doi:10.3969/j.issn.1000-436x.2014.z1.021

扁平化高校基础网络架构探索与研究

林初建，张四海
（南开大学 信息化建设与管理办公室，天津 300071）

摘 要：在系统分析校园网现状的基础上，通过在校园网核心部署 BRAS 设备和高密度交换机，实现了网络核心的扁平化；通过旁路部署计费系统，采用 IPOE 技术，结合本地转发的无线组网方式，辅助联动式日志采集系统，实现了统一认证；综合全局安全策略、基于应用的互联网流量优化策略以及缓存系统的部署，实现了校园网边界的优化。实践表明，对基础网络进行系统性的扁平化改造，在提高网络性能，满足网络管理内在要求的同时，还可以提升网络用户的使用体验。扁平化的网络基础架构，在高校校园网中是切实可行的。
关键词：校园网；扁平化；统一认证；边界优化
中图分类号：TP393.1 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0107-06

Research at flat underlying network architecture of campus

LIN Chu-jian, ZHANG Si-hai
（Office of Information Construction and Management, Nankai University, Tianjin 300071, China）

Abstract: By systematic analysis of the status quo on the campus network, via deployment of BRAS and high-density switches, we deployed a flat network core, by deployment of accounting system through a bypass way, using IPOE access technology, combined with local forwarding wireless networking, assisted with linkage logging system, we achieved a unified user access certification, and we optimized the network boundary by integrating of global security policy, strategies for Internet traffic optimization base on application protocols and the deployment of caching system. Practice shows, flat underlying network architecture improves the network performance, meets the inherent requirements of campus network, while also improves users' experience. Flat network architecture is feasible for campus network.
Key words: campus network; flat; unified authentication; boundary optimization

1 引言

高校校园网作为教学科研的重要支撑平台之一，是高校信息化建设的基础设施，在高校的教学科研活动中发挥着重要作用。随着信息化建设与各种业务系统的深化，原先复杂的多核心多三层架构已无法适应新的发展需求，基于扁平化架构的基础网络成为校园网新的建设方向。扁平化校园网的建设目标主要集中在加强网络的准入准出认证机制，适应和满足国家法律及政策对于校园网用户的行为要求；加强校园网络设备的集中统一管理，降低校园网的管理难度和减少维护工作量；建设多业务承载网络，满足各类业务、各类应用和不同用户各种业务承载拓展的需求[1]。总之，整个校园网要实现高性能、易管理、精细化、可随需扩展的接入方式、用户实名制上网。

从网络核心架构、用户认证以及边界优化等多层面出发，围绕高性能、易管理、精细化、实名制等角度，结合南开大学校园网扁平化部署实施过程，对校园网整体基础网络架构的扁平化进行初步的探索和研究。

2 校园网基础架构分析与扁平化部署实施

2.1 单核心大二层的扁平化基础架构

传统校园网多数采用了“核心—汇聚—接入”的多级分层模型拓扑架构，不同层次负责不同的业务功能，如图 1 所示[2]。在多级分层模型的拓扑架构下，核心层负责用户数据分组的快速转发，通常

收稿日期：2014-10-14

采用高性能三层交换机；汇聚层介于核心层和接入层之间，负责用户分组的三层终结、分组路由以及访问控制等功能，在传统校园网中，一般采用分区域的方式部署三层汇聚交换机；接入层主要负责用户数据的二层转发、用户接入认证、用户端安全策略控制等功能。

三层或者多层架构的特点，在于设备性能和业务需求倒挂，高性能的核心设备仅负责三层分组转发，低性能的汇聚和接入设备却需要承担用户接入认证、协议终结和应用隔离等诸多功能；单一业务的承载需要依赖于多个业务层面的参与，各业务层面边界不够清晰，缺乏对业务的集中管理控制；由于三层汇聚设备的相对独立部署，无法对用户和应用进行统一的精细化管理和控制[3]。传统的三层架构，已经无法适应校园网高性能、规模化多业务承载的现实需要。

对网络架构进行功能上的重新规划和界定并简化，是解决传统多层网络架构所带来的问题关键。对网络架构进行扁平化，就是对原先边界模糊的业务层面的清晰化，通过整个校园网的业务部署模式，在逻辑上对校园网各层的功能进行重新界定和划分，而不仅仅只是网络拓扑层次的简化。

南开大学校园网核心扁平化升级选择了“单核心大二层”的技术路线，采用高性能的宽带远程接入服务器（BRAS, broadband remote access server）设备作为校园网核心，采用高密度万兆交换机替代汇聚层设备，网络拓扑蜕变为“核心—接入”的扁平化二级架构，如图 1 所示。

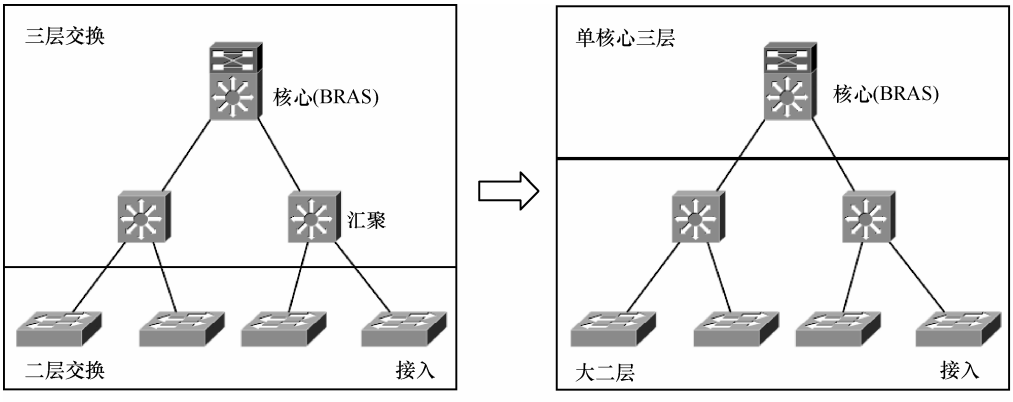
1) 核心层部署

BRAS 设备主要负责校园网业务的承载、三层分组的路由以及用户认证计费相关业务。高校网络规模的快速扩张、用户数量和应用业务的急剧增加，对校园网核心提出了多业务承载的需求。校园网除承载用户高速访问互联网数据之外，还需承载传输一卡通、能源计量采集以及多媒体教学等信息业务系统数据，业务系统对网络带宽的需求和安全要求也趋于多样化。依据用户业务策略，通过在 BRAS 设备上动态配置在线业务的服务质量（QOS）、计费方式以及安全策略，做到统一全局下发，可以实现业务的规模化部署，简化了网络的配置管理。通过 BRAS 设备结合认证计费系统对用户身份进行认证，在认证状态下设置用户的控制属性、速率控制和访问权限等，实现用户访问网络的计费、日志和审计；通过对用户访问目的地址进行差别管理，区分用户的访问不同业务或互联网区域的流量，实现不同的费率级别计费，达到校园网用户的精细化控制管理的目的。

2) 汇聚和接入层部署

南开大学校园网采用了高性能、低延迟的高密度交换机，同时负责有线和无线接入设备的链路汇聚以及用户数据分组的二层透传和快速转发。高密度交换机通过堆叠技术，虚拟化为一台单一的设备，以多个万兆链路聚合的方式接入至 BRAS 设备，既实现了链路冗余，也起到了高速转发分组的作用。

接入层则主要负责用户端的安全控制策略。由于局域网本身的开放性和用户行为的不可控性，易带来各种网络故障。比如广播包过多造成广播风暴；ARP 病毒引起的网关欺骗，导致局域网整个子网中断；DHCP 分组广播欺骗造成的网络中断等。



(a) 多级多层次模型架构 (b) 单核心大二层扁平化架构

图 1 多级多层次模型架构与单核心大二层扁平化架构

通过在接入交换机上配置广播包抑制、ARP 防护以及 DHCP 侦听等功能，对用户的接入进行端口上的隔离。

2.2　计费系统和用户认证

2.2.1　认证计费系统的部署

认证计费系统为高校校园网提供实时的基于用户组的接入策略功能，包括接入时段、使用量、访问地址及端口、认证方式、防代理私接策略等，为高校校园网提供全方位的用户接入管理和差异化业务运营，是高校校园网用户身份认证和计费营收的核心系统。

认证计费系统在校园网中的部署，一般分为网关和旁路方式。在网关部署方式下，认证计费系统以网桥或路由模式，部署在网络核心设备和边界路由器之间，在配合 BRAS 设备或以 Web 方式进行认证的同时，通过统计在线用户对应的 IP 地址产生的流量或在线时长，对用户进行计费。在旁路部署方式下，认证计费系统可以在 BRAS 设备三层可达的任意位置部署，和 BRAS 设备进行联动，通过与 BRAS 设备交互 RADIUS 认证记账分组，对用户进行认证和计费。在线用户的流量和时长记账分组，由 BRAS 进行统计后实时同步给认证计费系统。

认证计费系统一般基于 X86 架构，通过在此之上开发的软件对用户的流量分组进行统计，从而对用户进行计费。因为 X86 架构性能的原因，在网关方式下，往往成为核心至边界的转发瓶颈，为用户数据分组的转发增加不可避免的延迟，同时也造成了潜在的单点故障威胁。而在旁路部署模式下，用户流量不再通过认证计费系统转发。通过 BRAS 设备强大的硬件性能可以实现用户流量的精准统计，认证计费系统只需要对记账分组进行处理。因此，在认证计费系统的部署上，南开大学校园网采用了旁路部署的方式，既简化了网络拓扑层次，减少用户数据分组的跳数，又降低可能存在的网络故障风险，如图 2 所示。

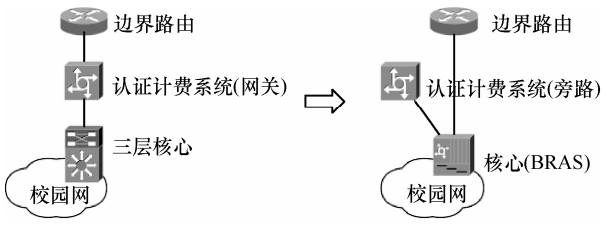


图 2　认证计费系统部署的扁平化

2.2.2　用户认证方式的选择

局域网用户访问网络的身份认证过程，一般分为准入和准出 2 个步骤，也就是所谓的“二次认证”。准入认证应用于对用户接入局域网进行身份认证，通常应用在无线局域网接入场景和对安全需求较高的有线局域网；准出认证则对用户访问互联网进行身份认证。在有些情况下，也会采用“一次认证”，用户一次登录，同时实现局域网准入和互联网准出，但这会给用户造成互联网流量。局域网用户接入认证主要有 802.1x 认证、Web 认证、IPOE 认证和 PPPOE 认证等 4 种方式。

1) 802.1x 认证

802.1x 认证是基于 802.1x 协议下的认证方式，802.1x 协议的前身是 IEEE 802.11 无线局域网协议，802.1x 认证方式在高校校园网中的应用一度较为广泛。为了弥补 802.1x 协议本身的漏洞，网络设备厂商对 802.1x 进行了标准不一的私有扩展，这就造成了协议的不兼容性。如果接入层交换机采用了不同厂商设备，就无法做到统一管理，也存在发布客户端的难度。因此，高校校园网逐渐摒弃了 802.1x 认证方式，而选择了 IPOE 或者 PPPOE 作为用户的接入认证方式。

2) Web 认证

Web 认证方式不使用客户端，依赖于 Web 浏览器来完成用户地认证。在 Web 认证方式下，认证计费服务器一般部署在网络核心设备和边界路由器之间，由用户访问互联网的请求流量触发 Web portal 认证界面，通过用户名和密码来对用户进行认证。Web 认证方式通常只能进行用户的互联网准出认证，而无法做到局域网准入认证。

3) IPOE 认证

IPOE（IP over ethernet）认证是通过扩展 DHCP 选项字段 OPTION 形成的一种认证方式。DHCP 负责在局域网范围内动态分配主机的 IP 地址，OPTION 字段则用来携带用户终端类型和接入位置等信息。DHCP 服务器依赖 OPTION 字段的不同，为用户分配不同业务的 IP 地址，并采取不同的控制策略[4]。在 IPOE 认证方式中，BRAS 设备在承担用户接入网关的同时，也承担 DHCP 服务器的功能，配合外置的认证计费系统，对用户的身份信息进行认证。IPOE 既可以用来准入认证，也可以用于准出认证。

4) PPPOE 认证

PPPOE（point to point protocol over ethernet）

是在以太网上承载 PPP 协议的一种认证方式。通过 PPPOE 协议，以太网上的主机和远程接入设备 BRAS 建立点到点的连接，BRAS 结合认证计费系统对接入的每一个主机进行认证和计费。和 IPOE 类似，PPPOE 可以自动为用户分配 IP 地址，既可以用于准入认证，也可以用于准出认证。

高校校园网丰富的局域网资源和对互联网访问流量进行计费的策略，使用户产生了只访问局域网资源的需求，再加上安全要求，高校校园网既要针对只访问校园网资源的用户进行准入认证，还需要针对访问互联网的用户进行准出认证，或同时进行准入和准出认证。因此，在认证方式技术路线的选择上，南开大学校园网选择了 IPOE 和 PPPOE 的认证方式，以满足用户的“二次认证”需要。通过 IPOE 和 PPPOE 动态为用户分配 IP 地址，简化用户接入局域网的步骤，避免了为用户静态指定 IP 地址造成的 IP 地址冲突等问题。

“二次认证”的过程，在客观上增加了用户访问网络的复杂程度。因此，在保证安全接入的前提下，通过对 BRAS 设备和计费系统的二次开发，在南开大学校园网部署实施了“无感知”认证技术，基于用户终端的 MAC 地址，对用户首次接入校园网进行身份认证，一旦记录到用户的 MAC 地址后，用户后续的校园网准入通过 BRAS 设备和认证计费系统的联动自动完成。通过在 BRAS 上设置用户访问策略，只在用户访问互联网时或首次接入校园网时，才弹出 Web portal 认证界面。既保证了“二次认证”的安全需求，也简化了用户访问网络的步骤。

2.2.3 有线无线用户统一认证

由于无线和有线认证方式的不同，以及多品牌无线设备存在的客观现实，一个校园网部署多套认证计费系统，是高校校园网普遍存在的情况。这造成了多套认证计费系统之间计费信息难以同步、无线网络之间用户无法漫游、有线和无线账号无法通用的现实状况。不同校园区域、不同网络场景，认证方式的不同，也给用户带来使用上的困扰，特别是无线校园网和有线校园网之间的用户认证无法统一。

由于南开大学校园网扁平化过程中采用了旁路方式部署认证计费系统，认证计费系统不再以网关方式部署在核心与路由之间，无线用户的流量无法直接由计费系统统计，要求无线用户也通过核心 BRAS 设备进行认证和计费，这就需要对无线和有线的二层接入进行统一，把核心 BRAS 设备同时作为无线用户的三层接入网关。在无线组网的技术路线选择上，南开大学校园网采用了本地分布式转发的模式，无线局域网用户业务 VLAN 的数据流在接入交换机上直接封装相应的 VLAN 标记头部，以二层方式和 BRAS 的逻辑子接口进行数据交换，由 BRAS 来处理业务数据。这样无线校园网就形成了天然的“大二层”，做到了和有线网络从接入到认证的融合统一。有线无线统一采用了基于无感知认证的 IPOE 和 PPPOE 认证。

2.2.4 用户上网行为日志联动采集机制

随着网络安全形势的日益严峻，校园网也同样面临迫切详尽审计用户的上网行为的需要，以做到网络行为有据可查。传统方式下，一般通过认证计费系统、用户上网行为审计系统以及边界路由设备等对用户的网络行为进行记录，并输出日志系统进行存储和后续的检索分析。

各系统输出的日志中，用户上网行为信息的有关字段往往并不完备。如用户认证计费系统，可以记录用户访问网络的用户名、IP 地址、源端口、MAC 地址以及访问目标 IP 地址、目的端口，但无法记录到用户 IP 经过边界路由器 NAT 转换后的 IP 地址和端口信息，无法形成完整的用户网络访问日志信息。一些边界路由设备虽然也具备用户认证功能，但由于网络用户数据库系统通常与认证计费系统深度耦合，边界路由设备即便支持 RADIUS，但通常不用于用户访问网络的认证，因此无法记录用户名以及 MAC 地址等信息。用户上网行为审计系统虽具备深度分析和记录用户网络行为的能力，但由于部署位置常常在边界路由之外，因此无法记录到用户名，需由第三方系统提供用户和 IP 地址的映射关系。在实际的部署情况中，因为各种系统用户上网行为信息的采集相对独立，不可避免地重复存储，极大浪费了存储空间。用户信息在不同系统中的映射关系的缺失，需要人为检索多方系统的日志来匹配有关用户网络访问的日志信息，操作复杂，效率较低。

鉴于以上原因，南开大学校园网在扁平化部署认证计费系统的同时，通过与边界路由设备配合，定制开发部署了联动式日志采集系统，统一采集输出用户上网行为日志信息。用户发起认证通过后，认证计费系统向边界路由主动实时推送用户登录

的信息，边界路由把接收到的用户登录信息，与 NAT 日志以及用户访问互联网的目的 URL 形成多元组的映射，输出至单一的日志采集设备并进行统一审计，从而避免了日志的重复采集、重复存储和重复查询的问题。

2.3 网络边界优化

校园网部署环境中，网络边界不再仅仅承担分组选路和 NAT 的功能，还需要承担起安全防护、流量优化、用户安全审计等一系列的功能。在传统的部署方式下，需要在边界串联部署多个硬件设备从而负责不同的业务功能。通常由防火墙承担安全防护功能、负载均衡或流控设备进行流量优化、部署安全审计系统对网络中的流量进行深度分组分析，在必要时对非法流量进行隔断。串联部署的方式，不仅在客观上增加了用户数据交换的延迟，而且还增加了潜在的多个故障点。单一的设备故障，就会造成全网中断。因此，网络边界的优化，也应该是校园网基础架构扁平化的一部分。在部署过程中，南开大学校园网采用了新型的多业务安全网关作为路由边界设备，并采取了一系列的优化措施，以达到简化网络边界的目的。

2.3.1 全网防护的防火墙策略

高校校园网在为用户提供网络接入之外，还需要提供各种业务系统的信息服务，比如主页、邮件等面向互联网开放的 Web 服务。高校院系部门众多，各单位部门信息服务系统的安全难以由信息化管理部门统一控制，为众多的信息服务系统分别配置安全策略也给工作带来了一定的难度。由于用户安全意识的匮乏，用户计算机遭受网络攻击的情形也时有发生。

为此，南开大学校园网采取了对外部主动发起的流量进行全网阻断的安全策略，仅允许校园网内部用户主动发起网络访问请求。部署安全漏洞扫描系统，结合安全网关进行二次开发，只对通过安全漏洞扫描系统审计过的网站和主机开放互联网访问权限，避免了来自外部的网络威胁，同时也避免了部署额外的防火墙设备增加故障点。

2.3.2 基于应用策略路由优化出口带宽

由于不同互联网服务运营商之间网络资源的分布不均衡和人为的互联互通障碍，高校校园网往往存在多个互联网出口。在传统方式下，一般在路由器上采用基于运营商 IP 地址的策略路由为用户数据分组进行选路。高校用户群体集中而活跃，互联网出口的流量存在较多的 P2P 等非关键业务流量，HTTP 等关键业务流量的带宽反被挤占而无法得到保障，用户无法正常访问学术资源，为了提高网络访问质量，一般在网络边界部署了网络流量控制或负载均衡设备，对部分 P2P 等非关键业务进行限速、封杀等措施[5]。

基于目的地址的策略路由仅仅为用户访问目的网络的路由进行了优化，无法做到对关键业务的带宽保障。在边界部署流量控制或负载均衡设备可以起到对某些协议的流量限制，但无法为用户带来良好的访问体验。流量控制设备特征库地更新与应用软件流量特征更新的相对滞后，也会造成流量控制策略的失效，无法从根本上解决问题。

在出口边界的优化上，南开大学校园网不再部署流量控制设备限制非关键业务流量，而是通过多业务安全网关，针对不同的应用协议进行引导。以“优质带宽保障关键业务”为原则，通过基于应用协议的策略路由，在访问质量较好的带宽链路上保障常见的 HTTP 等少量关键业务流量，其他流量通过缺省路由的方式转发至低等级宽带链路上，同时基于 DNS 劫持等方式，把优质互联网资源定位到对应的运营商网络。这样既保障了关键业务地快速访问，也避免了非关键业务对有限的优质带宽的挤占。而且安全网关只需要做到识别关键业务的流量，即便是无法识别非关键业务流量的特征，也可以由缺省路由转发至低等级链路的出口。

2.3.3 基于缓存的互联网资源访问优化

对于互联网信息的访问，仅仅资源充足已经无法满足高校用户的需求，对视频等热点资源的快速访问，已经成为用户访问网络的迫切需要。在优化边界带宽的同时，南开大学校园网部署了网络内容缓存服务器，把用户原先需要通过互联网下载的资源暂存到本地网络。用户下载时，通过重定向技术，把用户的点击重新导向局域网的缓存服务器上，达到快速访问、快捷下载的目的。

3 结束语

通过以上各层面，各系统的部署，从系统整体上在南开大学实施了校园网基础架构的扁平化。在简化的网络拓扑结构下，优化了用户路由跳数，用

户数据分组从主机只需经过“两跳”就可以到达运营商网络，提高了网络转发整体性能，也降低了网络存在的故障点，增加网络的稳定性。简化明晰的业务层次，更加易于管理。用户接入方式的统一，更有利于对用户进行精细化的实名制管理。

参考文献：

[1] 刘春艳.校园网扁平化架构的研究与设计[J].信息与电脑(理论版),2014(4):35-36.
LIU C Y. Research and design of flat campus network architecture[J]. China Computer and Communication, 2014, (4):35-36.

[2] 申继年,邱家学.校园网组网架构的比较与分析三层交换架构 vs 扁平纯路由架构[J].中国教育网络, 2012, (1):44-45.
SHEN J N, QIU J X. Comparison and analysis of the campus network architecture: three-layered switching architecture vs plain routing architecture[J]. China Education Network,2012(1):44-45.

[3] 吴乃忠.基于扁平化架构的下一代高校校园网的建设研究[J].电子世界,2012(9):28-29.
WU N Z. Research of next-generation campus network construction based on flat architecture[J]. Electronics World, 2012(9):28-29.

[4] 南静.校园网认证计费系统的设计与实现[D].临汾:山西师范大学,2013.
NAN J. Design and Implementation of Authentication and Accounting System for Campus Network[D]. Linfen: Shanxi Normal University, 2013.

[5] 田爱包.浅谈基于应用协议的网络多出口设备在高校的应用[J].微型电脑应用,2014,30(4):56-58.
TIAN A B. Discussion on deployment of multi-outbound-port campus network device based on application protocol[J]. Microcomputer Applications, 2014,30(4):56-58.

作者简介：

林初建（1979-），男，浙江瑞安人，南开大学信息化建设与管理办公室实验师，主要研究方向为计算机网络。

张四海（1977-），男，安徽歙县人，南开大学信息化建设与管理办公室主任，高级工程师，主要研究方向为信息化。