

海通证券基于 IPv6+金融广域骨干网的建设案例分享

(海通证券供稿 上海局指导)

一、背景

为贯彻落实习近平总书记关于网络强国的重要思想，全面深入推进 **IPV6** 规模部署和应用，加快促进互联网演进升级，中央网信办等三部门联合印发《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》。海通证券以建设国际一流投行为使命，积极融入国家高质量发展进程，坚定不移推进 **IPv6** 规模部署和应用，以全面推进 **IPv6** 技术创新与融合应用，开启基于 **IPv6+** 的金融广域骨干网的探索与建设。

“海通证券 **IPv6+** 金融广域骨干网”项目以“**IPv6+**”技术为驱动，加强金融基础设施建设，为公司位于张江、金桥、南方数据中心构建基于“**IPv6+**”的业界领先、标准架构、快速稳定、智能弹性的证券广域骨干网络，形成“上海+同城+异地”两地三中心网络架构，实现海通证券整体业务能力、运维能力、数据容灾备份能力的全面有效提升。再保持海通证券广域骨干网络的先进性的同时，能够快速应对未来证券业务的变化。

二、建设目标

近年来，以头部银行和大型证券公司为代表的金融机构在数字化转型进程中面临新的挑战。随着异地、同城中心数据备份、数仓等大流量业务所占比例持续增加，金融网络承载的数据类型发生了显著变化，对数据中心之间的骨干网络安全、快速、低成本传输需求持续上升，对金融专网的承载能力提出了进一步的要求。

同时，为匹配国家 IPv6+ 政策驱动，以金融科技战略规划为指引，借鉴互联网企业/头部银行设计理念，结合软件定义网络的架构转型，构建下一代 IPv6+ 核心骨干网络，达到匹配政策规划、提升业务效益、引领行业标准的目标。海通证券率先展开了 IPv6+ 网络的研究与建设，基于 SRv6 的新一代 IPv6+ 创新协议簇首先在海通证券金融骨干网验证落地，并逐渐向 DC 和园区延伸，在提升业务体验、业务能力、运维能力以及降低成本、降低风险等方面效果明显。

在政策与技术共同驱动下，本项目重点研究海通证券下一代 IPv6+ 骨干网络的建设方案和技术创新。通过广泛深入的洞察研究，归纳总结了以海通证券网络业务为代表的“IPv6+ 金融专网”的关键需求，即“骨干网络架构的整体规划”“证券业务传输的质量保障”“数据中心间大流量的负载分担”“网络智能运维以及实时监控”。在此基础上，充分结合海通证券新业务、新技术发展需求和面向未来设计

理念，项目组提出构建业界领先、智简弹性的下一代 IPv6+ 骨干网网络，需要具备以下五大能力：

1. 网络稳态基础架构，灵活扩展
 - 层次化、模块化稳态基础网络架构。
 - 骨干与 DC 解耦，与业务解耦，弹性扩容。
2. 业务融合承载，一网多用
 - 网络资源集约化，一张网络承载多业务，逻辑隔离。
 - 网络统一、技术统一、运管统一。
3. 业务智能调度，流量工程
 - 流量工程，智能算路，智能调度。
 - 负载均衡，合理利用带宽资源。
4. 业务高可靠保障，故障自愈
 - 网络设备、链路、隧道高可靠、业务端到端保护。
 - 业务随流检测，快速定界定位，路径调优故障自愈。
5. 智能高效运维管理，流量可视
 - 随流检测/主动探测链路质量，流量 SLA 可视。
 - 实时状态采集，精确监控网络状态。
 - 提供北向网络服务，提供二次开发能力。

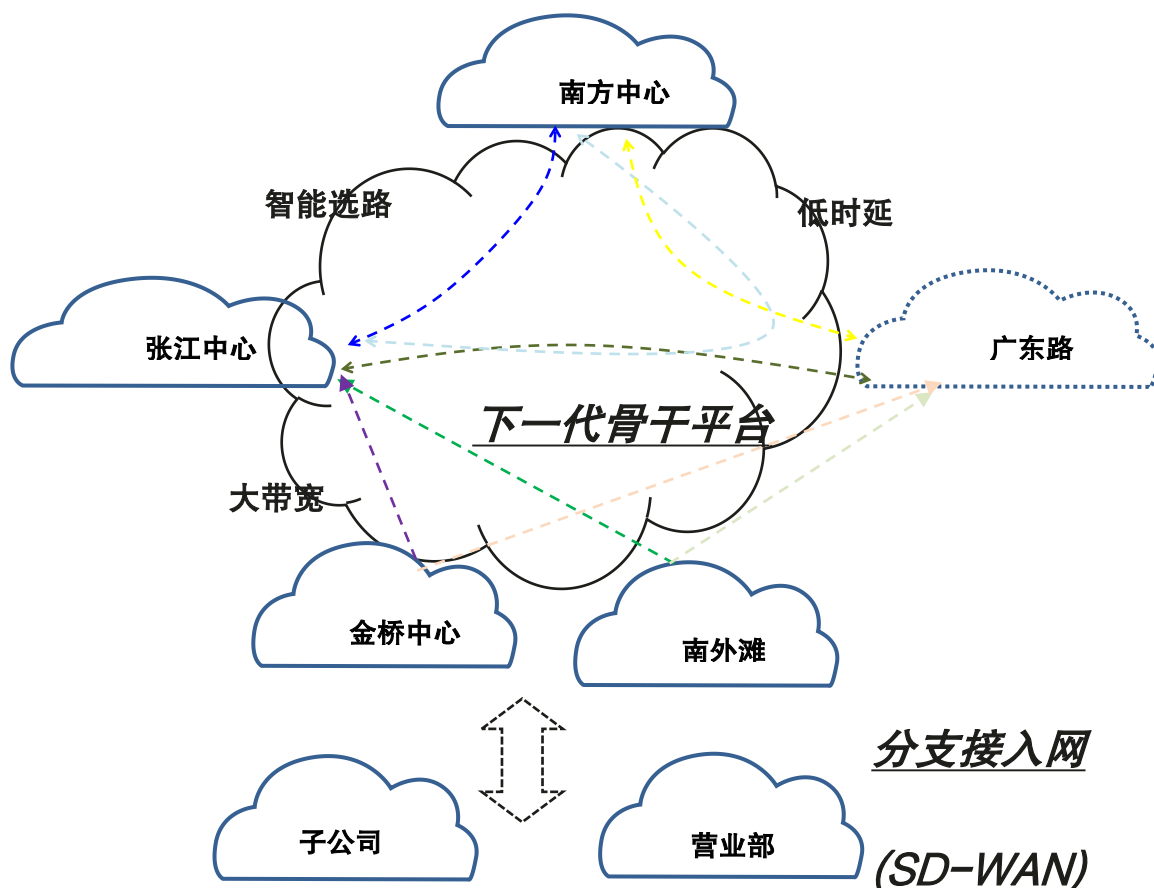
三、技术方案

（一）方案架构

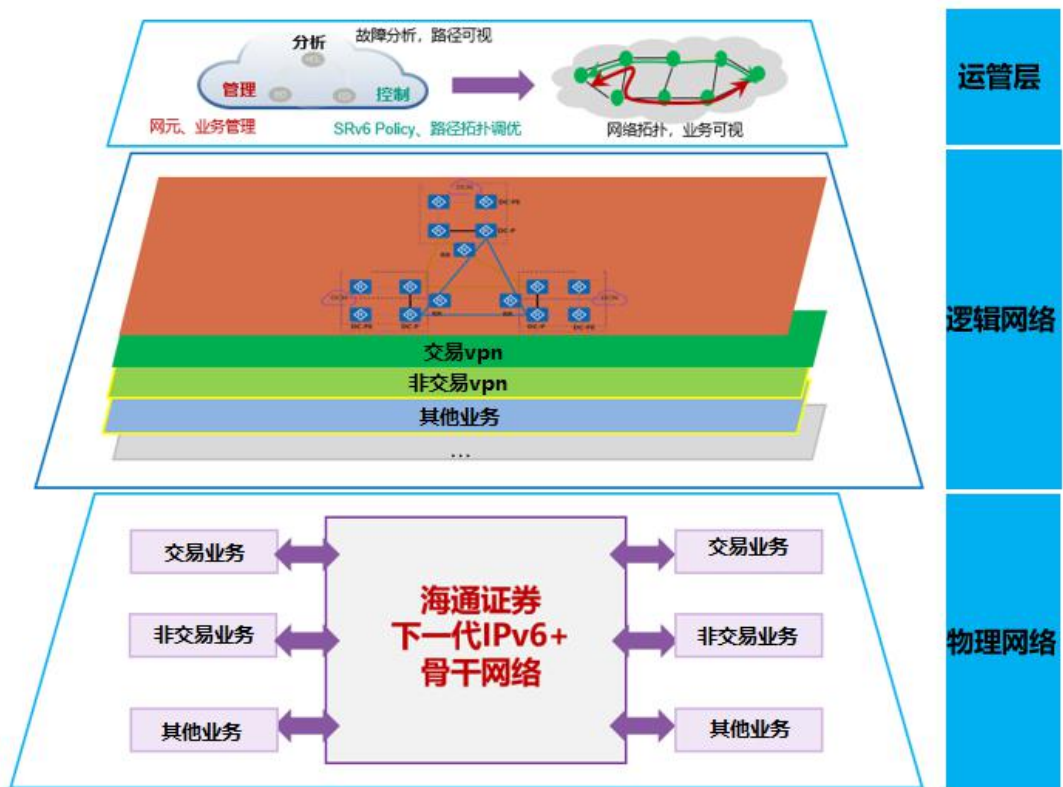
SRv6（Segment Routing IPv6），基于 IPv6 转发平面的段路由，是新一代 IP 承载协议。类似过去的 mpls vpn，

srv6 也依赖标签转发，不同的是 srv6 采用现有的 IPv6 转发技术，通过灵活的 IPv6 扩展头，实现网络可编程，同时简化了网络协议类型，具有良好的扩展性和可编程性，可满足更多新业务的多样化需求。

证券行业的发展趋势是提供线上化、数字化、智能化和个性化的金融证券服务。需要在客户价值管理、智能风控、智能投研、运营支撑等方面提升核心能力。承载核心应用和系统的数据通信网络是证券行业数字化转型、打造核心竞争力必不可少的基础。海通证券广域骨干网是整体网络的核心组成部分，负责数据中心、总部、分支机构之间的互联互通，并且支撑上层应用快速发展，通过数字化转型打造新的核心竞争力。海通证券下一代 IPv6+ 骨干网络整体架构如下图：



海通证券数据中心随着业务规模的快速增长，服务器数量相应快速增长，骨干网承载业务量也不断增长。此外，海通证券在部署私有云之后，开始逐步尝试部署公有云业务，向外输出金融服务。传统核心骨干网需要不断演进，实现两地三中心的高速可靠互联，承载多云之间不同的业务流量。海通 IPV6+ 骨干网络需要层次化设计部署，分为运管层、逻辑网络和物理网络。



1、运管层：网络管理、控制和分析

- 自动化业务发放、智能算路、智能分析、智能调度、智能运维，北向接口开放可编程。

2、逻辑网络：Overlay 敏态业务逻辑网络

- 基于 VPN 等技术构建多张逻辑网络，实现多业务融合

承载。

- **SRv6 TE Policy** 实现链路隧道动态调度，资源合理利用，安全可靠、故障自愈。

3、物理网络：**Underlay** 稳态基础物理网络

- 层次化、模块化设计，提供超宽网络能力。
- 骨干与 **DC** 解耦，灵活扩容。

海通证券下一代 **IPV6+** 广域骨干网络有以下价值体现：

- “稳” + “敏” 网络架构：基于开放架构，采用 **underlay+overlay** 二层组网，通过 **underlay** 网络保留传统网络的“稳”，通过 **overlay** 网络实现业务的“敏”，可靠灵活。
- 网络服务化：网络提供 **NAAS** 服务，应用通过 **API** 调用相应的网络服务；软件定义网络，提供网络可编程能力，提供北向二次开发能力。
- 智能调度，合理分配带宽资源，降低线路成本：链路动态调优，业务合理编排，灵活调度，端到端保证业务 **SLA** 质量，提高业务效益，降低专线成本。
- 业务/网络可视、故障定界定位，提高运维效率：业务质量随流检测，实时监控网路状态，故障定界定位，网络运维可视化、智能化，降低人工操作失误风险，大幅提高网络运维效率。
- 技术领先，打造业界标杆：满足国家 **IPv6+** 战略，满

足国家自主可控政策，行业 **SRv6** 建设样板，为行业骨干网络建设提供标准。

（二）项目方案

海通证券主要分为张江、广东路、金桥以及异地南方等数据中心，两地三中心网络架构。通过对业务的调研和洞察，海通证券骨干网络在以下方面需要改进：

- 网络架构：整体骨干网络架构需要统一规划，目前主要是基于设备按需建设。
- 网络技术方案：部分场景下（如行情、资讯、大数据等）流量达到链路带宽峰值；部分业务未做负载均衡，链路承载业务不均。
- 网络自动化和服务化：传统网络依靠人工部署，自动化程度不高，无法适配弹性资源扩展、业务快速下发的需求。
- 网络运维：缺少统一的运维评估指标体系；现网已部署网管等运维分析工具，网络监控覆盖不完整，缺乏对重要业务的端到端可视化监控、智能运维分析能力；问题定位效率不高。

随着业务的快速发展，海通证券数据中心间业务的带宽压力日益增加，为适配业务快速变化，解决当前骨干网络遇到的问题 and 诉求，采用基于 **IPv6** 技术的创新协议 **SRv6**、**iFIT**、智能运维等 **IPv6+** 创新技术，构建规划海通证券下一代 **IPv6+** 广域骨干网，以下是本次项目的具体方案：

1、设计规划原则：统一规划骨干网络

依据层次化，高可靠，模块化，智能化设计原则，构建弹性的证券骨干承载网；实现多业务融合承载，多链路灵活接入、动态调整和快速部署；完成 IPv6+ 智能网络演进。

2、网络逻辑架构：标准架构、业务灵活扩展

骨干网络作为生产、交易、办公的传输网络，最主要的功能是稳定、可靠地高速转发企业内的各类业务流量。按照网络规划原则规划目标架构模型，分为核心层、汇聚层和接入层，实现数据中心与骨干网松耦合，层次化组网，业务灵活接入，灵活扩容，技术方案平滑演进。

3、SRv6 policy 规划：保障海通核心业务传输质量，实现业务流量负载分担

SRv6 policy 具备路径可编程能力，SRv6-Policy 可提供基于带宽，时延，路径分离等定制化要求的路径规划，可视、可规划、可约束；SRv6 policy 使用 color 属性作为关键字；SRv6 policy 根据不同业务对应 color 入对应隧道，做相应 SLA 保障。

四、项目成效

(一)基于 **SRv6** 软件定义骨干网,实现流量灵活调度、提升专线带宽利用率

海通证券的张江数据中心与南外滩数据中心通过 4 条专线连接，其中 2 条专线转发交易业务，另 2 条专线转发非交

易业务。通过应用 **IPv6+** 创新承载技术，能够实现业务融合承载，减少专线数量，有效降低线路成本，同时还要对交易和非交易业务进行差异化质量保障，优先保障交易业务的转发。

（二）广域骨干网方案实现应用业务、网络运维一体化

通过采用 **IPv6+** 链路质量检测创新技术，实现高精度检测真实业务质量，快速感知和排除故障，提高运维效率，实时保障业务体验。

通过骨干网控制分析器与上层应用业务检测系统对接联动，使业务与网络关联，业务质差问题实现分钟级定界。同时采用 **IPv6+** 链路质量检测技术，对网络真实业务流进行特征标记，以直接检测网络的时延、丢包、抖动等性能指标的检测技术，并采用 **Telemetry** 技术实时上送检测数据，最终通过可视化界面直观地向用户呈现逐包或逐流的性能指标。显著提高网络运维及性能监控的及时性和有效性，保障 **SLA**，实现智能主动运维。