Computer Science and Application 计算机科学与应用, 2022, 12(12), 2684-2690
Published Online December 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.1212272

Hans汉斯

校园网数据中心IPv4向IPv6过渡的分析

——以伊犁师范大学为例

张体谅，张　斌*，刘新茂，李　杨，王彦同

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：2022年11月1日；录用日期：2022年11月30日；发布日期：2022年12月5日

摘　要

本文以伊犁师范大学为例，分析校园网络运行机制，缺乏IPv6网络栈点，旨在推进IPv4向IPv6过渡的建设，并进一步结合IPv6的相关技术，对校园网数据中心IPv4向IPv6过渡进行深入研究，通过IPv6可扩展性安全性机制，制定IPv6地址规划原则，建立SRv6端到端的快速网络通道，建立零信任数据中心模型，利用IPv4/IPv6双栈协议、隧道技术、动态翻译实现校园站群平台、DNS解析平台以及各个应用系统IPv4向IPv6的过渡，为偏远地区高校IPv6网络开放共享提供借鉴。

关键词

伊犁师范大学，数据中心，IPv4，IPv6，过渡，双栈，零信任

Analysis of IPv4 to IPv6 Transition in Campus Network Data Centers

—Taking Yili Normal University as an Example

Tiliang Zhang, Bin Zhang*, Xinmao Liu, Yang Li, Yantong Wang

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

Received: Nov. 1st, 2022; accepted: Nov. 30th, 2022; published: Dec. 5th, 2022

Abstract

Taking Yili Normal University as an example, this paper analyzes the campus network operation

*通讯作者。

文章引用: 张体谅, 张斌, 刘新茂, 李杨, 王彦同. 校园网数据中心 IPv4 向 IPv6 过渡的分析[J]. 计算机科学与应用, 2022, 12(12): 2684-2690. DOI: 10.12677/csa.2022.1212272

mechanism, and the lack of IPv6 network stacks, aims to promote the construction of IPv4 to IPv6 transition, and further combines IPv6-related technologies to conduct in-depth research on the transition from IPv4 to IPv6 in campus network data centers, establishes an SRv6 end-to-end fast network channel through IPv6 scalability security mechanism, establishes a zero-trust data center model, and uses IPv4/IPv6 dual-stack protocol, tunneling technology, Dynamic translation realizes the transition from IPv4 to IPv6 on campus station group platform, DNS resolution platform and various application systems, and provides reference for the open sharing of IPv6 networks in universities in remote areas.

Keywords

Yili Normal University, Data Center, IPv4, IPv6, Transitional, Dual-Stack, Zero Trust

1. 引言

目前 IPv6 技术逐渐走向成熟，在教育行业 IPv6 地址已经分发，很多高校和企事业单位已经完成 IPv6 初步建设，随着伊犁师范大学规模扩大，IPv4 资源产生了制约性，伊犁师范大学按照教育部改革要求和跟进 IPv6 步伐[1]，在友校建立 IPv6 网络的启发和帮助下，数据中心阶段性由 IPv4 过渡 IPv6 [2]，建设过程充分利用扩展性和安全性。在 IPv6 扩展性方面，在 IPv6 扩展报头加入相关字段，实现快速传输；在 IPv6 安全机制方面，利用 IPsec 字段，确保端到端的安全传输；打造安全可控的 IPv6 网络环境。

截止 2022 年 9 月，我校师生 20,000 人，IPv4 节点 3000 个，教育网分配的 IPv4 网络地址不足，随着智慧校园的建设和部分物联网设备的初步运行，跟随教育部严格要求下 IPv6 的部署指日可待，在此背景下，数据中心阶段性由 IPv4 过渡到 IPv6，本文以伊犁师范大学为研究对象，探索 IPv4 过渡到 IPv6 的方法，为偏远地区高校的 IPv6 网络建设管理提供参考。

1) 建立 IPv6 双栈[3]数据中心，完成对外公众服务的双栈的改造工作，部署在学校数据中心，范围涉及互联网络出口区域、DMZ 区域、及相应的对外服务应用系统。

2) 学校广域网连接校园内部和数据中心，内部业务和内部应用互访的关键通道，内网采用 SRv6，部署双栈隧道满足过渡期间 IPv4 和 IPv6 的承载诉求。

3) 构建 IPv6 端到端的实验田，为后续的循序演进构建基础，学校数据中心的内部应用需要逐步的开发改造，以信息中心为试点站，信息中心和数据中心的测试区进行 IPv6 改造，打通试点站和数据中心的 IPv6 互访通道，为应用系统的改造提供端到端[4]的测试验证环境，为内部应用的平滑升级奠定基础，同时也可以基于端到端的网络积累 IPv6 的技术经验。

2. IPv4 to IPv6 过渡网络模型

2.1. 地址规划

2.1.1. 地址规划分析

1) 实施 IPv6 语义化建模及地址规划，基于组织、业务、机构语义化建模，多极化地址规划管理[5]。

2) 实施 IPv6 地址分配与流程管理，快速 IPv6 地址分配，静态 + 动态方式基于工单流程的地址分配管理。

3) 实施 IPv6 地址扫描与检测分析，IPv6 地址扫描发现，状态检测 IPv6 自动定位，安全基线管控。

4) IPv6 地址回收及重分配，制定 IPv6 可视化回收流程。

2.1.2. 地址安全分配方式

1) 终端配置 IPv6SLAAC 无状态分配方式

在 IPv6SLAAC 模式下，无网关只分配链路本地地址，采用 RS-133 和 RS-134 路由器请求，当 IPv6SLAAC 存在网关时网络终端自动向网关发送路由请求信息，配置 IPv6 地址的网关收到请求，发送路由通告，终端会生成 IPv6 地址采用 EUI-64 配置方式：将接口的 MAC 地址转换为 IPv6 接口标识，16 进制的 MAC 地址转换为 2 进制-->第 7bit 如果为 0，表示该 MAC 地址是全局管理地址，将其取反-->在 MAC 地址中间插入 FFFE-->48bit+16bit=64bit-->2 进制转换为 16 进制。

主机获得网络部分 + 自己的 MAC 地址构造 IPv6 地址，通过 RA 抑制报文，避免占用更多带宽。

配置：Switch(config)#ipv6unicast-routing

Switch(config)#Interfacevlan1

Switch(config-vlan)#ipv6address2001:13::1/64

Undoipv6ndrahalt(RA 抑制报文)

目前安卓系统不支持 DHCPV6EUI-64 配置，安卓操作终端配置 SLAAC 方式。

2) 配置 HCPv6 服务器

为弥补了 IPv6 无状态地址自动配置的不足，配置 HCPv6 服务器为 DHCPv6 客户端分配 IPv6 地址。客户端向服务器发送配置申请报文(申请包括 IPv6 地址、DNS 服务器地址等参数)，服务器根据策略返回携带相应配置信息的报文。

DHCPv6 服务器分配一个完整的 IPv6 地址给主机，并提供 DNS 服务器地址等其它网络配置信息。DHCPv6 服务器也能提供无状态 DHCPv6 服务，即 DHCPv6 服务器不分配 IPv6 地址，仅需向主机提供 DNS 服务器地址和域名等其它配置信息，主机 IPv6 地址仍然通过路由器公告方式自动生成。

在路由器中如果 M 标记 = 1，终端会向 DHCP 服务器请求 IPv6 地址，当 O 标记 = 1，终端会向 DHCP 其他设备比如 DNS、搜索后缀请求其他数据地址，地址是否冲突是有 DAD 检测机制来评估。

配置

Switch#interfacevlan1

#ipv6ndmanaged-config-flag

#ipv6ndother-config-flag

根据学校应用按照如下表 1 对终端地址进行规划：

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

IPv6 终端类型	子网前缀	分配方式
终端用户	/64	SLAAC
设备 LoopBack 地址	/128	静态配置
设备互联地址	/127	静态配置
管理地址	/64	静态配置
对外提供服务的业务系统	/64	静态配置
校园网络用户	/64	有状态 DHCPv6

2.2. 快速网络转发模型

1) 利用双栈、隧道协议实现数据中心 IPv4/IPv6 的共存应用。

2) 建立安全端到端通道，IPSec [6]集成到网络双栈传输中，将双栈网络配置为仅允许在建立了安全通道之后再进行数据包传输。数据中心配置为只处理通过安全通道发来的数据包。在这个系统中，实际上已经在两个主机之间创建了一个“安全的虚拟专线”，只有安全的流量才能通过。

3) 双栈网络的基础之上，拓展 IPv6 报文结构，扩展头插入 SRH，并压入一个显式的 IPv6 地址栈，在核心交换节点不断的进行更新网络目的地址和偏移地址栈的操作来完成 IPv4/IPv6 逐跳转发，建立业务驱动网络模型，数据快速到达目的，将多个路由路径标识模块组合起来，形成 SRv6 路径，路径可编程。利用网络编程中的网络指令，数据转向下一个目的地，具体为在网络出口侧和核心交换侧开启 SRv6，中间节点采用传统 IPv4/IPv6 双栈结构。

2.3. 零信任网络安全模型

根据图 1 数据中心 DNS 系统和站群服务器同时开启双栈协议，建立安全边界安零信任模型，在数据中心和网络出口各建一堵墙，确保数据中心安全和出口安全。整个网络不可信，无论从本地网络还是互联网络通过任意协议访问双栈资源，需提供正确的身份标识，经过双栈认证、网络流量加密、应用层无感知实现数据中心零信任模型体系。假定攻击者可以使用任意 IP 地址进行通信，仅使用 IP 地址或物理位置作为标识符来保护资源是不够的。所有主机，甚至处于相同“可信区域”的主机，都必须提供正确的身份标识。对于攻击者发起主动攻击或者被动攻击，通过监听网络流量获取相关信息，进行风险处置。

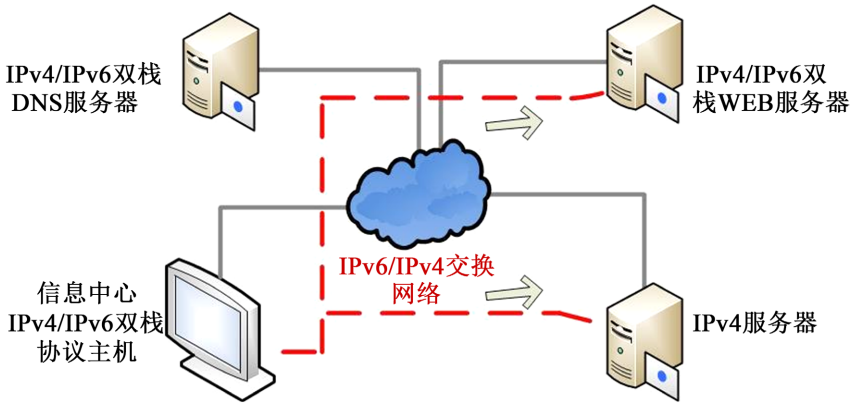

Figure 1. Dual-stack architecture diagram of data center deployment
图 1. 数据中心部署双栈体系图

2.4. 信息中心隧道模型

按照图 2 信息中心部分终端配置纯 IPv6 地址与数据中心站群系统和其它应用服务器进行通讯，站群和 DNS 系统配置双栈协议，其余的保持网络结构不变，对信息中心网关设备和数据中心网关设备配置 IPV4toIPv6 隧道协议[7]，实现纯 IPv6 业务的访问和 IPV4toIPv6 的互访。配置上配置静态地址隧道，降低动态隧道的伪造和非法接入威胁，并且设定精细的过滤策略。零信任用户采用客户端模式和隧道认证方式利用加密包过滤等手段规避 IPV4 与 IPv6 之间的交叉感染。

IPv6 网关不开启 DHCP 服务器，在路由器中设置 M 标记 = 1，终端向单独配置 DHCP 服务器请求 IPv6 地址，实现 IPv4 区域终端快速获取 IPv6 地址并且与 IPv6 区域终端地址互联互通，实现教学区、实验室安全快速访问 IPv6 网络，为智慧化校园、智慧化课堂、物联网发展提供基础。IPv6 建设完成将会急

速提升对数据中心的访问速率，同时相对 IPv4 网络极大降低丢包率，且扩展性极强，终端获取地址快，不会出现广播风暴、ARP 攻击等网络攻击，方便运维管理人与维护，增强稳定性和安全性。

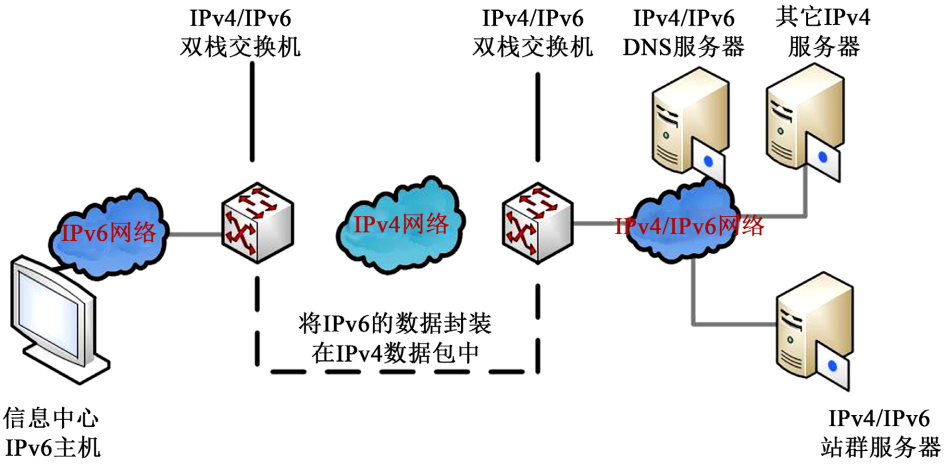

Figure 2. Data center deployment tunnel diagram
图 2. 信息中心部署隧道体系图

2.5. 网络出口模型

IPv6 不进行 NAT 转换，采用 IVI [8]动态翻译技术云服务器模式，实现对外发布的 IPv6 资源共享。在网络出口实行转发层面和控制平面分离，保持原有 IPv4 策略安全基础，出口防火墙、IPS、WAF 全设备同步支持 IPv6，扩展内外网资源实行零信任机制，减少内外网访问者的身份和策略合规性，把应用资源从公共领域消失，关闭所有双栈不必要的 TCP 端口，拒绝非必要的接入，通过身份认证访问，确保内外网双栈资源安全溯源。

2.6. 核心参数

2.6.1. 站群系统

把学校主站和各个子网站集成到站群平台，建立主站和子站集成的网站体系，通过双栈协议实现各个网站集成，主站和子站形式上相互独立，逻辑上独立交叉[9]。分别配置 IPv4/ IPv6 双栈前端 Web 服务器、发布服务器、数据库服务器。

1) 前端 Web 服务器部署 WEB、视频、附件等资源

2) 发布服务器配置静态页面服务

3) 数据库服务器提供数据支撑

4) 相关参数

SOCKET 参数：打开 IPv6SOCKET 功能，并绑定对应接口和地址。

地址参数：把程序或网页中以 IPv6 地址直接写入的文件 URL 或链接 URL 更换成域名。

函数参数：把程序或网页代码中存在无法处理 IPv6 地址的函数更换成同时支持 IPv4 和 IPv6 的函数。

结构参数：把程序中存储 IP 地址的数据空间(IPv4 为 32 位)更换为同时支持 IPv4 (32 位)和 IPv6 的变量结构、数据库结构或(128 位) API。

5) 访问方式：通过 IVI 无状态翻译实现互联网通过 IPv4 网络访问校内 IPv6 站群系统。校内访问通过 IPv6 或者 IPv4 的网络访问，教育网络平台可以直接通过 IPv6 访问校园网站群系统。

2.6.2. DNS 系统

通过权威和递归解析实现 DNS 系统双栈解析[10]，DNS 主机系统开启双栈协议，添加 AAAA 记录，对外发布 IPv6 解析地址，记录类型为 AAAA，主机记录为域名的前缀。

以下是 DNS 系统规划的 IPv6 域名地址

host:dns1.ylnu.edu.cn

ipnum:219.247.32.342001:250:1813:1003::2

host:dns2.ylnu.edu.cn

ipnum:219.247.32.352001:250:1813:1003::3

1) 权威 DNS 分析

开通 DNS 系统 IPv6 网络，在 DNS 启用 ylnu.edu.cn 域名解析，解析记录内容与 IPv4DNS 服务器中 ylnu.edu.cn 域名下的解析记录一致，在站群上发布的站点配置 AAAA 记录，记录值为站群发布机地址。

学校现有权威域名为 ylnu.edu.cn 域名记录都是 A 记录，那么首先需要建一个 ylnu.edu.cn 的权威域，把主机头对应的 AAAA 记录添加上。

2) 添加地址库

预留 IPv6 运营商地址库，关闭对外解析线路的递归解析，防止外部 DNS 攻击和对外业务的开放而导致的设备压力增加问题。

3. 实施效果

根据教育部统计检测结果，伊犁师范大学二三级链达到百分之百。从校园网入口到门户网站和 DNS 系统支持 IPv6 的访问，其安全性保持的到保障。

通过 https://ipw.cn/ipv6webcheck/?site=ylnu.edu.cn 等相关网站进行 IPv6 测试，实现了资源共享，表 2 为校园网主站平台，https://www.ylnu.edu.cn/的测试结果。

Table 2. Test points and results
表 2. .测试要点和结果

序号	测试要点	结果
1	网站 ylnu.edu.cn 域名 IPv6 解析能力	可以解析
2	网站 ylnu.edu.cnIPv6 访问能力	可以访问
3	网站首页 IPv6 访问成功率	访问成功率大于 80%
4	网站首页内容 IPv6 和 IPv4 的一致性	一致
5	网站首页布局 IPv6 和 IPv4 的一致性	一致
6	站 www 域名具备完整的 IPv6 域名授权体系	具备
7	网站二级链接 IPv6 支持率(不计算外链)	80%
8	网站三级链接 IPv6 支持率(不计算外链)	80%
9	网站 www 域名解析时延	1MS
10	网站首页访问时延	1MS

4. 展望

通过建立数据中心 IPv4 过渡 IPv6 网络运行机制，有效推动我校 IPv6 共享工作，在方便教师教学、

科研工作的同时，也积累了宝贵经验。自运行机制建立以来，我校 IPv6 认可度不断提高，通过双栈网络端到端设置－零信任数据中心搭建－站群双栈建设－DNS 双栈建设等，有效推动数据中心 IPv6 资源共享，为偏远地区高校网络做借鉴。IPv6 数字化校园网络演进之路漫长，未来要充分利用其扩展性和可编程性，加速下阶段 IPv6 推进工作。

1) 校园可同步启动办公园区网络的 IPv6 改造工作，建办公区优先改造，制作样板积累经验，形成改造规范指南，指导各个校区和院系 IPv6 改造，指定广域网双栈隧道切换单栈的时间节点，推动学院和各校区积极进行改造。

2) 随着智能制造的发展物联网应用系统将在企业生产网络大规模部署，大量的终端需要接入企业的生产网络，所以学校物联网络应及时 IPv6 的改造，为海量终端的接入提供充足的地址空间。

3) 数据中心内部应用访问逐渐切换 IPv6 通道，对外物联网访问按需保留 IPv6 通讯能力，在本阶段，应主要聚焦 IPv6 的逐步迁移工作，工作结束之后，学校的数据中心网络、数据中心内部应用系统、广域网以及办公园区全面完成 IPv6 改造，从办公园区到数据中心的应用系统访问实质上已经切换到 IPv6 单栈通道，此时数据中心网络和应用系统可直接切换到 IPv6 的单栈运行。

4) 等到外部的互联网全面 IPv6 化以后，老旧的生产园区公共终端和系统退网即可实现全面 IPv6 网络的单栈。

基金项目

伊犁师范大学校级科研项目(2021YSYB094)。

参考文献

[1] 邬贺铨. 加快 IPv6 规模部署支撑网络强国建设[J]. 中国网信, 2022(1): 31-34.

[2] 赖济海, 罗万伯, 王丹霞. IPv4/IPv6 过渡的安全评估[J]. 信息安全与通信保密, 2005(9): 61-63

[3] 黄萍. 基于 IPv6 协议的双栈技术研究与应用[J]. 微型电脑应用, 2022, 38(1): 206-208.

[4] 余波, 揭凌雁, 胡凯, 王丽芳. 推动解决 IPv6 端到端“通车”问题[J]. 通信企业管理, 2022(6): 70-71.

[5] 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.

[6] 张军. 移动 IPv6 网络安全问题及解决对策[J]. 信息系统工程, 2022(9): 115-118.

[7] 涂金龙. 高校网站及业务系统支持 IPv6 访问改造的技术路线研究[J]. 电脑知识与技术, 2022, 18(15): 35-37.

[8] 方睿钰, 陈阳, 沈佳杰, 王新. 复旦大学校园网 IVI 部署实践与思考[J]. 中国教育网络, 2020(11): 55-56.

[9] 史德伟, 刘洋, 林杰, 孙小影. 端到端 IPv6 的高校网站群部署方案设计[J]. 信息技术与信息化, 2021(10): 190-193.

[10] 高秋燕. 基于高校的 IPv6 网络安全研究与实现[J]. 信息系统工程, 2021(2): 55-56.