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

本文以当前校园网中存在的两种组网架构为研究对象，根据校园网的自身特点和需求，从技术特点、运维管理、安全控制、认证方式等方面对两种组网架构进行分析比较，同时针对如何选择适应校园网环境的组网架构提出了参考建议。

■文／申继年 邱家学

近年来，随着网络技术的发展，运营商的网络架构正从复杂化的多层架构走向扁平化架构。借鉴运营商的成功经验，校园网架构模式也发生了变化，“扁平化纯路由架构”悄然在高校中兴起。目前一些高校已经部署或正在部署“扁平化网络”，但是“扁平化纯路由架构”是否真的适合校园网的需求，还须进一步分析和研究，本文正是针对传统的“三层交换架构”和“扁平纯路由架构”做以下分析与探讨，为高校的组网架构选型提供一些参考。

校园网中网络架构模式

三层交换架构模式

1. 三层交换架构模式简介

目前绝大多数高校校园网采用的是以路由交换机技术为主的分级模型架构，即“核心－汇聚－接入”。每个层次分别实现不同的业务功能。

核心和汇聚采用三层交换机，接入采用二层交换机。其结构为交换方式，协议以二层交换协议为主，三层路由协议为辅，三层、两层协议混用，其三层路由协议在核心层和汇聚层上实现，二层交换协议在核心层、汇聚层、接入层三个层次上实现。

2. 三层交换架构模式功能特点

核心层是校园网的主干，主要目的是尽可能快地交换数据，这一层不应该进行复杂的、消耗系统资源较大的数据包操作，也不能进行减慢数据交换的处理。不应当在核心层进行诸如访问控制列表和数据包过滤之类的操作。核心负责传输穿过校园的数据流，不进行任何处理器密集（如路由选择）的操作。核心层所处理的数据流比其它层次要大很多，核心层应当能尽可能快地传输数据流。

汇聚层是访问层和核心层之间的分界点，它负责用户的三层终结、路由、ACL、QoS等功能实现。汇聚层保证了整个校园网的稳定性，例如，如果一个或若干个子网遭受到广播风暴攻击，分布层设备可以防止该风暴扩散到核心和网络其它区域。

接入层是最终用户被许可接入校园网的大门，它是负责用户的接入、相互的隔离、802.1x或Web认证的准入，以及DHCP侦听和ARP动态检测（避免ARP攻击）、双栈组播控制与分发等功能。另外，在客户端使用Web或802.1x准入认证后，交换机可自动绑定用户的IP+MAC+端口信息做源地址报文检查，可以有效地防范账号盗用、防IP篡改、防MAC篡改、防ARP攻击等，从而实现了灵活性与安全性的有效结合。

扁平纯路由架构模式

1. 扁平纯路由架构模式简介

扁平化架构不是简单地把网络从三层结构压缩成二层结构，而是考虑网络规模的大小、业务的多样性、功能区的划分等多种因素，尽量简化网络层次，使网络趋近扁平。扁平化的架构模式并非必须或一定就是物理联接层次上的减少，而是指网络逻辑层次的简化。对于大型高校可以是三层架构、二层架构混合方式组网。

2. 扁平纯路由架构模式特点

扁平化网络架构将传统三层架构各个层次模糊的功能区分清晰化，实现了核心业务控制层和网络接入层分离，实现用户、业务控制的集中化。

核心层作为整个网络的控制层，提供集中的业务控制和管理功能，要求设备性能足够强大；从接入层直接到核心层之间的设备都是使用二层功能，通过802.1q VLAN直接连结到核心路由器，所以网络接入层设备一般只需提供基本的二层VLAN隔离功能，不涉及到业务功能。因此部署新的业务和功能时，网络接入层设备无需考虑其是否支持，也无需考虑设备型号，只需要考虑接入端口的扩充、上行带宽的增加，充分保护了原有低端设备的建设投资。

两种组网模式比较

校园网的特点

校园网主要是为学校教学、科研、办公、管理和生活等提供安全、高速的网络服务，有资源共享、信息交流、协同办公以及娱乐休闲等多种功能。与运营商的网络环境、用户环境、应用环境相比有着很大的不同，呈现以下特点：

1. 高速的链路通道

当前高校校园网一般是万兆骨干，万兆或千兆汇聚上联，百兆桌面接入，有着高速的链路通道。

2. 校内资源丰富，应用系统种类多

校园网内资源丰富，存在多种应用系统，既有BBS、FTP和在线视频等应用服务，又有OA等办公系统，主要满足师生的科研、办公与学习，还提供一定娱乐休闲功能。

3. 用户群密集且活跃

校园网内包括大量的学生机房，有的高校还包括学生宿舍网，学生用户数量大，且大量使用各种P2P应用，消耗了大量的校园网核心带宽和出口带宽；学生用户群体有着强烈的好奇心，喜欢尝试新鲜事物，网络攻击现象活跃。

4. 路由简单

校园网IP分配较固定，且有规律；内部路由数量较少（最多在几百条左右），无需复杂寻址。

5. 校园网数据流向规律

每个学校由于资源建设情况和用户的组成不同，校园网的流量分布也有所区别，且具有一定的规律性。校园网数据流向主要分三类：①客户端至数据中心服务器；②客户端至Internet出口；③各个业务区域之间互访。例如，如果校园网资源丰富（BBS、在线视频或FTP服务），第一种流量较大；相反如果校园网资源比较少，校园的用户获取资源主要是通过Internet，则第二种流量为主要流量；校园网内各业务之间的互访比较频繁，第三种流量也占有一定比重。校园网数据流向比较集中，需要快速转发。

两种组网架构在校园网中的应用比较

在校园网中，三层交换架构和扁平纯路由架构对比如表1所示。

综上所述，扁平化纯路由架构在运营商网络中大面积部署，带来很好的收益，但能否满足校园网特有的业务需求以及用户环境，还未经过大量实际应用来证明，且技术上还存在许多不足。三层交换组网技术目前较为成熟，但也存在一些问题。在校园网的环境中，两种组网方式都不是完美的，各有自己的优势，同样也存在自身的缺点。

当然，每个高校的业务需求也不尽相同，网络建设者应该分析自己学校的特点与业务需求，选择适合本校情况的组网模式。建议在校园网中，针对路由查找能力需求不强，校园网内业务数据访问比较多，数据转发能力要求高的环境，采用三层交换架构；建议校园网内部交换流量较少、对用户隔离要求较高或存在大量路由查找业务的环境，为保证良好的安全管理和高效的路由投递，采用扁平纯路由架构模式。CEN

（作者单位为中国药科大学）

表1 三层交换架构和纯路由扁平架构对比

	三层交换架构	扁平纯路由架构
设备要求	核心和汇聚设备：性能较强的三层交换机； 接入层设备：控制功能较强的二层交换机。由于很多功能需要接入层设备支持，比如端口限速，端口隔离，pvlan，portal，802.1x等，对接入层设备功能要求很高，且最好为同一厂商。	核心设备：高性能路由器，性能足够强大、接口丰富； 接入和汇聚层设备：只需支持Vlan功能的二层交换机，兼容多家厂商设备。
核心层	核心采用高性能的三层交换机，利用ASIC实现三层数据的高速转发，效率很高。大多数校园网数据流向比较集中，且内部路由数量较少，需要快速转发，无需复杂寻址，高性能的三层交换机能够很好满足这方面的要求。	核心采用高性能的路由器，基于软件的查找路由表，对数据进行投递，效率不及高性能三层交换机。但路由器有着比交换机更灵活的Qos和更强大的路由处理能力。
架构特点	校园网用户内部数据交换直接通过接入交换机或者汇聚交换机转发，无需经过核心骨干网，减少核心骨干网流量，降低核心骨干网超负荷风险，有效、合理的使用了核心骨干网资源。校园网IP分配较固定，且有规律，内部路由数量较少，组网模式采用全交换，满足校园网的高速数据交换。	组网采用纯路由模式，在转发每个数据报文前，都需要CPU去查找路由表。校园网用户内部数据交换量比较多，如QQ文件传送、文件共享等，所有流量都需经过BRAS，增加了BRAS的负担。同时，这些流量经过核心骨干网转发，增加了核心骨干网的额外开销，增加了扩容核心骨干网带宽的几率。
运维管理	有些配置在核心层完成，有些在汇聚和接入层完成，许多策略配置需要各层统筹规划。接入层的策略较多，且设备数量非常庞大，维护人员工作量大。	策略配置与维护集中在核心层，很多配置只在核心层即可完成，且该层设备数量少，维护量集中，但对维护人员技术水平要求高。
精细化管理	为了提高校园网内部的高速转发，校园网的精细化管理应在网络出口和接入层。因为真正带宽紧缺的地方是在出口，而不是在内部。在校园网出口部署专业的流控设备，通过流控设备可实现基于IP或用户名的策略定义，比如下行带宽、会话数和多种应用类型的控制。 在接入层部署：在接入层主要实现802.1x或WEB的用户准入和安全的自动防护功能，从而保证了网络的稳定性。	每个接入层端口对应核心设备的一个子接口，所有控制都在核心设备完成，方便实施，并可批量化管理，可以多交换机上某个端口或某些端口做特定的设置（如限速、保障带宽等）。由于BRAS设备只能对上下行带宽进行控制，对会话数和应用无法控制。因此当用户在使用P2P和访问WEB时，用户访问WEB浏览会非常慢，从而用户上网体验较差。
认证方式	准入认证：采用802.1x或WEB认证方式，便于为不同用户提供灵活接入，在接入层部署，针对端口管理，接入层设备存在厂商要求。802.1x或WEB认证可提供用户访问校内资源免费，访问校外资源收费；同时，用户访问校外资源被限速的情况下，校内资源的访问带宽不会被限速。 网关认证：学校校园网无需认证即可接入，需要访问校外网络的时候，采用专门的认证计费设备实现。	准入认证：PPPoE，在核心部署，针对端口管理，需要增加BRAS设备。在PPPoE认证下，利用Qos对每个用户访问校内和校外资源带宽进行统一限速。假如用户认证后访问校外资源的带宽限制为2M，同时访问校内资源的带宽也被限制为了2M，导致用户访问内网速度慢，失去了高速校园网的意义。 网关认证：BRAS设备作为校园网出口的网关，用户使用L2TP VPN拨号的方式访问访问校外网络，故障较多。

校园网组网架构的比较与分析

作者：申继年， 邱家学
作者单位：中国药科大学
刊名：中国教育网络
英文刊名：China Education Network
年，卷(期)：2012(1)