Computer Science and Application 计算机科学与应用, 2023, 13(12), 2305-2313
Published Online December 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1312230

Hans汉斯

基于IPv6+校园网络体系研究

——以伊犁师范大学为例

张体谅，张　斌*，刘新茂，李　杨，王俊龙，徐庆敏

伊犁师范大学信号检测与控制技术重点实验平台，新疆　伊宁

收稿日期：2023年11月22日；录用日期：2023年12月19日；发布日期：2023年12月26日

摘　要

随着网络新技术的发展和校内业务子系统的不断增多，校园网暴露出很多不足之处：(1) IPv6配置复杂，接入设备要求高，难以维护；(2) 校内部分终端无法使用IPv6网络，(3) IPv4、IPv6网络没做到统一认证，为了解决这些问题，进行网络扁平化改造、总体设计IPv6+校园网络体系，通过IPv6地址顶层设计、研究地址获取方式、打通校内IPv6网络通道、增加安全认证等几个维度进行设计，为师生解决燃眉之急，在教学、科研上给师生提供良好的IPv6平台。也为2030年完成IPv6全网单栈最终目标的演进进行过渡和探索，为本地区IPv6+网络建设提供依据。

关键词

IPv6+，顶层设计，体系，一体化

Research on IPv6+ Based Campus Network System

—Taking Yili Normal University as an Example

Tiliang Zhang, Bin Zhang*, Xinmao Liu, Yang Li, Junlong Wang, Qingmin Xu

Key Experimental Platform for Signal Detection and Control Technology, Yili Normal University, Yining Xinjiang

Received: Nov. 22nd, 2023; accepted: Dec. 19th, 2023; published: Dec. 26th, 2023

Abstract

With the development of new network technologies and the increasing number of business subsystems on campus, the campus network has revealed many shortcomings: (1) IPv6 configuration

*通讯作者。

文章引用: 张体谅, 张斌, 刘新茂, 李杨, 王俊龙, 徐庆敏. 基于 IPv6+校园网络体系研究[J]. 计算机科学与应用, 2023, 13(12): 2305-2313. DOI: 10.12677/csa.2023.1312230

is complicated, and the requirements for access equipment are high and difficult to maintain; (2) some terminals on campus cannot use IPv6 network, and (3) the IPv4 and IPv6 networks have not achieved unified authentication. In order to solve these problems, we have carried out a network flattening transformation and overall design of IPv6+ campus network system is designed in several dimensions, including IPv6 address top-level design, research on address acquisition methods, opening up IPv6 network channels on campus, and increasing security authentication, so as to solve the urgent problems for teachers and students, and to provide a good IPv6 platform for teachers and students in teaching and scientific research. It also conducts transition and exploration for the evolution of the final goal of completing IPv6 single-stack for the whole network in 2030, and provides the basis for the construction of IPv6+ network in the region.

Keywords

IPv6+, Top-Level Design, System, Integration

1. 引言

我校针对信息化发展制定“十四五”规划，以加快校园数字化发展、制定 IPv6 发展的相关战略规划。目前处于跨越拐点的关键阶段，不断提升对 IPv6 发展与能力的认识，多措并举重，推动我校 IPv6 规模部署和应用走向深入，为师生提供良好的网络环境和信息支撑[1]。

随着我校智慧校园的推进，一站式服务办公的上线和微服务的不断更迭，对业务数据的安全和业务带宽大要求越来越高，加之物联网业务的不断普及导致校内 IPv4 资源严重不足，师生对 IPv6 资源的需求越来越高，尤其是在科研和实验平台搭建上，由此推出 IPv6 网络。但在 IPv6 部署时，因地址规划凌乱、终端、内容源处理机制、网络适配、安全认证等问题，面临网络质量劣化、投诉定位难，影响运维和用户感知等挑站。为顺利落实国家 IPv6 战略规划，设计 IPv6+校园网络体系，利用 SRv6、网络切片、IFIT、BIERv6 等扩展协议，网络分析、自动调优等网络技术，在智能、安全、超宽、广联接、确定性和低时延六个维度全面提升校园 IPv6 网络能力，助力打造无处不在的智能 IPv6 联接，构建万物互联的智能世界。

根据 IPv6+层次化的网络结构和它独特的报文结构、灵活的扩展性等，在校园内构建一套符合我校 IPv6+网络的全新网络规划，通过顶层规划 IPv6 地址、打通 IPv6 网络隧道，实现终端无感知认证从而构建 IPv6+网络的全新网络规划体系。

2. 相关模块设计

2.1. IPv6 地址设计模块

目前申请到的是全球单播地址(GUA 地址)有教育网统一分配，该地址所在网络信息可以被发布到 Internet 上，也是我们通常所说的公网地址；表示形式是：IPv6 地址/前缀长度。其中“前缀长度”是一个十六进制数，表示改地址的前多少位是地址前缀，根据收到地址进行层次化规划，设计原则如下。

1) 层次化原则

减少 IPv6 网络地址碎片，增强路由聚合能力，提高网络路由效率，将 IPv6 地址段划分为相对独立

的几个字段，每个字段可以单独规划，实现路由汇聚。

2) 安全性原则

相同业务属性具有相同的安全要求，业务之间的互访需要进行安全控制，同一种业务属性划分到同一段地址空间，有利于安全设计和策略管理。

3) 连续性原则

IPv6 地址段之间，段内地址保持连续，避免地址浪费，有利于管理和地址汇总，减小路由表，提高路由效率。

4) 可扩展性原则

地址分配预留一定的余量，预留扩展字段，满足后续网络扩展时的需求。

按照固定前缀 + 1 级区域 + 2 级区域 + 3 级区域 + 接口地址的思路，对网络地址、平台地址、用户地址、接入网地址进行整体规划，所有地址的前 48 位为申请的固定前缀。Loopback 口地址使用/128，点到点链路建议使用/127，VRRP 链路建议使用/112，整体规划按照表 1 设计[2]。

Table 1. IPv6 Network address scheme
表 1. IPv6 地址规划

固定前缀	1 级区域 校区编号	2 级区域 业务编号	3 级区域 子业务编号	接口地址
48 bit	4 bit	4 bit	8 bit	64bit
固定	0-F	0-F	0-FF	0000::FFFF:FFFF:FFFF:FFFF
具体分配	0-预留	0-互联	00-互联	0000::FFFF:FFFF:FFFF:FFFF
	1-本校区	1-核心平台	01-DNS	1101::FFFF:FFFF:FFFF:FFFF
			02-03-预留	1103::FFFF:FFFF:FFFF:FFFF
			04-站群	1104::FFFF:FFFF:FFFF:FFFF
	2-新校区	2-智慧校园	00-06-预留	1206::FFFF:FFFF:FFFF:FFFF
			07-09-智慧校园	1209::FFFF:FFFF:FFFF:FFFF
			A-FF 预留	1A09::FFFF:FFFF:FFFF:FFFF
	3-F 预留	3-核心层	0	1300::FFFF:FFFF:FFFF:FFFF
		4-汇聚层	0	1400::FFFF:FFFF:FFFF:FFFF
		5-接入层	0	1500::FFFF:FFFF:FFFF:FFFF
		6-7 预留	0	1700::FFFF:FFFF:FFFF:FFFF
		8-9 有线终端	0	1900::FFFF:FFFF:FFFF:FFFF
		9-C 无线终端	0	1C00::FFFF:FFFF:FFFF:FFFF
		E-设备管理	0	1E00::FFFF:FFFF:FFFF:FFFF
		F-lookback	0	1F00::FFFF:FFFF:FFFF:FFFF

1 级区域：占用 1 位，4 bit，1 代表本校区，2 代表新校区，3-F 预留。

2 级区域：占用 1 位，8 bit，根据学校业务需求进行设计。

3 级区域：占用；两位，8 bit，划分具体业务需求。

接口地址：可根据需求按照 IPv4 地址，用后 8 位进行类比取值。

学校按照设计规则颁发 IPv6 地址并以文本形式形成记录，同时借助 IPv6 地址管理工具做到有效管理。

2.2. IPv6 地址获取模块

2.2.1. 调查研究

1) 获取方式分析：

SLAAC (Stateless Address Auto Configuration，无状态地址自动配置)：根据网关设备通告 RA (Router Advertisement，路由器通告)报文中携带的网络前缀生成网络 ID，根据 EUI-64 算法生成接口 ID，通过两者结合生成一个 IPv6 地址。

DHCPv6：配置 DHCPv6 Server 硬件服务器并配置 IPv6 PD 地址池，地址池给 DHCPv6 客户端分配 IPv6 地址前缀。

PD 场景中包括两个角色：Delegating Router 和 Requesting Router。Requesting Router 根据实际需要到 Delegating Router 上申请、释放 IPv6 前缀。Delegating Router 实现 IPv6 网段的配置，并根据 Requesting Router 的请求分配地址段。

2) 终端环境分析：校园终端各式各样，通过调查 Android 5.0 或以上版本，Win 10 (v1709)以上版本和 IOS 支持从 SLAAC 获取地址，但是不支持 DHCPv6。

3) IPv6+相关报文分析：IPv6 ND 报文用于地址发现，NS/NA 报文主要用于地址解析，RS/RA 报文主要用于无状态地址自动配置，Redirect 报文用于路由器重定向

4) 采用关键技术

路由器发现：路由器在与其相连的链路上发布网络参数等信息，主机捕获次信息后，可以获得全球单播 IPv6 地址前缀、默认路由、链路参数(链路 MTU)等信息。

接口 ID 自动生成：主机根据 EUI-64 规范或其他方式为借口自动生成借口标识符。

重复地址检测：根据前缀信息生成 IPv6 地址或手动配置 IPv6 地址后，为保证地址的唯一性，在这个地址可以使用之前，主机需要检验此 IPv6 地址是否已经被链路上的其他节点所使用。

前缀重新编址：当网络前缀变化时，路由器再与其相连的链路上发布新的网络参数信息，主机捕获这些信息，重新配置前缀，链路 MTU 等地址相关信息。

2.2.2. 具体实现

部署 DHCPv6 服务器和 SLAAC 混合模式实现在特殊环境下的模块设计，具体过程如下：

1) 数据中心服务器配置 IPv6 静态地址。

2) 终端通过 DHCPv6 Server 服务器获取地址，配置网瑞达 DHCPv6 Server 服务器并在网关设备上设置 M 标记为 1 和其它路由参数配置。

3) 终端通过 SLAAC 地址获取分配实现：在网关设备上设置 O 标记为 1 和其它路由参数。思路为网关设备通告 RA (路由器通告)报文中携带的网络前缀生成网络 ID，根据 EUI-64 算法生成接口 ID，通过两者结合生成一个 IPv6 地址，配置如图 1。

在核心交换机上配置发送 RA 消息来通告网络前缀，让不支持 DHCPv6 的终端通过 SLAAC 进行地址获取，分别以利旧 IPv4 网关为基础，并配置 DHCPv6 Server 服务器，部分特殊终端地址通过 DHCPv6 分配，配置如图 2。

针对 DHCPv6 和 SLAAC 两种形态具体配置如图 3 和图 4。

核心交换机(作为网关)：需要承载 DHCPv6 终端以及 SLAAC 终端的网关工作

需要同时开启上述接入交换机的安全功能，比如 DHCPv6 Snooping、ND Snooping 以及 SAVI 功能攻击者仿冒网关设备恶意发送的 RA 报文可以认为是非法报文，私自设置 DHCPv6 服务器的行为称作私设

DHCPv6 Server。对于非法 RA 以及私设 DHCPv6 Server 的解决措施，其核心在于直接丢弃非法设备发送过来的报文，从根源上解决问题。

Figure 1. SLAAC implementation methodology
图 1. SLAAC 实现方法

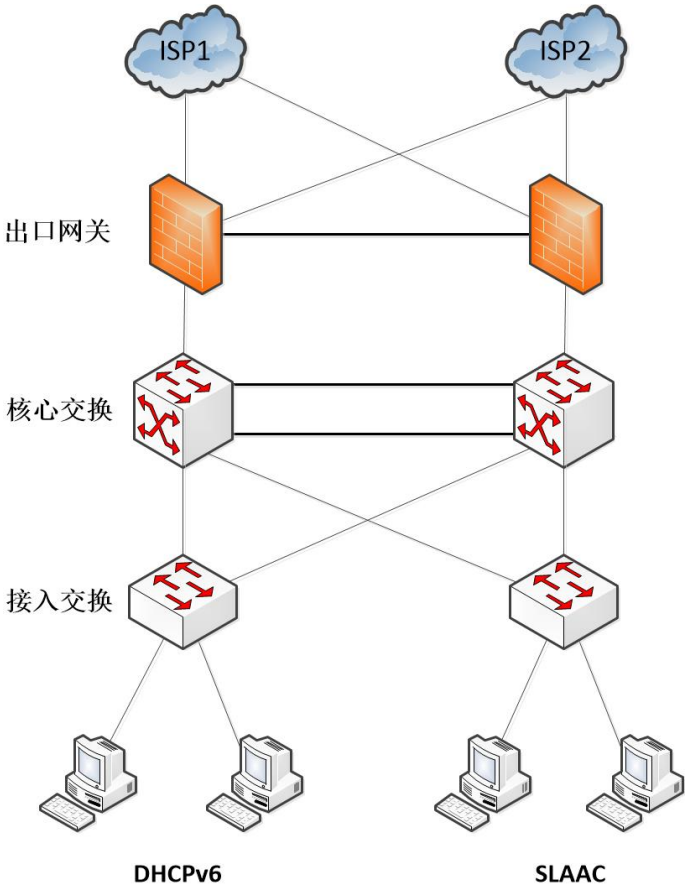

Figure 2. Basic topological map
图 2. 基本拓扑图

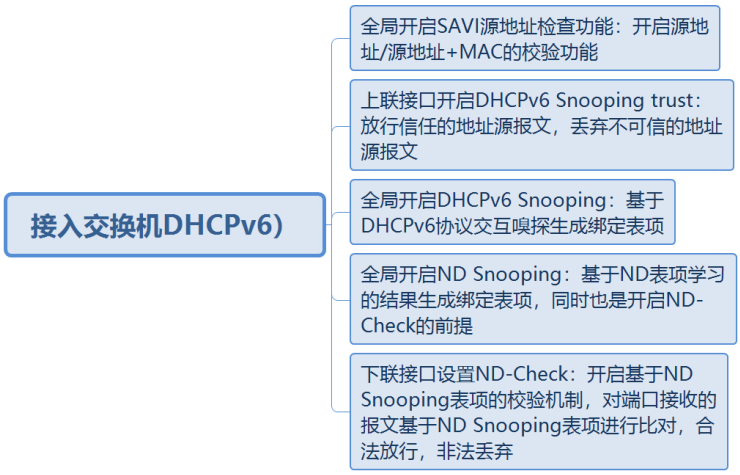

Figure 3. Accessing the switch DHCPv6 settings
图 3. 接入交换机 DHCPv6 设置

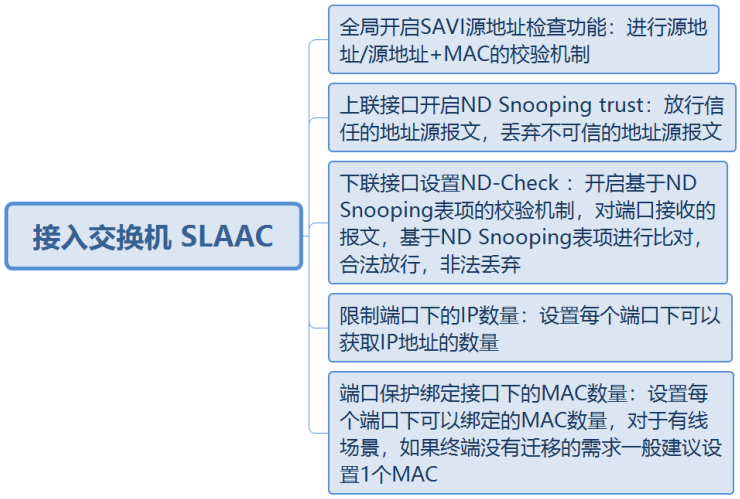

Figure 4. Access switch SLAAC settings
图 4. 接入交换机 SLAAC 设置

2.3. 网络通道模块

1) IPv4 基础架构保持不变，在原有 IPv4 网络的基础之上所有设备升级为 IPv4/IPv6 双栈网络，所有设备的二、三层组网模式及角色不变，即 L2、L3 与 IPv4 网络保持一致，IPv6 的路由协议设计与原 IPv4 网络保持一致，核心设备与汇聚层启用 OSPFv3，设置开销值，分的若干网络区域路由聚合收敛，划入 Area0 区域，所有的 L3 设备运行 IPv4、IPv6 双栈协议，保证存在高数据链路数据优先走。

2) 按照 IPv6 的地址分配遵循聚类(Aggregation)的原则，校园网路由通过 OSPFv3 或者静态路由相结合的方法，建立全网 IPv6 通道，在路由表中可以用一条记录(Entry)表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度，使 IPv6 通道速度更快。

3) 利用 IPv6IPSEC 拓展协议，对网络层的数据进行加密并对 IP 报文进行校验，增强了网络安全。

4) 通道安全防火方面建立被屏蔽子网体系结构，设置外部路由防火墙、数据中心防火墙、堡垒主机构成校内防火墙系统，数据中心防火墙保护数据中心安全，堡垒机保护数据中心应用系统的安全，同时

在各个应用系统之前放置 IPv4/IPv6 反代设备，对于不支持 IPv6 的应用系统通过反代进行转换，实现 IPv6 网络的畅通和数据中心相对的安全[3]。

5) 有线无线网络建设

从 AC-核心交换-POE 交换整体模块改造和升级，部分终端通过双栈技术打通 IPv6 有线无线隧道。特殊终端利用 ISATAP 自动建立隧道的过渡技术，通过将 IPv4 地址嵌入到 IPv6 地址当中，将 IPv6 包封装在 IPv4 中传送，在主机相互通信中抽出 IPv4 地址建立隧道，从而实现被 IPv4 隔离的 IPv6 孤岛之间的连接。实现 IPv6 有线无线一体化管理，FitAP 可以通过 IPv6 网络注册到 IPv6AC 模块，并建立 CAPWAP(无线控制器与 AP 设备通讯协议)，利用集中转发模块，实现 IPv6 AC 无线控制器对 IPv6 AP 的配置自从下发，实现 IPv6+有线无线体系。终端通过 IPv6 正常访问 IPv6 网络及 IPv6 业务。利用 IPv6 扩展性性进行网络融合，打造 IPv6+的有线无线融合网络，师生无感知的体验 IPv6 带来的便捷性[4]。

2.4. 安全认证模块

我校原认证接入方式主要为 IPv4 802.1X 接入认证方式。随着学校信息化建设的深入发展，接入方式已逐渐显现出其弊端，IP 冲突、ARP 病毒攻击、广播风暴等日益凸显，导致认证慢、上网卡等问题[5]，考虑更换认证方式 Portal 认证。

1) Portal 采用先获取地址，在进行拨号上网；

2) Portal 认证后，师生每人一个用户名，每个用户名注册后全校通用，能够实现精准溯源；

3) IPv6 不存在 ARP 报文，由 ND 报文取代 ARP 报文，消除 ARP 病毒攻击；

4) IPv6 用的是任播协议，不存在广播类型，消除广播风暴。

为保证终端认证和安全可靠传输设计 IPv4/IPv6 双栈体系认证体系，把固定 IP 接入及 802.1X 认证升级为 Portal 认证，并搭建 IPv4/IPv6 双栈体系认证平台，建设思路为配置网瑞达 DHCPv4/DHCPv6 设备数据推送到华为 BRAS 设备，华为 BRAS Radius 服务器报文重定向至城市热点 Portal IPv6 服务器进行弹框认证，BRAS 设置为 AAA 认证，城市热点为 Portal 弹框及计费功能，利用 IPv6 的隐私保护机制实现在 WEB 认证情况下对用户 IPv4 联动 IPv6 无感知认证，为 IPv6 指定了支持身份验证、数据完整性和数据保密性的扩展。最终实现 IPv6 终端认证、端到端认证、服务端认证[4]，认证拓扑如图 5。

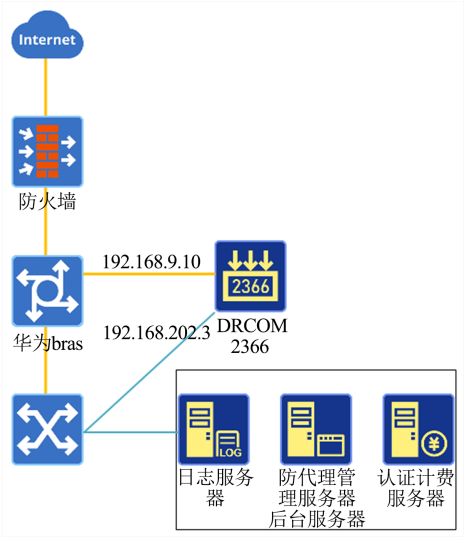

Figure 5. IPv6 authentication network architecture diagram
图 5. IPv6 认证网络结构图

校园内实现网络认证策略执行点的统一，通过城市热点计费系统，同一个账号实现不同的上网方式，不同认证区域的计费认证，认证过程由 BRAS、认证服务器、Portal 服务器完成，在办公区和教学区校园网无线用户免费使用，学生在宿舍区采用有偿，教师用户免费，多个运营商网络跟学校 AC 采用光纤连接，对应运营商用户 SSID 的相应 VLAN 数据包通过 Trunk 口，透传到 BRAS [6]。

终端认证：配置网瑞达 DHCP IPv4/IPv6 系统实现全网 IPv4/IPv6 用户的 IP 实名准入，系统通过与校园统一身份认证系统的单点登陆对接，用户使用统一身份认证系统账号完成实名绑定 MAC 后，获取到 IPv4/IPv6 地址接入网络，大大加强了网络接入安全管理。

服务端认证：通过城市热点计费认证系统与华为 BRAS 对接，实现不同认证方式的 IPv4/IPv6 地址通知机制，通过与 BRAS 的 Radius 报文交互实现 v4v6 联动上下线，交互报文包括上下线、CoA、计费更新报文等，通过 AC 本地或者集中转发模式中，在 AP 或者 AC 上设置与认证平台的联动机制，在 AP/AC 上过滤非法报文。

端到端认证：保证端到端数据数据安全传输，在传输网络中进行认证，在网络端开启验证和信任机制，防止非法接入，实现端到端安全无感知认证[7]，效果如图 6。

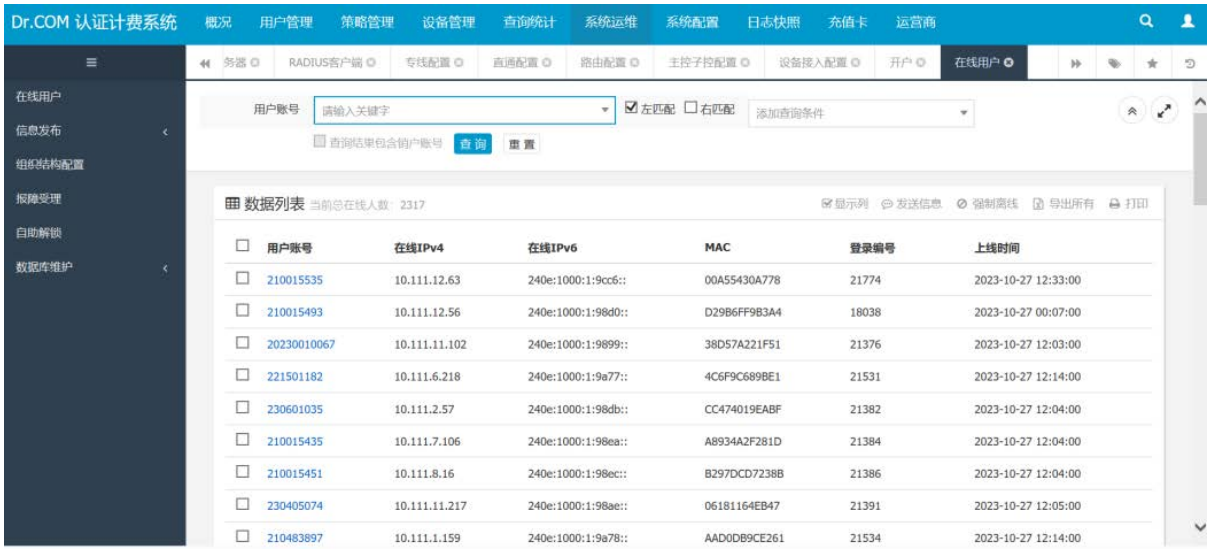

Figure 6. IPv6 authentication results
图 6. IPv6 认证结果

3. 结语

学校建得好不好看，主要看基建；建得好不好用，主要看信息化。我校基于 IPv4/IPv6 高速融合网络，充分利用大数据、物联网、人工智能等新一代信息技术，推进信息技术与学校事业发展深度融合、致力建设“安全、可靠、精准、可扩展”的 IPv4/IPv6 网络[8]。

利用 IPv6+扩展协议，通过 4 个模块的研究和设计，建立了一套符合 IPv6+校园网络体系标准，师生通过 IPv6+校园网络平台快速访问 IPv6 网络资源，同时做到认证溯源，实现 IPv6 终端精准定界，推动校内 IPv6 转化，支撑网络、终端、业务等发展，提高 IPv6 校内师生业务感知。

在此基础之上我校搭建 IPv6+实验室，不断完善开发 IPv6+相关特性，推动 IPv6 稳步向前发展。

我校通过各个模块的构建，能够更好的完成 IPv6 网络的一体化运维，但是做好网络安全运维，是一个持续的过程，要持续不断加强策略部署、安全防范，如安全设备对 IPv6 环境过滤。网络隔离设计、IPv6

报文捕获、入侵事件等要深入研究，只有持续不断的完善研究才能更好的推进 IPv6 的网络建设；目前我们属于 IPv6+ 1.0 时期，也就是 IPv4/IPv6 双栈时期，可以利用 IPv6 自身的特性来简化网络的业务部署，但是针对这个时期我们更应该用这个良好的契机打造和稳固网络底层机构；建立一张完整的 IPv6 体系是校园网 IPv6 发展的重要一步，在这个基础上我们才能向 2.0 甚至 3.0 时代迈进[9]，要持之以恒的向智能、安全、超宽、广联接、确定性和低时延六个维度来推动 IPv6 发展和全面提升校园网 IPv6 网络能力。

基金项目

伊犁师范大学校级科研项目(2023YSYY008)。

参考文献

[1] 邬贺铨. 加快 IPv6 规模部署支撑网络强国建设[J]. 网信军民融合, 2022(Z1): 7-10.

[2] 顾欢. 浅谈有线电视网络 IPv6 地址规划[J]. 网络安全和信息化, 2021(11): 63-65.

[3] 张杰. 高校校园网 IPv6 的部署与管理策略——以攀枝花学院 IPv6 建设为例[J]. 数字技术与应用, 2023, 41(9): 128-130. https://doi.org/10.19695/j.cnki.cn12-1369.2023.09.42

[4] 沈敏虎, 万俨慧, 向望, 等. 复旦大学 IPv6 多网融合建设新一代校园网[J]. 中国教育网络, 2023(4): 51.

[5] 罗辉琼, 聂瑞华. 基于 IPv4/IPv6 双协议栈的校园网认证接入研究[J]. 中国教育信息化, 2013(9): 87-90.

[6] 曾炜. 一种 IPv4/IPv6 双栈校园网统一身份认证技术研究[J]. 网络安全技术与应用, 2020(12): 96-100.

[7] 李聪, 孙吉斌, 解冲锋. 基于 IPv6 的 5G 专网终端身份认证技术与应用[J]. 移动通信, 2022, 46(8): 47-52.

[8] 陈永杰. 马传连: IPv6 创新赋能构筑校园新未来[J]. 中国教育网络, 2021(11): 51-52.

[9] 刘萌. 金融业 IPv6 规模部署应对思考[J]. 金融科技时代, 2021, 29(10): 90-93.