国融证券 IPv6 部署落地实践

（国融证券供稿 内蒙古局指导）

IPv6 部署是一个复杂的系统工程，需通过分阶段对网络、业务终端、安全等各个层面进行改造与升级。针对公司的现状，国融证券通过搭建支持 IPv4/IPv6 双栈模式网络环境，推进面向互联网应用系统完成 IPv6 部署改造。

一、背景

IPv6 是英文“Internet Protocol Version 6”（互联网协议第 6 版）的缩写，是互联网工程任务组（IETF）设计的用于替代 IPv4 的下一代 IP 协议。由于 IPv4 最大的问题在于网络地址资源有限，严重制约了互联网的应用和发展。IPv6 的使用，不仅能解决网络地址资源数量的问题，而且也解决了多种接入设备连入互联网的障碍。

2016 年 3 月国务院发布的《第十三个五年规划纲要》中提出超前布局下一代互联网，全面向互联网协议第 6 版（IPv6）演进升级。2018 年 12 月中旬，中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会印发《关于金融行业贯彻《推进互联网协议第六版（IPv6）规模部署行动计划》的实施意见》（银发[2018]343 号），要求加快金融行业软硬件基础设施和应用系统更新步伐，完成金融领域公共管理、民生公益等服务平台 IPv6 改造。

为了贯彻落实《推进互联网协议第六版(IPv6)规模部署

行动计划》的要求，国融证券开始了 IPv6 的探索实践。

二、 目标

我公司面向公众服务的互联网应用系统涉及 IPv6 改造的数量为 14 个，按照访问方式分为 Web 浏览器（4 个）、APP 客户端（5 个）、PC 客户端（5 个）。

完成改造需要公司前期搭建灵活的支持双栈模式的网络环境，适配面向公众的 14 个应用系统支持 IPv4/IPv6 连接访问的改造需求，同时具备与 IPv6 改造前同等的业务连续性保障能力。并在此基础上，后期持续推进和扩展 IPv6 应用的规模部署和网络架构的衍生，最终完成从 IPv4 到 IPv6 的平滑演进和顺利过渡。IPv6 建设演进路线如图 1 所示。

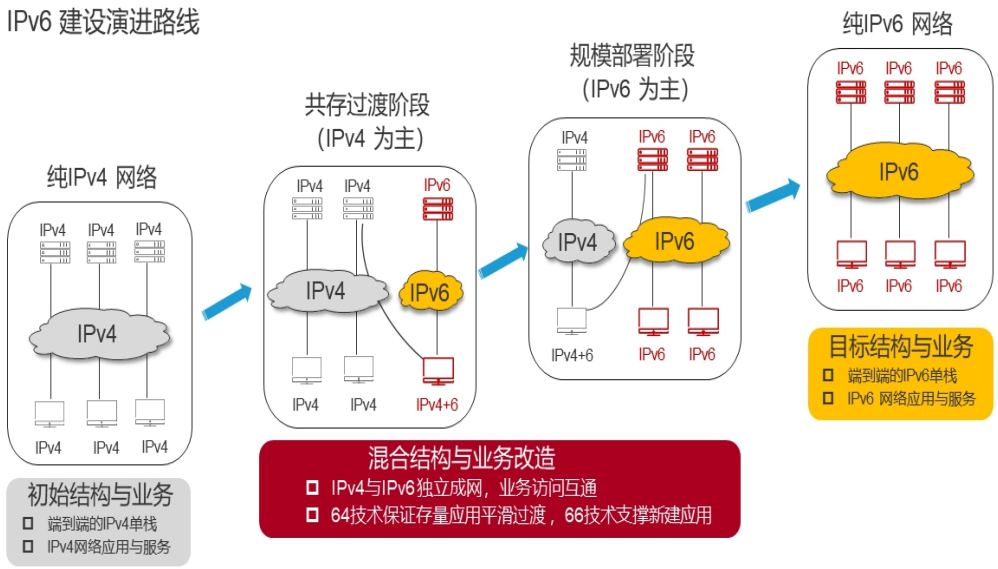

图 1 IPv6 建设演进路线

三、 做法和经验

（一）组织保障

成立 IPv6 工作小组，由公司首席信息官担任组长，成员

部门包括信息技术中心、业务管理部、经纪运营部等多个部门。由信息技术中心负责制定总体方案、网络规划、IPv6 基础环境建设、应用系统改造、系统部署；由经纪运营部负责应用系统推广，收集用户反馈；由业务管理部负责分支机构协调支持。信心技术中心

根据工作小组分工安排，各成员部门指定专人开展相应的工作，并与多家应用系统厂商、系统集成商反复进行技术交流与方案讨论。根据目前 IPv6/IPv4 整体应用情况及我公司信息系统、网络设备现状，我们制定了推进的 IPv6 改造方案。分为如下几项工作：向原有线路电信运营商申请 IPv6 地址段，在原有 IPv4 网络上搭建专用的 IPv6 网段；对公司官网、APP 等 14 个应用系统进行开发改造（通常包括服务端和客户端），实现 IPv4/IPv6 双栈协议，着重解决性能、地址分配调度等技术问题；加强 IPv6 网络安全防护，部署 WAF 防火墙等设备，确保网络安全；完善配置 DNS 解析配置，支持智能双栈解析，根据客户的网络状况分配合适的地址，给用户更好的 IPv6 体验。

（二）资源投入

为确保 IPv6 改造项目实施顺利进行，我司投入了充足的人力和资金。

公司 2019 年初成立了 IPv6 工作小组，仅涉及公司内部信息技术人员就包括网络工程师、安全工程师、服务器虚拟化管理员、Web 应用开发工程师、APP 开发工程师、产品 UI 设计师、各相关应用系统管理员等多个岗位。背后还包括

14 个应用系统的厂家工程师、网络服务商工程师等相关人员。

（三）技术路线

在技术上，本次 IPv6 工程改造项目主要按照如下几个原则进行改造。

1、合理利用现有资源。在确保系统网络的安全和可用性基础上，充分利用公司 IT 基础设施现有投资对已有 IPv4 网络与安全基础架构的资源，通过升级、验证测试等方式完成 IPv4/IPv6 双栈模式改造，同时，统筹考虑网络与 DDoS 流量清洗、互联网接入线路、负载均衡设备、防火墙、IPS/IDS、Web 应用防火墙、三层交换机网关、DNS 解析等，确保 IPv6 具有和 IPv4 同等的性能和安全等级。

2、合理规划 IPv6 地址。新申请 IPv6 地址段，在原 IPv4 网络上并构建支持 IPv4/IPv6 网络。在部署前期就进行 IPv6 地址的合理分配和预留，按照不同数据中心不同安全区域，不同应用系统逐层规划 IPv6 地址。接口、网关等地址推荐采用从 IPv4 地址演化的方式分配 IPv6 地址，方便记忆和后期问题排查。

3、确保应用溯源支持。应用系统接入服务器优先考虑通过 IPv6/IPv4 双栈模式改造，进而支持 IPv6 协议，确保能够对访问应用的 IPv6 地址进行溯源。

4、递进式推进兼顾风险。应用系统后台数据库服务器、业务中间件暂保留为 IPv4 结构，确保后台服务器的稳定性。

网络改造：IPv6 流量走势如图 2 所示，外网（电信、联

通）防火墙收到客户端请求后基于路由转发给应用负载，进入应用负载，命中业务 VS，根据负载需求将目的地址转换为实际服务器地址，基于路由转发向综合网核心交换机，WAF 进行二层透传，核心交换机基于直连路由转发给相应服务器。

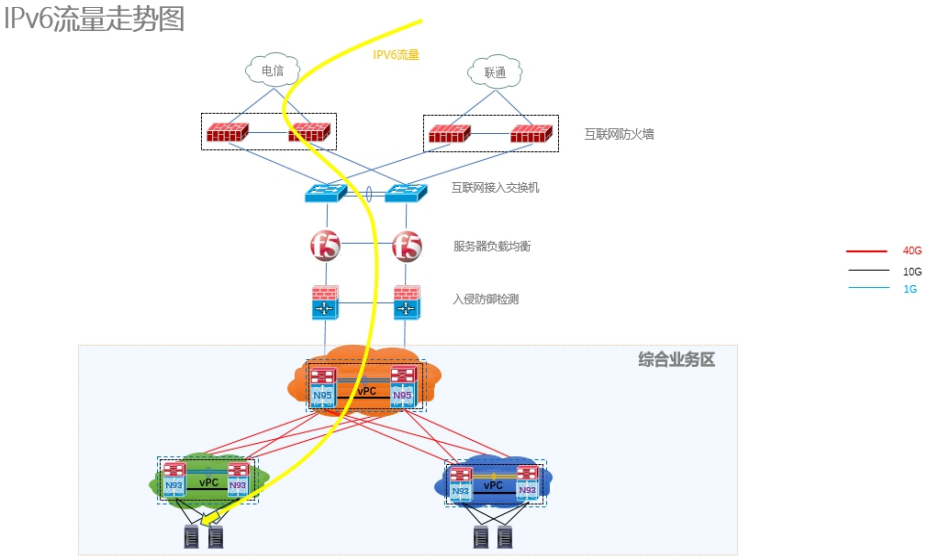

图 2 流量走势图

应用系统改造：以公司 APP 为例，如图 3 所示，红色部分为改造点。APP 服务器端使用统一均衡程序进行连接管理和动态均衡，并且对各种网络环境进行适配。客户端经过改造后会自动检测网络环境，对于支持 IPv6 的环境，会优先使用 IPv6 的连接。整个过程对用户来说是完全无感知的，以做到系统的平滑升级。

当均衡服务检测到客户端通过 IPv6 环境访问（域名解析到 IPv6 地址）时，均衡返回优先返回各接入服务器的 IPv6 地址，当均衡服务检测到客户端通过 IPv4 环境访问（域名解

析到 IPv4 地址）时，均衡返回优先返回各接入服务器的 IPv4 地址。客户端根据均衡服务返回的地址顺序连接接入服务器。

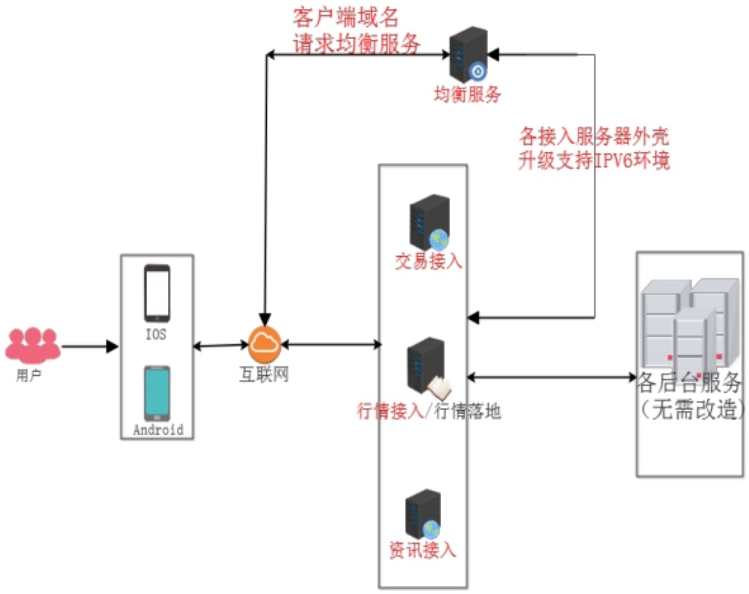

图 3 应用系统改造

（四）安全保障

为确保 IPv6 项目推进的同时，不影响原有 IPv4 应用的正常使用，保障平稳过度，主要的安全保障措施有如下。

1、构建 1 套与生产环境相仿的网络测试环境，在测试环境完成相关设备版本升级支持 IPv6 协议，配置网络参数完成 IPv6/IPv4 双栈模式改造，然后在此环境下进行 14 个应用系统和网络的充分测试，以彻底解决发现的和潜在的问题。测试一段时间后，最后按照测试环境的经验将生产环境完成 IPv6/IPv4 双栈模式改造，最后配合各相关应用系统负责人，在变更时间窗口内完成 IPv6 各应用系统的上线。

2、应用的升级发布采用灰度模式，循序渐近地安排实施，在测试环境中完全通过之后再进行逐步切换。

3、根据网络流量和应用系统访问情况，对 IPv6 与 IPv4 用量进行对比，有针对性地制定 IPv6 扩容方案，确保升级中系统容量使用率在正常范围。

四、 成效及后续

截至 2020 年底，公司已全部完成面向公众服务的互联网的 14 个应用系统的 IPv6 改造。根据对现有数据的统计分析，以上应用系统接入 IPv4/IPv6 的总体比例差不多是 5：1，其中 APP 服务器接入 IPv4/IPv6 的总体比例差不多是 3：1。

应用系统 IPv6 改造是一项长期性的工作，无论其客户端和服务端，未来很长一段时间内都会是 IPv6 和 IPv4 网络共存的情形。需要网络、应用改造中注重逐步演进，平稳过渡。