



专题: IPv6 技术与应用

基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成方案

况鹏, 刘莹, 何林, 任罡

(清华大学网络科学与网络空间研究院北京信息科学与技术国家研究中心, 北京 100084)

摘要: 将可扩展的用户身份标识嵌入 IPv6 地址中, 不仅为追溯用户身份和精细管控用户行为提供可能, 而且有利于提高互联网的安全性、可审计性和可信性。目前提出的嵌入用户身份标识的 IPv6 地址生成方案存在 DHCPv6 客户端开发复杂或临时地址租约难以管理等问题, 均不易于实际部署。考虑到身份认证与地址分配之间的时序逻辑, 提出一种基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成方案, 通过在二层进行用户身份认证, 随后进行 IPv6 地址分配, 解耦了身份认证与地址分配过程, 避免了为各操作系统开发新的扩展 DHCPv6 客户端以及为 DHCPv6 服务器维护临时地址租约等限制, 更加具备可部署性。

关键词: 用户身份标识; IEEE 802.1x; DHCPv6

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019289

IEEE 802.1x-based user identity-embedded IPv6 address generation scheme

KUANG Peng, LIU Ying, HE Lin, REN Gang

Institute for Network Sciences and Cyberspace, Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China

Abstract: Embedding extensible user identities into IPv6 addresses not only provides the possibility of tracing the user identity and finely controlling the user behavior, but also helps to improve the security, auditability and credibility of the Internet. Current schemes that embed user identity within IPv6 address are hard to deploy in practice due to the complexity of DHCPv6 client development or the complicated management of temporary address. Considering the sequential logic between identity authentication and address allocation, a IEEE 802.1x-based user identity-embedded IPv6 address generation scheme was proposed. By conducting identity authentication using layer-2 mechanisms and then assigning IPv6 addresses, this scheme decoupled the process of identity authentication and address allocation, and avoided the limitation of developing new extended DHCPv6 clients for each operating system and maintaining temporary address leases on DHCPv6 servers, which was more deployable.

Key words: user identifier, IEEE 802.1x, DHCPv6

收稿日期: 2019-10-28; 修回日期: 2019-12-18

通讯作者: 何林, he-l14@mails.tsinghua.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61772307, No.61402257); 国家重点研发计划基金资助项目 (No.2018YFB1800405, No.2018YFB1800404, No.2017YFB0801701)

Foundation Items: The National Natural Science Foundation of China (No.61772307, No.61402257), The National Key Research and Development Program of China (No.2018YFB1800405, No.2018YFB1800404, No.2017YFB0801701)



1 引言

互联网在设计之初没有考虑对 IP 分组源地址的真实性进行验证,由此引发的源地址伪造问题给互联网的安全造成巨大的威胁,如何进行源地址验证、加强源地址的真实性和可信性成为互联网安全研究领域的重要内容之一。Ye^[1]提出的网络接入认证控制系统建设的技术方案从接入层面出发来解决不可信终端引发的安全问题。Wu 等^[2]提出源地址验证体系结构 (source address validation architecture, SAVA) 包含 3 个粒度: 接入网、域内和域间。其中, 接入层的解决方案源地址验证提高 (source address validation improvement, SAVI)^[3] 技术可以将源地址与主机接入点的链路属性绑定, 并用于后续过滤伪造源地址的报文。在保证源地址真实的情况下, 将源地址与其他标识空间关联映射可以扩展 IP 地址的内涵^[4-6]。基于 SAVI^[3] 的 NIDTGA^[7-8] 系统将可扩展的用户身份标识嵌入 IPv6 地址, 不仅为追溯用户身份和精细管控用户行为提供了可能, 而且提高了互联网的安全性、可审计性和可信性。

目前存在的嵌入用户身份标识的 IPv6 地址生成方案有两种: 第一种, 扩展 DHCPv6 协议^[7-8], 在交互消息中携带含有用户认证信息的选项, 在主机请求地址的过程中完成对用户的认证和嵌入用户身份信息的 IPv6 地址的下发。然而这种方式需要对 DHCPv6 客户端进行修改, 具有很大的开发和维护成本。第二种, 二次地址分配^[9], 即为主机分配租约期较短的临时地址, 在用户完成认证及临时地址过期后, 为主机分配嵌入用户身份信息的 IPv6 地址。这种方式避免了对 DHCPv6 客户端的修改, 但是较短的临时地址租约以及用户的不确定认证行为会增加 DHCPv6 服务器的负担, 较长的临时地址租约会影响用户体验。

本文通过分析用户认证和地址分配之间的时序逻辑关系, 提出一种基于 IEEE 802.1x 的嵌入用

户身份标识的 IPv6 地址生成方案。通过在二层进行用户身份认证, 随后进行 IPv6 地址分配, 解耦了身份认证与地址分配过程。本文方案既避免了对 DHCPv6 客户端的修改, 也避免了临时地址租约可能导致的 DHCPv6 服务器压力增大和用户体验下降的问题, 更加具备可部署性。

2 相关研究

2.1 IEEE 802.1x

IEEE 802.1x 协议是一种基于端口的网络接入控制协议, 可在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。类似于双因子认证^[10], IEEE 802.1x 协议协同端口及用户设备口令信息来验证用户身份。如图 1 所示, IEEE 802.1x 的认证系统通常包括客户端、设备端、认证服务器 3 个实体。客户端一般为一个用户终端设备, 通过 EAPOL 发起 IEEE 802.1x 认证, 设备端通常为支持 IEEE 802.1x 协议的网络设备, 对所连接的客户端进行认证, 认证服务器通常为 RADIUS 服务器, 用于实现对用户进行认证、授权和计费。

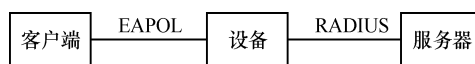


图 1 IEEE 802.1x 认证系统的体系结构

2.2 DHCPv6

IPv6 动态主机配置协议 DHCPv6 (dynamic host configuration protocol for IPv6)^[11] 是针对 IPv6 编址方案设计, 为主机分配 IPv6 地址/前缀和其他网络配置参数的一种带状态协议。

如图 2 所示, 使用 DHCPv6 协议分配 IPv6 地址涉及 4 步交互过程: 首先, DHCPv6 客户端发送 Solicit 报文寻找能够为其分配 IPv6 地址的 DHCPv6 服务器。其次, DHCPv6 服务器回复 Advertise 报文, 通知客户端可为其分配 IPv6 地址。然后, DHCPv6 客户端基于 Advertise 报文中服务器优先级等参数, 选择优先级最高的一台服务器,

向该服务器发送 Request 报文, 请求服务器确认为其分配 IPv6 地址。最后, DHCPv6 服务器回复 Reply 报文, 确认将 IPv6 地址分配给客户端使用。

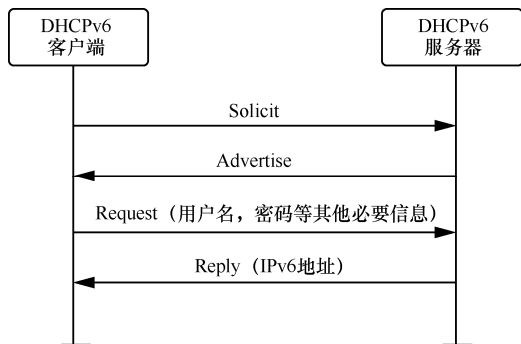


图2 IPv6 地址分配流程

2.3 NIDTGA

通过在 IPv6 地址中嵌入用户身份标识, 使用 SAVI^[3]机制确保 IPv6 源地址真实性, NIDTGA^[7-8]提供了一个可方便追溯用户身份、精细管理用户行为的 IPv6 地址生成与管理系统。NIDTGA 设计了一种可扩展的网络身份标识 NID, 用户登录时仅需要在 Request 消息中携带 NID 和密码, DHCPv6 服务器在收到消息后查询管理用户信息的 NID 管理服务器进行第三方认证, 认证通过后即将 NID 嵌入 IPv6 地址中并发送给 DHCPv6 客户端, 随后客户端主机自动配置上该 IPv6 地址。本文基于 NIDTGA 系统框架, 设计了一种全新的基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成方案, 旨在提高 NIDTGA 系统的可部署性。

3 嵌入用户身份标识的 IPv6 地址生成方案设计

3.1 设计选择

3.1.1 身份认证和地址分配的时序选择

为了向主机分配嵌入用户身份信息的 IPv6 地址, 身份认证和地址分配必须被正确有效地完成, 且身份认证必定发生在嵌入用户身份的地址分配过程之前, 如何选择两者的完成时序是 IPv6 地址生成与分配方案所面临的难点。扩展 DHCPv6 协

议^[7-8]的方案本质上是将上述两个过程融合, 即 DHCPv6 客户端与 DHCPv6 服务器交互的过程既为用户提供身份认证, 也为用户分配地址, 此方案面临的主要困难在于需要定制扩展 DHCPv6 客户端, 这涉及对主机各类操作系统的移植和维护。而二次地址分配方案^[9]本质上则是推迟了分配嵌入用户身份标识的 IPv6 地址的过程, 由于没有 IP 地址无法完成常见的 Web Portal 认证, 但为 DHCPv6 客户端分配临时地址为此提供了可能。此方案面临的主要困难则在于需要维护大量临时地址租约, 且需考虑如何为主机分配合适的租约以达到既不增加 DHCPv6 服务器的租约管理复杂度又不降低用户体验的目标。新方案的时序选择应尽量避免上述问题。

3.1.2 身份认证和地址分配方式的选择

其实, 并非没有 IP 地址就无法完成对用户的认证, 二层认证方案天然的在时序上占有优势。首先利用二层认证方案进行用户身份认证, 然后为主机分配嵌入用户身份信息的 IPv6 地址, 这使得身份认证和地址分配解耦, 避免了对主机侧的 DHCPv6 客户端的修改和大量的临时租约的维护。

目前常见的接入认证方式包括: MAC 地址认证、Web Portal 认证、PPPoE 认证和 IEEE 802.1x 认证。其中, MAC 地址认证适用于对无法提供账号和密码的哑设备进行认证, 如网络打印机等, 但在本系统里需要主机提供用户身份标识和密码进行认证, 因此 MAC 认证不满足系统的需求。Web Portal 认证的过程为: 用户主机首先通过 DHCP 协议获取 IP 地址, 但在认证之前访问任何网络资源时都会被重定向到 Portal 门户页面, 用户在该页面上输入账号和密码进行认证后, 便可以顺利访问网络资源。显然, Web Portal 认证也与本系统要求的先认证后分配地址的时序不符合。PPPoE 认证需要增添昂贵的 BRAS 设备, 而普通交换机一般自带 IEEE 802.1x 功能。据调研, 接入



CERNET2 的高校中,有超过 36%的高校表示在未来升级无线网络时愿意使用 IEEE 802.1x 认证,而只有 10%的高校愿意使用 PPPoE。因此本方案趋向于选择 IEEE 802.1x 作为主要的认证方案。

目前 IPv6 地址分配的方式可以分为两类,静态配置和动态分配,而动态分配方式则又包含无状态地址自动分配 (stateless address auto configuration, SLAAC)^[12]和有状态的自动分配(dynamic host configuration protocol for IPv6, DHCPv6)^[11]。由于需要在 IPv6 地址中嵌入用户身份标识,而静态配置需要用户手动地给主机配置 IPv6 地址,无法实现 IPv6 地址的统一配置,另外,无状态地址自动分配 (SLAAC) 只能通过 RA 报文配置主机 IPv6 前缀,无法完成用户身份标识的嵌入,因此 DHCPv6 是最佳选择。

3.2 设计难点

3.2.1 认证与地址分配关联

设计 IEEE 802.1x+DHCPv6 方案的主要难点在于如何正确且有效地将两个过程关联,即对于一个已通过 IEEE 802.1x 认证的用户,如何识别出其使用的 DHCPv6 客户端申请地址的请求。DHCPv6 协议采用 DUID 区分 DHCPv6 客户端,而 IEEE 802.1x 协议则采用用户名来区分用户。需要寻找一个属性来关联这两个过程。

由于 IEEE 802.1x 和 DHCPv6 都用到二层的 MAC 地址,因此 MAC 地址可以作为关联认证和地址分配的属性。IEEE 802.1x 可以将主机的 MAC 地址作为属性在 RADIUS 认证请求中携带,但是 DHCPv6 协议的 DUID 的生成方式有多种,使用 MAC 地址生成 DUID 只是其中最常见的方式。并且,主机往往含有多网卡,实时进行接入认证请求的网卡并非一定是生成 DUID 的 MAC 地址所属的网卡。因此,需要解决 DHCPv6 客户端地址请求归属网卡的 MAC 地址传递问题。该问题的解决办法是由第一跳 DHCPv6 中继在地址请求消息里携带客户端的 MAC 地址,目前该方法已由

IETF 标准化为 RFC6939^[13]。因此,可以通过 MAC 地址关联用户认证和地址分配过程。具体的关联方式如图 3 所示,在客户端与 RADIUS 服务器进行 IEEE 802.1x 认证过程中,客户端会发送 EAP-Response Identity 报文,该报文会携带用户身份 UID 及主机 MAC 地址,RADIUS 服务器验证通过后会将该 MAC 地址发送给 DHCPv6 服务器。在 DHCPv6 地址分配过程中,DHCPv6 客户端发送给 DHCPv6 消息会携带 DUID 标识符,该标识符嵌入了主机的 MAC 地址,DHCPv6 服务器可以基于 DUID 识别客户端身份。

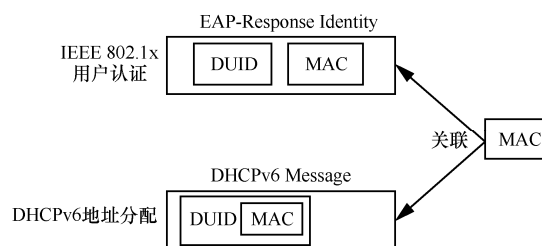


图3 用户认证与地址分配关联

3.2.2 大规模部署

为了增强方案的大规模部署能力,新设计的方案应该具有容易被各个管理域和用户接受采纳的特性。新方案至少应该具备以下特性。

- 无需用户主机侧修改,即用户无需更改主机配置,无需安装要求高权限的客户端。例如,扩展 DHCPv6 协议的方案需要为各个操作系统开发定制的 DHCPv6 客户端,这增加了开发成本和部署难度,在部分操作系统上要求高权限也降低了用户体验。
- 不增加地址租约管理难度。新方案与原始 DHCPv6 协议相比,不能增加较大的租约管理难度以及处理开销。目前的临时地址方案则会增大 DHCPv6 服务器的租约管理难度。
- 新方案使用的机制应避免对现有网络设备的大规模更新,现有网络设备支持使用的

机制且对各个管理域改动较少会增大新方案被采纳的可能。

3.3 基本思想

本方案设计的基本思想如图 4 所示, 用户首先采用 IEEE 802.1x 进行身份认证, RADIUS 服务器采集用户认证信息及主机的 MAC 地址, 认证完毕后, RADIUS 服务器向 DHCPv6 服务器发送已认证用户列表, DHCPv6 服务器接收到客户端请求后查询已认证用户列表获取当前地址请求对应的用户身份标识, 并生成嵌入该身份标识的 IPv6 地址, 最后, DHCPv6 服务器向客户端下发该 IPv6 地址。

3.4 登录流程

综上所述, 基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成系统的流程如图 5 所示。

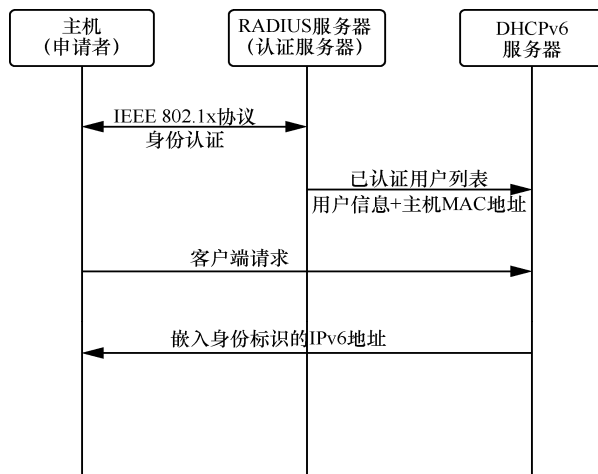


图 4 IEEE 802.1x+DHCPv6 基本流程

基于 IEEE 802.1x 的用户身份认证的步骤如下。

- (1) 主机发送 EAPOL 报文发起认证过程。
- (2) 无线 AC 或交换机收到 EAPOL Start 报文后, 发送 EAP-Request Identity 报文响应主机的认

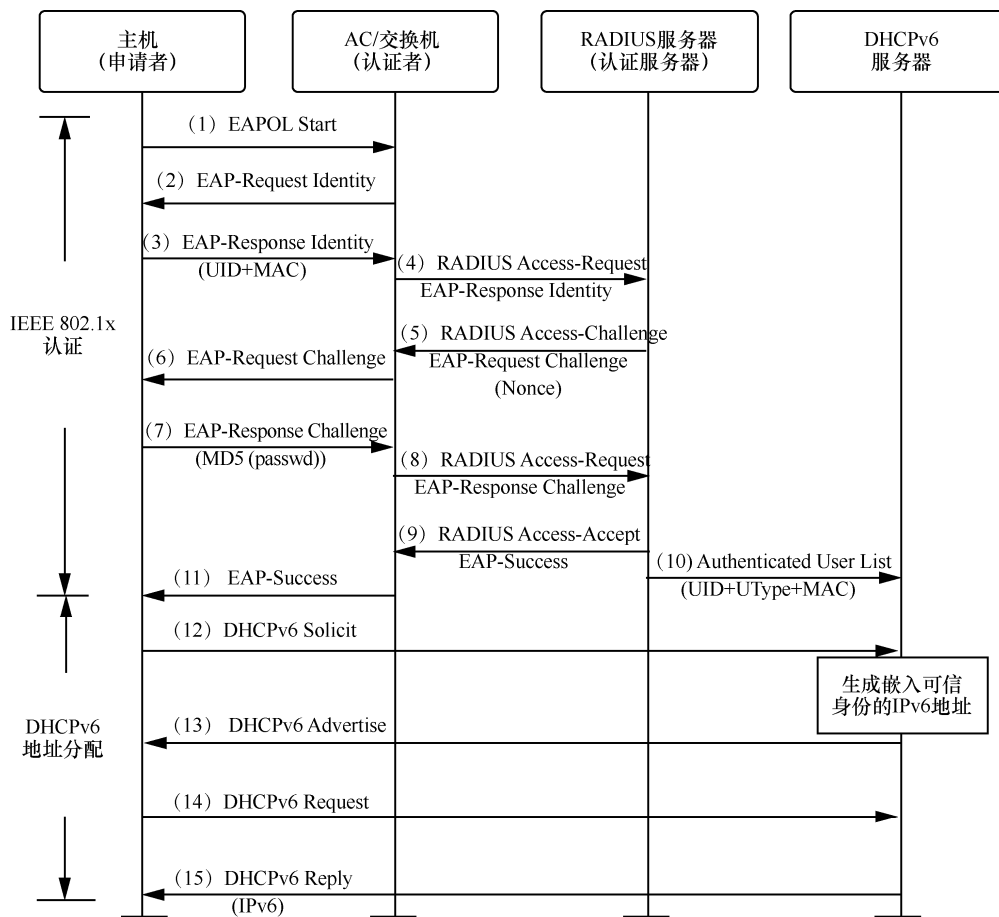


图 5 基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成和分配流程



证请求, 请求主机的用户身份标识。

(3) 主机回复 EAP-Response Identity 报文响应 EAP-Request Identity, 将用户身份标识发送给无线 AC 或交换机。

(4) 无线 AC 或交换机将用户身份标识、MAC 地址等信息封装在 RADIUS Access-Request 报文中并发送给 RADIUS 服务器。

(5) RADIUS 服务器提取出 RADIUS Access-Request 报文中的用户身份标识并在用户数据库中查找。如果查找失败, 则丢弃该报文; 如果该用户身份标识存在, 则提取出对应的用户密码等信息, 然后随机生成一个密码字, 并用该密码字进行 MD5 加密, 得到并保存密文。同时将该密码字封装在 RADIUS Access-Challenge 报文中, 发送给无线 AC 或交换机。

(6) 无线 AC 或交换机收到 RADIUS Access-Challenge 报文后, 向主机转发其中的 EAP-Request Challenge 报文。

(7) 主机用 RADIUS 服务器发来的随机加密字与其密码等信息进行相同的加密算法运算, 将生成的密文封装在 EAP-Response Challenge 报文中并发送给无线 AC 或交换机。

(8) 无线 AC 或交换机收到 EAP-Response Challenge 报文后将其封装在 RADIUS Access-Request 报文中并发送给 RADIUS 服务器。

(9) RADIUS 服务器解析 RADIUS Access-Request 报文后得到主机生成的密文, 并与第(5)中的密文进行对比, 如果一致, 则认证成功, 将 EAP-Success 消息封装在 RADIUS Access-Accept 报文中, 发给无线 AC 或交换机; 如果不一致, 则回复 RADIUS Access-Reject 报文。

(10) RADIUS 服务器将已认证用户列表<用户名, 用户类别, MAC 地址>发送给 DHCPv6 服务器。

(11) 无线 AC 或交换机收到 RADIUS 服务器发来的 RADIUS Access-Accept 报文后提取 EAP

Success 报文并转发给主机。

使用 DHCPv6 获取嵌入用户身份标识的 IPv6 地址的步骤如下。

(12) 主机收到 EAP-Success 消息后, 发起 DHCPv6 Solicit 消息请求查询可为其分配地址的 DHCPv6 服务器。

(13) DHCPv6 服务器收到 Solicit 报文后提取出 MAC 地址, 并在已认证用户列表<用户名, 用户类别, MAC 地址>中查找, 如果查找到该 MAC 地址, 则使用对应的用户身份信息生成 IPv6 接口标识, 然后组合 56 bit 的 IPv6 前缀、8 bit 的用户类别标识以及 64 bit 的 IPv6 接口标识生成 IPv6 地址, 并返回 Advertise 消息; 否则, 丢弃报文。

(14) 主机收到 DHCPv6 Advertise 消息后, 发送 DHCPv6 Request 消息请求地址。

(15) DHCPv6 服务器响应 Reply 消息分配地址, 主机收到 DHCPv6 Reply 消息后配置 IPv6 地址。

4 嵌入用户身份标识的 IPv6 地址生成方案评估

4.1 实验拓扑

按照图 6 的网络拓扑部署本文提出的基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成和分配方案。AP 上开启一个新的名为“NIDTGA-IEEE 802.1x”的 SSID, 并开启 IEEE 802.1x 认证。AC 上开启 RADIUS 客户端功能, 并指向 RADIUS 服务器。第一跳 DHCPv6 Relay 中开启 RFC6939^[13]功能, 使其支持在 Relay-Forward DHCP 消息中携带 MAC 地址选项, 以实现 MAC 地址关联用户认证和地址分配过程。RADIUS 服务器开启 RADIUS 认证功能, 其会对主机用户名及密码进行验证。DHCPv6 服务器扩展了 DHCPv6 协议, 其会维护 IPv6 地址分配相关状态, 并为主机分配嵌入用户身份标识的 IPv6 地址。

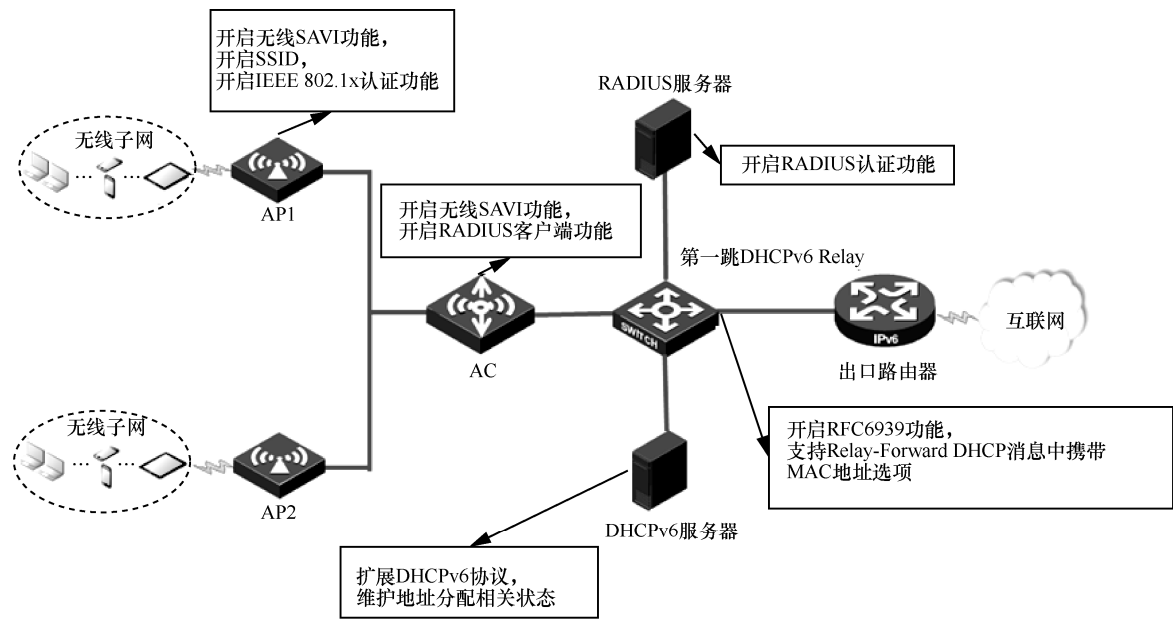


图6 系统部署拓扑

4.2 实验评价

首先验证了系统的正确性和有效性。分别测试了装有 Windows10、CentOS 和 iOS 操作系统的主机，DHCPv6 服务器使用开源的 KEA DHCP 软件。嵌入用户身份标识的 IPv6 地址生成功能可以内嵌在 KEA DHCPv6 服务器代码中实现（以下简称地址生成内嵌方案），也可以另行实现并通过网络通信将生成的地址发送给 DHCPv6 服务器（以下简称地址生成外放方案）。每台主机通过连接 SSID “NIDTGA-IEEE 802.1x”，在弹出的认证框里输入用户名和密码，认证完成后获得嵌入用户身份标识的 IPv6 地址并可以访问外网，具体见表 1。

还测试了完成一次用户身份认证以及获取嵌入用户身份标识的 IPv6 地址的时间，测试共计 100 次，并计算平均时间开销。其中，对用户采用 IEEE 802.1x 认证平均耗时为 302 ms，地址分配测

试结果见表 2。由表 2 可知，地址生成内嵌方案在实现嵌入用户身份标识的情况下，地址分配的时间和原始 DHCPv6 的时间相差约为 41 ms，时间增长 4.58%，是可以被接受的。而地址生成外放方案则使用了约 2 125 ms，比原始 DHCPv6 多使用 1 099 ms。多出的时间主要用于外放的地址生成服务和 DHCPv6 服务器通信。用户从认证到使用地址生成内嵌方案获取嵌入用户身份的 IPv6 地址的总时间为 1 506 ms，这对于用户是无感知的，不影响用户体验。

表2 IPv6 地址分配时间对比

方案	耗时
原始 DHCPv6	1 026 ms
地址生成内嵌方案	1 067 ms
地址生成外放方案	2 125 ms

表1 IPv6 地址分配情况

主机	NID	IPv6
Windows10	80000b1cc5	2402:f000:3:481:a203:72d0:336:366d
CentOS	80000d86b0	2402:f000:3:481:41d9:9d81:7d58:6cfa
iOS	8000000001	2402:f000:3:481:a149:332b:60ae:9962



表 3 3 种方案可部署性评估

方案	是否需要开发 DHCPv6 客户端	是否需要维护临时地址租约	网络设备需要支持
扩展 DHCPv6	是	否	SAVI
二次地址分配	否	是	SAVI
IEEE 802.1x 方案	否	否	SAVI、IEEE 802.1x

表 4 主流操作系统对 IEEE 802.1x 认证的支持

操作系统	Windows	Linux	MAC OS X	iOS	Android
支持情况	Windows XP 起均支持	主流发行版均支持	MAC OS X 10.3 起均支持	iOS 2.0 起均支持	Android 1.6 起均支持

为了评估扩展 DHCPv6 协议、二次地址分配、IEEE 802.1x 方案的可部署性, 本文对是否需要开发 DHCPv6 客户端、是否需要维护临时地址租约、是否需要网络设备功能等指标进行了评估, 结果见表 3, 扩展 DHCPv6 协议方案需要针对不同操作系统定制开发 DHCPv6 客户端, 不利于实际部署使用; 二次地址分配方案不仅需要 DHCPv6 服务器多次对续约 RENEW 消息进行处理, 还需要其管理临时地址的分配及回收, 降低了 DHCPv6 服务器的并发处理能力, 不利于大规模使用; IEEE 802.1x 方案对 DHCPv6 客户端以及 DHCPv6 服务器没有过多的要求, 唯一的附加点是需要操作系统及网络设备提供对 IEEE 802.1x 协议的支持, 从表 4 及表 5 中可知, 当前主流操作系统及网络设备均提供了对 IEEE 802.1x 协议的支持, 综上所述, IEEE 802.1x 方案具备最佳的可部署性。

表 5 网络设备对 IEEE 802.1x 认证的支持

网络设备支持情况	AP	AC	交换机
华为	支持	支持	支持
华三	支持	支持	支持
锐捷	支持	支持	支持
Cisco	支持	支持	支持

5 结束语

本文提出了一个基于 IEEE 802.1x 的嵌入用户身份标识的 IPv6 地址生成与分配方案, 通过将用户身份认证和地址分配流程解耦, 在二层进行身份认证, 继而再进行地址分配, 很好地解决了目前嵌入用户身份标识的 IPv6 地址生成方案存在的问题, 不仅避免了对 DHCPv6 客户端的修改, 也避免了对 DHCPv6 协议的扩展。此外, 该方案还不需使用临时地址, 避免了临时地址租约的维护。基于以上这些优点, 本方案在实际部署方面占有很大优势, 目前即将在教育网进行大规模地部署。

参考文献:

- [1] 叶水勇. 基于网络接入认证对终端设备的管控研究[J]. 电力信息与通信技术, 2018, 16(5): 41-46.
YE S Y. Research on management and control of terminal equipment based on network access authentication[J]. Electric Power Information and Communication Technology, 2018, 16(5): 41-46.
- [2] WU J, BI J, LI X, et al. A source address validation architecture (sava) testbed and deployment experience[R]. 2008.
- [3] WU J, BI J, BAGNULO M, et al. Source address validation improvement (SAVI) framework[R]. 2013.
- [4] ANDERSEN D G, BALAKRISHNAN H, FEAMSTER N, et al. Accountable internet protocol (AIP)[C]//ACM SIGCOMM 2008 Conference on Data Communication, August 17-22, 2008,

Seattle, WA, USA. New York: ACM Press, 2008: 339-350.

- [5] NAYLOR D, MUKERJEE M K, STEENKISTE P. Balancing accountability and privacy in the network[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(4): 75-86.
- [6] LEE T, PAPPAS C, BARRERA D, et al. Source accountability with domain-brokered privacy[C]//The 12th International on 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] LIU Y, REN G, WU J, 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.
- [9] 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. Non-client migration scheme for IPv6 address generation system based on Web portal[J]. Journal of Southeast University(Natural Science Edition), 2017(S1): 80-85.
- [10] 李晓伟, 杨邓奇, 陈本辉, 等. 基于生物特征和口令的双因子认证与密钥协商协议[J]. 通信学报, 2017, 38(7): 89-95.
LI X W, YANG D Q, CHEN B H, et al. Two-factor authenticated key agreement protocol based on biometric feature and password[J]. Journal on Communications, 2017, 38(7): 89-95.
- [11] DROMS R, BOUND J, VOLZ B, et al. Dynamic host configuration protocol for IPv6 (DHCPv6)[R]. 2003.
- [12] THOMSON S, NARTEN T, JINMEI T. IPv6 stateless address autoconfiguration[R]. 2007.
- [13] HALWASIA G, BHANDARI S, DEC W. Client link-layer address option in DHCPv6[R]. 2013.

[作者简介]



况鹏 (1995-), 男, 清华大学网络科学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。



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



何林 (1991-), 男, 清华大学网络科学与网络空间研究院博士后, 主要研究方向为网络结构和协议设计。



任罡 (1979-), 男, 清华大学网络科学与网络空间研究院副研究员, 主要研究方向为网络结构设计、下一代互联网结构和网络安全。