



专题: IPv6 技术与应用

一种面向 Portal 认证的 IPv6 可信地址分配机制

周江^{1,2}, 李贺武^{2,3}

- (1. 清华大学深圳研究生院, 广东 深圳 518055;
2. 北京信息科学与技术国家研究中心, 北京 100084;
3. 清华大学网络科学与网络空间研究院, 北京 100084)

摘要: 随着网络规模的增长, 对网络进行精细化管控变得尤为重要。在下一代互联网中将用户可信身份嵌入 IPv6 地址后缀形成可信地址, 能够进一步提高网络行为的可追溯性。目前已有研究基于 Portal 认证配合 DHCPv6 将用户的身份信息嵌入用户终端的 IPv6 地址中, 但是为了分配可信地址而改动的 DHCPv6 过程造成了机制对用户终端不透明, 无法大规模部署。提出了一种面向 Portal 认证的 IPv6 可信地址分配机制, 通过服务器信令交互配合软件定义网络 (SDN) 技术实现 IPv6 可信地址的间接分配, 而且与地址分配方式无关。最后, 实现了一个原型系统并在江苏南京电信现网机房评估了其可行性和性能, 结果表明此机制在对终端透明的情况下仅带来很少的额外开销。

关键词: 地址分配; 可信地址; IPv6; 软件定义网络

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019288

A general way to assign IPv6 trusted address under portal authentication

ZHOU Jiang^{1,2}, LI Hewu^{2,3}

1. Graduate School at Shenzhen, Tsinghua University, Shenzhen 518055, China
2. Beijing National Research Center for Information Science and Technology (BNRist), Beijing 100084, China
3. Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China

Abstract: As the network scale grows, it is especially important to fine-tune the network. In the next-generation Internet, embedding the user's trusted identity into the IPv6 address suffix to assign trusted addresses can further improve the traceability of network behavior. At present, many studies have attempted to embed the user's identity information into IPv6 addresses based on portal authentication and DHCPv6, but the modification of DHCPv6 makes it not transparent to the terminal. A mechanism for trusted address assignment in IPv6 networks based on portal authentication was proposed. The collaboration between servers and software-defined networking (SDN) technology was used to realize the indirect assignment of IPv6 trusted addresses. Finally, a prototype system was implemented and its feasibility and performance were evaluated in the network of Nanjing Telecom in Jiangsu. The results show that the mechanism only brings little overhead and it is transparent to the terminal.

Key words: address assignment, trusted address, IPv6, software defined networking

收稿日期: 2019-12-01; 修回日期: 2019-12-11

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0801702)

Foundation Item: The National Key Research and Development Plan of China (No.2017YFB0801702)

1 引言

随着互联网用户数量的增加和网络技术的发展,网络中恶意行为的频率和规模正在急剧增加,互联网安全面临严峻挑战,不仅有各种各样的攻击对网络基础设施产生巨大威胁,还有一些不当言论和行为在危害原本纯洁的网络环境。据统计,DDoS 攻击在 2018 年就达到了超过 1 Tbit/s 的惊人速率^[1],严重降低了因特网的服务质量。造成这些攻击背后的关键原因是现在网络中没有将网络行为关联到其用户身份的机制,无法通过精确标识符定位,因此网络恶意行为屡禁不止。

在因特网的创立初期,由于其仅用于学校之间的学术交流,网络环境比较简单,所以网络安全并不是一个值得思考的问题。但是在现代社会中,互联网已成为社会中重要的基础架构,全球拥有超过 39 亿网民,当前迫切需要寻求解决方案来追溯网络作恶者来增强因特网的问责机制。除此之外,网络中还应该部署防止 IP 欺骗的机制来保护用户身份的有效性,SAVI^[2]和 SAVA^[3]提供了不同网络粒度下源地址验证解决方案,这为进一步的网络审计和溯源提供了保障。

近年来,已经有许多研究者提出了增强网络行为追溯性相关的方案^[5-6],但实际上由于缺乏有效性和兼容性,大多数机制并未得到实际部署。为了提高网络中行为的可追溯性,将用户身份与 IP 地址关联起来非常重要,以此网络管理员可以更轻松地找到网络作恶者身份。实际上,将用户身份嵌入 IPv6 地址能有效地提高网络审计和追溯能力,但是传统的地址分配机制不涉及任何身份嵌入,因此如何透明地分配可信地址仍然是一个问题。考虑到当前比较常用的 IEEE 802.1x^[12]和 Portal^[4]认证,两者完全相反的地址分配和认证顺序使得目前没有两者通用的可信地址分配机制,而 IPv6 中两种地址分配方式 DHCPv6^[10]和 SLAAC^[11]也是阻挠可信地址透明分配的重要因

素。尤其是在 SLAAC 中地址由终端自身生成,为了便于实际部署如何在不改动终端的情况下为终端分配可信地址也是难题之一。目前已有研究基于 Portal 认证来分配可信地址,但是其机制对终端兼容性不佳,无法在实际中部署,如何适配 Portal 认证来向用户终端透明地分配可信地址的问题亟待解决。

目前在可信地址方面的研究主要有:

- NIDTGA^[7]给出了如何将用户身份嵌入地址的解决方案,描述了详细的身份信息嵌入地址过程,但是没有提及地址的分配过程;
- 参考文献[8]提出了基于修改地址租约期来实现的二次地址分配方案来解决可信地址在 Portal 认证下的分配问题,但是此方案仅支持 DHCPv6,具有较大的部署局限性,而且方案对终端也是不透明的;
- 参考文献[9]扩展了 DHCPv6 协议来支持可信地址分配,在 DHCPv6 交互报文中带有认证信息来完成可信身份的获取然后嵌入地址,该方案同样仅支持 DHCPv6,且需要修改已有协议,不具备良好的可部署性。

本文提出一种基于 Portal 认证的 IPv6 可信地址分配机制。根据 Portal 认证和地址分配顺序的特点,设计服务器之间可信身份通信接口,实现了用户认证后可信身份告知接口下发终端的可信身份并生成可信地址,最后通过 SDN 技术转换地址这种间接的方式在网络第一跳处将可信地址应用到终端的原始地址上。本机制不仅避免了用户终端的任何改造,实现了用户无感知分配可信地址,而且解决了地址分配方式难适配的难题,无论终端地址通过 DHCPv6 还是 SLAAC 获取都一律在网络侧转换为可信地址,所以本机制具备更好的可部署性。

2 背景

由于本文提出的是基于 Portal 认证下的 IPv6 可信地址分配机制,考虑到本机制实现使用到了



SDN (software defined networking, 软件定义网络) 技术, 本节将会简单介绍 Portal 认证和 SDN 技术。

2.1 Portal 认证

Portal 认证通过弹出或者跳转到认证网页的方式为用户认证提供了一种通用的认证途径, 因为现实情况中移动终端的多样性, 在终端上安装特殊的认证客户端进行认证入网是难以普及的。考虑到当前基本所有智能终端都配备了 Web 浏览器, 通过弹出网页的方式进行认证无疑能够适配绝大多数终端, 因此 Portal 认证在当前的公共场所入网认证中非常普及。如图 1 所示, Portal 认证系统典型的组网方式包括 4 个基本要素: 认证客户端、接入设备、Portal 服务器和 AAA 服务器。其中认证客户端需要拥有支持 HTTP 协议的浏览器或者 Portal 客户端, 接入设备为交换机、路由器或者无线控制器 (AC), 其主要功能为认证前将用户所有 HTTP 请求重定向到 Portal 服务器, 认证后则允许用户访问网络资源, Portal 服务器用于处理用户的认证请求以及提供一些网页上的个性化服务, 而 AAA 服务器一般为 RADIUS 服务器。

相比于另一种主流认证方式 IEEE 802.1x, Portal 认证不需要特殊的客户端, 仅需要终端支持浏览器即可, 所以 Portal 认证时需要终端已拥有 IP 地址。而 IEEE 802.1x 认证为二层认证, 不需要也不允许终端在认证之前获得 IP 地址, 因此具有更高的安全性, 但是其需要特定客户端软件。更重要的是在计费方面, IEEE 802.1x 认证仅支持根据在线时长计费, 无法统计流量计费, 因此 IEEE 802.1x 认证更常见于公司、园区等地区。而 Portal 认证比较灵活, 在 Web 认证页面中可以插入各种广告和认证提示, 也可以支持手机验证码登陆, 所以 Portal 认证在公共场所如机场应用更加广泛、用户量更大。

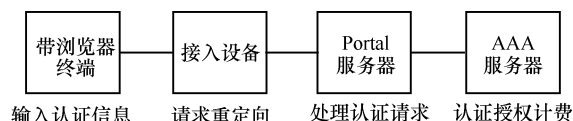


图 1 Portal 认证系统的一般结构

2.2 软件定义网络

SDN 是一种新型网络架构, 核心理念是希望应用软件参与对网络的控制管理, 满足上层业务需求, 通过自动化部署简化网络运维。传统的网络架构在 SDN 中被拆分为应用、控制、转发三层分离的架构, 如图 2 所示。控制功能上移到了服务器, 而上层应用和底层转发设施被抽象成多个逻辑实体。SDN 网络是一种集中式控制的网络架构, 主要由 SDN 控制器通过北向接口接收上层应用需求, 通过南向接口向转发层下发控制指令, 包括链路发现、拓扑管理、策略制定、表项下发等。其中南向接口协议已有 OpenFlow 等国际标准, 而北向接口方面还缺少业界公认的标准。在本文中, 应用层主要为 Portal 认证服务, 控制层由 RYU 实现的 SDN 控制器组成, 其中南向接口协议使用常见的 OpenFlow 协议。转发层则由软件实现的虚拟 SDN 交换机组成。

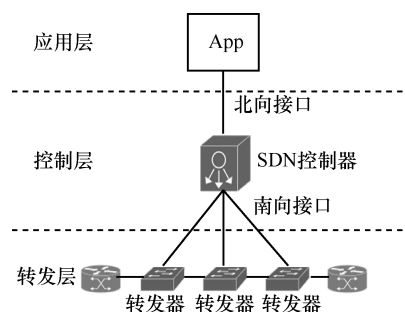


图 2 SDN 网络的一般体系架构

3 机制设计

3.1 设计目标及难点

本方案目标为设计一种基于 Portal 认证的 IPv6 可信地址分配方案, 其能够适配当前主流的 Portal 认证并给终端透明地分配 IPv6 可信地址, 可信地址是根据用户身份信息使用可信地址生成算法生成, 将用户身份编码进 IPv6 可信地址后缀使得网络管理更加方便。

本方案的主要难点为 Portal 认证中认证过程

依赖于终端事先获得的 IP 地址,由于终端在 Portal 认证中需要先获得地址再使用此地址与 Portal 服务器通信进行认证,破坏了身份获取和地址分配的时间顺序。此前的工作大都基于 IEEE 802.1x 认证为用户分配可信地址,在 IEEE 802.1x 认证中终端仅通过二层认证报文完成认证,然后再获取 IP 地址,此时网络侧已知道用户身份,可以为其分配可信地址。然而在 Portal 认证中未认证终端获取地址时其身份信息无法被服务器获取,从而无法在其认证前为其分配可信地址。

3.2 基本思想

考虑网络侧无法获取未认证终端的可信身份,用户终端的可信地址分配必须发生在用户认证之后,同时为了满足用户无感的要求实现可信地址的透明分配,本方案采取在网络第一跳处对认证用户报文进行地址转换的操作,实现用户无感知地通过可信地址进行上网。这种通过转换实现的间接可信地址分配方案既满足用户通过可信地址上网的要求,也避免了 IPv6 下可信地址分配难以适配 DHCPv6 和 SLAAC 的问题,因为无论其原始地址如何获得,都会在网络第一跳被转换为可信地址。

本方案主要思想为通过设计实现 Portal 服务器与 SDN 控制器的接口,在终端完成认证后,由 Portal 服务器告知 SDN 控制器通过认证的终端的 MAC 地址、原始 IP 和身份信息,SDN 控制器生成并下发可信地址转换流表到 SDN 交换机,基本流程如图 3 所示。

3.3 可信身份告知接口设计

可信身份告知接口主要包括 Portal 服务器和 SDN 控制器之间的 Request 和 Response 消息组成。其中,Request 消息是在完成每次认证之后由 Portal 服务器发送给 SDN 控制器用于生成可信地址和相关 SDN 转换流表项。而 Response 消息是在 SDN 控制器收到身份信息后用于告知 Portal 服务器可信地址生成的结果。当 Portal 服务器发送 Request

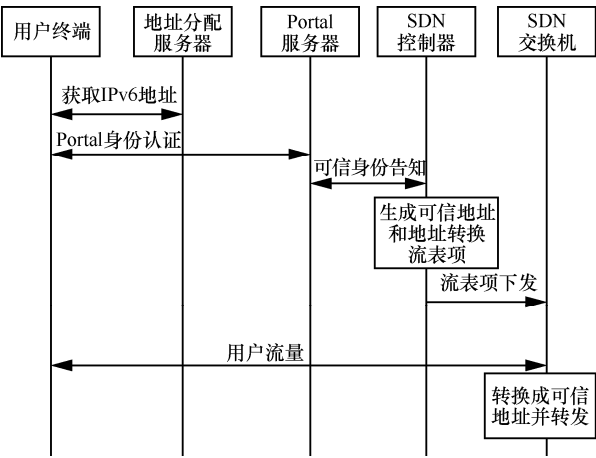


图 3 基于 Portal 认证的 IPv6 可信地址分配方案基本流程

消息后收到代表成功的 Response 消息,代表用户可信地址分配完成,可以正常上网。如果可信地址生成失败,则 Portal 服务器会在用户登录的 Portal 网页上显示相应的错误信息。

Request 消息主要包含 5 个参数,见表 1。

- Link_addr: 认证终端的 MAC 地址,用于在接入网中标识终端。
- IPv6_prefix: 认证终端的 IPv6 地址前缀。
- IPv6_suffix: 认证终端的 IPv6 地址后缀,此部分为原始后缀不包含任何身份信息。
- Identifier: 用户身份,用户注册时填写,在手机验证码登录中为用户手机号。
- Hash_code: 前 4 个参数的 sha-256 散列值,用于校验消息完整性。

表 1 可信身份告知接口中的 Request 消息格式

参数	类型(必填/可选)
Link_addr	string(必填)
IPv6_prefix	string(必填)
IPv6_suffix	string(必填)
Identifier	string(必填)
Hash_code	string(可选)

Response 消息包含 4 个参数,见表 2。

Status: 可信地址生成状态,“0”表示成功;“1”或其他非“0”字符串表示失败。



Message: 可信地址生成成功则为“success”，失败则为具体错误信息，如地址重复等。

Identifier: 用户身份，同 Request 中的 Identifier，用于告知 Portal 服务器记录。

IPv6_trusted: 根据 IPv6 前缀和用户身份生成的可信地址，用于告知 Portal 服务器记录，如果生成失败则为空。

表 2 可信身份告知接口中的 Response 消息格式

参数	类型（必填/可选）
Status	string（必填）
Message	string（必填）
Identifier	string（必填）
IPv6_trusted	string（必填）

3.4 SDN 可信地址转换

当用户完成认证并且 Portal 服务器成功告知 SDN 控制器用户身份且生成可信地址后，可信地址的转发流表项也会下发到 SDN 交换机中。当用户终端正常上网时，用户终端发出的网络分组在经过 SDN 交换机时，SDN 交换机会依据原始分组头部信息中的 MAC 和 IP 地址匹配来流表，找到对应的操作指令，将源 IP 地址转换为相应的可信地址再将网络分组转发出去，流程如图 4 所示。同样地，当通信对端向用户终端发来分组时，在其经过 SDN 交换机时，SDN 交换机会根据其目的地址即可信地址匹配流表，将目的地址更改为终端的原始地址，然后转发给终端。

整个可信地址转换流程中对于用户终端是无感知的，不需要用户终端进行任何改造即可让用户使用可信地址进行上网。

4 评估

4.1 实验拓扑

本文搭建了实验床原型验证机制在 Portal 认证下的可行性和有效性，其中所用服务器皆为现有的免费开源代码实现，本文提出的机制是在现有开源代码的基础上改造来实现的。

实验床原型拓扑如图 5 所示，其中 Portal 认证服务器增加了和 SDN 设备的可信地址告知接口，其他非 SDN 设备没有经过任何改造。图 5 中（SAVI）无线控制器为支持源地址验证功能的无线控制器，如果用户修改自己 IP 地址则用户数据分组会被丢弃，（SAVI）交换机同理。

4.2 实验评价

本文首先验证了机制的可行性和兼容性，选择了 3 台 PC 测试终端和 2 台手机终端进行测试，分别为装有 Windows 10、Ubuntu 16.04、MACOS 10.14.6 的 PC 终端和装有 Android 9 和 iOS 12 的手机终端。可行性的测试项主要包括 Portal 认证方式下的可信身份告知，SDN 转换流表下发和可信地址通信，其中可信告知指终端能成功通过 Portal 认证且 SDN 控制器成功获取用户的可信身份；SDN 转换流表下发指 SDN 控制器生成用户终端可信地址并成功下发给 SDN 交换机；

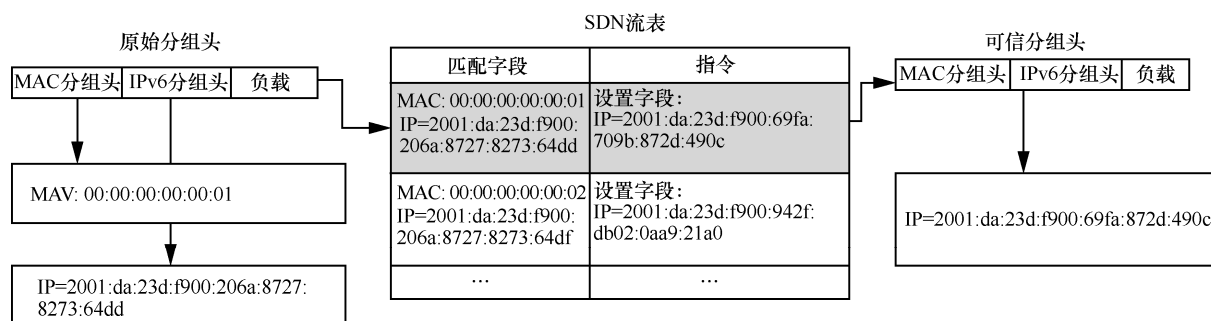


图 4 SDN 交换机上的可信地址转换流程

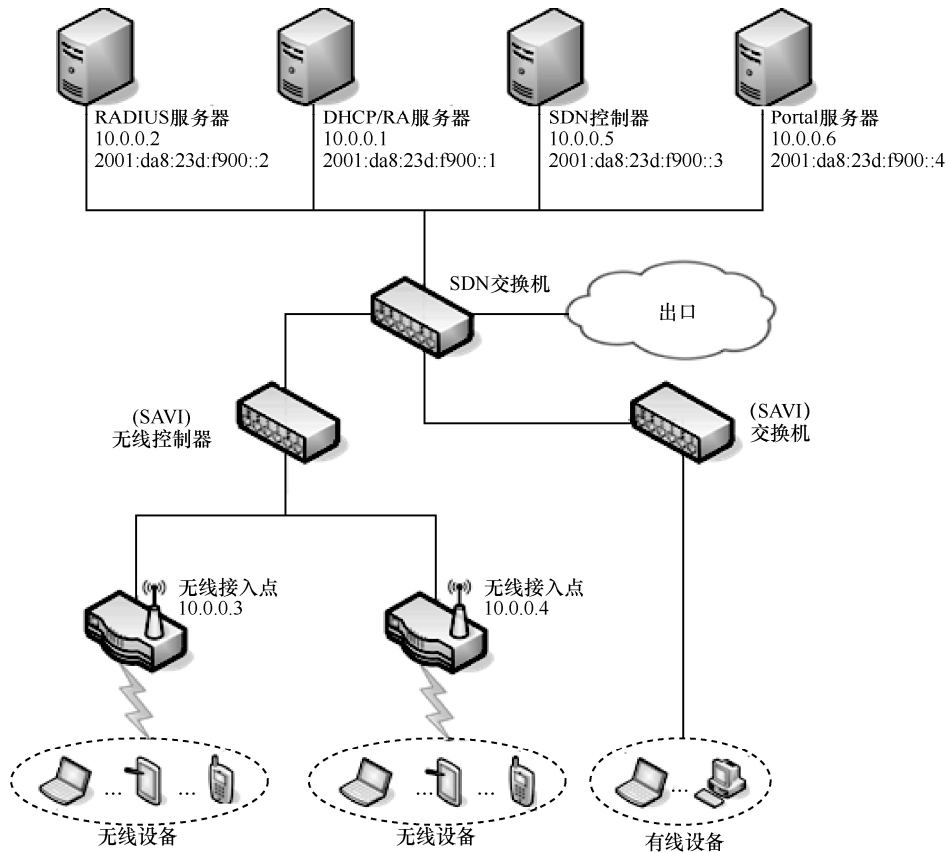


图5 实验床原型拓扑

可信地址通信指认证完成的终端可以使用可信地址与外网设备正常通信，详细测试结果见表3。

表3 本机制在多终端上的兼容性测试结果

终端操作系统	可信身份告知	SDN 转换流表下发	可信地址通信
Windows 10	√	√	√
Ubuntu 16.04	√	√	√
MacOS 10.14.6	√	√	√
Android 9	√	√	√
iOS 12	√	√	√

在机制的性能测试方面，主要测试了本机制相比原始的 Portal 认证带来的额外时间开销，考虑本机制中额外增加了服务器之间的通信，包括 Portal 服务器和 SDN 控制器的通信、SDN 控制器和 SDN 交换机的通信，本文分别进行了时间开销测试。

Portal 服务器和 SDN 控制器的可信身份告知通信时延是本机制额外增加的，考虑终端到 Portal

服务器认证本来就有一定时延存在，所以这里分别测试了原始 Portal 认证时延和 Portal 服务器将可信身份告知给 SDN 控制器这一额外时延，时延测试 50 次，取平均值为最终测试结果，结果见表4。相比原始 Portal 认证时延，本机制增加的通信接口时延并不显著，不会影响到用户使用体验。值得注意的是，可信身份告知这部分额外时延可以通过调整网络拓扑被进一步优化。

表4 Portal 认证及额外通信时延

测试项目	时间开销
Portal 认证	1 416 ms
Portal 服务器告知可信身份	239 ms
总和	1 655 ms

其中，本机制用地址转换实现的可信地址分配机制带来的主要额外时间开销包括SDN控制器中的流表项生成时间开销和SDN控制器下发流表



到 SDN 交换机的时间开销这两部分,每部分测试 50 次取平均值,最后将两个平均值加和得到总的 SDN 设备额外时间开销,结果见表 5。可信地址和流表项生成的计算量在现有服务器算力基础上开销非常小,时延可以忽略,而网络拓扑的改变会显著影响流表下发时延,所以 SDN 控制器与 SDN 交换机不宜相隔太远。综合两项时延,SDN 设备的引入并不会带来明显时间开销,这一过程对用户来说仍是无感的。

表 5 基于地址转换的可信地址分配时延

测试项目	时间开销
可信地址及流表项生成	5.18 ms
流表项下发	32.41 ms
总和	37.59 ms

5 结束语

本文提出的基于 Portal 认证的 IPv6 可信地址分配机制,仅基于网络侧服务器的改造,适配 Portal 这种当前电信主流认证方式为用户分配可信地址,加强了对网络的管控。在 Portal 认证中由于终端未认证就获得了地址,为了实现对终端透明,所以对终端的地址统一采用可信地址转换的方法,同时也使本机制与地址分配方式无关,对于 DHCPv6 和 SLAAC 分配的地址均支持其到可信地址的转换。基于本机制实现的原型系统不仅在本地通过了测试,还接入江苏省南京市电信现网环境进行了测试,测试结果均符合预期。

参考文献:

- [1] Kaspersky DDoS intelligence report for Q3 [EB]. 2018.
- [2] WU J, BI J, BAGNUL M, et al. Source address validation improvement (SAVI) framework[R]. 2013.
- [3] WU J, BI J, LI X, et al. A source address validation architecture (sava) testbed and deployment experience[R]. 2008.
- [4] 颜敏,尹曾,杨熙.面向中小企业随选网络的自助服务平台 portal 研发实践[J].电信科学,2017,33(12): 170-177.

YAN M, YIN Z, YANG X. R&D practice of self-service platform portal for small and medium-sized enterprises[J]. Telecommunications Science, 2017, 33(12): 170-177.

- [5] ANDERSON D, BALAKRISHNAN H, FEAMSTER N, et al. Accountable internet protocol[Z]. 2008.
- [6] LEE T, PAPPAS C, BARRERA D, et al. Source accountability with domain-brokered privacy[C]//The 12th International Conference on emerging Networking Experiments and Technologies, December 12-15, 2016, Irvine, California, USA. New York: ACM Press, 2016: 345-358.
- [7] LIU Y, REN G, WU J P, et al. Building an IPv6 address generation and traceback system with NIDTGA in address driven network [J]. Science China Information Sciences, 2015, 58(12): 1-14.
- [8] 李智涛,刘莹,任罡. IPv6 地址生成系统基于 Web portal 的无客户端迁移方案[J]. 东南大学学报(自然科学版), 2017(S1): 80-85.
LI Z T, LIU Y, REN G, et al. Non-client migration scheme for IPv6 address generation system based on web portal[J]. Journal of Southeast University (Natural Science), 2017(S1): 80-85.
- [9] 周端奇,毕军,姚广. 基于 IPv6 源地址验证的一种可信身份系统[J]. 通信学报, 2014, 35(Z1): 20-26.
ZHOU R Q, BI J, YAO G. Trustworthy identity system based on IPv6 source address validation[J]. Journal on Communications, 2014, 35(Z1): 20-26.
- [10] DROMS R, BOUND J, VOLZ B, et al. Dynamic host configuration protocol for IPv6 (DHCPv6)[R]. 2003.
- [11] THOMSON S, NARTEN T, JJINMEI T. IPv6 stateless address autoconfiguration[R]. 2007.
- [12] IETF. IEEE 802.1x remote authentication dial in user service (RADIUS) usage guidelines: RFC 3580[S]. 2003.

[作者简介]



周江(1995-),男,清华大学研究生,主要研究方向为有线无线一体化安全接入。



李贺武(1974-),男,博士,清华大学副研究员,主要研究方向为无线移动网络、天地一体化信息网络。