IPv6 地址结构标准化研究综述

张千里 姜彩萍 王继龙 李 星
(清华大学网络科学与网络空间研究院 北京 100084)

摘 要 随着 IPv6 网络商用化的进行和大面积部署,IPv6 相关的研究正在成为新的研究热点.相对于 IPv4 而言,IPv6 地址有 128 比特,因此其生成、使用、安全等方面的情况也要比 IPv4 复杂得多,而对 IPv6 地址结构的深入了解,是进行 IPv6 地址规划、IPv6 网络测量、IPv6 网络安全以及下一代互联网网络体系结构等方面研究的基础.涉及 IPv6 地址结构方面的互联网标准数量众多、内容涵盖面广,这些都不利于全面了解 IPv6 地址结构.本文总结了目前 IPv6 地址结构相关的标准,包括 IPv6 全球单播地址结构、IPv6 组播地址结构、IPv6 任播地址结构等,在简要介绍各种地址结构的基础上,特别介绍了 IPv6 地址结构中几个和 IPv4 显著不同的地方.首先,IPv6 地址通常可以分成子网前缀和接口标识两个部分,与 IPv4 相比 IPv6 增加了接口标识生成方案,而且 IPv6 接口标识的生成方案与 IPv6 安全和隐私保护紧密相关;其次,IPv6、IPv4 将长期共存,因此过渡技术必不可少,而过渡技术中的地址结构与普通 IPv6 地址有所不同;最后,IPv6 网络中多宿主机的情况更加普遍,导致了广泛存在的地址选择问题.针对这一问题,除了通过建立 IPv6 网络的源地址选择策略和目的地址选择策略来解决之外,定位符与身份标识分离也提供了一种解决思路.随着 IPv6 的进一步广泛部署,物联网中的 IPv6 地址结构以及 IPv6 地址安全方面的研究得到了越来越多的关注.物联网的广泛应用促使 IPv6 加速部署,但由于物联网本身的一些特点如最大报文长度较短、要求能耗较低等,物联网中 IPv6 的接口标识生成方案通常要保证所生成的接口标识便于压缩.另一个得到越来越多重视的研究方向是 IPv6 地址安全,与 IPv4 网络的情况有所不同,IPv6 网络欠缺大规模使用的安全经验,大量支持 IPv6 的设备对 IPv6 协议的实现也只实现了基本功能,而由于 IPv6 较 IPv4 有更为复杂的应用场景,因此 IPv6 网络的安全问题逐渐成为一个突出的问题.本文对这些方面的研究进行了简要的介绍.

关键词 IPv6 地址;IPv6 网络管理;IPv6 网络安全
中图法分类号 **DOI 号** 10.11897/SP.J.1016.2019.01384

A Survey on IPv6 Address Structure Standardization Researches

ZHANG Qian-Li JIANG Cai-Ping WANG Ji-Long LI Xing
(*Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing* 100084)

Abstract With the commercialization and wide deployment of IPv6 network, IPv6 related research is becoming a new research hotspot. Compared with IPv4, IPv6 address has 128 bits; its generation, application and security are much more complicated. The understanding of IPv6 address structure is of great value in researches like IPv6 address planning, network measurement, network security and next generation Internet architecture. There are a number of RFC standards related to IPv6 address structure; these standards cover a wide range of topics, which makes it difficult to understand the IPv6 address structure comprehensively. This paper summarizes current IPv6 address structure related standards, including IPv6 global unicast address structure, IPv6 multicast address structure, IPv6 anycast address structure. Based on the brief introduction of various address structures, several significant differences between IPv4 and IPv6 address structures

收稿日期:2018-05-14;在线出版日期:2018-12-28.本课题得到国家重点研发计划项目(2017YFB0503703)资助.**张千里**,博士,副研究员,主要研究方向为下一代互联网体系结构、网络安全等.E-mail:zhang@cernet.edu.cn.**姜彩萍**,硕士,高级工程师,主要研究方向为计算机网络等.**王继龙**,博士,教授,主要研究领域为下一代互联网体系结构、网络测绘等.**李 星**,博士,教授,主要研究领域为下一代互联网体系结构、网络安全、网络测量等.

are introduced. Firstly, IPv6 addresses can be divided into two parts: subnet prefix and interface identifier. Compared with IPv4, IPv6 interface identifier has its own generation method, and IPv6 interface identifier generation scheme is close related to IPv6 address security and privacy. Secondly, IPv6 and IPv4 will coexist for a long time; therefore transition technology is widely deployed. IPv6 address in transition technology is often different from that in normal situation. Finally, multihoming is more common in IPv6 networks, which results in the difficulty in address selection. To deal with this problem, one approach is to establish source address selection policy and destination address selection policy. Another solution is locator/identifier separation related schemes. With the further deployment of IPv6, IPv6 address structure in the Internet of Things, and IPv6 address security have absorbed growing research interest. The widespread application of the Internet of Things has accelerated the deployment of IPv6. However, due to the limitation of the Internet of Things itself, such as the smaller MTU and limited energy capacity, generation scheme usually needs to ensure that the generated interface identifier is easy to compress. Another research topic is IPv6 address security. Unlike IPv4, IPv6 lacks security experience in large-scale application. Moreover, a large number of devices only support IPv6 in a basic manner, but IPv6 has more complicated application scenarios than IPv4. The IPv6 security situation has worsened for the above reasons; this article provides a brief introduction on these aspects.

Keywords　IPv6 address; IPv6 network management; IPv6 network security

1　引　言

互联网上的每一个节点都依靠 IP 地址互相区分和相互联系，IP 地址成了整个互联网互联互通、身份区分的基础. 互联网体系结构中，网络应用、网络路由、网络安全和管理，都围绕着 IP 地址而来. 随着 IPv4 地址的逐渐耗尽和物联网的大面积推广，IPv6 正在以越来越快的速度走向大规模商用，这要求网络工程师和研究者对 IPv6 技术具有更加深入的了解. 与 IPv4 相比，IPv6 最大的特点就是具有大得多的地址空间，这一巨大的地址空间，为各种新应用的开展提供了可能，同时，也带来了 IPv6 地址生成、使用、安全等多方面的问题.

IPv6 地址生成方面的挑战主要在于如下几点. 首先，IPv6 地址具有 128 比特，其生成方式较 IPv4 要复杂得多. IPv6 地址可以清晰地分成两个部分，即用于网络路由的子网前缀(subnet prefix)和用于子网内寻址的接口标识(Interface ID，IID)[1]，这两部分的生成方式有所不同：一般而言，子网前缀是在进行 IPv6 组网时，终端用户通过运营商、地区互联网注册中心(Regional Internet Registry，RIR)、互联网数字分配机构 IANA(The Internet Assigned Numbers Authority)等一层一层分配得来，而用户接口标识的生成方案是 IPv6 所独有的问题，接口标识长度较长，如何能够既可以承载新的功能，同时又不产生额外的安全风险，需要进行精心的设计. 第二个挑战在于，IPv6 的应用场景较为复杂，例如由于更广泛的物理网络支持所带来的不同，如 IPv6 在用于 802.15.4 网络[2]中时，为便于包头压缩，经常需要对 IPv6 地址进行压缩，因此需要生成便于压缩的地址. 此外，无状态自动配置方式(Stateless Address Autoconfiguration，SLAAC)[3]也为 IPv6 所独有，这也使得 IPv6 地址生成方式更为复杂.

作为 IPv6 网络体系结构的一部分，IPv6 地址需要满足各种层出不穷的应用需求，IPv6 有很多不同于 IPv4 网络中的新情况出现. 首先，在 IPv6 网络中，需要考虑过渡方面的地址规划问题①. IPv6 过渡方案便于在 IPv4 网络向 IPv6 网络演进的过程中，业务的共存和互相访问，而过渡方案中 IPv6 的地址指定方式与普通情况颇有不同. 其次，在 IPv6 网络中，多宿的情况要比 IPv4 中普遍得多，很多 IPv6 节点都具有多个前缀及地址，因此如何进行地址选择，或者如何能够屏蔽地址选择所带来的问题，也是一个重要的研究课题. 最后，IPv6 具有单播地址、组播地址、任播地址等地址类型，由于地址空间较大，使

① IETF Softwires (softwire) Working Group. https://datatracker.ietf.org/wg/softwire/about/

得可以针对不同的应用需求设计新的地址结构.对标准化的地址结构进行研究,有助于研究者理解新应用方案中地址的设计.

随着 IPv6 网络的不断发展,IPv6 安全风险也开始得到众多研究者的关注.尽管 IPv6 地址有 128 比特,大大减少了被扫描的风险,但是 IPv6 地址长度的增加,以及一些地址生成方式的问题,导致了 IPv6 用户可能面临事件追踪与关联等风险,从而可能导致用户隐私泄露.IPv6 安全风险的另外一个方面来自于 IPv4 网络中的各种方案和设计已经经历了长时间大规模的实际考验,相对而言较为成熟,而 IPv6 中的大部分设计和应用还缺乏时间、规模方面的考验,因此可能存在着一些安全隐患,而众多 IPv6 开发者或设备厂商,对 IPv6 的实现也仅仅是最基本的,这也是 IPv6 网络安全风险的一个来源.最后,由于 IPv6 应用场景复杂,各种问题容易交织在一起,形成新的安全风险.因此随着 IPv6 的大规模商用,近年来 IPv6 安全风险方面的研究也越来越多,其中相当一部分都是与地址相关的.

针对这些问题已经有相当多的研究,其中一些被广泛认可的研究成果以 IETF RFC 的形式发表出来.互联网工程任务组 IETF(Internet Engineering Task Force)从 1995 年[4]起,即开始推动 IPv6 的发展,二十多年来,大量 IPv6 地址结构相关的 RFC 得到发表,内容涵盖了单播地址结构、组播地址结构、任播地址结构、路由选择、IPv6 过渡、IPv6 安全和隐私保护、物联网等多个领域,大量的标准对于全面了解 IPv6 地址结构造成了较大的困难.本文将通过梳理这些标准,全面介绍地址生成、使用和安全方面的以 IETF RFC 形式发表的成果,这样一方面有助于知晓现有地址使用方案可能存在的问题,从而提出更有吸引力的解决方案;另一方面,也有助于 IPv6 地址规划、网络测量、网络安全、网络体系结构等领域研究工作和标准化工作的开展.除非特别指出,本文中所提及的 RFC 均为当前使用的有效版本.

本文第 2 节将介绍 IPv6 地址的总体结构;第 3 节将介绍全球单播地址结构,包括特殊的单播地址、全球单播地址的分配、规划、获得和运维等;第 4 节和第 5 节将分别介绍 IPv6 组播地址结构和 IPv6 任播地址结构;第 6 节将介绍过渡方案中 IPv6 地址结构;第 7 节将介绍 IPv6 接口标识生成方案与相关的隐私保护和安全问题;第 8 节将针对 IPv6 下更为普遍的多宿主机问题,介绍相关的地址选择、路由选择以及定位与身份标识分离方面的研究;第 9 节将简要阐述未来 IPv6 地址体系结构标准化研究方向;最后在第 10 节进行总结.

2 IPv6 地址结构概述

IPv6 地址结构最早定义于 RFC1884[4],之后经过 RFC2373[5]、RFC3513[6]的几次更改,最终形成了目前有效的版本 RFC4291[1],IPv6 的文本表示法也于 RFC5952[7]中确定,IPv6 地址通常使用冒号十六进制形式表示,即 x:x:x:x:x:x:x:x,每个 x 都以十六进制表示一个 16 比特长的整数,且里面的字母用小写表示,如 2402:f000:9:3001:9bb7:0:0:1.其中多个 0 块可以由双冒号符号“::”表示,但此符号只能在地址中出现一次.例如,地址 2402:f000:9:3001:9bb7:0:0:1 的压缩形式为 2402:f000:9:3001:9bb7::1.IPv6 地址前缀的表示方法类似于 IPv4 中的 CIDR 表示方法,使用地址前缀和前缀长度来标识,如 2000::/3.

根据 RFC4291[1],IPv6 地址按照其用途可以分为单播、组播和任播三种地址,单播地址标识了一个接口,组播地址标识了一组接口,任播地址在单播地址区间内分配,但是可以指定给多个接口(通常属于不同节点),发送到这些地址的数据包被路由到最近的一个接口,这三类 IPv6 地址分别实现了不同的需求,如图 1 所示.

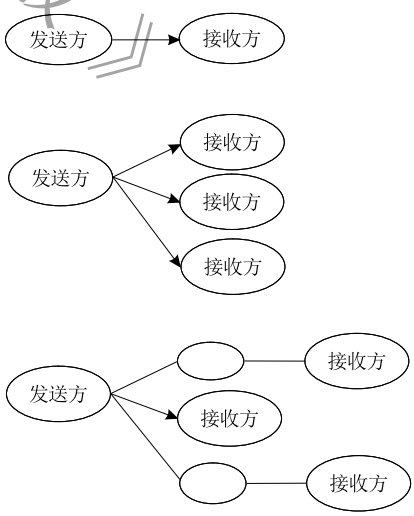

图 1 单播(上)、组播(中)和任播(下),单播地址标识了一个接口,对应一个接收方;组播地址标识了一组接口,具有多个接收方;任播地址可以指定给多个接口,发送到任播地址的数据包被路由到最近的一个接口

总体而言,互联网工程任务组负责互联网协议标准化方面的工作,IETF 的技术文档以 RFC 形式

发表，而地址的具体分配则最终在互联网数字分配机构 IANA(The Internet Assigned Numbers Authority)完成. 关于 IPv6 地址的规划，可以大致按照前 3 比特来理解，::/3 用于分配特殊地址，常常用于 RFC 中指定具有特殊意义的 IPv6 地址；2000::/3 作为全球单播地址，是各个运营商、用户等得到的地址；唯一本地地址、链路本地地址以及组播地址在最后的 e000::/3 地址块中，IPv6 地址空间的大致分配方案如表 1 所示.

表 1　IPv6 的地址空间分配概况

地址块	分配用途及其 RFC 来源
0:0:0:0:0:0:0:0- 1ff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC4291[1]
200:0:0:0:0:0:0:0- 3ff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC4048[8]
400:0:0:0:0:0:0:0- 1fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC4291[1]
2000:0:0:0:0:0:0:0- 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	全球单播地址 RFC4291[1]
4000:0:0:0:0:0:0:0- fbff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC4291[1]
fc00:0:0:0:0:0:0:0- fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	唯一本地单播地址 (Unique Local Unicast) RFC4193[9]
fe00:0:0:0:0:0:0:0- fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC4291[1]
fe80:0:0:0:0:0:0:0- febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff	链路单播地址 RFC4291[1]
fec0:0:0:0:0:0:0:0- feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	IETF 保留 RFC3879[10]
ff00:0:0:0:0:0:0:0- ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	组播地址 RFC4291[1]

::/3 地址块通常用于分配那些不能全球路由的、具有特殊语义的地址. 在 RFC4291[1] 中，定义了几个和 IPv6 套接字编程相关的特殊 IPv6 地址，如::1/128 是单播绕回地址，如果一个应用程序将数据包送到此地址，IPv6 堆栈会转送这些数据包到同样的接口(相当于 IPv4 中的 127.0.0.1/8)，而::/128 为未指定地址，它的所有比特皆为零，这个地址不可指定给任何网络接口，通常用于套接字编程中代表本地的未指定接口. RFC4038[11] 中定义的地址块::ffff:x.y.z.w/96，用于 IPv4 地址 x.y.z.w 映射成的 IPv6 地址，对于双栈系统上的纯 IPv6 应用，在接收到 IPv4 请求的时候可以将 IPv4 地址映射为这一块中对应的 IPv6 地址，从而便于纯 IPv6 应用处理. RFC6666[12] 中定义了 100::/64，目的地址为该地址块的流量将被丢弃，这一地址块主要用于定义于 RFC5635[13] 和 RFC3882[14] 的远程被触发黑洞(Remote Triggered Black Hole，RTBH)中. RTBH 技术将发往被攻击者的流量通过隧道转给流量监听节点进行分析. 这些方法中都将具有特定源或目的的地址的下一跳指向一个单播前缀，而这一单播前缀与路由器的 discard、null 或隧道接口相连接. 为了不与全球单播地址相混淆，特别约定使用 100::/64 这一单播前缀. 一些过渡措施也使用了::/3 网段的地址，这些相关研究将在第 6 节过渡方案中进行详细介绍.

2000::/3 为全球单播地址，也是大多数 IPv6 网络使用的 IPv6 地址来源，可以供全球运营商进行分配，我们将在第 3 节介绍这一地址块的更详细的相关标准化工作.

除了全球单播地址之外，RFC 4193[9] 定义了 fc00::/7 作为唯一本地单播地址(Unique Local Unicast，ULA)，格式如图 2 所示，如果 L 比特为 1 说明是本地指定的，全局标识(Global ID)是一个 40 比特伪随机数，16 比特的子网标识(Subnet ID)用来标识本地的子网. 这一地址虽然是单播地址，但不可全球路由，因此通常被用于进行本地通信，且同时具有全局唯一特性，它们不应出现在全球 IPv6 路由表中，主要用来方便若干个本地 IPv6 网络互联.

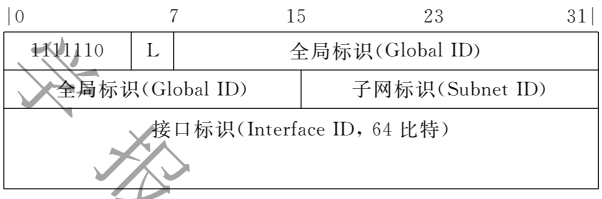

图 2　唯一本地单播地址

RFC4291[1] 也定义了 fe80::/10 这一链路本地地址用于本地连接，格式如图 3 所示，中间 54 比特为 0，后面 64 比特为接口标识，这些地址只在链路本地有效，通常用于自动地址配置、邻居发现等.

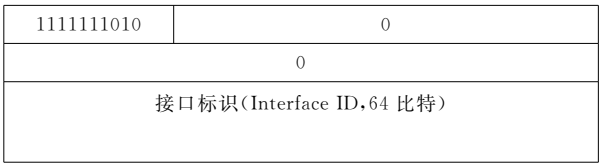

图 3　链路本地地址

组播地址的分配方式与全球单播地址相比要简单一些，对于临时的组播地址，可以由各个用户自由指定，但是使用范围通常受到约束. 对于永久的组播地址，则需要向 IANA 申请，由于 IPv6 中没有广播，因此使用广播的众多应用都需要以组播来替代.

除了 IETF 本身的 RFC 标准可以向 IANA 申请分配永久组播地址之外，其他的标准化组织机构也可以向 IANA 申请永久组播地址.

任播地址是在单播地址的空间中分配，既可以是通过 BGP 配置的全球任播地址，也可以是运营商通过自己的内部路由配置来实现的局部任播地址，IETF 的 RFC 标准中定义了一些知名的任播地址.

在 IPv6 的发展过程中，一些地址或者用法会由于种种原因被废弃，例如曾用于 IPv4 兼容地址的::/96，现已废除. 用于指明地址只在站点范围内有效的站点本地地址 fec0::/10，也已在 2004 年 9 月的 RFC3879[10] 中被舍弃，新的实现中不应该支持这类型的地址.

3 IPv6 全球单播地址结构

在 IPv6 网络的使用和运行中，我们接触到的地址一般都是全球单播地址，来自于 2000::/3 地址块，定义于 RFC4291[1]. 从全球单播地址块到最终用户，需要经历多个过程. 首先，在 IETF 的 RFC 中可以将其中的地址块作为具有特殊意义的地址块分配出去，其它的 IPv6 地址，一般以大块的形式分配给各个地区互联网注册中心(Regional Internet Registry, RIR)，各个互联网运营商 ISP 则从自己所属的 RIR 处获得/32 大小的地址块，然后再将这些地址块分配给自己的成员单位，成员单位会进一步将地址块以/64 或更大的地址块为基础进行切割，从而规划自己的网络. 在设计完成后，子网内的接入节点还需要根据不同的地址生成方式，来得到接口标识，本节将针对这些方面进行分别介绍.

3.1 RFC 中定义的全球单播地址

一些具有特殊意义的单播地址，没有分配在::/3地址块中，而是分配到了 2000::/3 地址块中，究其原因，主要是这些特殊的地址块，本身也需要全球可路由，因此不太适合分配在::/3 地址块中. RFC 中直接分配的全球单播地址，主要是为了满足各种特殊用途，如测试文档用的 IPv6 地址块. 定义于 RFC5180[15] 的 2001:2::/48，在 IPv6 的测试时使用；定义于 RFC3849[16] 的 2001:db8::/32，主要用于文档示例中.

此外，随着时间的变迁，一些直接分配的地址也已经被废止，如定义于 RFC2471[17] 的 6bone 地址 3ffe::/16，已经于 2006 年 6 月的 RFC3701[18] 中废止. 有关当前 IPv6 网络中的特殊单播地址方面的信息，可以参考 IANA 站点①.

3.2 全球单播 IPv6 地址的分配和规划

地区互联网注册中心 RIR 从 IANA 得到大块地址后，负责将这些大块地址分配给各个本地区的运营商 ISP. 目前全球有五大 RIR 机构，分别是服务于欧洲、中东地区和中亚地区的 RIPE(Reseaux IP Europeans)，服务于中美、南美以及加勒比海地区的 LACNIC(Latin American and Caribbean Network Information Centre)，服务于北美地区和部分加勒比海地区的 ARIN(American Registry for Internet Numbers)，服务于非洲地区的 AFRINIC(African Network Information Centre)以及服务于亚洲和太平洋地区的国家的 APNIC(Asia-Pacific Network Information Centre).

各个 RIR 负责本地区 ISP 的地址分配，也可以直接给最终用户分配，分配策略取决于各个 RIR 的政策. 各个 RIR 有自己的分配政策，例如 APNIC 的《IPv6 地址分配指导建议》②，RFC 6177[19] 中建议 RIR 给最终用户的地址块可以是/56 大小. 一般而言，ISP 从 RIR 得到/32 地址，然后根据需要给成员单位、更小的运营商或者最终用户分配/48 等大小的地址块，而成员单位、更小的运营商或者最终用户给子网分配/64 地址块，分配的流程如图 4 所示.

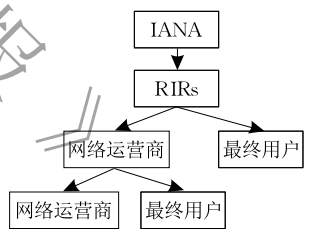

图 4 地址块分配过程

好的地址分配与规划方案需要满足可聚类、可扩展、易管理等多个需求. 可聚类要求地址分配与规划方案在路由上易于聚类，与 IPv4 中情况不同，IPv6 具有更大的地址空间，因此也希望在路由聚合方面具有更好的表现；可扩展性则要求，地址的规划设计应当充分考虑到未来网络规模的扩大、地址所属网络的变迁，使得在发生变化的时候改动尽可能小；易管理则要求网络中 IPv6 地址的规划应当体现

① IANA IPv6 Special-Purpose Address Registry. https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

② APNIC guidelines for IPv6 allocation and assignment requests. https://www.apnic.net/about-apnic/corporate-documents/documents/resource-guidelines/ipv6-guidelines/

出地理位置、组织边界、服务级别等多方面的因素. 如何通过简单可实施的规则实现这些地址分配与规划方面需求，RFC 5375[20] 给出了一些指导性的建议，其中包括给予最终用户的前缀大小、地址预留考虑、子网前缀长度、接口标识生成方案、特殊接口标识的规避等，并通过示例来说明实际情况中的规划. RFC5375[20] 中使用了 RFC3194[21] 中定义的主机密度比率(Host-Density Ratio，HD)来评估地址分配的效率，其中 HD 定义为 HD＝log(已分配的对象数目)/log(最大可分配的对象数目). RFC 4692[22] 针对 IPv6 网络中的 HD 值进行了进一步的讨论，并指出 HD 值为 0.8 时 IPv6 地址的使用效率仍然是非常低的.

相对而言，由于实际网络规划建设中的具体情况细节影响较多，IPv6 地址分配和规划大多是基于一些实践积累下来的原则和建议来进行，更细致的场景划分以及地址规划，还有待于更深入的研究.

3.3　IPv6 地址的获得

IPv6 地址可以分为子网前缀和接口标识两个部分，前者通常由网络运营商指定，可以据此进行网络路由；而后者则一般用来指定用户在一个子网内的标识. 关于子网前缀和接口标识的分界，根据 RFC4291[1] 规定，所有全球单播地址，只要前三个比特不是 000，则应当具有一个 64 比特的接口标识. RFC7421[23] 中曾经对子网前缀和接口标识的界限有过详细的研究，一般而言，子网前缀和接口标识都是 64 比特，唯一的例外定义于 RFC6164[24]，它规定了 127-bit 前缀用来建立路由器等设备间的点对点连接，以避免 ping-pong 问题可能引发的环路. 此外，对于一些基于翻译的过渡技术而言，子网前缀和接口标识的界限也有可能不是 64 比特，如定义于 RFC6877 的过渡技术方案 464XLAT [25] 尽管建议使用/64 前缀，但是如果没有获得/64 前缀也可以，因此可以认为并没有对前缀长度有要求. NAT64 中，定义于 RFC 6052 的无状态翻译[26] 和定义于 RFC6146 的有状态翻译[27] 都允许不同长度的前缀. 在现有的协议中，只有定义于 RFC 6741 的 ILNP (Identifier-Locator Network Protocol)[28] 对于 64 比特的边界具有依赖性. 总之，大部分的接口标识生成方案中长度均按照 64 比特设计，但是设计新的协议时也要考虑接口标识可能不是 64 比特.

网络中的节点可以通过自动获取或人工指定方式获得自己的后 64 比特接口标识(Interface ID，IID). 自动生成中，又可以分成 DHCPv6[29] 方式和无状态自动配置方式(Stateless Address Autoconfiguration，SLAAC)[3]. 针对无状态地址自动配置方案而言，主机根据算法生成链路本地地址，然后通过重复地址检测(DAD)[3] 检查地址是否唯一，重复地址检测通过后，主机在接收到路由器公告(RA)[30] 后，为接收到的路由器通告中的每个前缀配置一个或多个临时 IPv6 地址并检查地址是否唯一.

DHCPv6[29] 可以向 IPv6 主机提供有状态的地址配置或无状态的设置配置，这取决于路由器发送的路由器公告消息. 如果托管地址配置标记即 M 标记设置为 1，则要求主机使用 DHCPv6 协议来获取有状态地址. 如果其他有状态配置标记即 O 标记设置为 1，则表明主机需要使用 DHCPv6 协议来获取其他配置设置. 此外，由于 IPv6 中没有 IPv6 到 IPv6 网络的地址翻译，DHCPv6 还可以给节点分配前缀，也就是所谓地址委派 DHCP-PD[29]，通过地址委派，可以让下级连接点获得一个/56 或/64 大小的子网.

除此之外，在点对点协议 PPP(Point to Point Protocol)中，IPv6 控制协议 IPv6CP(IPv6 Control Protocol)[31] 主要负责在点对点链接终端双方上配置及停用 IPv6 协议模块，同时实现 IPv6 地址的配置，主要用于基于 PPP 的 IPv6 网络配置如点对点链路、虚拟专用网接入等方面.

由于接口标识的生成方案和 IPv6 地址安全研究较为相关，本文将在第 7 节中合并介绍.

4　IPv6 组播地址结构

组播地址定义于 RFC4291[1]，一个组播地址代表了一组接口，发往组播地址的数据包将发送给这一组接口，同时每一个接口也可以加入多个组播组. 组播可以分为任意源组播(Any-Source Multicast，ASM)和特定源组播(Source-Specific Multicast，SSM)两种[32]. ASM 支持多个发布者，终端节点可以加入或离开该组播地址所标识的组. 而 SSM 则有所不同，SSM 中，IP 报文由源地址 S 发布到一个 SSM 组播地址 G，接收者通过加入(S，G)所标识的频道来接收这些 IP 报文.

IPv6 的组播组地址格式如图 5 所示：最高的 8 个比特为 0xFF，标识此地址为组播地址，接着的 4 个比特为标志(Flag)位，标志位的最高位为 0；R 比特表示是否是内嵌 RP 的组播地址(定义于 RFC3956[33])；P 比特表示组播地址是否是基于单

播前缀生成的(定义于RFC3306[34]);T比特表示组播地址是永久分配的还是临时分配的,T为1时表示这是一个临时分配的组播地址,T为0时表示这是一个由IANA指定的知名组播地址.可以看出,标志位对一个组播地址的功能、生成方式等属性进行了标识,之后的4个比特表示组播的范围,常见的范围有本地接口(Interface-local)、本地链路(Link-local)、本地站点(Site-local)、本地机构(Organization-local)等. RFC 7346[35]中进一步定义了本地领域(Realm-local)范围,定义为同一种物理网络所覆盖的范围,对于IP-over-IEEE802.15.4网络,则是具有同一个个人范围内网络标识(PAN ID)的网络.本地接口、本地链路和本地领域范围的边界是自动定义的,全局范围没有边界,其他的边界则依赖于管理人员的配置.由于RFC4007[36]规定小的范围必须在更大的范围之内,而本地管理范围通常需要管理员配置,因此需要在配置时特别注意,所有的范围如表2所示,节点不能向一个范围域值为0的组播地址发送数据包,这样的数据包也会被直接丢掉;节点不能向一个范围域值为F的组播地址发送数据包,这样的数据包如果被接收到,视作范围为E的全球组播地址.

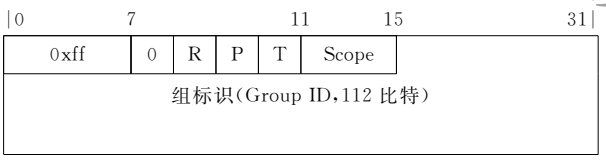

图5 组播地址结构

表2 范围的定义

范围	含义	定义于RFC4291,RFC7346
0	保留	
1	本地接口	节点的一个接口
2	本地链路	链路本地范围
3	本地领域	同一个物理网络覆盖范围
4	本地管理范围	最小的需要管理员配置的组播范围
5	本地站点	某一站点范围
6	未指定	
7	未指定	
8	本地组织	某一组织范围,含有多个站点
9	未指定	管理员可以使用未指定的范围来定义额外的范围
A	未指定	
B	未指定	
C	未指定	
D	未指定	
E	全局	
F	保留	

其余的比特为组标识,用于在组播地址中标识一个组播组.永久分配的组播地址和范围相互独立,例如,NTP服务器组的永久组播ID为0x101,则ff01:0:0:0:0:0:0:101为在同一个接口上的NTP服务器组;而ff02:0:0:0:0:0:0:101为在同一链路上的所有NTP服务器组;ff05:0:0:0:0:0:0:101为同一站点范围内的所有NTP服务器组;ff0e:0:0:0:0:0:0:101为所有互联网上的NTP服务器组.

组播地址既可以临时分配,只在某个特定部署范围内有效,也可以向IANA申请,获得永久的组播地址. RFC6308[37]中对各种获得组播地址的方案进行了总结,以下将详细介绍各类组播地址的生成方案.

4.1 临时组播地址生成方案

临时分配的组播地址中,标志位的T比特为1.对于临时分配的组播地址而言,如何在使用时避免冲突是一个重要的研究问题,针对这一问题,IETF提出了基于单播前缀的组播地址、内嵌汇聚点RP(Rendezvous Point)地址的组播地址以及链路范围内的IPv6组播地址.尽管临时组播地址也可以由动态分配[38]获得,但动态分配方式一直没有得到广泛应用.

4.1.1 基于单播前缀的组播地址生成方案

因为没有机构去分配组播地址,但是由IANA分配单播前缀,因此一种思路就是通过单播前缀生成组播地址就可以实现组播地址的不冲突.基于单播前缀的组播地址[34]结构如图6所示,4比特标志中P位和T位必须为1,表示此组播地址是一个基于单播前缀的组播地址,RFC3306[34]中规定后面8比特为保留位,必须为0,RFC7371[39]进一步规定的第17~20比特为FF2标志,并重命名第8~12比特作为FF1标志.plen的8比特表示前缀的具体长度(最长长度为64),后面64比特为网络前缀,以及32比特的组标识(Group ID).举例而言,IPv6地址块3ffe:ffff:1::/48对应生成的组播地址为ff3x:0030:3ffe:ffff:0001::/96,其中x为组播限制的范围.此外,根据RFC3306[34]的规定,如果plen和网络前缀均为0,则是特定源组播地址(Source-Specific Multicast Addresses,SSM),范围ff3x::/96,x为组播限制的范围,RFC7371[39]中允许FF1的第一比特设置为1,因此SSM的范围还可以为ffbx::/96.

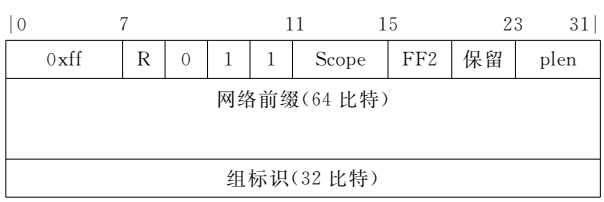

图6 基于单播前缀的组播地址

根据 RFC3307[40] 规定，组 ID 范围为 0x00000001 到 0x3fffffff 的组播地址必须设置 P 比特和 T 比特为 0，由于 SSM 地址中 P=1 且 T=1，因此 SSM 地址 ff3x::/96 和 ffbx::/96 不能使用 0x00000001 到 0x3fffffff 的组 ID. 组 ID 范围 ff3x::4000:0-ff3x::7fff:ffff 由 IANA 分配，组 ID 范围 ff3x::8000:0-ff3x::ffff:ffff 供本地主机或服务器动态分配.

4.1.2　内嵌 RP 地址的组播地址生成方案

汇聚点(Rendezvous Point，RP)是组播网络中的一台作为组播共享树根节点的路由器. 内嵌 RP 地址的 IPv6 组播地址定义于 RFC3956[33]，当组播路由器收到这样组播组的数据包就可以检测出该组的 RP 地址. 其中 plen 不为 0 且不超过 64.

RP 地址可以根据 plen 所指示的，取网络前缀部分中的相应长度作为前缀，之后补 0，最后四比特为 RIID，这样随着 RIID 的不同，可能形成 15 个 RP 地址(RIID 为 0 的情况保留). 内嵌 RP 地址的 IPv6 组播地址区间为 ff70::/12，RFC 7371[39] 允许 FF1 标志之中的第一比特设置为 1 的情况，则内嵌 RP 的地址的 IPv6 组播地址还可以是 fff0::/12. 它的结构如图 7 所示.

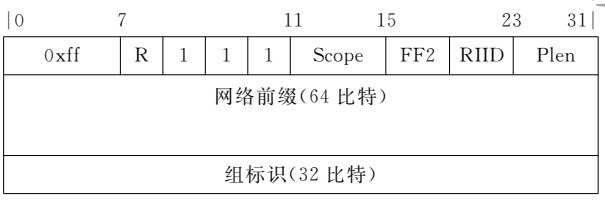

图 7　内嵌 RP 地址的 IPv6 组播地址

4.1.3　链路范围内的组播地址生成方案

RFC4489[41] 中定义了链路范围内的 IPv6 组播地址，这种组播地址中，标志位必须为 0011，范围必须小于等于 2，保留域必须为 0，plen 值为特殊值“11111111”(十进制 255)，然后是 64 比特的接口标识 IID，该 IID 为本链路使用的 IID，而且已经经过 DAD 检测. 它的结构如图 8 所示.

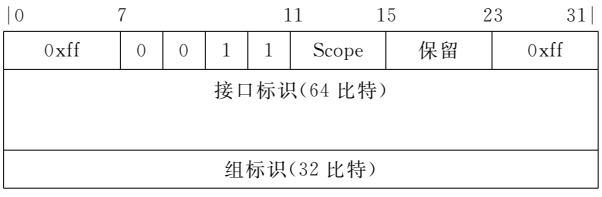

图 8　链路范围内的 IPv6 组播地址

这一地址主要用于在局域网内提供零配置服务中.

4.2　永久组播地址

除了临时组播地址之外，IANA 还批准了许多永久的组播地址，这些组播地址通常用于各种依赖于组播的服务发现①. RFC2375[42]、RFC4291[1] 总结定义了一些永久的组播地址，这些定义的组 ID 具有预定义的范围，不能作为其他范围的永久组播地址. 其中被请求节点(Solicited-Node)组播地址[1] 为节点单播和任播地址的一个函数，它通过把任播或单播地址的后 24 比特和前缀 ff02:0:0:0:0:1:ff00::/104 合并形成，格式为 ff02:0:0:0:0:1:ffxx:xxxx，例如，地址 4037::01:800:200e:8c6c 相对应的被请求节点组播地址为 ff02::1:ff0e:8c6c，这一地址主要用于邻居发现协议中，被请求节点的组播地址被节点用来获得相同本地链路上邻居节点的链路层地址，也可用于重复地址检测. 此外，ff0x:0:0:0:0:0:0:0(x 从 0 到 f)是协议保留的组播地址.

RFC3307[40] 定义了组播地址中组 ID 分配所需要遵循的规范. RFC 3307[40] 规定，RFC 2375[42] 定义的永久性组播地址由 IANA 分配，且必须设置 P 比特和 T 比特为 0，ID 范围为 0x00000001 到 0x3fffffff. 永久性的组 ID 可以和前面的 96 比特搭配用于指定不同范围内特定服务器的组播，所对应的组 ID 范围从 0x40000000 到 0x7fffffff. 临时 IPv6 组播地址使用 0x80000000 到 0xffffffff 的组 ID，且 T 比特必须为 1，这些地址由服务器或者主机来选择，具体可以参考 RFC2730[38].

随着 IPv6 组播的广泛使用，更多的永久性的 IPv6 组播地址被 IANA 分配. 除了 IETF 之外，另外一些标准化组织如 IEEE、UPNP 论坛等也纷纷向 IANA 申请了永久的 IPv6 组播地址. 之所以有大量的协议使用到了永久组播地址，主要是出于如下几方面的原因：

(1) 路由协议的需要. 在很多路由协议中，需要通过使用广播或者组播来发现参与者，如以下组播地址：所有路由器[1]、DVMRP 路由器[43]、OSPFIGP[44]、ST 路由器[45]、RIP 路由器[46]、EIGRP 路由器[47]、所有 MLDv2 路由器[48]、LL-MANET 路由器[49]、SL-MANET 路由器[50] 等.

(2) 局域网内的域名解析. 这方面有链路本地组播名字解析[51]、mDNSv6[52]、节点信息查询[53]. 主要意图为在局域网内，通过组播来进行局域网内的名字解析.

① IPv6 Multicast Address Space Registry. https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

(3)服务发现. 如 Service Location, Version 2[54]、NTP[55-56]、所有 DHCP 服务器[29]、所有 DHCP 代理[29]等.

(4)其他应用. 如 ff0x::db8:0:0/96 被定义作为文档使用[57].

研究者可以向 IANA 申请得到永久的组播地址①.

5 IPv6 任播地址结构

任播地址从单播地址空间内进行分配,并没有特殊的格式. 通过将服务部署于具有相同的任播地址,但在不同位置的多个节点,任播可以实现在单一地址下的更可靠、更有效的服务. RFC 4786[58]指出任播的部署可以实现粗粒度的负载均衡、减少拒绝服务攻击、便于确定流量来源、提高客户响应速度、便于单地址下实现可靠服务.

任播部署的核心问题在于如何通过路由系统的配置实现单地址、多节点的可达. 根据任播部署的范围,可以分为本地范围任播(Local-Scope Anycast)和全球范围任播. 本地范围任播通过在内部网关协议(Interior Gateway Protocol, IGP)的配置实现,而全球范围任播则需要在域间路由协议(Border Gateway Protocol, BGP)进行配置. 对于两者而言,配置又有所不同,例如配置内部路由可以不受前缀长度的限制,而域间路由配置时有可能无法宣告过小的前缀长度,RFC 4786[58]研究了这一问题并给出了一些推荐建议.

IPv6 任播地址提出后,在服务发现等方面得到了广泛的使用,与使用组播地址进行服务发现有所不同,基于任播地址的服务发现要求服务的提供方在数据包经过的节点上,因此通常用于 Middlebox 设备上的服务发现,这样的例子有:

(1) 2001:1::1/128,定义于 RFC 7723[59],用于端口控制协议(Port Control Protocol, PCP)[60],主要用于发现支持 PCP 协议的 NAT、防火墙或其他 Middlebox 设备,对应的IPv4任播地址为 192.0.0.9/32. 端口控制协议主要用于主机控制 NAT 设备或防火墙,从而实现个性化的数据包翻译或转发策略.

(2) 2001:1::2/128,定义于 RFC 8155[61],用于 TURN[62]协议. TURN 协议用于提高 P2P 应用的连接性[63],它使得即使连接的双方都在 NAT 之后也能建立连接. 这一任播地址主要用于寻找 NAT 穿越中继,相对应的 IPv4 的地址为 192.0.0.10/32.

(3) 2001:3::/32,定义于 RFC 7450[64],主要用于发现自动组播隧道协议(Automatic Multicast Tunneling, AMT)中继. AMT 用于将来自于组播网络中的组播数据,通过基于 UDP 的隧道封装,发送到没有连接到该组播网络的节点上,对应的 IPv4 任播地址为 192.52.193.0/24.

(4) 2001:4:112::/48,定义于 RFC 7535[65],用于 AS112 项目. 目前许多地方使用非全球唯一的 IPv4 地址如 10.0.0.0/8、192.168.0.0/16 的地址,有时会出现针对这些地址的逆向解析,鉴于这些地址只有局部意义,理想情况下应当由本地回答,但是这难于实现,AS112 项目意图建立一个这些请求的分布式的吸收点. 它使用了 IPv4 任播地址 192.31.196.0/24 和 IPv6 任播地址 2001:4:112::/48 来提供对这些请求的 DNAME[66]重定向,DNAME 可以将 DNS 解析从某个域名重定向到另外一个域名,和 CNAME 不同的是,CNAME 是在本域内的重定向,而 DNAME 则提供了跨域的重定向,例如,针对 example.com 的查询可以使用 DNAME 记录全部重定向到 example.net.

(5) 2620:4f:8000::/48,定义于 RFC 7534[67],也是用于 AS112 项目. AS112 项目中使用 IPv4 任播地址 192.175.48.0/24 和IPv6任播地址 2620:4f:8000::/48 来提供对内部地址逆向解析请求的授权回答.

除了用于服务发现之外,任播在局域网内也得到了应用. RFC 4291[1]中定义了子网路由器任播地址,其中子网前缀就是某一链路的子网前缀,接口标识为 0,发往这一地址的数据包被交给子网中的一台路由器,这一任播地址主要用于主机与任一个路由器通信时使用.

此外,根据 RFC 2526[68],以下地址将被保留作为子网内任播地址. 对于必须使用 EUI64 方式生成接口标识的网络而言,任播地址格式如图 9 所示,其中有 7 比特的任播标识,其中任播标识规范可以参考 IANA 网站②.

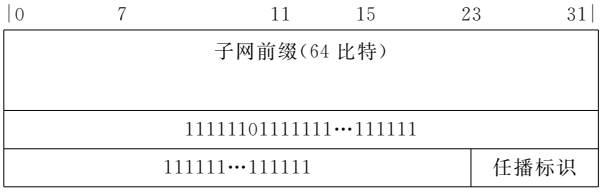

图 9 子网内任播地址(EUI64)

① Application for an IPv6 Multicast Address. https://www.iana.org/form/multicast-ipv6

② Internet Protocol Version 6 (IPv6) Anycast Addresses. https://www.iana.org/assignments/ipv6-anycast-addresses/ipv6-anycast-addresses.xhtml

以上就是 IPv6 任播地址方面的一些地址规划情况.

6　过渡方案中 IPv6 地址结构

IPv6 过渡方案主要解决在 IPv4 网络向 IPv6 网络演进的过渡期内,实现业务的共存和互相访问的问题.过渡方案中 IPv6 地址结构与纯 IPv6 网络中的主要区别在于,首先,过渡方案中常常需要建立 IPv6、IPv4 地址的对应关系,因此过渡方案中 IPv6 地址通常具有特殊结构;其次,在 IPv6 过渡方案中,由于地址具有特别语义,子网前缀和接口标识可以不以 64 比特为界.

过渡方案一般可以根据所采用的技术方案分为基于双栈的过渡方案、基于隧道的过渡方案以及基于翻译技术的过渡方案,而根据所使用的地址来区分,则可以分为使用网络特定前缀(Network-Specific Prefix,NSP)或知名前缀(Well-Known Prefix,WKP),网络特定前缀通常在归属于该运营商的前缀中选择,而知名前缀则是固定于协议中的前缀.

过渡方案中地址结构的另一个特色在于,大多数过渡方案的 IPv6 地址中,含有 IPv4 地址、端口号或端口集合等信息,主要的原因在于

(1)对于 IPv6 over IPv4 的 IPv6 孤岛连接类型的过渡方案[69],IPv6 地址中含有 IPv4 地址的主要原因是便于隧道端点地址的获取.IPv6 数据包在 IPv4 的隧道中传输,如果 IPv6 地址中含有 IPv4 地址,那么外部的 IPv4 头中的地址可以直接从 IPv6 地址中得到,这样就不用指明隧道的端点了,从而有利于隧道的自动建立,这样的例子有 6rd[70]、ISATAP[71]、6a44[72]、6to4[73]、Teredo[74]等.

(2)对于无状态的 IPv6 和 IPv4 的翻译技术而言,将 IPv4 地址嵌入到 IPv6 中,可以无需记录映射状态即可进行地址翻译,如无状态地址翻译[26].

(3)定义于 RFC2529 的 6over4[75]使用 IPv4 地址来生成 64 比特接口标识的原因主要是通过将 IPv4 地址嵌入到后 64 比特,可以得到一个全球唯一的接口标识.

(4)随着 IPv4 地址的耗尽,一些过渡方案中需要使用 NAT 卸载方式,将 IPv4 的 NAT 功能下放到用户端网络设备上执行,经过端口分配管理后,可以方便同一个 IPv4 地址在多个用户端网络的复用,通过特殊定义的 IPv6 地址,有利于端口分配管理方面信息的下发,如 MAP-T[76]、MAP-E[77]、Lightweight 4over6[78]等.

各个过渡措施的概述如表 3 所示,6.1 节将简要介绍基于网络特定前缀的过渡方案地址结构,而 6.2 节将介绍基于知名前缀的过渡方案地址结构.

表 3　过渡方案地址结构

过渡方案	前缀	地址结构特点
6rd	NSP	IPv4 地址
ISATAP	NSP	IPv4 地址
6a44	NSP	IPv4 地址
6over4	NSP	IPv4 地址
IVI	NSP WKP	IPv4 地址
MAP-T	NSP	IPv4 地址+端口集合
MAP-E	NSP	IPv4 地址+端口集合
Lightweight 4over6	NSP	IPv4 地址+端口集合
teredo	WKP	IPv4 地址+端口
6to4	WKP	IPv4 地址
RFC8215	WKP	未定义

6.1　基于网络特定前缀的过渡方案地址结构

基于隧道技术的使用网络特定前缀的过渡方案主要有如下几种:

(1)定义于 RFC5969[70]的 6rd 使用了运营商的 IPv4 前缀,因此 6rd 不需要把所有 32 比特的 IPv4 地址都嵌入到 6rd 前缀中,这样可以提供更多的子网 ID 给用户,或者可以使用更小的地址块.它的结构如图 10 所示.

n 比特	*o* 比特	*m* 比特	128-*n*-*o*-*m* 比特
6rd 前缀	IPv4 前缀	子网 ID	接口标识

图 10　6rd 地址结构

(2)定义于 RFC5214[71]的 ISATAP,地址构成方案如图 11 所示,它的 u 比特需要指明接口标识中的 IPv4 地址是否是全球地址,如果是则为 1,g 比特为 0,其他比特设置为 0x00005efe.

48 比特	16 比特	32 比特	32 比特
组织前缀	子网	*ug*00:5*efe*	IPv4 地址

图 11　ISATAP 地址结构

(3)6a44 定义于 RFC6751[72],使用运营商前缀,网关的 IPv4 地址、客户端的 IPv4 地址以及端口号都被嵌入到 IPv6 地址中.它的结构如图 12 所示.

48 比特	32 比特	16 比特	32 比特
6a44 前缀	网关 IPv4	端口	客户 IPv4

图 12　6a44 地址结构

(4)定义于 RFC2529[79]的 6over4 通过无状态地址自动配置生成 128 比特 IPv6 地址,它的结构如图 13 所示.

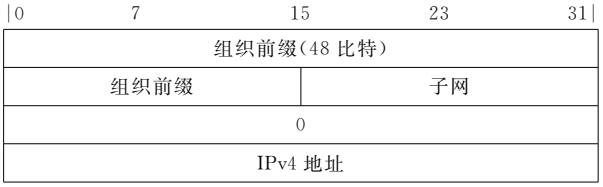

图 13 6over4 地址结构

在无状态翻译技术中,为了实现无状态的 IPv4 和 IPv6 之间的协议翻译,需要将 IPv6 地址和一个 IPv4 地址或者一个 IPv4 地址的部分端口建立对应关系,为此,RFC 6052[26] 定义了 IPv4 地址和 IPv6 地址的映射方法. 根据 RFC 6052[26],无状态翻译技术中,IPv6 前缀可以是 32、40、48、56、64、96 比特长,针对这些长度,所使用的映射方式如图 14 所示,其中后缀部分一般为 0.

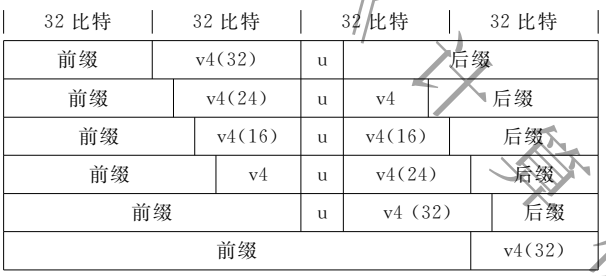

图 14 IVI 地址结构

鉴于 IPv4 地址越来越少,在 RFC 6052[26] 的基础上,进一步出现了可以复用一个 IPv4 地址的映射方案,分别为定义于 RFC7597[77] 的封装中的端口复用(Mapping of Address and Port with Encapsulation, MAP-E)和定义于 RFC 7599[76] 的翻译中的端口复用(Mapping of Address and Port using Translation, MAP-T). MAP 的核心技术是无状态地址和端口映射算法,其思想是利用 16 位的传输层端口对 IPv4 地址进行扩展.

基于 MAP 规则得到的 IPv6 地址由 IPv6 前缀、EA 比特(由 IPv4 子网标识和 *PSID* 组成,用于唯一标识不同的用户)、子网标识(用于标识一个用户使用的大于等于/64 的 IPv6 子网)和接口标识构成,它的结构如图 15 所示. 其中 EA 比特包含着该客户所用的 IPv4 地址的一部分以及端口信息. 客户通过其他方式得到 IPv4 地址前缀及其长度 r、o 的值,IPv6 前缀 n 的值. 如果 $o+r<32$,则说明客户对应于一个 IPv4 前缀;如果等于 32,则说明对应于一个 IPv4 地址;如果大于 32 则说明对应于一个 IPv4 地址的部分端口. 这时,多余的比特则是 *PSID*.

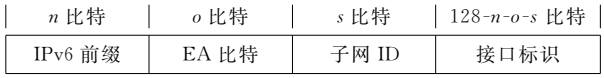

图 15 MAP 地址结构

在给定 *PSID* 之后,需要得到相应的端口范围,其算法为 $P=(R\times M)\times i+M\times PSID+j$,其中 i 和 j 为正整数,这些参数的意义如图 16 所示.

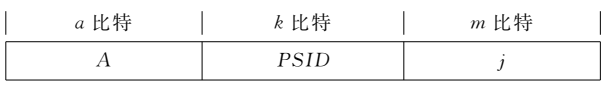

图 16 端口集合描述

在这一表示方法中,a(缺省为 6)比特的 A 表示需要排除的端口,为了排除系统保留端口 0-1023,在 a 为 6 比特的情况下,需要满足 $A>0$. *PSID* 的值从 0 到 $R-1$,其中 R 为 2^k,j 从 0 到 $M-1$,其中 M 为 2^m. 因此,对于 2001:db8:0012:3400::/56 前缀,假设已知 IPv4 前缀为 192.0.2.0/24,EA 比特长度 o 为 16,a 为缺省值 6,则可以得到 *PSID* 的长度 k 为 16−(32−24)=8,R 为 256,IPv4 地址为 192.0.2.18,*PSID* 为 0x34, $m=16-8-6=2$,M 为 4,取 $i=1,\cdots,63$,$j=0,1,2,3$ 则可以得到端口范围为:1232～1235,2256～2259,…,63696～63699,64720～64723.

在 MAP 规范下,接口标识格式如图 17 所示,在不使用端口复用的 IPv4 前缀或地址情况下,*PSID* 设置为 0,中间为 IPv4 地址.

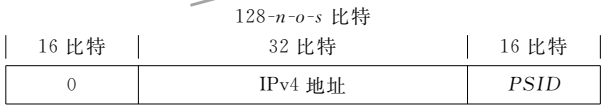

图 17 MAP 接口标识

轻量级 4over6[78] 使用了 RFC 7597[77] 的 MAP 方法生成 IPv6 地址的接口标识. 它的结构如图 18 所示.

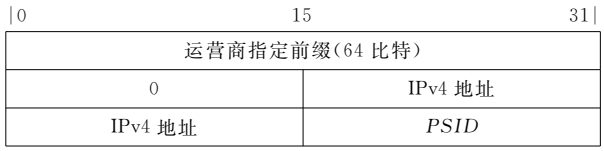

图 18 轻量级 4over6 地址结构

6.2 基于知名前缀的过渡方案地址结构

定义于 RFC3056[73] 的 6to4,它使用了 6to4 前缀 2002::/16,它的地址结构如图 19 所示.

图 19　6to4 地址结构

为了便于在一个自治域内提供过渡服务，RFC 6052[26]定义了 64:ff9b::/96 作为无状态地址翻译服务地址，这一地址校验和为 0、不可全球路由且后 32 比特用于存放全球可路由的 IPv4 地址.

RFC 8215[79]进一步规定 64:ff9b:1::/48 用于本地使用的 IPv4/IPv6 翻译机制，主要为了方便多种翻译机制在同一个网络中共存，同时不必申请运营商特定的前缀分配.

Teredo 定义于 RFC 4380[74]，后续经过 RFC 5991[80]进一步更新. Teredo 为处在 NAT 设备后的使用私有地址的 IPv6 孤岛提供隧道服务. 其中 IPv6 报文经过 IPv4 的 UDP 协议封装后发送. Teredo 中将 Teredo 服务器的 IPv4 地址、一些标志、UDP 端口号、Teredo 客户端的 IPv4 地址嵌入到 IPv6 地址中. 出于安全方面的考虑，UDP 端口号和客户端 IPv4 地址通过比特交换进行了混淆. 16 比特的标志位为 CRAAAAUG AAAAAAAA，如果 Teredo 客户端位于一个锥形 NAT 后面，“C”位设为 1，否则为 0，但 RFC 5991[80]将它改为始终为 0 以避免向陌生人暴露此情况. “R”位目前未分配，应该设为 0，“U”和“G”位为 0，12 个“A”位在 RFC 4380[74]规范中为 0，但在 RFC 5991[80]中更改为由 Teredo 客户端选择的随机位，以避免基于 IPv6 的扫描攻击. 它的结构如图 20 所示.

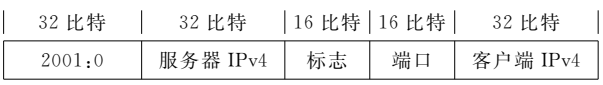

图 20　Teredo 地址结构

7　接口标识生成方案与地址安全

IPv6 地址安全与隐私保护研究是和 IPv6 地址接口标识生成方案的研究紧密相关的. 与 IPv4 相比，IPv6 具有非常大的地址空间，这使得最初的研究者认为 IPv6 网络的扫描不太可能，不过随后的研究表明，如果使用脆弱的接口标识生成方案，不仅扫描的风险依然存在，而且进行地址间关联分析的风险也变得不容忽视.

IPv6 的接口标识一般有 64 比特，既可以人工指定，也可以使用算法自动生成. RFC 7707[81]总结了常见的手工生成的接口标识，大约可以分成如下几类：

(1) 基于低字节的接口标识生成方案. 最常见的是所有的 IID 大部分设置为 0，如 2001:db8::1、2001:db8::2 等；最低的两个字节非 0 的情况也很常见，如 2001::db8::1:10、2001:db8::2:10 等；偶尔也有第三个最低字节非零的情况.

(2) 基于 IPv4 地址的指定方法. 最常见的情况是将 IPv4 地址四个字节作为 IID 的最后四个字节，如 2001:db8::192.0.2.1，也有将 IPv4 地址编码到每个 16 比特中的情况，如 2001:db8::192:0:2:1.

(3) 基于服务、端口号的生成方案. 这种情况中最常见的是将该服务器端口号和该服务器的编号嵌入到接口标识中，如对于 HTTP 的 80 端口服务器可以是 2001:db8::1:80 或 2001:db8::80:1，有时也有可能使用十六进制如 2001:db8::50.

(4) 基于单词的生成方案. 由于十六进制数字较难记忆，有时也会使用基于单词的生成方式，如 2001:db8::bad:café.

基于算法的自动生成方案最早定义于 RFC 2464[82]，即基于 MAC 地址的 IEEE EUI-64(IEEE 64-bit Extended Unique Identifier)生成方案，这一生成方案目前仍然用在一些主机中，用于生成不变的服务器接口标识. 这一接口标识通常可以由 48 位硬件地址得到，通过 IEEE 指定的公共 24 位制造商标识和制造商为产品指定的 24 位值的组合，中间嵌入 0xfffe 得到，这样的接口标识是随机器硬件固定的，也是全局唯一的. 在最后生成的接口标识中，需要将第 7 比特即 u(universal/local)比特[1]设置为 1，第 8 比特 g(individual/group)比特设置为 0，u 比特为 1 表示该接口标识具有全局含义，为 0 表示只有本地意义. g 比特为 1 表示该接口标识为组接口标识，不过后来的 RFC 7136[83]指出：除了 EUI64 之外的接口标识生成方案基本都将第 7 比特设置为 0. 由于后 64 比特可以由主机进行指定，RFC 7136[83]建议除非具有本地环境约束，IID 整体必须被第三方认作是不透明的比特字符串. 因此 u 比特和 g 比特的值在 IID 中没有特别的含义，新的 IID 生成方案可以任意使用这两个比特，例如在一些过渡方案中就是如此[84].

基于 EUI-64 的接口标识生成方案如图 21 所示.

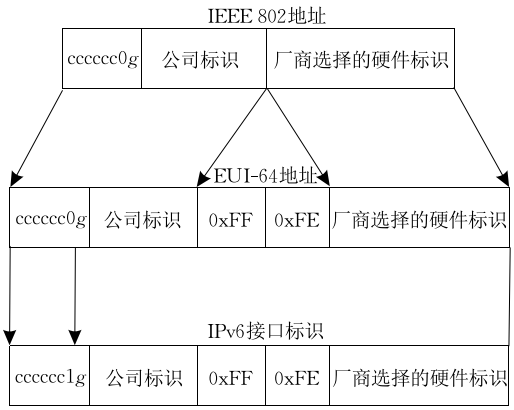

图 21 基于 EUI-64 的接口标识生成方案

7.1 保护用户隐私的接口标识生成方案

随着 IPv6 的广泛使用,EUI-64 方案的安全问题也不断得到研究人员的关注,如果接口标识基于 EUI-64 方案生成,就可以标识指定节点的通信,根据用户的前缀,可以轻松跟踪指定用户使用互联网的情况.为了解决这个问题并提供某种程度的匿名,在 RFC4941[85] 中描述了一种保护用户隐私的 IPv6 接口标识,它是随机生成的,并且随时间变化而变化.初始接口标识通过使用随机数字来生成.对于不能存储历史信息以便生成将来的接口标识的 IPv6 系统,每次初始化 IPv6 协议时都将随机地生成一个新的接口标识.对于有存储能力的 IPv6 系统,将存储历史值,在初始化 IPv6 协议时,通过以下进程创建新的接口标识:

(1)从存储区中检索历史值,如果没有的话就用随机值,并将这一随机值添加到根据 RFC4291[1] 所生成的接口标识(EUI-64)后.

(2)对步骤(1)中的随机值计算 MD5 哈希值.

(3)取步骤(2)中计算的 MD5 哈希的最左 64 位,将 u 比特设置为 0,作为备选的接口标识.

(4)将这一接口标识与 IPv6 保留接口标识(如保留作为子网任播的接口标识)和已经指定给本地设备的接口标识比较,如果发现这一接口标识不可用,则将最右 64 比特作为随机值重复步骤(2).

(5)保存所得的接口标识,同时将 MD5 的最右 64 比特作为随机值保存起来以便下次生成接口标识时使用.

根据此随机接口标识得到的 IPv6 地址就称为临时地址.

7.2 稳定、语义不透明的接口标识生成方案

临时地址通常用于向外发起连接时使用,不过临时地址也有一些问题,例如,临时地址变化频繁,导致日志记录变得更难于分析,这大大增加了网络管理成本,此外,在一些场合如嵌入式设备,采用临时地址也增加了部署的复杂程度.为此,RFC7217[86] 设计了一种稳定、语义不透明的接口标识生成方案(Stable, semantically opaque IID).这样产生的地址对于同一个子网、同一个网络接口而言,即使 DHCP 服务器不同,所产生的地址也是相同的.目前稳定、语义不透明的接口标识生成方案已经被 RFC8064[87] 推荐作为缺省的接口标识生成方案.

在这一生成方案中,随机生成但稳定的标识符 $RID=F(Prefix, Net\_Iface, Network\_ID, DAD\_Counter, secret\_key)$.其中 $F()$ 为一个不可逆的伪随机数生成函数,如 SHA-256,$Prefix$ 是 SLAAC 所用的前缀,Net_Iface 为接口标识所在的网络接口,$Network\_ID$ 为用于标识这一子网的特定网络数据,如 IEEE 802.11 的 SSID,$DAD\_Counter$ 为进行 DAD 检测的次数,初始化为 0,每次生成一个地址就加 1,对于每个 $\{Prefix, Net\_Iface, Network\_ID\}$ 组对应一个 $DAD\_Counter$. $secret\_key$ 为至少 128 比特的密值,所得到的 RID 从右开始的尽可能多的比特,就是所生成的接口标识.

针对 DHCPv6[29],RFC 7943[88] 定义的生成算法类似:$RID=F(Prefix \mid Client\_DUID \mid IAID \mid Counter \mid secret\_key)$,其中 $Client\_DUID$ 为 DHCPv6 唯一标识(Unique Identifier,DUID);$IAID$ 为身份关联标识(Identity Association Identifier,IAID),$secret\_key$ 为 DHCP 服务器所设置的一个密值.

通过使用这些接口标识,能够有效地减少用户所面临的地址关联分析和隐私挖掘风险.

7.3 绑定地址与主机的接口标识生成方案

除了地址生成方案所带来的用户隐私保护和安全风险之外,在 IPv6 网络中,另外一个重要的安全风险来自于局域网内安全风险.IPv6 使用邻居发现协议(Neighbor Discovery Protocol,NDP)[89-90] 来进行 IPv6 地址到链路层地址的映射,从而实现邻居发现(Neighbor Discovery,ND)、网关发现(Router Discovery,RD)、地址自动配置(Address Autoconfiguration)、地址解析(Address Resolution)、邻居不可达检测(Neighbor Unreachability Detection,NUD)、重复地址检测(Duplicate Address Detection,DAD)以及重定向(Redirection)等功能.NDP 协议建议使用 IPSEC 来保护 NDP 协议,不过如何部署方面缺乏相应的细节.在没有额外的安全防护措施下,邻居发现协议面临各种如包括地址假冒、中

间人等安全风险[91-92]，为此，安全邻居发现协议(SEcure Neighbor Discovery，SEND)[93]通过使用新的带有公钥的 NDP 选项来实现对邻居发现协议的安全保护.为了在不使用公钥基础设施的情况下验证公钥和地址的绑定关系，研究者们设计了加密生成接口标识(CGA)方案.

加密生成接口标识(CGA)方案定义于 RFC 3972[94]，是一个具有特定用途的接口标识生成方案.CGA 的基本思想是将一个公钥签名通过一个哈希函数加到 IPv6 的接口标识里去，从而实现用户公钥和 IPv6 地址的绑定.在每次产生 CGA 前，主机会首先产生一对公共/私有密钥对.对公共密钥和辅助参数进行哈希计算产生 IPv6 地址的接口标志符，在此接口标志符前面加上本地网络前缀得到的 IPv6 地址.私有密钥用来对来自这个地址的消息进行签名认证，它的形成如图 22 所示.伪随机序列由计算机随机生成，在每次生成 CGA 的过程中使用，通过加入此随机数来加强抗攻击能力；子网前缀指的是本地子网前缀，冲突数为无符号整数，必须是 0、1 或 2；公共密钥为存储自己的公共密钥.扩充区域在 RFC 4581[95]中进行了进一步规范.RFC 3972[94]中要求使用 SHA-1 算法进行哈希，而且哈希得到的 HASH2 也要满足最左面的 16×SEC 比特为 0，RFC4982[96]考虑到 SHA-1 算法可能的安全问题，将 SEC 数设置为一个所用算法和需要满足前 n 比特为 0 的标识.在 CGA 所生成的接口标识中，u 比特和 g 比特均为 0.

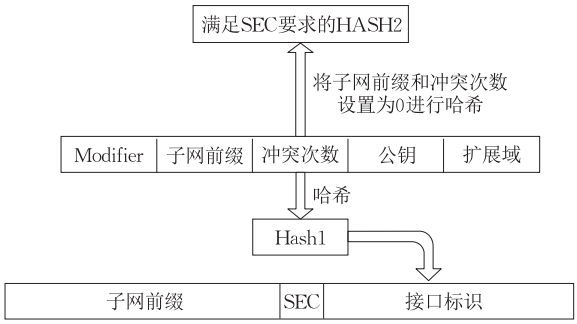

图 22　CGA 生成方式

尽管基于 CGA 方案的 SEND 协议提供了一种局域网内地址欺诈的解决方案，不过该技术并未得到广泛应用，主要原因在于该方案依赖于对各个终端节点的修改，这使得部署起来相对复杂.针对 NDP 协议的安全问题，IETF 成立了真实源地址验证 SAVI (Source Address Validation Improvements)①工作组来专门研究这一问题，并提出了 DHCP 下的 SAVI 方案[97]、混合地址下的 SAVI 方案[98]、针对 SLAAC 生成和手工指定地址的 SAVI 方案[99]等，这些技术得到了更广泛的应用.

另外一个需要考虑主机与地址绑定的问题来源于多宿主机，在 IPv6 网络中，主机常常具有多个来自不同子网的地址，RFC 5535[100]定义了基于哈希的地址生成方式(Hash-Based Addresses，HBA)，通过生成现有前缀以及一些随机值的哈希，来建立多个 IPv6 地址和同一个多宿主机的绑定，这样流量被重新路由后，也不必担心被路由到一个攻击者上.例如，对于具有前缀 A,B,C,D 的多宿主机，将产生前缀列表 $P=(A,B,C,D)$以及一个随机数 M，然后将生成新的地址：$A \parallel H(M \parallel A \parallel P)$、$B \parallel H(M \parallel B \parallel P)$、$C \parallel H(M \parallel C \parallel P)$、$D \parallel H(M \parallel D \parallel P)$，这样根据前缀列表和一个前缀，就可以仅仅检查地址的低比特就知道该地址是否属于这一多宿主机.HBA 使用了 CGA 地址生成算法，但是定义了一种新的扩展，其中扩展类型为 16 比特的标识，扩展数据长度为 16 比特的无符号整数，表示扩展项的不包含头四个字节的长度，P 比特标志用于标识是否公钥包含于 CGA 参数集的公钥域中；保留域为 31 比特的保留项，必须设置为 0，$Prefix[1\cdots n]$为 1 到 n 的 64 比特前缀，HBA 格式如图 23 所示.

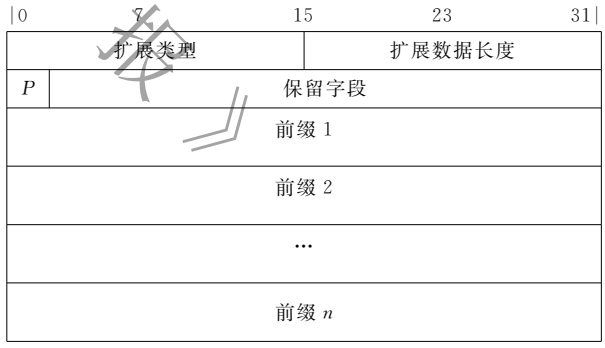

图 23　HBA 接口标识生成方案

7.4　IPv6 地址安全与隐私保护

如前所述，具体到 IPv6 地址结构所相关的安全研究，可以大致分为局域网内安全、扫描、隐私保护等.RFC 7721[101]根据 IID 的变化特性，把 IID 分为恒定的(Constant)、稳定的(Stable)和临时的(Temporary).所谓恒定的 IID，就是当节点从一个 IPv6 链接转移到另外一个时，接口标识仍然不会变

① Source Address Validation Improvements (savi). https://datatracker.ietf.org/wg/savi/about/

化;所谓稳定的 IID,就是在某种特定的上下文环境中不变的 IID,例如,只要在同一个链接下就保持不变,但当移动到另外一个链路时就会变化;所谓临时的 IID,就是那些随时间而变化的接口标识.此外,根据 IID 是否语义透明,可以分为语义不透明的 IID 和语义透明的 IID.对于语义不透明的 IID 而言,IPv6 的后 64 比特可以看作为随机的二进制字符串.随着互联网对于隐私保护的重视,IETF 在 RFC 8064[87]中推荐将稳定语义不透明的接口标识生成方案作为缺省生成方案,但是实际上,其他地址生成算法仍然在广泛使用.

RFC7721[101]针对长时间的事件关联、位置跟踪、地址扫描、特定设备的缺陷发现等方面对现有的 IPv6 地址生成方案进行了研究.这些安全风险如下:

(1)长时间的事件关联.在一个地址的有效期间,这一地址上所发生的事件可以进行关联分析,例如,对于 IEEE EUI-64 而言,一个网络设备,即使变换了链路,仍然可以进行关联性分析.如 RFC 4941[85]所述,使用恒定的接口标识,很容易导致用户的隐私泄露.

更多关于事件关联方面的信息可以参考 RFC 6973[102].除此之外,基于 IPv4 地址生成的 IPv6 接口标识也面临着类似的关联分析问题.

(2)位置跟踪.由于 IPv6 地址分成前 64 比特具有位置相关信息的部分和后 64 比特的接口标识,如果后 64 比特保持恒定,则可以根据前 64 比特来进行位置跟踪.通过主动测量,也可以探测到某一个链路中是否存在某个接口标识.

(3)地址扫描.虽然 IPv6 的地址空间非常之大,使得理论上扫描难以进行,由于一些地址生成方式的问题,会导致地址空间大大减少,如 RFC 7707[81]所述,在 EUI-64 中,MAC 地址中的 24 比特的组织唯一标识(OUI),以及生成过程中中间的两个固定值字节(0xff,0xfe)可以大大减少可能的接口标识数目.

(4)特定设备的缺陷发现.EUI-64 生成方式暴露了硬件地址,根据这一硬件地址,可能可以推测出相应的操作系统等信息,从而可以进行更有针对性的缺陷攻击.

常见的接口标识生成方案的安全风险如表 4 所示.

表 4 常见接口标识生成方案的安全风险

	事件关联	位置追踪	地址扫描	特定设备缺陷
EUI-64	设备使用期	设备的使用期	可能	可能
手工静态	地址使用期	地址使用期	取决于生成方式	取决于生成方式
恒定的语义不透明	地址使用期	地址使用期	不能	不能
CGA	Modifier 和公钥的使用期	不能	不能	不能
稳定的语义不透明	在某个 IPv6 链路	不能	不能	不能
临时	地址使用期	不能	不能	不能
DHCPv6	租约时间	不能	取决于生成方式	不能

过渡措施由于采取了独特的地址生成方案,也带来了一些隐私和安全问题.例如,Teredo 将 IPv4 地址和端口嵌入到 IPv6 地址中,且 RFC 4380[74]中将多余的比特设置为 0,这也就使得攻击者可以很容易地根据 Teredo 所使用的 IPv4 地址和端口来扫描 IPv6 地址(由于很多 NAT 中端口并非随机分配).为此,后来又增加了 12 随机比特[80].另外一些过渡措施如 RFC5214[71],RFC6052[26],也使用 IPv4 地址来生成 IPv6 地址,这使得攻击者更容易进行端口扫描.其他一些措施如 RFC7596[78],RFC7597[77],RFC7599[76]使用 IPv4 地址和端口集合 ID(很多 NAT 中这并不随机).

另外,尽管子网标识有 64 比特,不过一些 RFC 中推荐了地址空间的分配方案如 RFC5375[20],其中一些建议包括从低 ID 到高 ID,如从 2001:db8:0::/64, 2001:db8:1::/64 开始分配;使用十六进制或十进制的号码;使用 VLAN 号;在双栈的情况下使用 IPv4 子网号等等,这也增加了 IPv6 地址空间扫描的风险.针对这些安全风险,RFC 4890[103]给出了一些相关的过滤建议.

总的说来,由于 IPv6 已经进行的安全检验还十分有限,IPv6 地址结构的安全仍然有待于进一步研究.

8 多地址下的寻址及路由

IPv6 网络与 IPv4 网络的另外一个重要的区别在于,IPv6主机通常有多个IPv6地址,有时还具有

多个前缀，那么主机在进行互联网通信时，应当使用哪一个地址呢？此外，在具有多个前缀的情况下，应当选择哪个地址对应的网关作为缺省网关呢？针对这些问题，有两种解决的思路和方法，第一种是按照现有互联网的体系结构，选择其中之一作为源地址和缺省路由；另外一种，则是通过将对上层应用的标识（身份标识）和进行路由的标识（位置标识）区分开来，实现上层应用与位置无关，这需要对现有的体系结构进行较大的改变，以下我们将分别介绍这两种思路下的研究成果与标准.

8.1　多地址下的地址与路由选择策略

RFC4191[104]中针对多宿主机的路由选择问题，建议在路由通告中使用 Prenference 来进行标志，RFC8028[105]中进一步规定，多宿主机在接收到多个路由通告时，应当优先选择含有前缀信息的路由通告以得到缺省路由器，而不理会路由通告中的优先权值.

源地址选择策略往往和目的地址选择策略相结合，在实际使用之中，目的地址常常也是一个域名解析成的多个地址集合，因此，如何选择源地址、目的地址的组合，是多地址下寻址和路由需要研究的问题.

针对多个目的地址，RFC 6724[106]规定了客户端排序的方法. 由于多个目的地址中可能含有 IPv4 地址，RFC6724[106]规定将 IPv4 地址变为 IPv4 映射成的地址，首先避免其中不可到达的地址；其次当有组播地址时，选择那些范围匹配的地址；第三要避免弃用的地址；然后按照移动时的 Home 地址、具有匹配标志的地址、更高优先权的地址、原生 IPv6 地址、具有较小的范围的地址、具有最长匹配前缀的地址的顺序来进行选择，其中地址的标志、优先权由系统的策略表定义，缺省的策略表如表 5 所示.

表 5　缺省的策略表

前缀	优先权	标志
::1/128	50	0
::/0	40	1
::ffff:0:0/96	35	4
2002::/16	30	2
2001::/32	5	5
fc00::/7	3	13
::/96	1	3
fec0::/10	1	11
3ffe::/16	1	12

在进行源地址选择时，RFC 6724[106]推荐的顺序是，和目的相同的地址、具有合适的范围的地址、避免使用弃用的地址、优先移动时的 Home 地址、所用的接口的地址、和下一跳相同的前缀、具有匹配的标志的地址、临时地址（不过用户可以通过类似 RFC5014[107]的 API 进行其他选择）、最长匹配的前缀的地址.

针对源地址/目的地址组合选择的问题，RFC 8305[108]提出了 Happy-eyeball 方案. Happy eyeball 方案建议，在双栈的情况下，应当优先访问 IPv6 地址的域名服务器，在该服务器没有应答的情况下，可以做一定的标志并使用其他服务器地址. 此外，如果客户端有到各个目的地址的 RTT 值，应该优先选择较小的 RTT 的对应地址. 如果客户端记录了过去使用过的地址，那么应该在优先选择使用过的地址，这有助于一些如 Fast Open（定义于 RFC7413[109]）、或 HTTP Cookie 之类的措施的使用. 之后这些地址将被交叉排序出来，也就是说，如果第一个地址属于某个地址族，那么第二个地址应当为另一个地址族，这样以避免由于某个地址族的连接问题导致耽搁过长时间. 有的客户端由于更倾向于使用某个地址族的地址，可以设置多个连续的该地址族的地址，这个数目可以在“First Address Family Count”设置中指定. 对多个地址的连接需要一个接着一个的进行，如果有一个成功，其他的连接就可以终止了. 连接请求发送的间隔可以通过“Connection Attempt Delay”指定，建议缺省值为 250 ms.

目前虽然有了这些标准，然而如何在多地址、多地址族的情况下进行快速最优策略选择，仍然有较多的实际问题存在，有待于进一步研究解决.

8.2　定位与身份标识分离相关的研究与标准

在 TCP/IP 协议中，IP 地址同时起到了定位和身份标识的作用，而上层的应用则一般建立在以源地址、源端口、目的地址、目的端口、协议为基础的五元组会话基础上，这使得一个会话难以同时使用多个地址；此外，如果地址因为主机移动等原因发生变化，原有的绑定关系则被破坏，需要建立新的会话，因此导致移动 IP 上的问题. 为了解决这些问题，IETF 进行了许多关于将 IP 地址的定位、身份标识功能分离方面的研究，其中有代表性的工作有位置、身份分离协议 LISP（Locator/ID Separation Protocol）[110]、主机标识协议 HIP（Host Identity Protocol）[111]以及基于 IPv6 中介的站点多宿 SHIM6（Site Multihoming by IPv6 Intermediation）.

HIP 协议体系结构定义于 RFC4423[111]，如图 24 所示. 目前 HIP 协议的版本为 HIPv2，定义于 RFC 7401[112]. HIP 协议中，在传输层和 IP 协议之间引

入了新的 HIP 层，HIP 层标识称为主机标识 HI（Host Identity），它是代表主机身份的签名算法所对应的公钥，主机标识标签 HIT（Host Identity Tag）是 IPv6 地址格式的 HI 的哈希，用于作为主机的身份标识，而通信时所采用的地址则只用于数据发送，即使终端 IP 地址发生变更，通信也不会被中断.

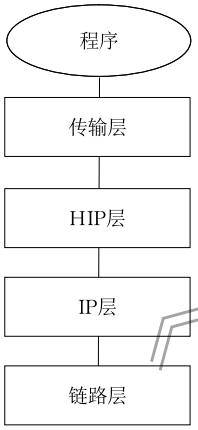

图 24 HIP 协议框架

HIPv2[112]协议中，主机标识标签是一种叠加网络中可路由密码学生成的哈希标识 ORCHIDv2（Overlay Routable Cryptographic Hash Identifiers Version 2），它定义于 RFC 7343[113]，可以被现有 IPv6 的 API 中应用层所看到，但不能出现在 IPv6 数据包包头中，也不能在网络中路由. RFC 7343[113]中定义了 ORCHIDv2 地址块 2001：20::/28，这一地址的后 100 比特中，前 4 比特为生成算法标识，后 96 比特由上下文标识和输入比特字符串连接后哈希的中间 96 比特构成. 定义于 RFC 4843[114]的 ORCHID（Overlay Routable Cryptographic Hash Identifiers）使用的 2001：10::/28 也因为被 ORCHIDv2 的推出而被废弃.

LISP[110]协议的主要思想是将 IP 地址分为两类，一类是终端标识（Endpoint Identifiers，EIDs），另一类则是位置标识（Routing Locators，RLOCs）. 主机通过 EID 用于标识主机身份，其长度为 32 位（IPv4）或 128 位（IPv6），必须全球唯一且不能用作 RLOC. IPv6 中，端点身份标识具有自己特殊的地址空间，RFC 7954[115]定义了 2001：5::/32 作为部署 LISP 时的端点身份标识地址空间，预计有效期到 2019-09，不过可以延迟到 2022-09. RLOC 用于标识主机位置，其长度为 32 位（IPv4）或 128 位（IPv6），通常分配给路由器，用于填写 LISP 外层包头的源地址或目的地址，通过使用隧道封装技术，LISP 无需对主机协议栈做任何修改，也不需要对网络中现有的基础设置做大规模改进，只需添加相对较少的具有特殊功能的隧道路由器即可实现位置、身份的分离.

SHIM6 思想是修改终端网络协议栈，在 IP 路由子层之上，IP 目的端子层之下插入 SHIM 层，实现位置与身份标识的分离[116]，如图 25 所示. 上层应用所看到的是标识符，而具体的网络通信则通过 IP 层的地址来实现，在通信过程中一直保持上层标识（Upper-Layer IDentifier，ULID）不变，应用层并不知道下层链路的变化. 为了保证上层所看到的标识不会变化，同时便于上层的应用层程序的开发，RFC 5533[116]认为可以使用唯一本地地址（ULA）来作为上层标识.

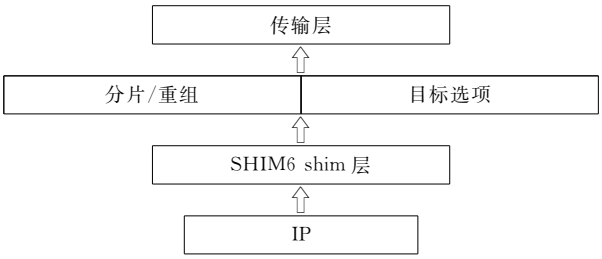

图 25 SHIM6 体系结构

目前而言，这三种新的体系结构都没有得到广泛使用，主要的问题在于，在 IP 层解决定位与身份标识分离，需要依赖于终端操作系统的支持，因此难以实现渐进式的部署. 此外，尽管移动 IP、多宿下的性能优化是两个重要问题，然而也并非普遍存在，因此在 IP 层解决这一问题容易产生代价大、收效不明显的问题. 目前 IETF 进行的多路径 TCP① 方面的研究，正在得到更多的重视.

9 未来 IPv6 地址体系结构标准化的研究方向

IPv6 的提出到现在已经有二十多年，与研究者的预期有所不同的是，IPv6 最初并未得到广泛的应用，这主要是由于两个原因造成，首先 IPv4 通过 CIDR、NAT 等技术，地址的使用效率大大提高了；另一方面则是由于互联网体系结构的瘦腰模型中，IP 层是其中核心的一个环节，微小的改动都需要较长时间的过渡. 近年来，IPv6 的发展速度大大加快，

① IETF Multipath TCP（mptcp）Working Group. https://datatracker.ietf.org/wg/mptcp/about/

首先是因为多年来的积淀使得设备支持程度较高，大部分网络设备、操作系统都可以支持 IPv6 了；其次，物联网的加速应用使得 IPv6 使用范围不断扩大，现有的 IPv4 网络受限于地址数目，难以解决海量物联网设备的高并发上网，而 IPv6 最主要的优势即是其巨大的地址空间；第三，IPv4 地址的枯竭也使得 IPv6 网络的发展速度大大加快了.

在 IPv6 地址结构方面，未来的研究热点主要有如下两个方面，首先是 IPv6 地址结构在新场景、新用途方面的研究，最主要的是物联网中的 IPv6 地址结构研究；其次是 IPv6 地址结构的安全和隐私问题. 以下我们将就这两个方面进行详细阐述.

9.1　物联网中的 IPv6 地址结构研究

新应用场景中最重要的是物联网应用，物联网中接入设备数量将会有爆炸性增长，因此 IPv6 成为物联网中自然的选择.

物联网的物理网络标准有很多，其中较早得到深入研究的是 IEEE802.15.4[2]，IEEE 802.15.4 网络主要为个人区域网络(Personal Area Network，PAN)和无线个人区域网络(Wireless Personal Area Network，WPAN)设计，以便把几米范围内的多个设备通过无线方式连接在一起，使它们可以相互通信甚至接入局域网或互联网. IEEE 802.15.4 具有网络最大传输单元小、传输速率低，以及设备低能耗、计算能力有限、数量极大、经常处于睡眠状态等特点，无法直接将 IPv6 协议应用上去[2]. 为此 IETF 的 6LoWPAN 工作组引入了 6LoWPAN 适配层，以便进行 IPv6 包头的压缩，如图 26 所示. IETF 的 6LowPAN 工作组制定了两种压缩算法 LOWPAN_HC1[2,117] 和 LOWPAN_IPHC [118].

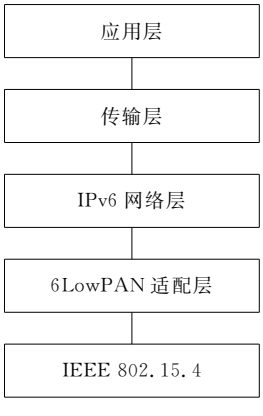

图 26　6LowPAN 体系结构

为了方便 IPv6 地址的压缩，根据 RFC4944[117]，在基于 IEEE802.15.4 的网络中，IPv6 地址可以基于 EUI-64 方案得到，不过也可以根据 16 比特的短地址得到 48 比特的伪硬件地址：左 32 位由 16 位 0 和 16 位 PAN ID(如果不知道 PAN ID 就用 16 位 0)组成，最后与 16 比特的短地址相连接. 然而，在合成的接口标识符里，为了表示这一接口标识不是全局唯一，“全局/本地”(U/L)位应当设置为 0. IPv6 的源地址和目的地址通常都使用链路本地地址，这样便于直接从地址中得到 802.15.4 的 MAC 地址. 对于 16 比特的短地址而言，RFC4944 规定第一比特为 0 时为单播地址，前三比特为 100 时为组播地址，其他地址保留.

为了保证 16 比特短地址的唯一性，RFC6775[119] 中建议可以使用 DHCPv6、基于地址登记选项(Address Registration Option)的重复地址检测 DAD 等方法来保证. 如果使用了地址登记选项 ARO，那么必须要包含源链接层地址选项 SLLAO(定义于 RFC4861[30])，而且被登记的地址必须是 NS 消息的源地址.

目前 IETF 的主要工作是针对 6LoWPAN 适配层在各种低功耗 WPAN 网络上设计新的适配方案，其中都包含地址生成方案，如 RFC7428[120] 中设计了 G.9959 网络上的 IPv6 地址生成方案，RFC7668[121] 定义了 Bluetooth LE 网络下的 IPv6 地址生成方案，RFC8163[122] 针对 6LoWPAN 在主-从/令牌数据链路协议(Master-Slave/Token-Passing，MS/TP)中的地址方案进行了设计，RFC8105[123] 针对 6LoWPAN 在 DECT(Digital Enhanced Cordless Telecommunications，DECT)网络上的使用进行了规范. 基本的思想均是基于硬件地址或 16 比特短地址来生成接口标识，以便实现 IPv6 地址的压缩.

在 6LoWPAN① 工作组工作的基础上，IETF 成立了 6lo② 工作组、6tisch③ 工作组、lpwan④ 工作组等进行不同场景下 IPv6 的物联网上标准化研究. 此外，RoLL⑤ 工作组主要讨论低功耗网络中的路由协议，CoRE⑥ 工作组主要讨论资源受限网络环境下的信息读取操控问题，旨在制订轻量级的应用层协议.

① IPv6 over Low power WPAN (6lowpan). https://datatracker.ietf.org/wg/6lowpan/about/
② 2IPv6 over Networks of Resource-constrained Nodes (6lo). https://datatracker.ietf.org/wg/6lo/about/
③ IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). https://datatracker.ietf.org/wg/6tisch/about/
④ IPv6 over Low Power Wide-Area Networks (lpwan). https://datatracker.ietf.org/wg/lpwan/about/
⑤ Routing Over Low power and Lossy networks (roll). https://datatracker.ietf.org/wg/roll/about/
⑥ Constrained RESTful Environments (core). https://datatracker.ietf.org/wg/core/about/

这些物联网相关的工作组中，很多刚成立不久，物联网相关研究正在如火如荼地展开.

9.2 IPv6 地址隐私与安全

IPv6 网络兼具设备支持广泛和设备支持不成熟两个特点，一方面 IPv6 经过二十多年的研究，已经得到广泛支持，大部分网络设备和软件都宣称支持 IPv6. 但另一方面，IPv6 的支持又都是初步的、不成熟的：很多支持仅停留在最简单功能的实现，标准中一些实施难度较大、但不体现为功能增加的安全设计容易被忽略，因此支持是初步的；IPv6 虽然已经有大规模使用，但是使用方式单一，远不及 IPv4 中经过各种场景、各种应用的考验，因此 IPv6 支持又是不成熟的.

针对这一现状，随着 IPv6 大规模商用的提速，IPv6 安全方面的隐忧也越来越多. 增加 IPv6 安全风险的还有一个因素就是 IPv6 面临的应用场景远远比 IPv4 要复杂得多，复杂环境下可能会产生更多的安全问题. 例如 IPv6 和 IPv4 的混合使用、IPv6 在低能耗物联网上的大规模使用和地址压缩，都可能产生新的安全风险. 例如，在 6LoWPAN 中，为便于进行 IPv6 包头压缩，很多接口标识都使用了较为简单的形式. RFC 8065[124] 研究了 6LoWPAN 中的安全风险，提出了可以使用哈希算法，既能够保证无状态的包头压缩，又可以得到覆盖面较广的接口标识，但是如何能够不影响包头压缩的效率，则仍然有待于研究. RFC 8065[124] 中建议让接口标识具有较短的有效时间，从而避免扫描或事件关联的发生.

目前 IPv6 地址安全方面的研究，仍然主要集中在地址生成方案可能引发的扫描、隐私泄露等方面的问题，未来随着更多应用场景的出现，各种安全问题可能会越来越多地出现. 与物联网相关的研究有所不同的是，安全和隐私保护方面的研究，通常分散到各个工作组中，因此相对而言跟踪更为复杂.

10 总结与结论

本文总结了目前 IPv6 地址结构相关的标准，包括 IPv6 全球单播地址结构、IPv6 组播地址结构、IPv6 任播地址结构等，在此基础上，特别介绍了 IPv6 过渡技术中的地址结构研究，以及 IPv6 安全和隐私保护相关的 IPv6 接口标识的生成方案研究. 与 IPv4 网络不同的是，IPv6 网络中多宿主机的情况更加普及，本文介绍了 IPv6 网络中多地址下的地址选择和路由选择问题与解决方案，并简要概述了定位与身份标识分离方面的研究进展. 物联网的快速发展使得 IPv6 正在加速得到广泛部署，物联网中 IPv6 地址结构是一个目前和未来都重要的研究方向. 与 IPv4 网络所经历的长期检验不同，IPv6 协议设计中针对大规模应用中的安全问题缺乏经验，此外 IPv6 协议的实现也只是满足于基本实现，考虑到 IPv6 较 IPv4 有更为复杂的应用场景，IPv6 的安全研究将会越来越受到关注.

参 考 文 献

[1] Hinden R, Deering S. IP Version 6 Addressing Architecture. RFC 4291, February 2006

[2] Kushalnagar N, Montenegro G, Schumacher C. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, August 2007

[3] Thomson S, Narten T, Jinmei T. IPv6 Stateless Address Autoconfiguration. RFC 4862, September 2007

[4] Hinden R, Deering S. IP Version 6 Addressing Architecture. RFC 1884, December 1995

[5] Hinden R, Deering S. IP Version 6 Addressing Architecture. RFC 2373, July 1998

[6] Hinden R, Deering S. Internet Protocol Version 6 (IPv6) Addressing Architecture. RFC 3513, April 2003

[7] Kawamura S, Kawashima M. A Recommendation for IPv6 Address Text Representation. RFC 5952, August 2010

[8] Carpenter B. RFC 1888 is Obsolete. RFC 4048, April 2005

[9] Hinden R, Haberman B. Unique Local IPv6 Unicast Addresses. RFC 4193, October 2005

[10] Huitema C, Carpenter B. Deprecating Site Local Addresses. RFC 3879, DOI10.17487/RFC3879, September 2004

[11] Shin M-K, Hong Y-G, Hagino J, et al. Application Aspects of IPv6 Transition. RFC 4038, March 2005

[12] Hilliard N, Freedman D. A Discard Prefix for IPv6. RFC 6666, August 2012

[13] Kumari W, McPherson D. Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF). RFC 5635, August 2009

[14] Turk D. Configuring BGP to Block Denial-of-Service Attacks. RFC 3882, September 2004

[15] Popoviciu C, Hamza A, Van de Velde G, Dugatkin D. IPv6 Benchmarking Methodology for Network Interconnect Devices. RFC 5180, May 2008

[16] Huston G, Lord A, Smith P. IPv6 Address Prefix Reserved for Documentation. RFC 3849, July 2004

[17] Hinden R, Fink R, Postel J. IPv6 Testing Address Allocation. RFC 2471, December 1998

[18] Fink R, Hinden R. 6bone (IPv6 Testing Address Allocation) Phaseout. RFC 3701, March 2004

[19] Narten T, Huston G, Roberts L. IPv6 Address Assignment to End Sites. BCP 157. RFC 6177, March 2011

[20] Van de Velde G, Popoviciu C, Chown T, et al. IPv6 Unicast Address Assignment Considerations. RFC 5375, December 2008

[21] Durand A, Huitema C. The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio. RFC 3194, November 2001

[22] Huston G. Considerations on the IPv6 Host Density Metric. RFC 4692, October 2006

[23] Carpenter B, Chown T, Gont F, et al. Analysis of the 64-bit Boundary in IPv6 Addressing. RFC 7421, January 2015

[24] Kohno M, Nitzan B, Bush R, et al. Using 127-Bit IPv6 Prefixes on Inter-Router Links. RFC 6164, April 2011

[25] Mawatari M, Kawashima M, Byrne C. 464XLAT: Combination of Stateful and Stateless Translation. RFC 6877, April 2013

[26] Bao C, Huitema C, Bagnulo M, et al. IPv6 Addressing of IPv4/IPv6 Translators. RFC 6052, October 2010

[27] Bagnulo M, Matthews P, van Beijnum I. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. RFC 6146, April 2011

[28] Atkinson R J, Bhatti S N. Identifier-Locator Network Protocol (ILNP) Engineering Considerations. RFC 6741, November 2012

[29] Mrugalski T, Siodelski M, Volz B, et al. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 8415, DOI 10.17487/RFC8415, November 2018

[30] Narten T, Nordmark E, Simpson W, Soliman H. Neighbor Discovery for IP version 6 (IPv6). RFC 4861, September 2007

[31] Haskin D, Allen E. IP Version 6 over PPP. RFC 2472, December 1998

[32] Bhattacharyya S. An Overview of Source-Specific Multicast (SSM). RFC 3569, July 2003

[33] Savola P, Haberman B. Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address. RFC 3956, November 2004

[34] Haberman B, Thaler D. Unicast-Prefix-based IPv6 Multicast Addresses. RFC 3306, August 2002

[35] Droms R. IPv6 Multicast Address Scopes. RFC 7346, August 2014

[36] Deering S, Haberman B, Jinmei T, et al. IPv6 Scoped Address Architecture. RFC 4007, March 2005

[37] Savola P. Overview of the Internet Multicast Addressing Architecture. RFC 6308, June 2011

[38] Hanna S, Patel B, Shah M. Multicast Address Dynamic Client Allocation Protocol (MADCAP). RFC 2730, December 1999

[39] Boucadair M, Venaas S. Updates to the IPv6 Multicast Addressing Architecture. RFC 7371, September 2014

[40] Haberman B. Allocation Guidelines for IPv6 Multicast Addresses. RFC 3307, August 2002

[41] Park J-S, Shin M-K, Kim H-J. A Method for Generating Link-Scoped IPv6 Multicast Addresses. RFC 4489, April 2006

[42] Hinden R, Deering S. IPv6 Multicast Address Assignments. RFC 2375, July 1998

[43] Waitzman D, Partridge C, Deering S. Distance Vector Multicast Routing Protocol. RFC 1075, November 1988

[44] Moy J. OSPF Version 2. STD 54, RFC 2328, April 1998

[45] Topolcic C. Experimental Internet Stream Protocol: Version 2 (ST-II). RFC 1190, October 1990

[46] Malkin G, Minnear R. RIPng for IPv6. RFC 2080, January 1997

[47] Savage D, Ng J, Moore S, et al, Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). RFC 7868, May 2016

[48] Vida R, Costa L. Multicast Listener Discovery Version 2 (MLDv2) for IPv6. RFC 3810, June 2004

[49] Chakeres I. IANA Allocations for Mobile Ad Hoc Network (MANET) Protocols. RFC 5498, March 2009

[50] Macker J. Simplified Multicast Forwarding. RFC 6621, May 2012

[51] Aboba B, Thaler D, Esibov L. Link-local Multicast Name Resolution (LLMNR). RFC 4795, January 2007

[52] Cheshire S, Krochmal M. Multicast DNS. RFC 6762, February 2013

[53] Crawford M, Haberman B. IPv6 Node Information Queries. RFC 4620, August 2006

[54] Guttman E. Service Location Protocol Modifications for IPv6. RFC 3111, May 2001

[55] Mills D. Network Time Protocol (Version 2) Specification and Implementation. RFC 1119, September 1989

[56] Mills D, Martin J, Burbank J, Kasch W. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905, June 2010

[57] Venaas S, Parekh R, Van de Velde G, et al. Multicast Addresses for Documentation. RFC 6676, August 2012

[58] Abley J, Lindqvist K. Operation of Anycast Services. BCP 126, RFC 4786, December 2006

[59] Kiesel S, Penno R. Port Control Protocol (PCP) Anycast Addresses. RFC 7723, January 2016

[60] Wing D, Cheshire S, Boucadair M, et al. Port Control Protocol (PCP). RFC 6887, April 2013

[61] Patil P, Reddy T, Wing D. Traversal Using Relays around NAT (TURN) Server Auto Discovery. RFC 8155, April 2017

[62] Mahy R, Matthews P, Rosenberg J. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). RFC 5766, April 2010

[63] Srisuresh P, Ford B, Kegel D. State of Peer-to-Peer (P2P) Communication Across Network Address Translators (NATs). RFC 5128, March 2008

[64] Bumgardner G. Automatic Multicast Tunneling. RFC 7450, February 2015

[65] Abley J, Dickson B, Kumari W, Michaelson G. AS112 Redirection Using DNAME. RFC 7535, May 2015

[66] Rose S, Wijngaards W. DNAME Redirection in the DNS. RFC 6672, June 2012

[67] Abley J, Sotomayor W. AS112 Nameserver Operations. RFC 7534, May 2015

[68] Johnson D, Deering S. Reserved IPv6 Subnet Anycast Addresses. RFC 2526, March 1999

[69] Steffann S, van Beijnum I, van Rein R. A Comparison of IPv6-over-IPv4 Tunnel Mechanisms. RFC 7059, November 2013

[70] Townsley W, Troan O. IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) — Protocol Specification. RFC 5969, August 2010

[71] Templin F, Gleeson T, Thaler D. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). RFC 5214, March 2008

[72] Despres R, Carpenter B, Wing D, Jiang D. Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44). RFC 6751, October 2012

[73] Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. RFC 3056, February 2001

[74] Huitema C. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). RFC 4380, February 2006

[75] Carpenter B, Jung C. Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. RFC 2529, March 1999

[76] Li X, Bao C, Dec W, et al. Mapping of Address and Port using Translation (MAP-T). RFC 7599, July 2015

[77] Troan O, Dec W, Li X, et al. Mapping of Address and Port with Encapsulation (MAP-E). RFC 7597, July 2015

[78] Cui Y, Sun Q, Boucadair M, et al. Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture. RFC 7596, July 2015

[79] Anderson T. Local-Use IPv4/IPv6 Translation Prefix. RFC 8215, August 2017

[80] Thaler D, Krishnan S, Hoagland J. Teredo Security Updates. RFC 5991, September 2010

[81] Gont F, Chown T. Network Reconnaissance in IPv6 Networks. RFC 7707, DOI10.17487/RFC7707, March 2016

[82] Crawford M. Transmission of IPv6 Packets over Ethernet Networks. RFC 2464, December 1998

[83] Carpenter B, Jiang S. Significance of IPv6 Interface Identifiers. RFC 7136, February 2014

[84] Bao C, Li X, Baker F, et al. IP/ICMP Translation Algorithm. RFC 7915, June 2016

[85] Narten T, Draves R, Krishnan S. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941, September 2007

[86] Gont F. A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC). RFC 7217, April 2014

[87] Gont F, Cooper A, Thaler D, Liu W. Recommendation on Stable IPv6 Interface Identifiers. RFC 8064, February 2017

[88] Gont F, Liu W. A Method for Generating Semantically Opaque Interface Identifiers (IIDs) with the Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 7943, September 2016

[89] Narten T, Nordmark E, Simpson W. Neighbor Discovery for IP Version 6 (IPv6). RFC 2461, December 1998

[90] Thomson S, Narten T. IPv6 Stateless Address Autoconfiguration. RFC 2462, December 1998

[91] Nikander P, Kempf J, Nordmark E. IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756, May 2004

[92] Gashinsky I, Jaeggli J, Kumari W. Operational Neighbor Discovery Problems. RFC 6583, March 2012

[93] Arkko J, Kempf J, Zill B, Nikander P. SEcure Neighbor Discovery (SEND). RFC 3971, March 2005

[94] Aura T. Cryptographically Generated Addresses (CGA). RFC 3972, March 2005

[95] Bagnulo M, Arkko J. Cryptographically Generated Addresses (CGA) Extension Field Format. RFC 4581, October 2006

[96] Bagnulo M, Arkko J. Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs). RFC 4982, July 2007

[97] Bi J, Wu J, Yao G, Baker F. Source Address Validation Improvement (SAVI) Solution for DHCP. RFC 7513, May 2015

[98] Bi J, Yao G, Halpern J, Levy-Abegnoli E. Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario. RFC 8074, February 2017

[99] Nordmark E, Bagnulo M, Levy-Abegnoli E. FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses. RFC 6620, May 2012

[100] Bagnulo M. Hash-Based Addresses (HBA). RFC 5535, June 2009

[101] Cooper A, Gont F, Thaler D. Security and Privacy Considerations for IPv6 Address Generation Mechanisms. RFC 7721, March 2016

[102] Cooper A, Tschofenig H, Aboba B, et al. Privacy Considerations for Internet Protocols. RFC 6973, July 2013

[103] Davies E, Mohacsi J. Recommendations for Filtering ICMPv6 Messages in Firewalls. RFC 4890, May 2007

[104] Draves R, Thaler D. Default Router Preferences and More-Specific Routes. RFC 4191, November 2005

[105] Baker F. Carpenter B. First-Hop Router Selection by Hosts in a Multi-Prefix Network. RFC 8028, November 2016

[106] Thaler D, Draves R, Matsumoto A, Chown T. Default Address Selection for Internet Protocol Version 6 (IPv6). RFC 6724, September 2012

[107] Nordmark E, Chakrabarti S, Laganier J. IPv6 Socket API for Source Address Selection. RFC 5014, September 2007

[108] Schinazi D, Pauly T. Happy Eyeballs Version 2: Better Connectivity Using Concurrency. RFC 8305, December 2017

[109] Cheng Y, Chu J, Radhakrishnan S, Jain A. TCP Fast Open. RFC 7413, December 2014

[110] Farinacci D, Fuller V, Meyer D, Lewis D. The Locator/ID Separation Protocol (LISP). RFC 6830, January 2013

[111] Moskowitz R, Nikander P. Host Identity Protocol (HIP) Architecture. RFC 4423, May 2006

[112] Moskowitz R, Heer T, Jokela P, Henderson T. Host Identity Protocol Version 2 (HIPv2). RFC 7401, April 2015

[113] Laganier J, Dupont F. An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2). RFC 7343, September 2014

[114] Nikander P, Laganier J, Dupont F. An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID). RFC 4843, April2007

[115] Iannone L, Lewis D, Meyer D, Fuller V. Locator/ID Separation Protocol (LISP) Endpoint Identifier (EID) Block. RFC 7954, September 2016

[116] Nordmark E, Bagnulo M. Shim6: Level 3 Multihoming Shim Protocol for IPv6. RFC 5533, June 2009

[117] Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, September 2007

[118] Hui J, Thubert P. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, September 2011

[119] Shelby Z, Chakrabarti S, Nordmark E, Bormann C. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 6775, November 2012

[120] Brandt A, Buron J. Transmission of IPv6 Packets over ITU-T G.9959 Networks. RFC 7428, February 2015

[121] Nieminen J, Savolainen T, Isomaki M, et al, IPv6 over BLUETOOTH(R) Low Energy. RFC 7668, October 2015

[122] Lynn K, Martocci J, Neilson C, Donaldson S. Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks. RFC 8163, May 2017

[123] Mariager P, Petersen J, Shelby Z, et al, Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE). RFC 8105, May 2017

[124] Thaler D. Privacy Considerations for IPv6 Adaptation-Layer Mechanisms. RFC 8065, February 2017

ZHANG Qian-Li, Ph. D., associate researcher. His main research interests include next generation internet architecture, network security.

JIANG Cai-Ping, M. S., senior engineer. Her research interests include computer network.

WANG Ji-Long, Ph. D., professor. His research interests include next generation internet architecture, cyberspace surveying and mapping.

LI Xing, Ph. D., professor. His research interests include next generation interest architecture, network security, network measurement.

Background

Compared to IPv4, IPv6 address has more bits and is more complicated. Understanding the IPv6 address architecture is important in various IPv6 related researches such as IPv6 measurement, IPv6 management and IPv6 security. This survey gives a brief introduction of RFCes related to IPv6 address architecture; including IPv6 multicast address architecture, IPv6 anycast address architecture, and IPv6 unicast address architecture. Especially this survey illustrates the address architecture in various IPv6 transition techniques and the IPv6 interface ID generation schemes. IPv6 address related security issues, privacy consideration and address selection also are discussed in this survey. This work was supported by the National Key R&D Program of China (Grant No. 2017YFB0503703).