

国信证券互联网业务基于 IPv6 的探索与实践

(国信证券供稿 深圳局指导)

一、IPv6 改造意义和背景

面对互联网 IPv4 地址资源匮乏问题，IPv6 能够提供充足的网络地址和广阔的创新空间，是公认的下一代互联网商业应用解决方案，能够提供更广泛的互联网连接，促进物联网、5G、人工智能等新应用、新领域的创新，有助于显著提升我国互联网的承载能力和服务水平。

为贯彻落实国家制订的《推进互联网协议第六版（IPv6）规模部署行动计划》，加快推进基于 IPv6 的下一代互联网在金融行业的规模部署，促进互联网演进升级与金融领域的融合创新，根据中国人民银行、中国证券监督管理委员会等监管机构要求，证券基金经营机构推进基于 IPv6 的下一代互联网规模部署分阶段逐步落实。

二、IPv6 实施目标和具体实践

在人行、证监会的指引下，国信证券在 2019 年 8 月成立了 IPv6 改造专项工作小组，制定相应的工作计划和实施方案，并明确职责分工，协同组织包括网络、系统、安全、开发、应用等多方面资源，积极配合推动互联网协议第六版（IPv6），分阶段、分批次平稳过渡，最终实现：

所有软硬件基础设施均支持 IPv6，互联网相关域名解析设备均支持双栈，同时具有访问 IPv4/IPv6 地址。

面向公众服务的互联网应用系统保证在 IPv6 和 IPv4 环境下具备同等的业务连续运行保障性能。



图 1 互联网规模部署的三个目标阶段

（一）初期小范围实施，摸索积累 IPv6 改造经验

由于 IPv6 升级改造是一个系统性工程，IP 地址是生产系统运行的关键要素，地址的变化牵一发而动全身，需要网络、系统、应用、外部服务等多个方面配合完成，除此之外，启用 IPv6 对各个层面功能、性能及稳定性有待测试和试运行验证。针对初期小范围实施，我们采取了以下措施：

1. 结合外部调研摸查，制定适合国信的 IPv6 方案

针对 IPv6 互联网涉及的外部环境（如 CDN、DNS 域名解析、运营商、终端、互联网 IP 地址申请及备案等）调研，对同行业支持 IPv6 改造技术方案进行交流，并对网络、系统、安全等关键软硬件基础设施进行功能和性能测试，梳理评估当前基础设施升级方案，为后续的详细计划制定和部署

奠定了坚实基础。

2. 测试环境先行，探索方案可行性

由于缺少 IPv6 的实施经验，我司首先利用外网测试环境进行基础资源改造并测试，包括对上网行为管理的 IPv6 上网功能全方位验证，对互联网 DNS 和 GSLB 支持双栈 IPv6 接入验证。同时也为后续应用改造测试验证提供了基础环境。

3. 应用试点上线，积累 IPv6 经验

根据前期调研及测试，我司制定了门户网站 IPv6 改造初步方案，由于应用部署在主数据中心网站接入区，为了支持 IPv6 访问同时避免新引入的 IPv6 协议可能会带来的风险，前期决定采用新增网站 IPv6 接入新的安全区域专门用作网站区的互联网 IPv6 接入区。

网站 IPv6 接入区新增门户前端接入服务器配置 IPv6 地址用于接收来自互联网 IPv6 的访问，门户网站的后台保持原有不变，通过 IPv4 与新增的 IPv6 前端通信。

DNS 在原有的互联网 DNS 系统基础上新增 AAAA 记录，互联网防火墙、负载均衡和 WAF 等网络、安全架构与原有保持一致，从整体上保证了与原有 IPv4 环境运维工作的一致性。

2019 年底，我司实现了首个面向公众服务的应用系统对互联网提供 IPv6 连接访问，为后续其他应用实施积累了宝贵的经验。

（二）夯实基础，面向公众服务互联网应用规模部署支持 IPv6

为了满足 IPv6 规模部署最终要求,避免 IPv4/IPv6 协议转换的过渡方案长期并行,采取 IPv4/IPv6 双栈改造统一标准化,同时梳理覆盖的业务改造范围,组织软硬件基础设施、工具平台、应用改造方案评审及落地。

1. 加强基础知识和技能培养

组织开发和运维普及 IPv6 知识交流培训,了解现状及相关的技术,并形成相关的文档手册,为后续改造方案设计、开发、运维上线部署提供指导。

2. 基础设施先行

互联网接入区软硬件基础设施: 防火墙、负载均衡、web 应用防火墙、交换机、前端接入服务器等,改造这些可以处理互联网发起的 IPv6 流量。

互联网域名解析体系: 国信互联网 DNS 包括外部 DNS 和全局负载均衡,改造两者能够对互联网 IPv6 地址的客户端提供与 IPv4 网络下一致的地址解析服务。通过对公有云、私有云不同互联网接入区域基础设施 IPv6 改造,为后续的应用改造提供了很好的 IPv4 同等业务连续性保障基础环境。

3. 运维体系支持 IPv6

为了提高运行管理的效率,对 CMDB、ITIL 流程、云管、监控、中间件等工具平台支持 IPv6 对接。

4. 逐步推动应用改造，大规模支持 IPv6

根据用户规模、网络方案、应用改造难易程度等因素排期，分阶段进行评审，通过后进行应用部署，从单机到多集群控制灰度变更上线。

2020 年底我司平稳完成第二阶段 IPv6 大规模部署，包括基础设施的改造和现有面向公众服务互联网应用系统的大规模平稳升级。

（三）IPv6 持续推广、体系化建设

随着国内 IPv6 升级改造的进程加快，监管部门对全面支持 IPv6 的要求也在逐渐提高，2021 年底我司按照行业要求稳步推进 IPv6 持续改造和优化。

在两年多运行稳定前提下，基于成本考虑，将前期独立承载 IPv6 流量的网络设备逐步与 IPv4 设备整合，例如防火墙、Web 应用防火墙、DNS 和负载均衡等，不断降低硬件成本、精简网络，统一 IPv4 和 IPv6 的网络架构标准。

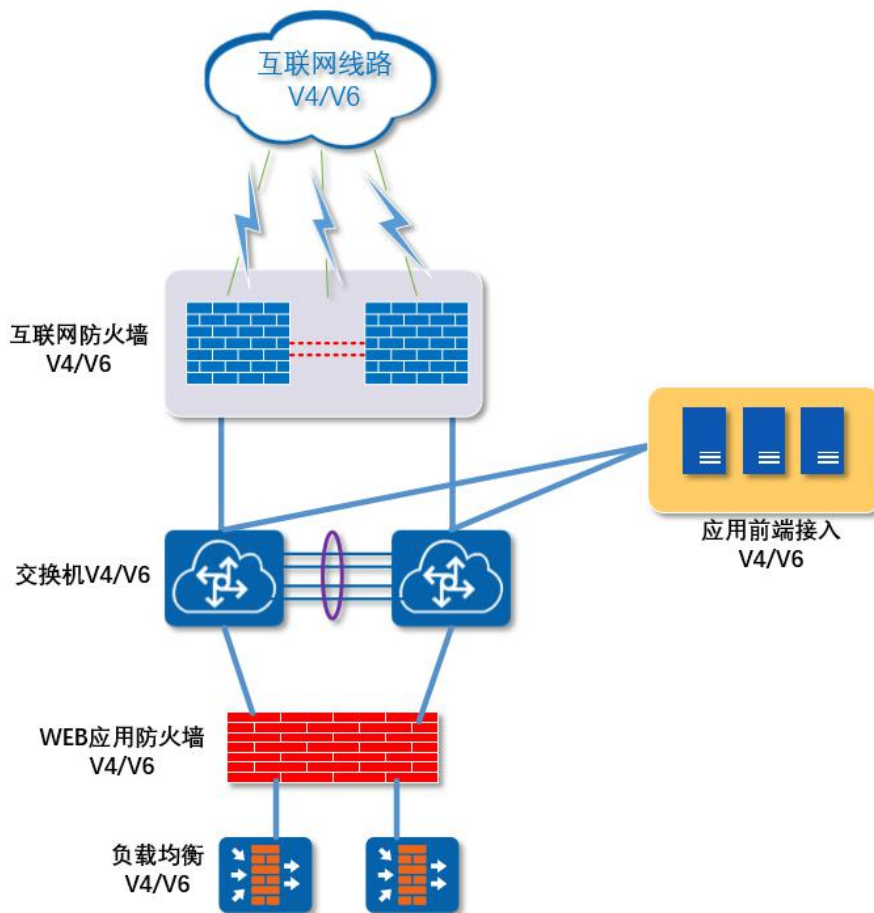


图 2 设备整合

在管理上，将支持 IPv6 作为新上互联网应用准入技术要求，夯实网络基础设施，优化不同级别应用多数据中心流量接入部署，健全监控运维体系，提高系统可用性，同时完善相关的网络安全管理。

三、IPv6 实施成果及未来方向

目前我司包括两地三中心、公有云等面向互联网区域所有软硬件基础设施均支持 IPv6，互联网相关域名解析设备均支持双栈，同时具有访问及防护 IPv4/IPv6 地址的能力。对互联网接入线路、设备多冗余，同时对 IPv4 和 IPv6 流量进行压测，评估更换新的设备进行整合来提升性能。通过设备

整合和统一管理，大幅降低了运行成本。

互联网接入应用全面具备客户端网络自适应 IPv4\IPv6 地址，服务端接入层接口支持 IPv6 伺服，满足安全防护处理、信息采集上报、高可用部署等要求。组织应用实施前评审，严格控制新上互联网应用上线 IPv6 准入标准，使得更多的互联网应用满足 IPv6 要求。

优化应用多数据中心接入部署，健全监控及运维管理体系：完善修订网络及安全相关管理制度覆盖到 IPv6 要求；对信息系统应急预案及演练步骤梳理完善并纳入演练场景；在网络层对 IPv6 用户流量进行实时监控，应用层对 IPv6 服务端口及服务进行可用性探测。

通过持续推动，目前我司覆盖的面向客户服务的系统包括 web 类应用（门户网站、微信等）、PC 端应用（金太阳网上交易、金太阳智能版等）、移动端应用（金太阳 APP 等），完成 17 个以上应用支持 IPv6 接入客户访问，同时关键应用活跃用户 IPv6 请求占比逐步提升：web 类超过 25%，PC 类超过 5%、移动 APP 超过 15%，通过权重控制及客户端寻址测速机制能有效支撑 IPv6 用户的增长。国信证券高标准、严要求积极参与证券期货行业 IPv6 规模部署，实践证明，IPv6 实施改造后能同等给客户带来持续稳定高质量的服务。

从国家长远的 IPv6 规划和发展来看，IPv6 的互联网流量占比会逐步提高，构建基于 IPv6 的核心支撑体系，从面

向公众服务转向内部业务系统，同时按照《金融服务机构面向公众服务的互联网应用系统 IPv6 支持评测指标》要求，系统质量、稳定性和安全性等方面需要持续提升。

四、IPv6 问题及建议

我司在各阶段改造过程中也遇到了一些问题和挑战：

1. IPv6 基础知识储备不足

IPv6 改造涉及的系统和人员多，需要做好多轮基础的知识培训和业务咨询，形成知识体系和规范标准对接。

2. IPv6 可用性及容量问题

改造依赖强有力的基础设施支持，包括多机房、多线路冗余，IPv4 和 IPv6 设备可以从最初区分开到逐步合并，提供稳定及高可用保障的环境，同时要为 IPv6 用户流量推广提供容量支撑。

3. 平台工具支持 IPv6 的改造复杂

应用规模部署依赖工具平台提升实施的效率和上线后的管理，需要对现有 CMDB、流程、云管、监控、中间件、持续交付等工具平台进行改造以便对 IPv6 上线提供支持，且各个工具之间存在相互依赖、数据交互的情况，对改造的成本和效率带来了很大的挑战。

总之在加快推进 IPv6 的规模部署工作中，对于券商机构来说其业务系统与基础设施规模庞大，改造工作将面临巨大挑战。面对 IPv6 改造的难点与挑战，我们需要在整个过

程中保障业务系统平稳运行，制定合理的改造方案。在安全可控的范围内，逐步推进各系统的改造工作，确保改造后的应用系统业务连续性及安全性。