专题：“IPv6+”网络技术创新体系

基于“IPv6+”的应用感知网络（APN6）

何林[1,2]，况鹏[1,2]，王士诚[1,2]，刘莹[1,2]，李星[1,2]，彭书萍[3]
（1. 清华大学网络科学与网络空间研究院，北京 100084；
2. 北京信息科学与技术国家研究中心，北京 100084；
3. 华为技术有限公司，北京 100095）

摘　要：互联网应用对网络带宽、时延、抖动、分组丢失率等方面的需求各不相同，而网络和应用的解耦导致网络无法有效感知应用的需求，因此难以为应用提供相应的服务质量 SLA 保障。提出一个基于 IPv6 的应用感知网络框架——APN6，通过将应用的需求信息封装在数据分组中，使网络能感知应用及其需求，便于网络进行流量调度和资源调整。设计了一种安全接入控制方案以解决 APN6 接入场景中存在的应用信息的伪造与篡改问题，确保 APN6 只对合法用户提供相应服务。

关键词：感知应用网络；APN6；SRv6；IPv6
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000–0801.2020257

Application-aware IPv6 networking

HE Lin[1,2], KUANG Peng[1,2], WANG Shicheng[1,2], LIU Ying[1,2], LI Xing[1,2], PENG Shuping[3]
1. Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China
2. Beijing National Research Center for Information Science and Technology, Beijing 100084, China
3. Huawei Technologies Co., Ltd., Beijing 100095, China

Abstract: Internet applications have different needs for network bandwidth, latency, jitter, and packet loss. However, the fact that the network and applications are decoupled makes it difficult for the network to be aware of an application’s requirements and ensure its quality of service (e.g., service level agreement, SLA). A framework called application-aware IPv6 networking (APN6) was proposed, which could encapsulate applications’ requirements into packets. Networks could be aware of an application’s requirements and perform traffic steering and network resource adjustment. Besides, a secure access control mechanism was designed to solve application information forgery and tampering issues in APN6, which ensured that APN6 only provided services to legal users.

Key words: application-aware networking, APN6, SRv6, IPv6

收稿日期：2020–06–10；**修回日期：**2020–08–12
通信作者：刘莹，liuying @cernet.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2018YFB1800405, No.2018YFB1800404）；国家自然科学基金资助项目（No.61772307）
Foundation Items: The National Key Research and Development Program of China (No.2018YFB1800405, No.2018YFB1800404), The National Natural Science Foundation of China (No.61772307)

1　引言

互联网上运行了各式各样的应用，为人们的生产生活提供了便利。据 Statista 统计，2020 年第一季度，主流应用商店的 App 可用数量累计超过 550 万[1]。图 1 展示了不同应用商店下可用 App 数量，其中 Google Play 下可用 App 数量最多，达 256 万。

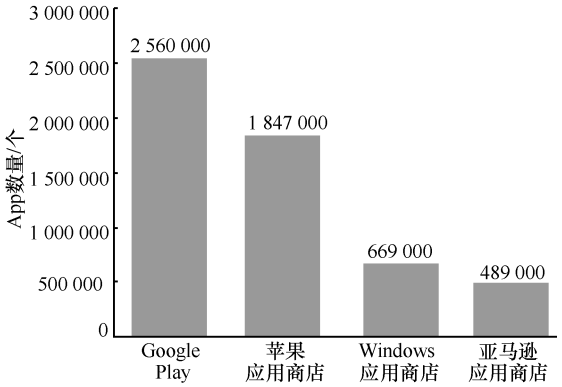

图 1　主流应用商店中可用 App 数量

虽然众多应用同时运行在互联网上，但它们对于网络带宽、时延、抖动和分组丢失率等的要求不尽相同，甚至相差极大。例如，在线视频和游戏等应用对网络提出了极高的要求，而文本类等应用的需求却容易满足。然而，当前的网络与应用是解耦的，网络无法细粒度感知应用的需求，因此难以为应用提供相应策略保证其服务等级协议（service level agreement，SLA）需求。5G 等技术的飞速发展催生了更多需求严苛的应用，更加剧了这种困境。目前，网络主要依赖流量五元组或深度分组检测（deep packet inspection，DPI）等方案进行服务区分。然而，这些方案却面临诸多挑战，最主要的挑战为数据分组无法携带充足的信息表达应用对网络性能等的需求。

与此同时，近年来，IPv6 成为全球互联网技术无可争议的发展方向，IPv6 互联网进入了快速发展期。2016 年 11 月，国际互联网架构理事会（IAB）发布公告，声明国际互联网工程任务组（IETF）正式放弃 IPv4，未来所有信息要全部建立在 IPv6 的基础上[2]。截至 2020 年 6 月，谷歌（Google）统计其全球 IPv6 用户访问约 32%左右[3]，24 个国家在 IPv6 上传送了超过 15%的业务量，美国、德国等国家的 IPv6 用户占比已接近或超过 50%。与此同时，构建于 IPv6 数据平面之上的段路由（segment routing over IPv6 dataplane，SRv6）[4]发展得如火如荼，目前正在互联网任务工程组 IETF 的 SPRING 和 6MAN 工作组进行标准化。SRv6 具备强大的网络可编程能力，可以更好地满足显示路径需求。

本文提出感知应用的 IPv6 网络（application-aware IPv6 networking，APN6），通过数据分组携带应用的标识和需求信息，即对应用信息的传递，并保证应用信息安全可靠，使网络感知应用并根据应用的需求为其提供优质的差异化服务。而网络在传送数据分组时，根据数据分组中的应用信息匹配网络对应策略，并选择相应的 SRv6 路径传输数据分组（如低时延路径），满足 SLA 需求，提高服务质量。

2　相关研究

本文涉及的相关研究包括 IPv6、SRv6 和相关跨层应用信息携带等。

2.1　IPv6 和 SRv6

IPv6 作为 IPv4 的下一代标准，解决了 IPv4 地址枯竭问题，并对 IP 地址作出了改进。相较于 IPv4 的 32 bit 地址，IPv6 采用了 128 bit 的地址，地址空间巨大，为 SRv6 提供了灵活的网络编程空间。同时，IPv6 支持使用扩展头传输可选信息（如逐跳选项报头、路由选项报头）等。SRv6[4]是段路由（segment routing，SR）在 IPv6 数据平面的应用。2020 年 3 月，IETF 通过了 SRv6 的 RFC，其沿用了路由选项报头格式，并定义了新的路由选项。段路由基于源路由的范式，可以实现根据多个不同子网或内网地址，选择性地将报文发往不同目的地址的功能。在段路由中，一个节点通

过段路由机制来操纵报文，这个段路由机制通常被实例化为有序的指令，即分段。段路由提供了一种机制：允许一条流经由特定拓扑路径，而仅需在段路由的入口节点维护流的状态。一个分段可与一个拓扑指令相关联，一个拓扑本地分段指示一个节点通过一个特定的网络接口发送报文，一个拓扑全局分段指示一个 SR 域通过一个特定的路径转发报文。一个分段也可与服务指令关联，例如限制报文必须经由分段对应的容器或者虚拟机处理。

在 SRv6 中，一个分段被编码为一个 IPv6 地址，一个有序的分段被编码为一个有序的 IPv6 地址列表。活跃分段由报文的目的地址指定，下一个活跃分段由段路由头部中指针指定。在 SRv6 段路由头部中，包含着几个关键字段：routing type，8 位路由类型标识符，取值为 4；tag，标记报文类别；segment list[0,⋯,*n*]，表示第 *n* 个分段的 128 bit 的 IPv6 地址。在段路由网络中，涉及 3 种类型节点：SR 源节点，发起携带分段的 IPv6 报文的节点；SR 传输节点，转发报文到下一分段的节点；SR 终端节点，接收到 IPv6 报文中目的地址被配置为本地分段的节点。在 SRv6 报文处理过程中，SR 源节点在 SRv6 报文中携带 SR 机制，以操纵报文走向，SR 传输节点基于其 IPv6 路由表以及 SRv6 报文中的目的地址转发报文，SR 终端节点按照配置策略处理 SRv6 报文。

目前，学术界涌现了众多关于 SRv6 的研究，如 segment ID 的表示[5]、SRv6 应用[6]等。

2.2 服务区分

已有一些基于传统网络协议的细粒度服务提供机制，这些服务定义允许对某些类型的流量给予优先或区别对待。但使用传统方式保证 SLA 时的挑战在于，数据分组无法携带足够的信息来指示应用程序并表达其服务/ SLA 要求。当前网络设备主要依赖流五元组的数据分组或进行深度数据分组检测。五元组粒度 ACL/PBR 被广泛用于流量工程中。但是，这些功能只能间接表示应用程序信息，不能为更细粒度的服务过程提供足够的信息。如果需要更多信息，则必须使用 DPI 提取该信息，DPI 可以深入检查数据分组以获取特定应用程序的信息。但是，这将为网络运营商引入更多的资本支出和运营支出，并带来安全性问题。

SRN[7]基于 SDN 和 DNS 协议扩展，通过在 SDN 控制器上实现 DNS 解析器，并扩展 DNS 协议，实现了服务器、终端主机与网络运营者的交互。用户终端和服务器通过扩展的 DNS 协议，将应用信息（如流量带宽与路径要求）传入网络运营者负责管理的控制器中心节点，由控制器进行统一的控制与分发，将其映射入 SRv6 路径进行服务质量控制。但是，此方法引起以下问题：整个循环很长且很耗时，不适合关键应用程序的快速服务提供；循环中涉及过多的接口，带来了标准化和互操作性方面的挑战。

2.3 国际标准化进展

APN6 在 IETF 标准规范目前主要包括如下几个方面。

（1）问题澄清

draft-li-apn-problem-statement-usecases-00[8]梳理了当前网络差分服务提供方面面临的问题和挑战，澄清了对 APN6 的需求。

（2）框架描述

draft-li-apn-framework-00[9]介绍了 APN6 的整体框架和关键元素。

（3）实际用例

draft-liu-apn-edge-usecase[10] 和 draft-zhang-apn-game-acceleration-usecase[11]分别介绍了 APN6 在边缘计算和游戏加速场景下的实际用例。

（4）APN6 封装

draft-li-6man-app-aware-ipv6-network-02[12] 介绍了 APN6 中应用信息在 IPv6 网络中的封装。

（5）APN6 边会

在 IETF105 和 IETF108 分别举办了 APN 的边会（side meeting）。来自 Bell Canada、Telefonica、

中国移动、中国联通 4 家运营商分别介绍了各自的应用案例（use case），阐述运营商网络对感知应用的诉求和可能的收益。应用案例包括业务/应用感知、内容分发网络、边缘计算和游戏加速。IETF 对当前类似的网络感知应用方案 Network Tokens、FAST、APN6 分别进行了介绍。最终通过具体场景分析，分别澄清了 APN 的隐私和安全问题，并明确了 APN 在 IETF 的工作将集中在网络域，并在不涉及安全和隐私的场景下进行。本次边会吸引了来自运营商、厂商、学术界等的广泛关注，共有 50 余位专家参会。与会专家对 APN6 的价值达成了一定的共识，希望能够成立邮件列表进一步讨论和推进。

3　APN6 框架设计

APN6 利用 IPv6/SRv6 报文自身的可编程空间，将应用信息携带在 IPv6 数据报文中传递进入网络，使网络感知到应用及其需求，从而为其提供 SLA 保障及相应的网络服务。本节主要介绍应用信息格式设计和安全接入控制方案。

3.1　应用信息格式设计

APN6 旨在让网络感知应用信息以实现满足应用服务质量目标，其中报文携带的应用信息提供网络识别应用、了解应用需求的关键信息，因此该应用信息格式设计是 APN6 的关键。APN6 应用信息格式设计遵循 3 条原则。

- 多样性：可以包含广泛的应用标识及其需求信息。
- 可扩展性：当有新的应用和需求信息提出时，能够灵活支持。
- 高效性：在路由器接收包含 APN6 消息的报文时，可以高效地提取、解析其中的应用标识及需求信息字段。

在本文设计中，应用信息包含两部分：应用标识信息和应用需求信息。其中，应用标识信息占 80 bit，应用需求信息占 48 bit，共计 128 bit。

3.1.1　应用标识信息

应用标识信息旨在提供一种便于网络区分不同应用、不同使用应用的用户等信息的报文选项。表 1 列出了应用标识信息设计，并说明了每个字段所占据的位宽，具体如下。

- App ID, 长度为 24 bit，标识发出数据分组的 App。24 bit 的位宽能够标识超过 1.6×10^7 个 App，足以涵盖当前主流平台活跃的 App。
- user ID，长度为 40 bit，标识发出数据分组的用户，即使用该 App 发出数据分组的用户标识。40 bit 能够标识超过 1 万亿用户。
- SLA，4 bit，标识数据分组所属用户在该 App 下的服务等级。
- session ID，4 bit，标识数据分组所属 App 的具体会话，即 App 下产生该数据分组的会话。
- reserved，8 bit，保留字段。

表 1　应用标识信息格式设计

App ID	user ID	SLA	session ID	reserved
24 bit	40 bit	4 bit	4 bit	8 bit

3.1.2　应用需求信息

应用需求信息为网络提供便于其感知应用需求（如带宽、时延、抖动、分组丢失率等）的信息。表 2 列出了应用需求信息格式设计。应用需求信息包括以下参数：

表 2　应用需求信息格式设计

bandwidth	latency	jitter	loss ratio	reserved
8 bit	8 bit	8 bit	8 bit	16 bit

- bandwidth，8 bit，表示应用请求网络带宽；
- latency，8 bit，表示应用能够接受的网络最大时延；
- jitter，8 bit，表示应用能够接受的最大抖动；
- loss ratio，8 bit，表示应用可接受的最大分组丢失率；

• reserved，16 bit，保留字段。

每个需求参数采用前 4 bit 表征单位，后 4 bit 表征取值的方式进行。以带宽为例，前 4 bit“0000”表示 1 M，“0001”表示 10 M，“0010”表示 100 M，并以此类推，后 4 bit 表示取值 0~9。例如，“00100011”代表 300 M 带宽需求。

3.1.3 分析

为了评估应用信息格式设计优劣，本文定义了几个评价指标：比特位数，衡量网络支持 APN6 所需解析报文的额外位数；有效比特占比，衡量应用信息中有效字段比率；可扩展度，衡量应用信息中保留字段比率。表 3 列出了应用信息格式评估，其中可以看出应用标识信息有效比特占比高于应用需求信息，而其可扩展度低于应用需求信息，这样设计的原因是应用标识信息相对固定，而应用需求信息根据不同类型应用有所不同，留足保留字段位数便于扩展，应用信息总长度固定，便于路由器提取、解析。

表 3 应用信息格式评估

类别	比特位数	有效比特占比	可扩展度
应用标识	80	90%	10%
应用需求	48	66.7%	33.3%
应用信息	128	81.25%	18.75%

3.2 安全接入控制方案

安全接入控制方案旨在解决 APN6 接入场景中存在的安全问题。在接入场景中，用户需与业务感知节点（如 CPE）建立身份信任，防止应用信息的伪造以及篡改。ISP 还需要获知用户发送 APN6 报文所携带的应用信息合法性进行确认，对符合用户身份的合法要求提供相应的服务。

3.2.1 场景与问题定义

针对 APN6 的接入场景进行如图 2 所示的定义。

图 2 中，用户设备在使用 App 时，将应用信息包括网络性能需求信息携带入 APN6 数据分组头（IPv6 的扩展报头，如逐跳选项报头）中，由业务感知边缘节点对 IP 报文进行源地址认证和完整性检测，同时检查 APN6 性能需求信息是否满足用户服务等级。在检测通过后，将其映射进入 SRv6 路径。

针对上述应用接入过程，本文针对以下几个接入场景进行分析，并设计安全接入控制解决方案。

（1）不同设备间的应用信息伪造

不同设备间应用信息伪造示意图如图 3 所示，

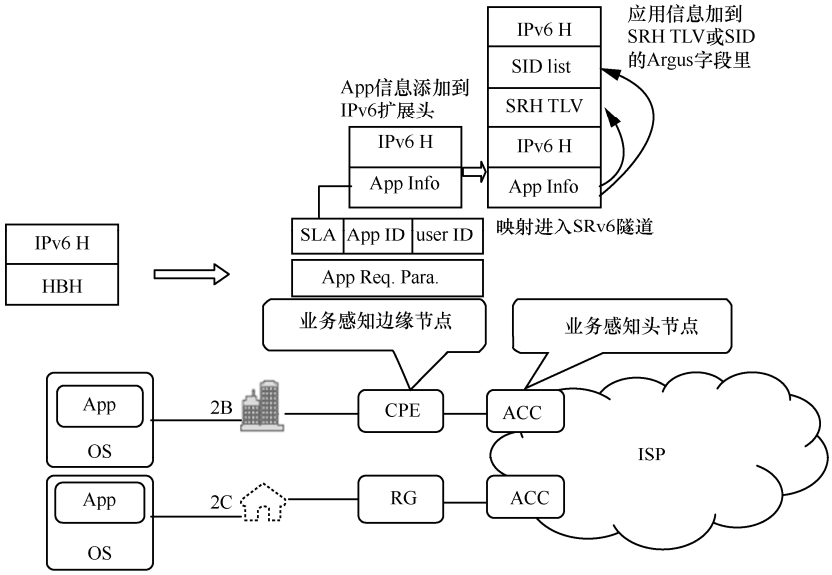

图 2 接入场景定义

设备 2 伪造使用设备 1 的应用信息，骗取网络为其分配更多资源。

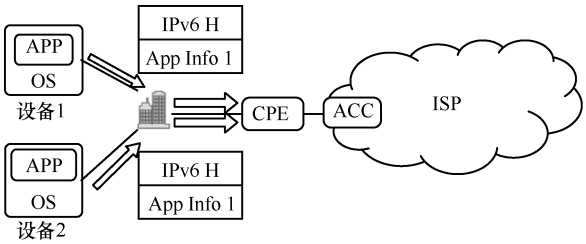

图 3　不同设备间应用信息伪造示意图

（2）接入链路上的应用信息篡改

接入链路上信息篡改示意图如图 4 所示，在接入链路上存在恶意中间设备，对正常设备发送的报文进行篡改或重放，影响正常用户获得的服务质量。

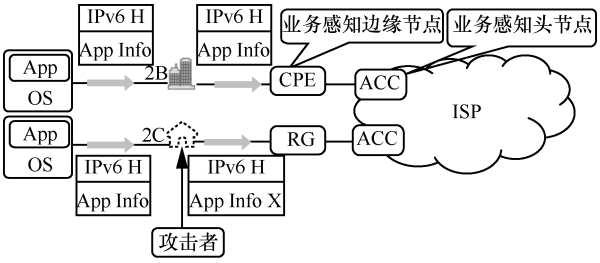

图 4　接入链路上信息篡改示意图

（3）APN6 业务感知节点对应用标识和需求信息的确认

业务感知边缘节点应对 IPv6 报头和应用信息进行真实性和完整性校验，防止伪造篡改用户信息与性能需求，防止用户越权请求资源分配。

3.2.2　安全接入控制流程

安全接入场景设计如图 5 所示，安全接入场景方案使用基于区块链的公钥管理系统和基于对称密钥协商的消息认证码，以保证 APN6 信息的真实性和完整性。方案流程如下。

步骤 1　用户主机设备，业务感知边缘节点和 App 服务商生成各自公私钥并在区块链公钥管理系统注册。

步骤 2　App 服务商与 ISP 进行协商，将该 App 的 App ID、user ID 及性能需求信息向 ISP 报备。

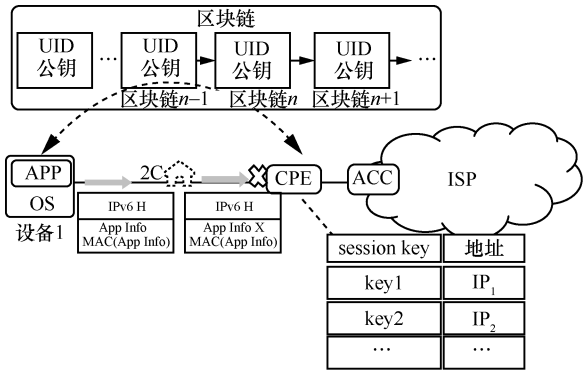

图 5　安全接入场景设计

步骤 3　主机连接网络后，设备操作系统与业务感知边缘节点相互进行公钥认证，协商共享对称密钥。

步骤 4　主机在发送报文时，对报文的 IP 源地址，APN6 数据分组中的 App ID、user ID、SLA 等应用信息以及时间戳和序列号生成摘要，并使用共享密钥进行签名，生成消息认证码。

步骤 5　业务感知边缘节点维护 IP 地址—消息认证密钥列表，对收到的报文携带的消息认证码进行校验，对校验成功且未超时的 APN6 数据分组进行应用需求信息的确认。

步骤 6　对校验签名通过的消息，检验其性能需求信息是否符合 App ID 及 user ID 的身份等级，对符合身份的，映射入 SRv6 路径；对不符合的，将其应用需求更改为所在身份默认等级，映射入 SRv6 路径。

4　结束语

本文提出了一个感知应用的 IPv6 网络框架——APN6。根据设计的应用信息格式，APN6 允许应用将其标识信息和需求信息在数据分组中封装携带，使网络能够根据应用信息进行流量调度和资源调整。此外，本文提出一种安全接入控制方案以确保 APN6 可识别伪造、篡改报文，并对合法用户提供正常服务。

在未来的工作中，本文将从有效性、效率、性能等方面对 APN6 进行验证。对于有效性，

本文将评估 APN6 可否允许应用在数据分组中携带应用标识及需求信息，网络可否基于应用信息进行灵活的流量调度及资源调整。此外，验证伪造、篡改的数据报文可否被 APN6 识别。针对效率，本文评估网络设备等处理 APN6 数据报文与普通数据报文速率差异，以衡量 APN6 引起的效率损失。针对性能，本文对比不同应用在使用 APN6 与不使用 APN6 间，其带宽、时延等不同 SLA 性能变化，以衡量 APN6 带来的性能提升。

参考文献：

[1] Number of Apps available in leading App stores 2020[Z]. 2020.

[2] IAB statement on IPv6[Z]. 2016.

[3] Google's statistics of IPv6 adoption[Z].2020.

[4] FILSFILS C, DUKES D, PREVIDI S, et al. IPv6 segment routing header (SRH): RFC8754[S]. 2020.

[5] TULUMELLO A, MAYER A, BONOLA M, et al. Micro SIDs: a solution for efficient representation of segment IDs in SRv6 networks[J]. arXiv preprint arXiv:2007.12286, 2020.

[6] 解冲锋, 蒋文洁, 马晨昊, 等. 面向视频云综合承载的 SRv6 的研究与实践[J]. 电信科学, 2019, 35(12): 2-7.
XIE C F, JIANG W J, MA C H, et al. Research and practice of SRv6 for integrated carrying of video cloud[J]. Telecommunications Science, 2019, 35(12): 2-7.

[7] LEBRUN D, JADIN M, CLAD F, et al. Software resolved networks: rethinking enterprise networks with IPv6 segment routing[C]// Proceedings of the Symposium on SDN Research. New York: ACM Press, 2018.

[8] LI Z, PENG S, VOYER D, et al. Problem statement and use cases of application-aware networking (APN): draft-li-apn-problem- statement-usecases-00 (work in progress)[Z]. 2020.

[9] LI Z, PENG S, VOYER D, et al. Application-aware networking (APN) framework: draft-li-apn-framework-00 (work in progress)[Z]. 2020.

[10] LIU P, GENG L, PENG S, et al. Use cases of application-aware networking (APN) in edge computing: draft-liu-apn-edge-usecase-00 (work in progress)[Z]. 2020.

[11] ZHANG S, CAO C, PENG S, et al. Use cases of application-aware networking (APN) in game acceleration: draft-zhang-apn-acceleration-usecase-00 (work in progress)[Z]. 2020.

[12] LI Z, PENG S, LI C, et al. Application-aware IPv6 networking (APN6) encapsulation: draft-li-6man-app-aware-ipv6-network-02 (work in progress)[Z]. 2020.

[作者简介]

何林（1991– ），男，博士，清华大学网络科学与网络空间研究院在站博士后，主要研究方向为互联网体系结构和协议设计。

况鹏（1995– ），男，清华大学网络科学与与网络空间研究院硕士生，主要研究方向为可编程网络和下一代互联网结构。

王士诚（1997– ），男，清华大学网络科学与与网络空间研究院硕士生，主要研究方向为 SDN 安全和源地址验证。

刘莹（1973– ），女，博士，清华大学网络科学与网络空间研究院副院长、副研究员，主要研究方向为网络结构设计、下一代互联网结构和路由算法与协议。

李星（1956– ），男，博士，清华大学网络科学与网络空间研究院教授，主要研究方向为下一代互联网体系结构、网络安全、网络测量等。

彭书萍（1982– ），女，博士，华为技术有限公司主任工程师，主要研究方向为 IPv6、SRv6。