证券行业中的下一代互联网协议 IPv6：技术，应用与挑战

（证券业协会供稿）

单位：证券业协会

部门：信息科技部

北　京

目录

一、背景介绍

随着互联网的普及和信息技术的快速发展，证券行业作为对信息技术高度敏感的基础服务类行业，正面临着数字化转型的挑战。相比传统的“数据大集中”的 ICT 建设模式，现代证券逐步转向“分布式平台+微服务化”的互联网证券新业态，证券机构管理的联接量从最初 PC 时代的 10 亿量级，增加到移动互联网时代的 40 亿量级，甚至未来产业互联网时代的 160 亿量级[1]，联接量级的几何式增长，成为证券行业的信息系统面临的重大挑战，为了应对互联网证券新业态的发展和实现面向互联网的关键信息基础设施的稳定运行，证券行业的网络架构亟待优化和重塑。

现阶段证券行业大部分的网络服务基于 IP 协议的第四个版本，IPv4。由于 IPv4 的互联网面临网络地址消耗殆尽、服务质量难以保证等问题，推动新一代互联网协议 IPv6 的规模部署已成为优化证券系统网络架构的关键步骤。以证券业为例，在 IPv4 环境下，目前所有证券机构无一例外都采用了无分类子网掩码、网络地址转换 Network Address Translation（NAT）等技术来缓解 IP 资源短缺所带来的问题，但都只是权宜之计。随着物联网等技术的急速发展和终端设备的不断增多，基于 IPv4 的互联网无法满足未来的万物智能，新一代互联网协议的全面部署迫在眉睫[2]。

2017 年 11 月,中共中央办公厅、国务院办公厅联合印发了《推进互联网协议第六版(IPv6)规模部署行动计划》，明确提出我国 IPv6 部署的总体要求、重点任务和实施步骤。

一行两会于2018年12月结合金融业的特点,联合发文《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)规模部署行动计划>的实施意见》（银发2018[343]号），就金融业部署提出了具体意见。2021年中央网信办、国家发展改革委、工业和信息化部联合印发《关于加快推进IPv6规模部署和应用工作的通知》，要求进一步推动基于IPv6的新型互联网在金融领域规模部署，促进互联网升级演进与金融行业的创新融合。

二、下一代互联网协议IPv6的技术分析

为解决IPv4地址空间与日趋增长的网络规模不匹配的问题，国际互联网工程任务组(The Internet Engineering Task Force.简称 IETF) 从1990年开始，提出了建设下一代IP协议。1998年12月，IETF正式推出互联网标准规范RFC2460，下一代网络协议Internet Protocol Version 6（IPv6）应需而生。IPv6的地址为128位二进制位，号称“可以为地球上每一粒沙子分配一个IP地址”，采用IPv6的下一代网络比IPv4网络更具扩展性，具体来说，IPv6技术具有如下特点：

（一）IP地址资源丰富，结构层次清晰

IPv6将现有的IP地址长度扩大4倍，由当前IPv4的32位扩充到128位，以支持大规模数量的网络节点，这样IPv6的地址总数就大约有3.4 X 10E38个。平均到地球表面上来说，每平方米将获得6.5 X 10E23个地址。根据中

国信息通信研究院发布的IPv6发展监测平台最新监测数据，截止2021年8月,我国IPv6分配地址用户数达16.10亿，IPv6活跃用户数达5.35亿，IPv6用户规模持续增长，已达世界前列[3]。足够满足当前新技术的发展需要。

此外，IPv6支持更多级别的地址层次，IPv6的设计者将IPv6的地址空间按照不同的地址前缀进行划分，并采用了层次化的地址结构，能够有效抑制路由表的快速膨胀，有利于骨干网路由器对数据包的快速转发。对证券行业来说，可以根据分支机构层次、部门、业务等进行划分，比IPv4下无分类子网掩码技术划分子网的方式更简便。

（二）报头优化，拓展灵活

IPv6在IPv4的基础上优化了数据包头部字段，删除了IPv4的头部长度、头部校验、中分片等不太常用的字段，增加了流标签等字段，并且修改了原地址、目的地址等选项，使得IPv6中需要被中间路由器处理的字段由12个降低到8个，从而加快了路由器的处理速度。与此同时，IPv6还定义了丰富的扩展头部字段，包括分片、移动选项、认证选项等，能够满足当前网络环境下提出的安全认证、移动网络、物联网等要求，并且对将来网络的发展提供了很好的扩展性。

（三）终端地址管理

在IPv4协议下，证券机构基本都采用手动配置静态IP地址的方式进行终端地址管理，耗费了大量人力、时间和管理成本，尤其在移动网络环境下，经常需要对地址进行调整。由于IPv6地址有128位二进制位，手动配置方式非常容易

出错，所以多数场景下可优先选用自动生成的方式。典型的IPv6地址自动分配方式有无状态地址自动配置、DHCPv6分配方式和EUI-64地址生成方式，均可以为设备分配特定的地址前缀和主机地址，能够在保证设备可回溯性要求的基础上，自动完成网络配置，实现网络通信，大大降低管理成本。

（四）网络传输认证与加密

对于证券行业，安全为网络运行的第一要素。网络传输层的安全协议IPSec是一种基于端对端的安全模式，即在源IP和目标IP地址之间进行加解密和安全认证，加密机制通过对数据进行编码保证数据的机密性，以防数据在传输过程中被他人截获造成失密，认证机制使IP通信的数据接收方能够确认数据发送方的真实身份，以及数据在传输过程中是否遭到改动。

但在IPv4环境下，IPSec是在原数据包的基础上封装一层认证包头部，需要对数据包进行修改，且IPv4的网络访问要经过多次NAT，大大降低了IPSec的可用性，故目前的证券机构主要是以应用层的安全手段为主，网络传输层为辅。

IPv6支持点到点的传输模式，且协议本身的扩展头部中已经定义了安全认证的字段，即IPv6协议包本身天然实现了加密认证的功能，使得网络传输更加安全，更能满足证券机构的安全访问需求。

三、IPv6 在证券领域的应用

目前，证券业对于广域网的创新改造领先于其他领域，并取得了一定的成功，已经从 IPv6 向“IPv6+”进行全面升级与实践。在政策驱动下，以证券公司为核心的一批证券机构已经从互联网接入 IPv6 为起点，逐步深入到内容改造，基于 IPv6 改造开拓了各类创新应用，改造范围涵盖互联网接入环境、服务器区域基础设施、互联网应用、安全系统和运维管理系统等多方面。

（一）支持完整的端到端业务

由于 IPv4 地址的短缺，目前证券行业的许多业务都只能基于 NAT 技术实现。采用这种技术带来的直接后果是网络复杂，管理成本高，而且性能低下。IPv6 所提供的丰富地址空间使每一个参与通信的设备或应用都具有自己的 IP 地址，使得端到端业务成为可能，这将极大简化网上电子交易的复杂性和可管理性。同时，由于 NAT 技术本身的局限，目前有很多业务在 NAT 下无法开展，而这些业务则可以在 IPv6 的支持下部署和实施。

（二）唯一标识交易身份

电子交易的安全性是证券信息化能否成功的关键。在国外，利用网络进行证券犯罪的案件越来越多，而且作案手法越来越隐秘。由于网络犯罪难以追踪和取证，因此利用信息技术进行证券犯罪有逐步扩大的趋势。IPv6 可以使每一个参与交易的个人或设备都能够分配一个唯一的地址，将该地址与交易者绑定后即可作为该交易者身份的唯一标识。这个地

址就像每个人的身份证一样，不论交易者身在何处，都可以利用该地址将整个交易过程记录下来，这为侦破利用网络进行的各种证券犯罪提供了极大的便利，也可极大地提高网络交易的安全性和不可抵赖性，增强人们对电子银行、信用卡、网上证券等电子业务的信任。

（三）满足 VPN 对业务地址的大量需求

正在蓬勃发展的虚拟专用网（VPN）在证券业有着广泛的应用，各项业务 VPN 对 IP 地址需求量巨大。采用 IPv6 技术，可以为每种业务单独划分一段地址空间，不仅简化了网络设计和管理，而且增强了业务 VPN 的安全性。无疑，这对很多全国性的证券公司都具有巨大的吸引力。

（四）内置的安全特性简化网络，降低成本

IPSec 在 IPv4 中是可选技术，而在 IPv6 中是必须的组成部分。这种内置的安全特性增强了 IPv6 网络的安全，使得 IPv6 网络从一开始就比 IPv4 网络更安全可靠，更容易赢得用户的信任。作为 IPSec 的一项重要应用，IPv6 集成了 VPN 的功能，使用 IPv6 可以轻松实现更为安全可靠的 VPN。同时，这种内置的安全特性为各种高层应用提供了基本的安全保障，各种高层的安全协议可以更方便、更快捷地与之融合，极大简化了网络的复杂性，降低了网络交易的成本。

（五）“IPv6+”的创新应用

“IPv6+”创新应用推进了证券机构网络服务化能力。例如在海量终端的物联网场景中，在 IPv6 的海量地址空间，无需大规模部署 NAT 设备，可实现网络端到端溯源，降低

安全隐患以及降低网络建设成本的同时，还可以通过“IPv6+”的应用识别能力可解决当前物联场景下网络层面业务识别、路径检测、路径选择问题。另外在数字货币的应用中，基于“IPv6+”的组播技术可以有效解决1:N联接问题，降低广域带宽，提升账本节点性能。同时，“IPv6+”低时延与时延控制技术，能够有效避免突发拥塞丢包和网络转发调度不确定时延，保障丢包以及时延在一个可控范围，提升跨中心交易协同业务的性能。

四、IPv6改造面临的挑战

（一）当前改造工作存在的问题

目前,证券行业已初步完成IPv6三年规模部署工作，门户网站和应用系统基本完成IPv6改造[4]。但是IPv6改造工作还存在一些难题。一是IPv6的服务能力还有待提高。证券行业IPv6现在仅达到“通路”的初级阶段,部分路段还存在单行、禁行、限行的情况。网络基础设施主要采用的还是NAT64、隧道技术和“双栈”技术,未实现IPv6单栈运行模式。应用系统以及底层系统开发还存在难度,基于IPv6的技术应用、系统架构和生态环境还不成熟,部分技术难点还有待突破,数据中心层次的IPv6整体规划改造和实施成功案例还不够多,IPv6总体服务能力还有待提高。例如部分单位的WAF、IPS、IDS、监控和日志审计平台的功能并不能直接支持IPv6,大部分还是通过NAT64的方式间接实现监控和管理,IPv6产业生态基础还很薄弱。

第二，目前IPv6部署和改造所涉及的网络、系统、应

用、服务、管理、安全、开发等方面均缺少证券行业标准,不能有效地为证券服务机构提供建设指引,因此建立体系完善的 IPv6 标准化体系迫在眉睫。

第三，但是在 IPv6 网络安全方面仍然存在安全威胁,IPv4 网络中的部分攻击类型同样会对 IPv6 产生攻击,IPv6 改造过程所采用的过渡机制也存在安全风险,例如采用“双栈”方式需要部署两套设备,通过不同运维系统进行维护,在策略制定、制度管理、人员配置等方面增加了管理的难度和复杂度,另外 IPv6 特有的安全漏洞和应用也同样带来新的安全风险。

（二）证券行业 IPv6 发展建议

针对上文提出的当前证券行业改造面临的挑战,如何推进进新一代互联网协议的应用，下面浅谈几个建议。

主动推广已有的科研成果，促进 IPv6 商业应用。连续通过重大专项和示范工程，继续深化 IPv6 技术创新和应用。支持路由器和交换机等 IPv6 核心产品进展及有关网络过渡技术的研究、验证和部署，加大对宽带接入服务器、防火墙、网络运营和网络治理应用软件等其他基于 IPv6 协议产品的支持，促进基于 IPv4 网络的内容和应用向 IPv6 迁移，推动 IPv6 研发与应用及产业链成熟完善。

目前我国 IPv6 的标准化工作取得了一定的成绩，首批 IPv6 的行业标准初步制定完成，包括 IPv6 网络总体要求、无状态地址配置、移动 IPv6、路由协议 OSPF 和 BGP4 等。然而，IPv6 应用技术规范等领域的证券行业标准还很缺乏。

所以要继续制定证券领域 IPv6 相应技术标准，完善 IPv6 系统评测、IPv6 应用技术规范、IPv6+”技术应用标准等领域的证券行业标准，结合新技术、新要求、新形势，加强 IPv6 在网络、安全、应用、运维、服务、代码开发等证券行业管理标准的研制和推进工作,为证券行业 IPv6 改造提供行业标准。

加强 IPv6 网络安全技术研究,包括 IPv6 网络下实现安全传输、数字加密认证、防范网络攻击等安全技术手段,扩大安全技术应用范围和场景。加强 IPv6 网络安全管理工作,按照网络安全等级保护相关要求,制定 IPv6 网络安全定级标准,识别 IPv6 网络风险隐患,提高 IPv6 网络安全保障能力。

五、总结

证券行业具有交易时间集中、市场高速变化、交易应用软件形态多样等特点，系统改造适配的环境较为复杂。通过近 2 年的改造工作，证券行业包括核心机构、监管机构和证券公司的各类网站及 APP、PC 客户端逐渐已实现 IPv6 网络全面覆盖，并实现了客户无感切换。但是，由于 IPv6 生态目前仍处于发展初期阶段，短期内网络通信质量和成熟的 IPv4 相比存在一定差距， 因此，证券行业需要持续推进 IPv6 网络在行内的规模化部署,促进下一代互联网与证券行业的深度融合，探索 IPv6 技术创新与业务整合的新应用、新模式、新业态。

六、参考文献

[1]Joseph Davies. 深入解析 IPv6（第三版）[M]. 北京：人民邮电出版社，2014.

[2]李星. IPv6 及其在金融领域的应用前景[J]. 金融电子化, 2004(04):10-12.

[3]前瞻产业研究院. 中国下一代互联网（CNGI）建设市场前瞻与投资战略规划分析报告[R]. 北京中研信息研究所, 2022.

[4]崔亮. 关于提升金融行业 IPv6 流量的思考和建议[J]. 甘肃金融, 2022(6):3.