财信证券 IPv6 规模化部署实践分享

（财信证券供稿 湖南局指导）

2017 年，国家发布的《推进互联网协议第六版(IPv6)规模部署行动计划》指出，推进 IPv6 规模部署和应用是加快网络强国建设、加速国家信息化进程、助力经济社会发展、赢得未来国际竞争新优势的紧迫要求。2021 年，国家发布了《关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知》，明确要坚定不移地推进 IPv6 规模部署和应用，为建设网络强国和数字中国提供坚实支撑。“十四五”规划和 2035 年远景目标纲要也明确提出了加快建设新型基础设施，全面推进互联网协议第六版（IPv6）商用部署的目标。财信证券股份有限公司（以下简称“我公司”）积极响应国家和行业推进 IPv6 规模部署的号召，于 2019 年开始启动 IPv6 改造部署，截止目前，已完成所有面向公众服务的互联网应用系统 IPv6 改造，并持续开展网络、应用、终端的 IPv6 升级改造工作，健全和完善 IPv6 监控运维体系和网络安全防护体系，稳步推进公司信息系统向下一代网络平滑演进升级。我公司在 IPv6 规模化部署工作中，积累了一些实践经验，可供分享和探讨。

一、实践分享

(一) 调研论证

由于 IPv6 协议与 IPv4 协议并不兼容，不能保证现有 IPv4 软硬件基础设施和安全设备一定能够兼容 IPv6 协议，同时，现有软硬件设施开启 IPv6 协议支持后，设备性能指标和处理能力可能无法满足业务需求。因此，我公司在改造方案设计之初，对现有的软硬件设施进行了盘点和调研，列出需进行升级或替换的软硬件基础设施，以科学制定改造方案和项目预算。

IPv6 协议栈比较复杂，初期应用尚不广泛，我公司要在“保障系统安全稳定运行”的前提下推进这一复杂工程，必须充分论证，知其然也知其所以然。因此，在制定改造方案前，我公司组织信息技术骨干通过三个途径尽快了解和掌握 IPv6 改造的细节：一是联系软硬件设备厂商、运营商进行技术交流，了解各厂商的 IPv6 技术方案、落地案例以及技术优势，博采众长；二是学习同行业头部单位的 IPv6 改造经验，取长补短；三是查阅技术资料、外文文献、RFC 标准等，吃透技术细节。通过这些举措，做到心中有底，进而选择符合我公司实际情况的技术路线，制定相应的改造方案。

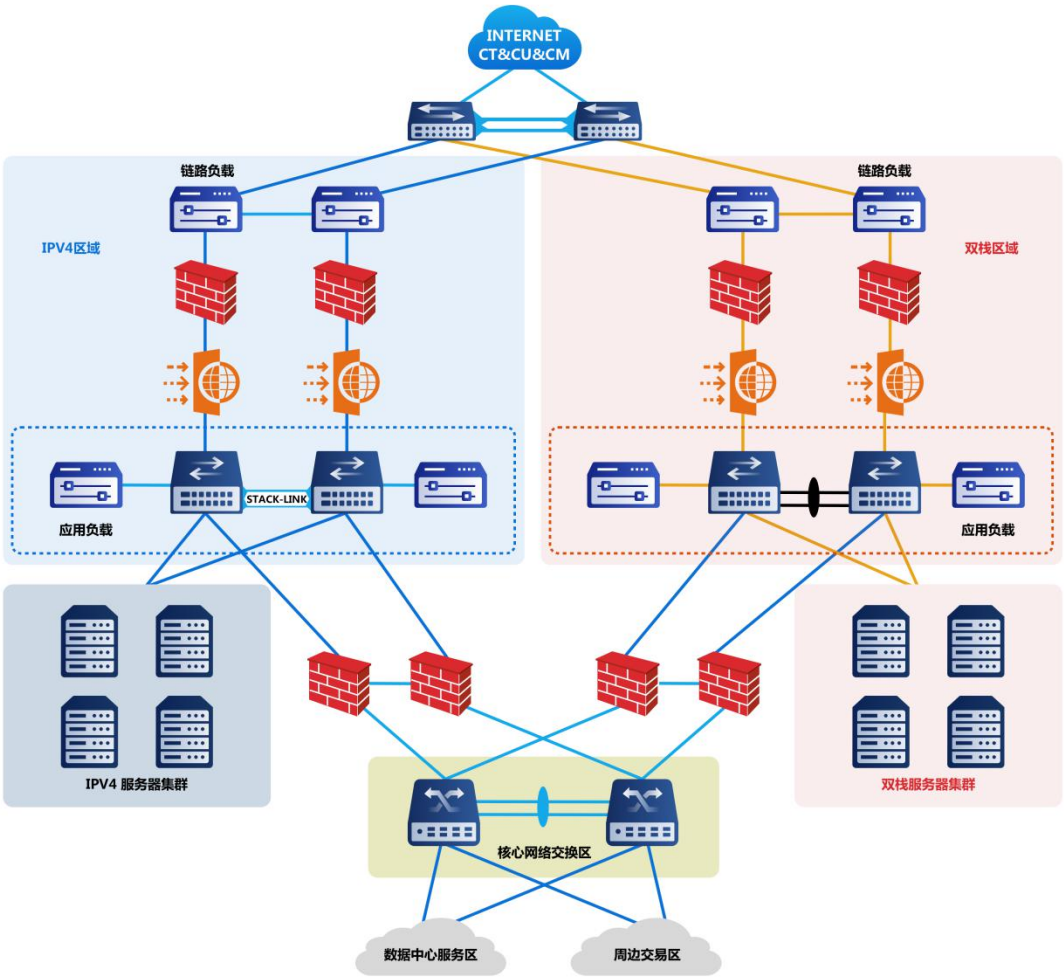
(二) 技术路线选择

IPV6 改造有双栈技术、隧道技术、地址协议转换技术等技术路线，改造最彻底的为 IPv4/IPv6 双栈技术。通过采用双栈技术，可保证服务端记录到客户端的真实源 IP，能满足合规审计、安全防护的场景需要，而其他改造技术都有改造不

彻底的局限性。采用双栈技术进行 IPv6 改造虽然前期成本较高，实施周期较长，但我公司对比了各技术路线的优劣性，经综合评估，从长远考虑，最终选择了 IPv4/IPv6 双栈改造技术路线，并且目前已顺利完成所有面向公众互联网系统的双栈改造。

(三) 网络架构设计和改造

为保证 IPv6 部署实施过程中现有系统的安全稳定运行，我公司在 IPv6 升级改造过程中，规划新建了 2 个支持双栈的互联网应用生产区域，同时改造现有测试区域。新建的双栈网络区域为 WEB 类业务区域和交易类(APP、PC 客户端接入)区域，接入 3 家运营商双栈线路实现入站负载均衡；改造现有测试区域实现双栈。互联网应用系统进行代码修改后，先在测试区域进行功能和兼容性测试，待测试完成，则迁移至新建的双栈生产区域。



为实现多运营商线路的入站负载均衡和线路冗余，我公司向电信、联通、移动 3 家运营商申请了多条 IPv6 双栈线路接入，分配了充足的 IPv6 地址。在完成 IPv6 线路改造的基础上，同步实现了在 IPv6 协议栈上的多线路高可用。

为实现多站点、多互联网线路之间的冗余切换，我公司自建了基于全局负载均衡（GSLB）技术的智能 DNS 系统。在 IPv6 改造过程中，需要对域名授权体系进行 IPv6 改造，因此我公司将智能 DNS 设备接入双栈线路并配置 IPv6 地址，支持同时发布 A 记录和 AAAA 记录，并实现了从 DNS 设备端到数

据中心互联网接入点的 IPv6 线路健康探测，达到互联网应用系统在 IPv6 线路上的全局负载，自动切换，完成了域名授权体系的 IPv6 改造升级。

为沿用 IPv4 网络的安全架构设计，我公司在 IPv6 内网环境使用 IPv6 唯一本地地址（fc00::/7），在互联网边界通过链路负载设备进行互联网应用系统发布，这样可防止 IPv6 内网环境直接暴露在互联网。对于内网 IPv6 地址的使用规划，我公司经综合评估，基于方便运维管理、保持使用体验一致性的考量，制定了 IPv6 地址配置管理规范，将 IPv6 地址前 64 位对应成 IPv4 的 C 类网段，IPv6 地址后 64 位对应成 IPv4 C 类网段的主机位，例如某主机的 IPv4 地址为 192.168.1.1，那么其分配的对应的 IPv6 地址就是 fc00:192:168:1::1。通过这样的规范化设计，IT 员工便于理解，网络管理员便于管理，解决了 IPv6 地址管理的困扰。

(四) 应用系统改造和迁移

我公司在应用系统改造过程中，遵循“递进式推进与增量式推进相结合”的原则，对于现有的存量应用系统，按照风险可控的原则逐步递进式改造。对于新建应用系统，在需求设计阶段，就将支持 IPv4/IPv6 双栈访问做为硬性需求，并纳入验收指标。

我公司存量互联网应用系统包括 BS 类系统（WEB 网站、H5 站点）和 CS 类系统（PC 客户端、APP 移动客户端）。BS

类系统采用标准 HTTP 协议，IPv6 改造的重点主要包括：一是系统数据库表结构的排查，涉及 IP 记录的字段需检查字段大小是否满足记录 IPv6 地址的需求，如果不满足则需进行扩展；二是代码层面涉及对 IP 地址的计算、校验、展示等处理逻辑时，需进行调整以支持 IPv6 地址；三是测试验证系统中间件和 nginx 等反向代理程序开启 IPv6 支持后，是否运行正常，性能吞吐是否下降。CS 类系统改造难度高于 BS 类系统，大多使用了厂商专用的 socket 通信协议，需修改网络层处理函数以支持 IPv6 协议栈通信。

我公司在存量互联网应用系统改造过程中，根据“先易后难、稳步推进”的原则，先进行 WEB 类系统改造，对于 APP 和 PC 客户端系统，则与厂商进行协作，基于厂商提供的双栈兼容版本进行改造。

在 IPV6 改造后的应用系统迁移生产环境过程中，我公司采取了“灰度发布”的稳健策略，不改变现有生产环境的配置，仅在新建的 IPv4/IPv6 网络环境下部署双栈应用系统，通过全局负载均衡（GSLB）技术，在该应用系统的域名节点池中，逐步增加双栈节点的比重，最终平滑完成全部迁移。

(五) 安全和运维体系建设

我公司在 IPv4 环境下建立了完善的安全防护体系和运维监控体系，安全防护体系方面采用了纵深防御的多层安全防护架构；运维监控体系方面覆盖了互联网线路监控、互联

网站点可用性监控、服务器和应用服务可用性监控、基于日志分析的业务质量监控等。

在 IPv6 双栈改造过程中，安全防护和运维监控技术措施也需要进行相应的适配改造，以保证 IPv6 双栈网络环境具备和 IPv4 网络环境同等的安全防护级别和运维保障能力。

在安全防护方面，对于不支持 IPv6 协议栈的 WEB 应用防火墙，我公司积极联系厂商要求其进行适配改造和软件升级。在测试过程中，我公司发现某款 WEB 应用防火墙底层 Linux 系统使用的网络内核参数没有优化，默认的 IPv6 邻居表空间不足，将导致邻居表溢出，产生丢包和连接中断等异常情况。据此情况我公司推断，基于 IPv4 协议栈的网络和安全设备会对底层 IPv4 网络内核参数进行调优，但是 IPv6 协议栈的参数调整可能会被忽略。因此，我公司举一反三，对其他网络安全设备进行了仔细排查，提前消除隐患。

在运维监控方面，我公司通过多个数据中心之间相互进行端口探测，并通过策略模型关联分析技术手段进行互联网线路和互联网站点可用性监测，在 IPv6 改造过程中，我公司对所有数据中心均进行了 IPv6 双栈线路改造，从而实现了各数据中心间 IPv6 协议栈上的互联网线路监测，IPv4 和 IPv6 互联网线路具备同等的可用性监测、故障预警和冗余切换能力。

二、总结思考

我公司互联网应用系统众多，系统类型庞杂，能平稳顺利、高质量完成全部面向公众互联网应用系统的 IPv6 改造，主要是得益于以下几方面：

(一) 自上而下，多部门协作

我公司深刻领会推进 IPv6 部署工作的战略要义，于 2019 年即成立了由公司总裁任组长，首席信息官任副组长，信息技术中心、网络金融部技术骨干为组员的 IPv6 专项工作领导组，充分保障人力及资金，统筹推进 IPv6 部署工作。

(二) 综合评估，方案科学

我公司在选择 IPv6 改造方案过程中，向厂商、服务商、运营商和行业头部单位进行调研交流，汲取宝贵经验；内部技术骨干团队积极学习，测试论证。通过详尽的前期调研、方案对比、综合评估，最终选取了符合我公司实际情况，且改造最彻底的双栈技术方案。通过从易到难的科学改造步骤，不断总结经验教训，持续完善技术方案，最终完成全部目标。

(三) 灰度推广，严控风险

我公司在 IPv6 改造过程中，始终遵循“保障系统安全稳定运行”的原则，为规避对于现有生产系统和网络环境的影响，我公司规划建设了独立的 IPv6 双栈区域，按照改造完一个、测试验证一个、迁移一个的策略，陆续将系统部署至 IPv6 双栈区域，通过此方式可隔离改造过程中可能出现的风险传导。同时，在系统迁移过程中，我公司通过全局负载均衡

（GSLB）技术对系统进行“灰度发布”，更进一步缩小了业务影响范围。通过网络架构设计和技术手段，我公司实现了IPv6改造过程风险可控，平滑推进。

IPv6规模化部署是一项持续性工作，后续我公司将在工作中不断总结经验，学习借鉴行业优秀方案，统筹规划，合理设计，持续提升部署工作的广度和深度。

财信证券股份有限公司

2022年9月