中金财富证券 IPv6 建设分享

（中金财富证券供稿 深圳局指导）

一、IPv6 建设背景和意义

IPv6（互联网协议第 6 版），是互联网技术的一次全面升级，是全球公认的下一代互联网商业应用解决方案，为下一代互联网的应用创新扩展广阔的空间。大力部署基于 IPv6 的下一代互联网，是中国建设网络强国、参与全球互联网技术发展、提升信息技术自主创新能力、提高产业高端发展水平的重要抓手和契机。

1. 国家战略与政策

党中央、国务院提出建设网络强国战略部署，国家有关机构也加快推进基于互联网协议第六版（IPv6）的下一代互联网规模部署，并下发一系列政策文件指导相关工作。中共中央办公厅、国务院办公厅 2017 年 11 月 26 日印发了《推进互联网协议第六版（IPv6）规模部署行动计划》（厅字【2017】47 号文）；2018 年 3 月，国资委综合局下发《关于做好互联网协议第六版（IPv6）部署应用有关工作的通知》；2018 年 12 月 24 日，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》等，为各行业 IPv6 建设提出了指导和规划。

2.IPv6 建设意义

国家安全方面,IPv6 规模部署和应用是互联网演进升级的必然趋势，能有效促进提升我国在下一代互联网领域的国际竞争力，提升我国在互联网领域的技术话语权，是我国由 IPv4 跟随到 IPv6 领跑的网络强国战略。经济方面，IPv6 提供几乎无限量的网络地址，维物联网产业发展提供基础空间。社会方面，IPv6 有效提升联网设备的端对端 IP 解析，及时响应服务，让互联网变得更快、社会生产效率更高。网络安全方面，IPv6 网络上所有联网的设备都将有单独的地址，且由于独特的报头结构，很多安全问题和信息溯源问题都将迎刃而解。

3.证券行业部署 IPv6 价值

2021 年，沪深两市连续 49 个交易日成交额破万亿，创下中国沪深两市成交额连续万亿以上历史最长记录。国内资本市场快速发展，资本流动性和交易量的增大，程序化交易、算法交易、高频交易的大量使用，造成追求更低交易时延的“竞赛”不断升级。IPv6 具有更快的传输速度，更简短的报文结构、更小路由表更小，极大的提高了转发效率，提供更低的传输时延，更加适应当前投资者对交易速度的追求。

安全是金融机构的生命线，中国证券市场对信息与通信技术应用广泛，随着用户网上交易、网络社交、网上直播等网络活动的不断增多，证券行业面临比较大的安全挑战，也对券商网络安全保障提出了更高要求。IPv6 相比 IPv4 在安全方面具有天然优势。IPv4 协议没有强制使用互联网安全协议（IPSec)加密数据，存在明文传输泄漏数据隐患，而 IPv6

将 IPSec 集成到了协议内部,为 IPv6 提供了一个身份认证、数据完整性和机密性的安全机制，在网络层认证和加密数据，为用户提供端到端的数据安全，保证数据不被劫持，使 IPv6 真正实现了网络层安全，为投资者提供了更安全的网络交易环境。

对于金融行业和我们证券行业来说，积极开展 IPv6 建设，融入国家网络强国战略，拥抱新一代互联网技术也具有极大的现实意义。首先是能够抢占下一代互联网用户的先机，根据中共中央办公厅、国务院办公厅联合印发的《推进互联网协议第六版(IPv6)规模部署行动计划》规划，未来 5 到 10 年我国将建成全球最大规模的 IPv6 商业应用网络，实现下一代互联网在经济社会各领域深度融合应用，成为全球下一代互联网发展的重要主导力量，届时我们的金融客户大多数将接入 IPv6 网络，对 IPv6 的应用需求将会激增。其次是能够为业务办理带来新的便利和效率提高,IPv6 为万物互联打下坚实基础，也为万物应用，包括万物办理金融业务带来新的方向和可能。再次是能够为业务模式和业务形态带来新的变化，也将带来新的应用场景。比如可以预见的未来几年，由于 IPv6 更高的安全性和万物互联的特性，将会推动区块链的加速应用落地，数字货币将会加快应用，届时金融行业与此相关的业务场景将会雨后春笋般出现。最后是 IPv6 将会对金融科技基础建设带来新的变化，真正意义上的多地、多活数据中心将会成为可能，为金融行业信息安全和业务连续性打下坚实的技术基础。

二、公司 IPv6 工作开展情况

我司为贯彻落实《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〉的实施意见》，在 2019 年底按人民银行要求，及时完成了门户网站和域名解析系统的 IPv6 部署工作，并通过人民银行的检测；2020 年底完成了对公众提供服务的互联网应用系统全面支持 IPv6 接入。

2021 年起，持续推进 IPv6 规模部署，逐步构建安全高效的下一代互联网。

三、公司 IPv6 建设思路

我司在 IPv6 建设规划和落地实施过程中，主要遵循了全面评估、同等安全防护标准、先易后难、先验证再推广的思路开展。

1、全面评估

在 IPv6 建设规划阶段，我们评估了业务处理全路径上的所有传输节点和处理节点是否已经或者可以支持 IPv6 传输和处理，是否能够正确传递、接收、处理和反馈 IPv6 数据包，对于无法传输和处理的节点，就是我们的改造建设方向和目标。

2、同等安全防护标准

IPv6 建设的出发点之一是安全可控，IPv6 的建设，不能以降低安全防护标准为代价。因此，在建设规划阶段，我们全面评估了安全防护能力，特别是互联网边界安全防护能

力，能够提供与 IPv4 同等的的防护标准。在建设实施过程中，我司也积极与安全服务商、安全防护产品厂商等保持沟通协作，及时对 IPv6 上线系统开展安全检测，一方面验证系统的 IPv6 免疫能力，另一方面验证当前的安全产品和措施在 IPv6 环境下的实际防护能力。

3、先易后难

我司在全面评估并做好充分准备的情况下，首先选取了较容易实施 IPv6 建设的 web 应用系统、特别是仅提供浏览器访问的、全静态页面的网站系统开展建设，通过 NAT64 地址转换的方式，将内网 IPv4 服务器地址转换成互联网 IPv6 地址,并通过在 HTTP 请求包头插入头字段带入客户端的真实 IPv6 地址来识别真实客户端。在积累了相关建设经验后，再推广实施网络层全栈 IPv6 建设和业务层应用系统 IPv6 改造建设，最终完成了网上交易系统、中金财富 APP 的 IPv6 建设。

4、先验证再推广

在 IPv6 落地建设过程中，对于 WEB 类应用，在完成某个系统建设后，我司充分发动 IT 技术人员、各服务商、合作供应商、安全厂商等，小范围使用 IPv6 环境进行 WEB 页面的遍历验证，验证无误后再进行全网发布。对于 PC 客户端和 APP，则是使用独立的 IPv6 客户端程序首先进行小规模的灰度发布和验证，持续迭代，逐步全面上线。

四、公司 IPv6 案例分享

我司的 IPv6 建设，根据不同的系统类型和不同的监管、

安全要求，采用了三种不同的实现技术：

1、对于 WEB 类应用，通过 NAT64 地址转换的方式，将内网 IPv4 服务器地址转换成互联网 IPv6 地址，并通过在 HTTP 请求包头插入头字段带入客户端的真实 IPv6 地址来识别真实客户端。

2、对于行情、资讯类 C/S、APP 应用，由于仅提供信息展示，不需要记录客户端真实 IP 地址，通过 NAT64 地址转换的方式，将内网 IPv4 服务器地址转换成互联网 IPv6 地址的方式，确保应用在 IPv6 环境下可正常使用。

3、对于交易委托类 C/S、APP 应用，出于满足监管记录客户端真实 IP 地址的要求，采用网络层全栈 IPv6 建设和业务层应用系统 IPv6 改造的方式，使用独立的 IPv6 客户端程序提供 IPv6 环境的接入。

（一）门户网站

门户网站的 IPv6 建设，是较为典型的 NAT64 转化方式，通过将内网 IPv4 服务器地址转换成互联网 IPv6 地址，并在 HTTP 请求包头插入头字段带入客户端的真实 IPv6 地址来识别真实客户端。

1、门户网站 IPv6 部署方案

经前期调研和评估，公司门户网站 IPv4 接入站点运营商线路可提供 IPv6 接入，且互联网边界防护设备、提供互联网地址转换的负载均衡设备等均支持 IPv6，IPv6 部署后设备不存在性能瓶颈。因此，公司选择了在现有接入站点进行部署的方案：在现有多家运营商接入线路上申请 IPv6 地

址，通过负载均衡设备将互联网 IPv6 地址转换为内网 IPv4 地址，并对门户网站页面内容进行梳理，对可能产生空窗问题的页面进行优化处理等。安全防护方面，与 IPv4 接入共享当前的安全防护措施，具体包括：DDoS 攻击防护、下一代防火墙、WEB 应用防火墙等。

2、门户网站 IPv6 实施情况

公司门户网站 IPv6 的具体实施，大体经历了线路和地址资源申请、门户网站梳理和优化、DNS 支持、门户网站 IPv6 上线等步骤。

1、线路和地址资源申请方面，门户网站接入站点包含电信和联通线路，均可提供 IPv6 地址资源。公司于 11 月 11 日完成两家运营商 IPv6 地址资源的申请，并同步向行政主管部门提交备案。

2、门户网站梳理和优化方面，对公司门户网站上页面内容以及第三方链接和内容进行梳理，对于直接引用的第三方内容进行优化处理，避免产生空窗问题。

3、DNS 支持方面，使用了第三方域名解析系统——阿里云 DNS 进行门户网站的 IPv6 域名解析。

4、上线实施方面，在服务器负载均衡设备上配置 IPv6 线路（接口、网关、路由等），以门户网站的 IPv6 接入站点，实现 IPv6 接入、互联网 IPv6 和内网 IPv4 的地址转换。安全防护方面，与 IPv4 接入共享当前的安全防护措施，具体包括：DDoS 攻击防护、下一代防火墙、WEB 应用防火墙等。

IPv6 访问终结于服务器负载均衡设备，负载均衡设备进行地址转换，内部保留 IPv4 环境。

（二）网上交易系统

网上交易系统由于采用客户端方式访问，以及行业监管特点，需要记录详细的客户 IP 地址，因此采用了全栈 IPv6 的建设方式。

1、网络节点的全栈 IPv6建设

经过对网上交易系统业务路径的及合规要求的评估，详细的客户 IP 地址至少需要在网上交易委托接口中间件上进行记录，因此在业务路径中包含互联网接入端和委托接口中间件在内的网络传输和处理的各个网络节点上，启用了 IPv6 网络传输模式。

2、IPv6网络对应用系统带来的挑战

对比现行 IPv4网络，IPv6为网上交易应用系统带来了终端网络协议栈自适应切换、算法性能和监管留痕等方面的挑战：

（1）终端改造

Windows 系统根据是否安装有 IPv6 协议栈来判定返是否返回IPv6地址，即存在 IPv6 配置时候，访问 DNS 会优先返回 IPv6 地址，而 Windows 系统默认即安装有 IPv6 协议栈，为满足客户可以根据自身需要手动选择是否使用 IPv6网络连接系统后台，客户端在同时支持 IPv4和 IPv6协议的前提下，需进一步改造支持自动（根据客户网络情形）和手动（客户自主选择）切换 IPv6协议。

（2）算法调整

IPv4 地址宽度为 4 字节，IPv6 地址宽度为 16 字节，为服务器地址策略算法（包括 IP 黑名单白名单、冻结机制等反外挂策略）带来更大的内存开销，需要进一步做针对性优化以保证系统性能。

（3）留痕接口适配

监管要求的留痕字段(交易客户端 IP 信息)需要更宽的字段宽度进行存储，进而影响交易委托、终端信息留痕、反外挂信息上报等接口范式，需要根据实际情况进行适配调整，同时满足 IPv4和 IPv6两种网络协议格式。

3、网上交易系统 IPv6实施

得益于前期网络安全团队的充分评估与提前准备，网上交易系统从客户端到委托中间件的各个网络节点均具支持IPv6协议传输，为应用系统的 IPv6建设奠定了坚实的基础。本次网上交易系统 IPv6实施主要分为需求梳理与方案确认、IPv6资源申请、测试部署、试运行与上线等几个阶段。

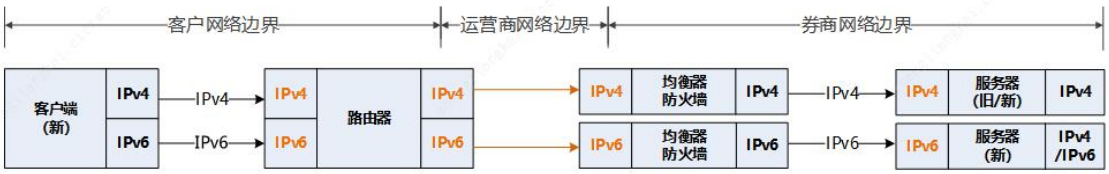
（1）需求梳理与方案确认

建设初期，根据我司梳理的系统改造需求和建设目标，网上交易系统开发商提供了双栈和转译两种建设方案，其中双栈方案是系统后台同时支持 IPv4和 IPv6两种协议，转译方案则是不改变原有后台环境,在接入层部署 IPv6转换设备，向内网开启 ISATAP 隧道转换功能将流量转换为 IPv4。两种方案优缺点对比如下：

方案名称	简介	优点	缺点

双栈方案	后台环境改造同时支持 IPv4 和 IPv6两种协议	全栈支持 IPv6 协议，可完整记录客户端地址	改动点多，建设周期长
转译方案	增加转换设备将 IPv6转移为 IPv4	改造简单，建设周期短	IPv6地址传输完整性无法保证，存在监管风险

经过分析调研，我们最终选用了双栈方案，该方案虽然建设难度相对较大，但是可实现系统内全栈 IPv6支持，在满足监管要求的同时更符合国家推进 IPv6规模部署的大方针。双栈方案改造目标如下：



（1）IPv6资源申请

由于公司门户网站先于网上交易系统进行改造，相关 IPv6资源均已申请就绪，系统涉及的各个网络节点均已实现对 IPv6协议的支持。

（2）测试部署

根据我司选定的建设方案，厂商针对终端双栈支持、监管留痕、反外挂算法优化等方面为我司进行了定制化开发，并配合我司进行了细致全面的功能测试与压力测试，部分测试结果如下：

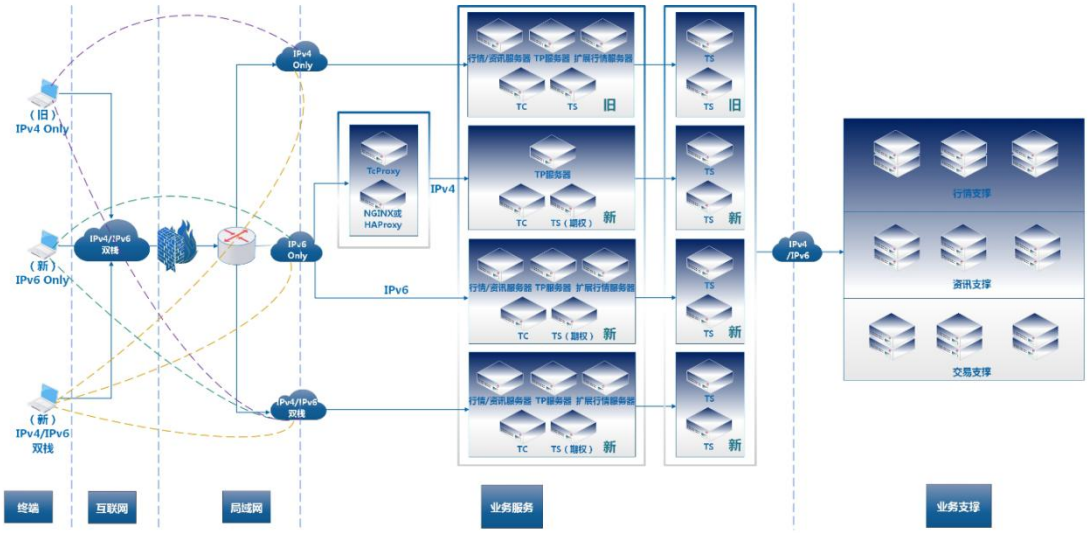
	子系统	测试项	测试结论
客户端	网上交易系统	客户端双栈、IPv6 代理、	符合预期

	（普通和信用）	线路选择、硬件信息留痕处理、信息回显。	
	网上交易系统（期权）	客户端双栈、IPv6 代理、线路选择、硬件信息留痕处理、信息回显、IPv6 行情连接。	符合预期
	网上行情资讯系统	客户端双栈、IPv6 代理、线路选择。	符合预期
后台	网上交易系统（普通和信用）	后端双栈、硬件信息留痕处理、信息回显、IP 黑白名单、IP 冻结、SC 业务切换。	符合预期
	网上交易系统（期权）	后端双栈、硬件信息留痕处理、信息回显、IP 黑白名单、IP 冻结。	符合预期
	网上行情资讯系统(沪深)	后端双栈、行情区域判定。	符合预期
	网上行情资讯系统(扩展)	后端双栈。	符合预期
	交易代理	后端双栈、IP 与端口信息透传。	符合预期
	反外挂系统	IPv6 信息上报	符合预期

		反外挂地址封锁和告警	

（1）试运行与上线

完成测试验证之后，我司在生产环境进行了部署升级，同时灰度上线了支持IPv6协议的客户端版本进行小范围推广使用。经过一段时间的平稳运行之后，正式上线了网上交易IPv6版本，生产环境部署拓扑如下图：



（三）中金财富APP

中金财富网上交易系统作为手机端交易的重要入口，承载着公司移动互联网的绝大部分流量。IPv6的改造需求对中金财富APP的稳定性、可靠性都带来了巨大的挑战。项目为了应对改造中可能产生的问题及异常场景，设计了一套灰度上线，可控发布，随时回滚的方案，以应对项目的复杂场景。

1、系统设计准则

该系统方案制定了几个基本准则：

（1）支持IPv4/IPv6双栈模式

对后台统一外壳服务程序，改造支持IPv4/IPv6双栈模式。可以在IPV6环境或IPV4环境，或IPV6加IPV4混合环境的支持。

（2）最小化服务端改造原则

使用统一外壳程序（dbmiddleware.exe)对外提供服务，所以只需要对其进行IPV6的改造，所有业务组件就都能支持IPV6环境下的调用。新版Dbmiddleware同时支持IPV4和IPV6请求处理，对券商来说，只需要更新此外壳即可。不用担心对现有业务产生影响。

（3）改造中避免“天窗”问题

互联网应用的页面内有其他网站（域名）的外链，如果外链的网站不支持IPv6访问，就会导致客户端采用纯IPv6环境（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。对原系统中涉及不兼容的IPV4外链，中焯进行检测提示第3方进行相应升级或用客户端采用中焯内部H5框架页面进行转换，后台用协议转换方式进行“天窗”问题的解决。

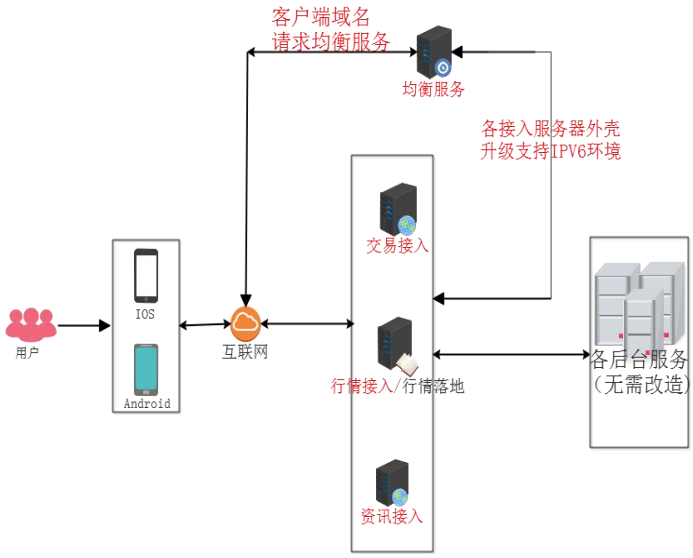
（4）无感知用户体验原则

使用统一均衡程序LoadBalanceInOne.dll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。

2、中金财富 APPIPv6系统拓扑



注：红色部分为改造点

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（IPV6地址+IPV4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（IPV4地址+IPV6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。

3、中金财富 APP 服务端改造方案

（1）统一接入服务器改造要点

服务器通讯模块支持 IPv4/IPv6双栈模式；

服务器之间的路由协议改造支持 IPv4/IPv6双栈模式；

服务器留痕支持 IPv4/IPv6双栈模式；

行情接入、交易接入、资讯接入、中间件等后台服务器对原有组件的100%支持。并且针对32位，64位服务器同时改造支持 IPV6。

（2）均衡组件改造要点

新版均衡组件 LoadBalanceInOne.dll 支持 IPv4/IPv6双栈模式，同时建议客户端配置的均衡服务器地址 采用域名方式,实现对 IPv4/IPv6双栈的智能 DNS 解析，同时支持域名发布 A 记录和 AAAA 记录。

新版均衡支持同时多个均衡地址进行连接,兼容新老客户端的均衡请求，保证支持 IPV6客户端版本升级过程中对老版本客户端的均衡支持。

增加客户端 IPV6或 IPV4属性返回，便于客户端进行。

增加 ActionVersion 参数设别，并根据不同 ActionVersion 值进行对应处理，完美同时支持客户端的各种版本。

4、中金财富 APP 客户端改造方案

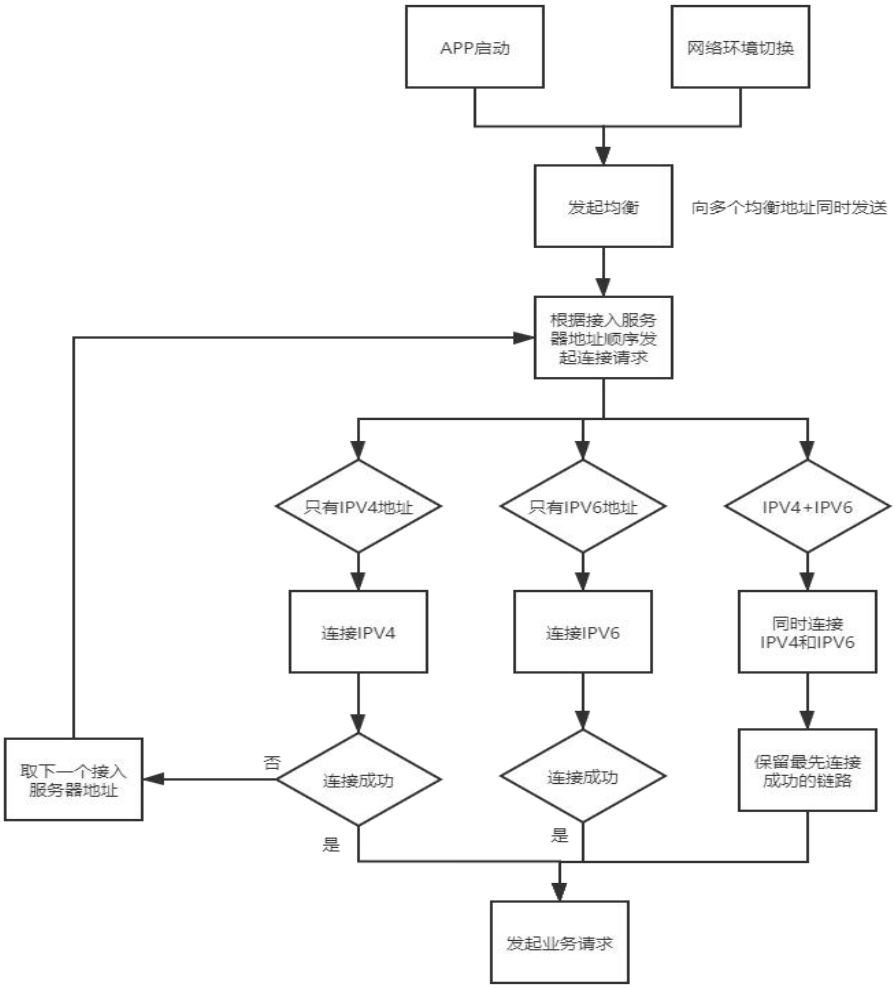
客户端在 APP 启动或者在网络切换时，发起均衡请求；并且对多个均衡同时请求。

在收到任何一个均衡的优先应答后，进行均衡数据处理，记录应答的各接入服务器列表地址。其他均衡的应答不做处理。

根据均衡服务器返回接入服务器地址列表，顺序连接对应的 IP 地址列表。

如果接入服务器只有IPV6则联IPV6,只有IPV4则连接IPV4，如果接入服务器同时支持IPV4和IPV6，则客户端同时发起IPV4和IPV6的连接,哪个链路先连接上则保留那个。

建立连接的通讯处理逻辑流程如下：



5、IPv6/IPv4双栈兼容测试

为了保证系统的平稳实施，专门设计了双栈兼容测试环节，以确保服务平稳过渡。

五、IPv6 工作开展经验

IPv6的部署实施过程中，我司总结了以下的经验：

一是需要提前评估全链条上的设备是否支持IPv6，对于不支持的设备需进行升级替换。

二是需对全链条上的设备性能进行评估，确保IPv6规模部署后设备不产生性能瓶颈。

三是提前对应用系统进行梳理，确保通过IPv6访问应用系统不产生空窗或不可访问等问题。

四是对于WEB类应用，使用当前IPv4接入站点资源进行IPv6规模部署，共用互联网线路、边界防护设备和设施等资源，通过互联网上IPv6地址NAT转换为内网IPv4地址，内部保留IPv4环境，节约资源同时避免对内部应用系统的大规模变更。

五是对于C/S类应用目前是按照IPv4/v6双栈方式来实现IPv6接入，搭建内网、公网、应用同时满足IPv6的环境，使用当前IPv4接入站点资源进行IPv6规模部署，共用互联网线路、边界防护设备和设施等资源。

六、IPv6建设展望与建议

建设部署IPv6，不论从国家战略布局、行业生产力发展、安全保障等角度，都有具有深远而实用的意义，且具备一定的政策环境、产业链条、实践积累。中金财富扎实推进IPv6网络建设，为业务和管理数字化水平高速发展奠定基石，取得了良好的推广和应用成效。

当然这项技术的发展仍在持续进步和演化，IPv6规模部署和应用也存在亟待解决的一些问题：一是主动改造的意愿不强。IPv6改造涉及终端、传输路径等方面的软硬件升级，

对技术水平和经济成本要求较高，短期内不能产生明显收益；二是应用支撑能力不足，IPv6流量尚未形成一定规模，IPv6应用不足的短板较为突出。针对此，提出一下几点建议，供行业同仁参考：

1、对于后续的IPv6规模部署，目前主要存在C/S类应用需要继续改造，需要行业内开发商进行改造支持，建议行业相关部门牵头组织和主要开发商进行商谈，降低行业整体改造成本，快速达成目标。

2、IPV6具备更高效的路由和数据包处理，建议行业相关部门引导行业参与者新增应用优先采用IPV6技术进行开发，从而利用已有的IPV6基础设施资源，提升行业客户体验。

期待未来IPv6技术取得更大突破，上下游形成更密切良好的协同规则和秩序，取得更广泛的应用成效，为行业数字化高速、高质量、安全发展保驾护航！

附：参考文献

1. 中共中央办公厅、国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》

2. IPv6 的机遇与挑战 《新经济导刊》李明 国务院发展研究中心 信息中心副主任

3. IPv6 的全面战争对中国互联网意味着什么？-钛媒体官方网站

4. 《5G 网络 IPv6 协议关键技术研究》《科研信息化技术与应用》2018 年 1 期 任勇毛,储华珍,周旭,范鹏飞,李灵玲