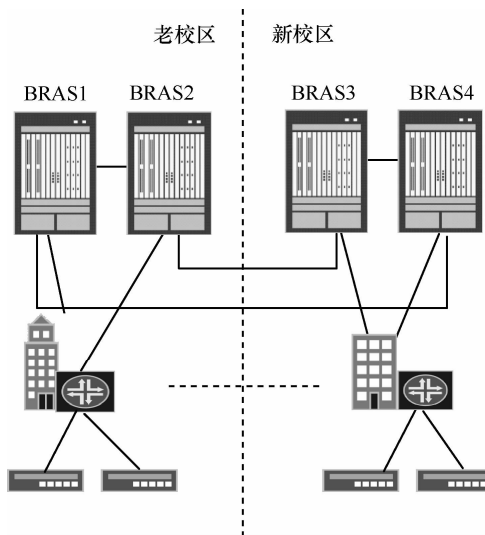


图 5 多校区 BRAS 热备

2) 部分不能隔离的业务受到影响

该结构下每个接入交换机端口都处于一个单独的 Vlan 中，实现了二层的完全隔离，且默认是需要通过认证请求才能接入网络的。这样就造成了校园网内部分不能隔离的业务受到影响。比如，同一个办公室或寝室内不能通过网上邻居的方式互传文件，所有的数据流量都必须经过网关，也就是 BRAS 才能实现内部文件的传递，以前“局域网”内的流量转向了校园骨干网络，对校园网吉比特骨干链路造成很大的压力，不过相对万兆骨干链路来说，这些流量不会造成任何影响。

还有，以前即插即用的网络打印机在此网络结构中也需重新调整，需要在 BRAS 上通过手工绑定 IP 地址的方式来保证网络打印服务。BRAS 上的配置可以通过脚本的方式实现，但统计校内各个办公室网络打印机的工作量却很大。

3) 无线校园网需本地转发

无线校园网中传统的集中式转发是将网内所有的 AP 管理、用户管理、数据流量全部集中在 AC 上，对 AC 的性能要求很高。随着移动智能终端的迅速普及，无线校园网的建设规模越来越大，用户也越来越多，AC 已经成为了无线校园网发展的瓶颈。有测试数据显示，在不同的信号场强中本地式

转发的平均延时只有集中式转发的 65%左右, 下载速度却达到了集中式转发的 125%左右^[5]。

有线无线一体化的扁平校园网要突破传统无线校园网结构的瓶颈, 实现有线无线的一体化, 无线部分就必须采用本地式转发设计。对控制流和数据流采用不同的处理方式, 只有 AP 的管理交给 AC 处理, 而用户的管理和数据流量则不再经过 AC, 直接穿过接入和汇聚交换机交由 BRAS 进行处理, 类似于胖 AP 模式, 如图 6 所示。

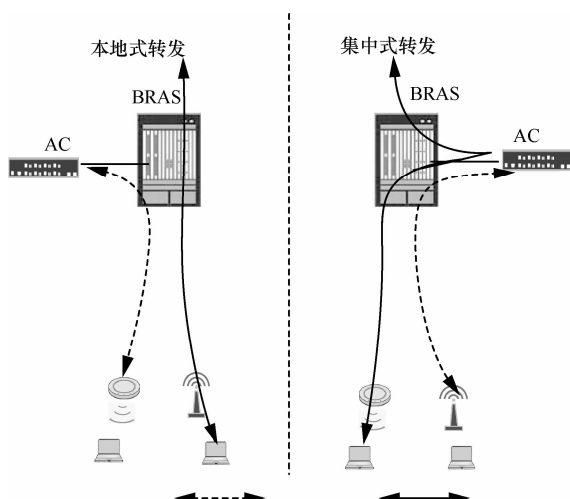


图 6 本地转发与集中转发

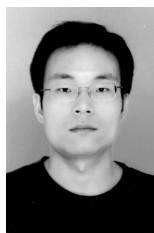
5 结束语

通过有线无线一体化的扁平校园网改造, 可以突破传统校园网的一些瓶颈, 将校园网划分为业务控制和业务接入 2 个层面, 在最大限度保护原有投资的前提下, 只需添加 BRAS 设备即可快速实现全网的有线无线融合、用户和设备的统一管理、IPv4/IPv6 双栈及多播等各种业务, 为校园网的私有云建设和三网合一打下基础。

参考文献:

- [1] 马安龙. 利用 QINQ 技术构建扁平化网络[J]. 电脑知识与技术, 2012, (5):3528-3529.
MA A L. Using QINQ technology to build a flat network[J]. Computer Knowledge and Technology, 2012, (5):3528-3529.
- [2] 刘紫燕, 黄义成, 胡峰. 业务感知技术的协议带校园网 QoS 研究与仿真[J]. 计算机工程与科学, 2011, (8):58-61.
LIU Z Y, HUANG Y C, HU F. Business perception technology agreement with campus network QoS research and simulation[J]. Computer Engineering and Science, 2011, (8):58-61.
- [3] 李战国, 张睿哲, 刘向东. 基于策略的三网融合体验结构研究[J]. 计算机科学, 2012, (9):74-77.
LI Z G, ZHANG R Z, LIU X D. Based on the strategy of triple play experience structure study[J]. Journal of Computer Science, 2012, (9):74-77.
- [4] 吕倩. 基于云计算及物联网构建智慧校园[J]. 计算机科学, 2011, (10A):18-21.
LV Q. Based on computing and Internet of things build wisdom campus[J]. Journal of Computer Science, 2011, (10A):18-21.
- [5] 维明世, 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, (6):81-85.
WEI M S, WEI E H, LIU J Y. WLAN local forward and forward the centralized application mode analysis[J]. Journal of Shandong University of Science and Technology(Natural Science Edition), 2010, (6):81-85.

作者简介:



谢胜军 (1977-), 男, 四川成都人, 西南民族大学工程师, 主要研究方向为网络运行管理研究。

殷锋 (1972-), 男, 侗族, 四川成都人, 博士, 西南民族大学教授, 主要研究方向为计算机应用软件测试。

周绪川 (1972-), 男, 四川成都人, 博士, 西南民族大学副教授, 主要研究方向为软件工程。