国海证券官网 IPv6 改造实施经验

（国海证券供稿 广西局指导）

一、IPv6 改造背景

IPv6 规模部署是中共中央、国务院关于建设网络强国的战略部署，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，也是互联网技术产业生态的一次全面升级，深刻影响着网络信息技术、产业、应用的创新和变革。2019 年 11 月，欧洲网络信息中心（RIPE NCC）表示，已从可用池中的最后剩余地址进行了最终的/22 IPv4 分配，IPv4 地址已经被用完。亚太互联网信息中心（APNIC）也表示能分配的 IPv4 地址已经非常稀少，只能满足部分客户少量地址申请需求。基于 IPv4 的标识体系已经无法满足未来互联网发展的需要。根据国际互联网协会（ISOC）的最新统计[1]，IPv6 的部署率，美国是 48%，加拿大是 34%，德国是 48%，法国是 46%，英国是 34%。作为发展中国家的印度，IPv6 的部署率更是达到 66%，超过了美国。从 ISOC 的数据可以看出，国际上不管是发达国家还是发展中国家都在积极部署 IPv6。作为互联网发展大国，我国 IPv6 规模应用部署势在必行。虽然我国目前获得的 IPv6 地址数量已经达到全球第一，但是如何把这些拥有众多地址的资源优势，转化为应用部署优势还需互联网相关从业者共同努力。人民银行、银保监会、证监会

联合编制并正式印发《金融行业贯彻推进互联网协议第六版（IPv6）规模部署行动的实施意见》（银发〔2018〕343号）（以下简称《实施意见》）。系统谋划了金融行业IPv6改造方案，提出了金融行业IPv6规模部署的规划和推进路径，强调了以“保障系统安全稳定运行”为前提，采取“应用系统改造与软硬件基础设施升级相结合、递进式推进与增量式推进相结合”的工作原则，明确了三阶段递进式工作任务表，增强了对金融行业IPv6规模部署工作的指导。

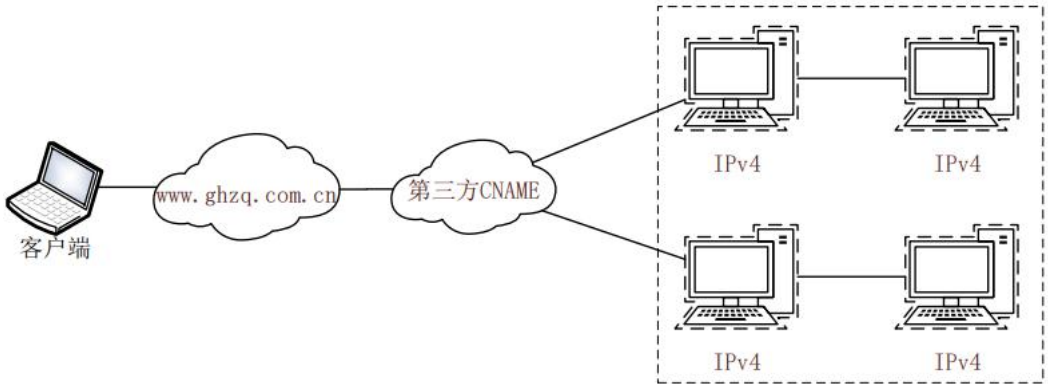
为贯彻落实人民银行、银保监会、证监会要求，我司组织相关技术部门于2019年开始研究官网IPv6改造技术方案，并在IPv4/IPv6双栈协议建设演进实践过程中积累宝贵的理论知识和实战经验。

二、系统双栈技术设计目标

双栈技术[2]是指网络设备、系统、安全及应用系统等平台在不改变现有物理部署的前提下直接启用IPv6协议，同时运行IPv4和IPv6，实现分别与IPv4或IPv6节点间的通讯。我司官网IPv4/IPv6双栈技术改造目标是既能确保纯IPv4网络的客户端能正常访问官网，也能确保纯IPv6的客户端正常访问官网，即我司官网可同时支持IPv4和IPv6两种协议访问，满足监管各项指标要求。为此，我司尝试了多种方案进行实践研究。

三、系统改造实践方案

1.单中心纯IPv4架构不变，借助第三方产品服务。



建设方案：官网原有系统纯 IPv4 部署架构（移动中心双服务）和网络安全防护策略不变，借助第三方平台产品服务（例如：网宿的 WSA、APPA）以实现当用户访问官网时，官网域名先经 DNS 解析至第三方平台提供的 CNAME，再由第三方平台将 IPv6 转换成 IPv4 之后再转发至我司原有的 IPv4 服务器，达到支持 IPv4/IPv6 双栈协议目标。

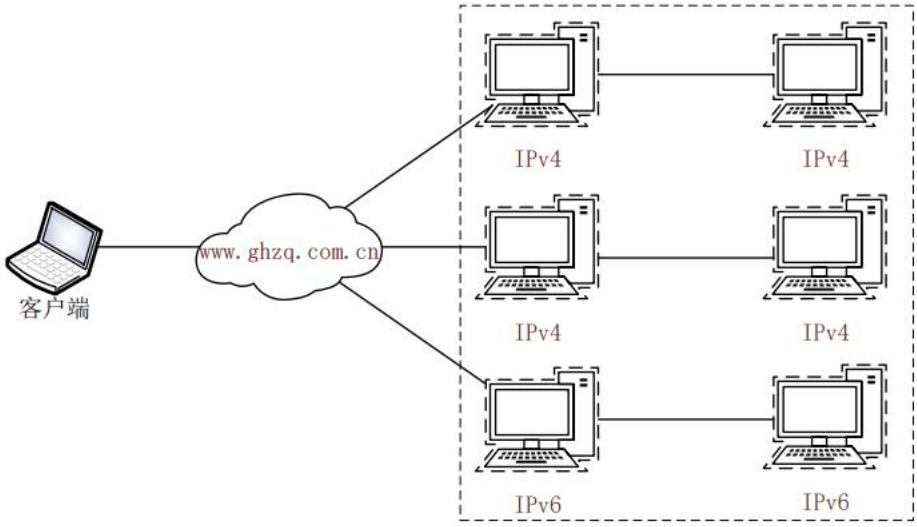
优点：原有系统纯 IPv4 部署架构和网络安全策略基本不用改造，无需额外采购相关设备搭建 IPv6 环境，无需重新部署系统或者新部署系统服务，即可满足监管要求，改造周期短，见效快。

缺点：客户访问官网时，域名经 DNS 先解析至第三方平台，再由第三方平台进行判断和转换，中间多一个转发环节，前端响应相对慢，影响客户体验；若涉及交易、用户敏感信息，则存在信息泄露等安全隐患；且第三方平台每年收费标准很昂贵。

该方案为我司最早与第三方平台共同探讨的技术方案，并在测试环境实践中论证可行，但综合各方面因素，该方案

因维护成本较高且不符合公司长远规划而被放弃。

2.单中心 IPv4/IPv6 混合架构。

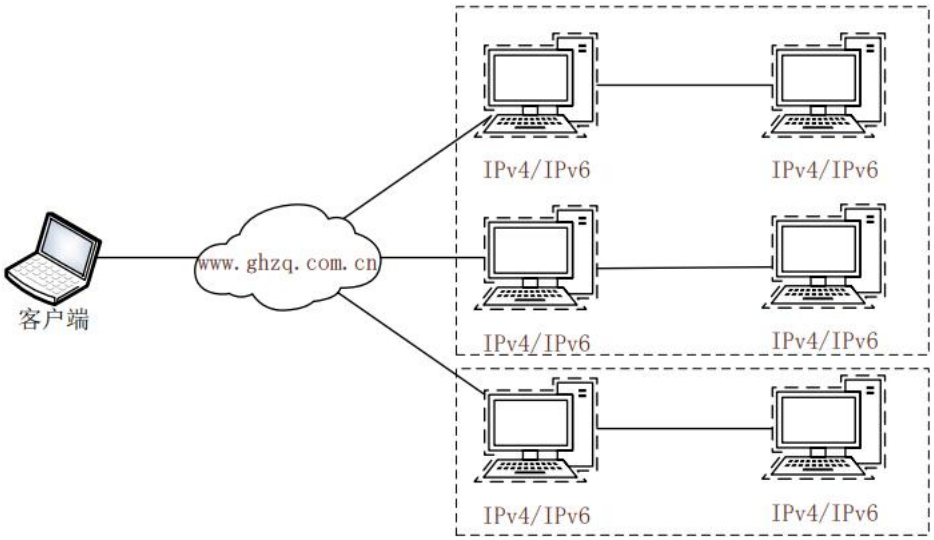


建设方案：官网原有系统纯 IPv4 部署结构（移动中心双服务）和网络安全防护策略不变，采购最基本的 IPv6 设备和网络资源在原移动中心新部署一组官网纯 IPv6 环境服务，采用与 IPv4 同等的网络安全防护策略；同时将新增的 IPv6 互联网 IP 与官网域名绑定,最终实现以 IPv4 为主、IPv6 为辅的双栈协议；当用户访问官网，官网域名经 DNS 解析时自动判断用户端是 IPv4 还是 IPv6 网络，从而转发至对应的服务器。

优点：原有系统纯 IPv4 部署架构和网络安全防护策略不用改造，新增的 IPv6 服务与原 IPv4 服务相互独立，互不影响，确保系统平稳过渡；所投入的人力物力相对较小，改造周期相对较短。

缺点：需新采购 IPv6 相关设备和网络资源搭建基础的 IPv6 环境，新部署一组官网服务；纯 IPv4 网络用户无法访

问官网 IPv6 服务，纯 IPv6 网络用户无法访问官网 IPv4 服务；一旦 IPv6 那组服务宕机，纯 IPv6 网络用户无法正常访问官网；当 IPv6 用户访问并发量大时，系统负载均衡可能出现瓶颈。



建设方案：采用全新服务器（同时支持 IPv4 和 IPv6），在移动中心新搭建两组官网服务，在阿里 ecs 私有云平台搭建一组官网服务，前端应用通过 nginx、后端应用通过 springcloud 将三组官网服务进行集群，并将官网域名与新部署的三组服务互联网 IP（IPv4 和 IPv6）进行绑定。

优点：双中心互备可以提高系统容灾备灾能力，通过集群可以提高系统吞吐率，实现负载均衡；每组服务同时支持 IPv4 和 IPv6 两种协议，可确保不管客户端是 IPv4 还是 IPv6 网络，均可以正常访问官网，且任何一中心任一组服务器宕机，均不影响客户体验。

缺点：需采购 IPv6 相关基础设备和网络资源搭建 IPv6 环境，重新规划好网络安全防护策略，人力物力投入大，改造周期长。

四、系统改造方案落地情况

为了确保系统平稳过渡，以最小的人力物力投入代价和最快的速度达到监管要求，我司第一阶段决定采用“单中心 IPv4/IPv6 混合架构”改造方案，于 2019 年底完成官网改造部署，并安排了专业测试人员对改造后的官网 IPv6 网络环境进行全方位的测试验证，测试的内容包含 IPv6 兼容性、健壮性和安全性等多个方面，验证的环节从客户端、服务器端、DNS 域名解析、访问响应时延到是否存在天窗等；在终端兼容性方面，包括对不同终端设备（电脑、平板、手机等）、不同操作系统（WIN10、WIN8、WIN7、MACOS、IOS、Android 等）、不同浏览器（Chrome、IE）的访问支持。借助国家金融行业 IPv6 发展监测平台对官网改造效果进行检测，逐条比对监管的要求，在为期连续 15 天的 IPv6 网络质量和稳定性测试中，测试覆盖中国电信、中国联通和中国移动三家运营商网络，测试期间 IPv4 和 IPv6 网络响应率 100%，响应时延均在 75 毫秒之内，系统可用性和稳定性均达到了预期设计要求。

为了提高系统的健壮性、容灾备灾能力、系统吞吐率以及响应速率，向客户提供更好的服务体验，我司官网 IPv6 改造第二阶段采用“双中心 IPv4/IPv6 一体化架构”改造方案。2022 年我司在多部门协同配合下，搭建好了双中心（移

动中心和阿里 ecs 私有云）IPv6 平台，并为官网新架构部署分配全新的高性能服务器和网络资源。目前系统已按新架构部署完成，系统安全防护等级均达到监管要求标准，系统各项指标都有了质的提高。

五、系统改造后面临的风险与问题

1.应用及运维风险

IPv6 线路风险：IPv6 目前访达率及稳定性尚不及原来的 IPv4 网络,运营商的线路与环境都在逐步改善中，对应用稳定要求较高的系统，需要及时观察监控，做好应急准备措施。

容量风险：IPv6 为新接入网段，随着应用的迁移，及客户访问环境的变化，容量可能需要较大的弹性，需要根据业务及网络的变化，做好评估与升级准备。

2.系统改造后预留问题

我司官网前端页面还存在其他网站应用的外链，这些外链涉及到不同的系统，有来自公司内部的，也有来自外部关联单位的。如果外链的网站不支持 IPv6 访问，就会导致客户端采用纯 IPv6 网络（IPv6 Only 客户端）去访问页面中这些 IPv4 的外链内容时，出现部分页面无法显示的“天窗”问题。涉及我司内部的系统，可以后续改造或者通过 nginx 反向代理或者程序本身代码调整的方式来实现。但涉及外部公司外链的情况，在纯 IPv6 的环境下还不能正常使用，这还有赖于 IPv6 整体环境的改善。

六、同行经验交流分享

IPv6 升级改造工作是一项复杂的系统工程,不仅仅是 IP 地址的变更，IPv6 相对 IPv4 虽有很多共通之处，但在技术细节、应用、运维方面又具备自身的独立性。虽然 IPv6 技术本身也很成熟,但由于推广和实际实施、运维经验的缺乏,即使专业的网络运维人员，没有经过系统的学习、培训及实践，也很难对 IPv6 有较为深入的理解。所以在 IPv6 网络与安全改造的方案制定和部署过程中，多与金融行业的同行进行技术交流和经验分享，从公司自身的实际情况出发，逐步完善 IPv6 网络与安全改造的方案，并就实施过程中出现的疑难问题进行技术探讨，及时调整实施方案，最终完整解决相关问题，并进行经验总结和分享。我司将在满足《实施意见》的前提下,坚持稳中求进的工作总基调,加强人员培训,充分积累 IPv6 改造和运维经验,积极稳步推进 IPv6 改造相关工作，逐步实现我司所有互联网业务对互联网提供 IPv6 连接访问，为我国金融行业向下一代互联网迈进贡献一份力量。

参考文献

[1] https://m.thepaper.cn/baijiahao_14105513

[2] https://blog.51cto.com/u_9691128/4569215