# 基于5G SA网络IPv6单栈的研究与实践

Research and Practice of IPv6 Single Stack Based on 5G SA Network

邢建兵[1]，史春磊[2]，高　沛[2]，蔡　超[2]，邱佳慧[2]，屠礼彪[1]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中国联通智网创新中心，北京 100048）

Xing Jianbing[1], Shi Chunlei[2], Gao Pei[2], Cai Chao[2], Qiu Jiahui[2], Tu Libiao[1] (1. China United Network Communications Group Co., Ltd., Beijing 100033, China; 2. Innovation Center of China Unicom Intelligent Network, Beijing 100048, China)

**摘　要：**

中国5G独立组网（SA）互联网网络已经全面进入了IPv4和IPv6双栈运行阶段，但如何引入IPv6单栈，成为当前运营商面临的新挑战。通过对IPv6单栈概念和技术的分析，提出了IPv6单栈网络部署方案，并进行了实践验证。实践证明，该方案是可行的。随着业务应用由IPv4向IPv6演进，IPv6的流量占比将大幅提升，基于实践和分析，提出了下一步IPv6发展的策略建议。

**关键词：**

5G SA；IPv6；下一代网络；NAT64；DNS64

**doi：**10.12045/j.issn.1007-3043.2024.06.014

**文章编号：**1007-3043（2024）06-0067-05

**中图分类号：**TP393.4

**文献标识码：**A

**开放科学（资源服务）标识码（OSID）：**

**Abstract：**

China's 5G Standalone networking（SA） Internet network has fully entered the operation of IPv4 and IPv6 dual stack operation, How to introduce IPv6 single stack has become a new challenge for current operators. Through the analysis of the concept and technology of IPv6 single stack, a deployment scheme for IPv6 single stack network is proposed and verified in practice, and the practice proves that the scheme is feasible. As service applications evolve from IPv4 to IPv6, the proportion of IPv6 traffic will increase significantly. Based on practice and analysis, strategy suggestions for the next IPv6 development are put forward.

**Keywords：**

5G SA；IPv6；Next generation network；NAT64；DNS64

**引用格式：**邢建兵，史春磊，高沛，等. 基于5G SA网络IPv6单栈的研究与实践[J]. 邮电设计技术，2024（6）：67-71.

## 0　前言

互联网协议第6版（IPv6）是互联网升级演进的必然趋势、网络技术创新的重要方向、网络强国建设的基础支撑，IPv6的发展在中国一直受到高度重视，目前5G SA互联网已经形成IPv4和IPv6双栈运行局面。2021年7月，中央网信办、国家发展改革委、工业和信息化部联合印发的《关于加快推进互联网协议第6版（IPv6）规模部署和应用工作的通知》明确指出，增强IPv6网络互联互通能力，积极推进IPv6单栈网络部署，是我国未来推进IPv6工作的重点任务之一。在国际上，美国计划到2025年联邦网络的80%将采用IPv6单栈部署。IPv6的发展主要呈现出两大趋势：一是IPv4/IPv6双栈向IPv6单栈发展；二是IPv6单栈不仅向纯IPv6过渡更彻底，而且使网络演进得更简单[1-2]。

网络协议栈是互联网运行的基础，是互联互通的基石。双栈技术作为一种在同一网络设备上同时部署IPv4和IPv6的技术方法，允许设备同时处理IPv4和IPv6流量，是一种平稳过渡的优选方案，也是现网中普遍部署的方案。然而，IPv4/IPv6双栈部署虽然实现了对IPv6协议栈业务的支持，但并未彻底解决IPv4的地址紧缺和安全可溯复杂等实质问题，而且网络维护成

收稿日期：2024-04-28

本高，安全风险大，不仅对设备提出很高的要求，增加了维护工作的复杂性，还给业务发展带来了困惑和阻碍。从双栈向单一协议栈演进，不仅可以降低网络维护工作量和用网成本，还能使网络架构更加简单、路由更收敛，降低互联网暴露面，从而使网络更加安全。

## 1 IPv6单栈的概念浅析

IPv6单栈网络是在网络中只保留IPv6协议栈，关闭IPv4协议栈，并以IPv6协议为核心进行编址及路由[3-4]。它支持SRv6的技术创新，也支持IPv6+的技术演进。IPv6单栈的目的是构建一种极简、智能、安全、绿色的新型网络，是IPv6发展的方向。IPv6单栈网络有2种形态：过渡形态和终极形态。

a）过渡形态。在过渡形态下，网络不仅要承载IPv6业务，也要承载存量IPv4业务。进入5G时代，IPv6的演进仍面临产业链成熟度不均衡的挑战，从终端产业链、网络产业链、业务产业链3个维度来分析，终端和网络产业链成熟度高于业务产业链。根据3GPP的标准设计和设备实现要求，5G网络和终端都支持IPv6。截至2023年5月，IPv6活跃用户数占网民数的比例已超过35%，而在中国，这一比例超过了70%。业务产业链正在按需升级，但仍有存量IPv4业务在提供服务，这些业务要求边缘网络支持IPv4业务流量的接入和穿越。

b）终极形态。在终极形态下，互联网业务全部为IPv6业务，网络中将不存在IPv4的业务流。届时，将关闭边缘的IPv4属性，网络中仅存在IPv6协议。

从双栈进入到IPv6单栈阶段，需要经历IPv6单栈网络逐步部署的过程。这个过程至少需要几年的时间，而且互联网业务要全部实现IPv6化还需要更长的时间，所以短期内实现IPv6单栈的终极形态是不现实的。另外，IPv6单栈网络的部署，一定程度上会促进互联网业务向IPv6迁移。如果不推进IPv6单栈的部署，持续保持双栈状态，则业务IPv6迁移的动力更加不足。所以部署IPv6单栈网络，既能承载IPv6业务，又能承载IPv4业务，推动过渡形态的IPv6单栈方案是必经之路。

## 2 IPv6单栈的技术分析

现阶段IPv6单栈面临的核心问题是，在逐渐关闭网络中的IPv4协议以后，网络中的设备如何承载存量的IPv4业务。针对这个问题，业界已经提出了多种技术方案，这些方案主要解决IPv6地址和IPv4地址之间的互通问题。例如，在4over6隧道技术中，DS-Lite采用了基于地址族转换路由器（AFTR）技术，而在主干网中则采用GRE隧道或无状态翻译技术等。

通常情况下，IP网络由多个自治域组成，各自治域又由不同的组织进行管理，并采用不同的路由和安全策略。如果不能很好地协同工作，可能导致网络中出现IPv6和IPv4数据包之间的多次转换，从而使网络变得复杂。因此，从双栈向过渡形态IPv6单栈的过渡方案主要有3种（见表1）。

**表1　IPv6单栈3种主要过渡方案**

| 方案 | 终端 | 网络 | 业务 | 过渡 | 终端 | 网络 | 业务 |
|---|---|---|---|---|---|---|---|
| 方案1 | v4 | v4 | v4 | → | v6 | v4 | v4 |
| 方案2 | v4 | v4 | v4 | → | v4 | v6 | v4 |
| 方案3 | v4 | v4 | v4 | → | v6 | v6 | v4 |

方案1：终端使用IPv6单栈地址，通过IPv4网络访问IPv4业务。该方案是可行的技术方案。

方案2：终端使用IPv4地址，网络使用IPv6单栈来访问IPv4业务。该方案需要所有业务接入的网络均达成一致的部署方式。针对未部署XLAT方案的业务接入区，将存在业务不可访问的情况。

方案3：终端和网络全部采用IPv6单栈来访问IPv4地址。该方案依赖于被访问的业务接入的网络部署IPv6和IPv4之间的转换技术，所以暂时不做深入的方案验证。

## 3 IPv6单栈部署的总体技术方案

针对以上分析，本文提出了一个IPv6单栈的总体技术方案，该方案构建了一个以IPv6为基础协议的终端分配和业务承载的网络体系。方案的核心是采用NAT64（NAT指网络地址转换）和DNS64（DNS指域名解析系统）技术，在终端只获取IPv6地址的情况下，仍能够支持对IPv6和IPv4业务系统的访问。IPv6单栈总体技术方案示意如图1所示。

技术方案主要包含以下3个部分。

### 3.1 5G SA网络分配终端IPv6单栈地址

在当前的5G SA[5]场景下，UE采用双栈地址，N1、N2、N3、N4接口采用IPv6单栈方式互通，N6接口采用双栈方式互通。结合3GPP的5G标准和IPv6单栈的思路，部署网络实现只给终端分配IPv6地址[6]。

网络侧主要完成以下配置调整。

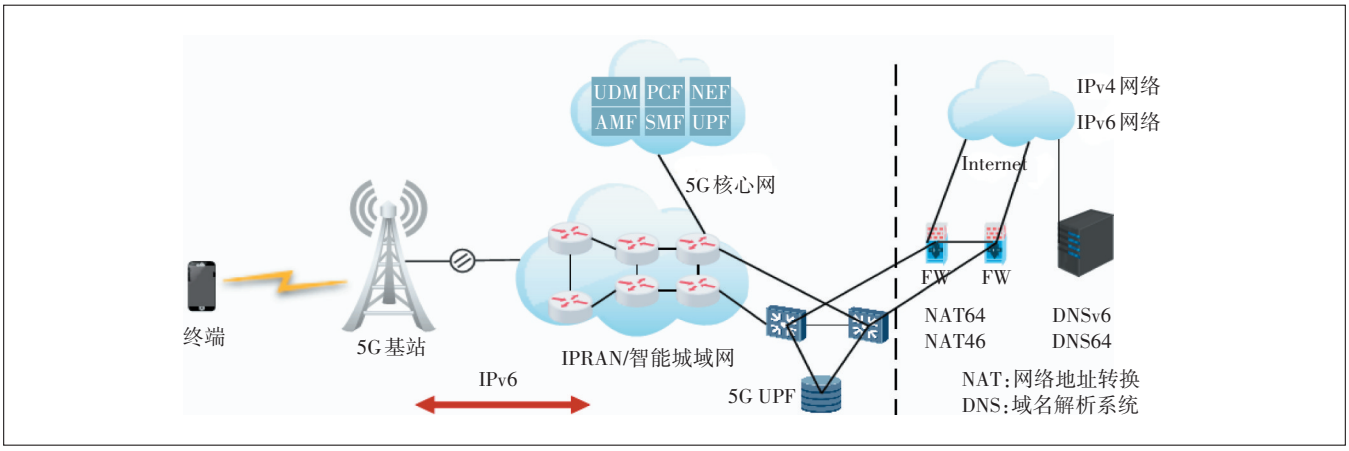


**图1**　IPv6单栈总体技术方案示意

a）新建用户DNN，完成在5GC控制面的配置，并配置IPv6单栈地址池。

b）当用户在5G SA网络登录时，网络侧根据用户签约的DNN选择对应的SMF、UPF，并为用户分配IPv6单栈地址。用户完成5GC的认证授权后，只获取IPv6单栈的地址。

### 3.2 DNS服务器实现DNS64功能

在IPv6单栈网络中，终端在完成5GC认证授权后，从网络侧只获得IPv6地址，但终端上可能存在支持IPv6的应用系统，也可能存在只支持IPv4的应用系统。如图1所示，当客户端访问只支持IPv4协议栈的网站或服务器时，其目的服务器的IPv4地址需要由DNS64服务器添加IPv6前缀Pref64合成IPv6地址。当终端向支持DNS64的DNS递归服务器发出AAAA类解析（IPv6地址解析）请求时，如果服务器返回的记录为空，说明该域名对应的服务器为IPv4单栈服务器。此时，DNS64服务器继续发出A类请求查询，并获得A类查询结果，DNS64支持将DNS查询信息中的A记录（IPv4地址）合成到AAAA记录（IPv6地址）中，即将IPv4应用服务器的IPv4地址映射成IPv6地址，是通过添加IPv6前缀Pref64来实现的，并将生成的AAAA类结果返回给终端，完成地址解析。当终端发起连接访问普通IPv6网站或其他服务器时，DNS64服务器将解析出IPv6的目的地址返回给终端。

### 3.3 防火墙实现NAT64功能

该功能可实现IPv6与IPv4网络地址和协议的转换，用于IPv6单栈客户端和IPv4业务端的数据传输，支持只拥有IPv6地址的终端发起连接并访问IPv4侧网络资源。NAT64功能适用于传输控制协议（TCP）、用户数据报协议（UDP）和Inernet控制报文协议（ICMP）。

IPv6单栈终端访问IPv4协议的应用或网站时，需要在5G的用户面功能（UPF）位置部署支持NAT64功能的设备。本方案采用UPF出口防火墙设备，防火墙设备支持NAT64功能。

终端收到DNS64的回复报文后，把解析的地址作为目的地址发往远端应用服务器。在获得AAAA类的解析结果后，该流量将被路由转发至UPF位置的出口防火墙（FW）上，源地址和目的地址的IPv6地址与IPv4地址在防火墙上进行转换或合成转换，从而实现访问IPv4业务端。需要补充说明的是，在防火墙中将IPv4地址合成IPv6地址采用的Pref64前缀与DNS64中解析后合成IPv6地址的Pref64前缀是一致的。

用户访问IPv4的业务流的工作流程如下。

a）当IPv6单栈终端发起访问IPv4应用的请求（数据上行）时，因IPv4地址资源紧张，不选择IPv4与IPv6一一对应的方式，而是选择IPv4+端口号的方式与IPv6对应。选定IPv4公网地址池的一个地址，作为出口地址。对于IPv6终端的源地址，其目的地址是加了前缀的IPv6地址。防火墙在收到终端发出的首个数据包时，会执行将源地址和目的地址的IPv6、IPv4之间的转换，从资源池中动态选取IPv4地址端口号，将源IPv6地址变换为IPv4地址+端口号的对应关系，利用该端口号在NAT64中建立和维护TCP和UDP的会话映射关系，在使用完毕后释放IPv4端口号，为目的地址剥离Pref64前缀，转换成目的IPv4地址。

b）当IPv4应用系统响应终端的业务请求时（数据下行），防火墙在收到应用系统的数据包时，实现源地

址和目的地址的IPv4、IPv6之间的转换。对于目的IPv4地址，根据防火墙中的映射会话将目的地址从IPv4地址转换成IPv6地址，同时进行端口和协议的转换；对于源IPv4地址，在防火墙中添加NAT64的映射前缀Pref64，进行IPv4到IPv6地址和协议的转换。

## 4 应用测试

### 4.1 IPv6单栈网络部署

根据5G SA组网IPv6单栈总体技术方案，某运营商在A市进行了IPv6单栈组网测试。现网网络组网如图2所示。本次IPv6单栈改造中，在现网UPF中新开DNN（CUV6TEST）供测试使用。5GC控制面仅分配IPv6地址。DNS开启DNS64功能，如果解析出IPv4地址，增加IPv6地址头64:ff9b，构造出IPv6地址；如果解析出IPv6地址则直接返回终端[7-8]。

对于防火墙，现网有2组防火墙，每组防火墙采用VSM多虚一部署方式，上联169 CR，下联人网UPF的EOR。设备互联均采用全100G接口，承载IPv4、IPv6双栈协议的业务流量。当前，针对IPv4业务，双栈协议防火墙开启NAT64功能模块，针对测试终端及客户分配的公网地址池，建立对应的NAT64策略，并添加DNS64设备构造的IPv6地址，确保测试终端在访问互联网IPv4资源时可以更好地实现IPv6到IPv4的地址转换，而在访问IPv6地址时可以直接访问。

### 4.2 完成终端侧相关配置

选定支持IPv6的测试手机，并为手机号签约新DNN。接下来，点击手机的设置按钮，依次选择移动网络、移动数据、接入点名称（APN）。在“接入点名称（APN）”界面中，点击右上角的新建APN，填入CUV6TEST；返回上级菜单，选择新建的CUV6TEST为接入点；将手机调整为飞行模式，再打开移动数据访问。

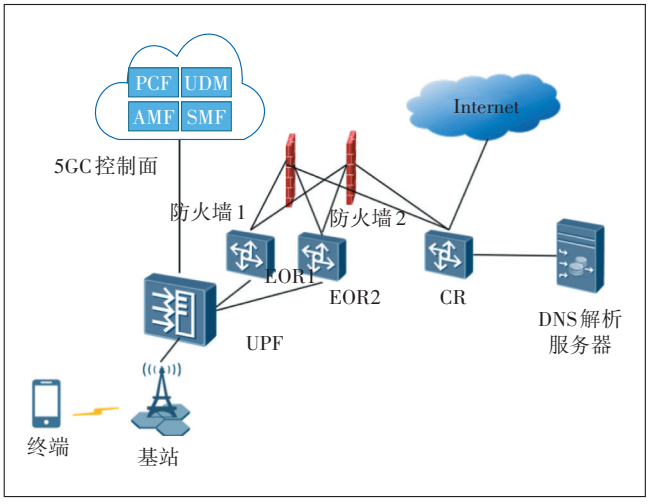


图2　IPv6单栈实践网络组网

### 4.3 通过业务访问验证IPv6单栈网络部署效果

#### 4.3.1 手机访问IPv4业务APP1实验

手机访问APP1时，DNS抓包数据如表2所示。当DNS服务器解析业务服务APP1时，请求IPv6地址时为空，又继续请求IPv4地址，此时，DNS增加IPv6地址前缀64:ff9b，返回终端IPv6地址64:ff9b:6548:cb21:443。

防火墙抓包数据如表3所示，当终端访问64:ff9b:6548:cb21:443时，防火墙完成NAT64转换，终端源地址转换成116.131.28.0:9089，目的地址转换成101.72.203.33:443，实现业务访问。

#### 4.3.2 手机访问IPv6业务APP2实验

手机访问APP2时，DNS抓包数据如表4所示，当DNS服务器解析业务服务APP2时，请求IPv6地址为2408:871a:6010:a:3:3fe:443，返回终端解析的IPv6地址。

防火墙抓包数据如表5所示，给UE分配IPv6地址，访问IPv6业务地址时，经防火墙可直接访问APP2的业务。

经测试，A市已完成端到端IPv6单栈部署，终端用户可通过IPv6访问互联网。当用户终端切换APN到CUV6TEST时，手机处于5G单栈SA状态。当访问IPv6业务时，手机可以直接通过IPv6报文交互；当访问IPv4业务，则通过DNS64和NAT64技术的转换，仍然能够进行网络访问。简而言之，用户可以通过IPv6来收/发短信、接打电话、浏览网页、使用APP。

### 4.4 其他说明：手机地址说明

在测试手机的状态信息-IP地址一栏可以看到IPv4地址。在RFC6333中有明确说明：192.0.0.0-192.0.0.7是互联网分配号码管理局（IANA）分配的用于DS-Lite模式下使用的地址。支持DS-Lite应用的手机（B4设备）根据RFC6333分配的地址进行IPv4应用（有些应用可能将IPv4固化在应用中）与远端IPv4服务器通信。这种通信通过IPv4 in IPv6隧道，在AFTR（支持DS-Lite的BRAS、防火墙或路由器）处终结手机发过来的IPv4 over IPv6的隧道设备、并进行IPv4的NAT，使得手机的应用通过IPv4访问远端IPv4 SERVER。此技术方案中不涉及使用这个IP地址。

表2　访问APP1 DNS抓包数据

| 终端IPv6地址 | 请求地址方式 | url | 解析结果 |
|---|---|---|---|
| 2408:841d:fb00:3:702c:78b0:28a1:5f6b.30141 | AAAA | ss0.xxxx.com | 空 |
| 2408:841d:fb00:3:702c:78b0:28a1:5f6b.30141 | A | ss0.xxxx.com | AAAA 64:ff9b:6548:cb21:443 |

表3　访问APP1防火墙抓包数据

| 序号 | 发起方源地址:端口→目的地址:端口 | 响应方源地址:端口→目的地址:端口 | 发起方/响应方报文数 | 剩余时间/老化时间/s |
|---|---|---|---|---|
| 4 | 2408:841d:fb00:3:702c:78b0:28a1:5f6b.30141→64:ff9b:6548:cb21:443 | 101.72.203.33:443→116.131.28.0:9089 | 7/9 | 1 783/1 800 |
| 5 | 2408:841d:fb00:3:702c:78b0:28a1:5f6b.30143→64:ff9b:6548:cb21:443 | 101.72.203.33:443→116.131.24.0:42403 | 36/47 | 1 790/1 800 |

表4　访问APP2 DNS抓包数据

| 终端IPv6地址 | 请求地址方式 | url | 解析结果 |
|---|---|---|---|
| 2408:841d:fb00:3:702c:78b0:28a1:5f6b.46724 | AAAA | ss0.xxxy.com | 2408:871a:6010:a:3:3fe:443 |

表5　访问APP2防火墙抓包数据

| 序号 | 发起方源地址:端口→目的地址:端口 | 响应方源地址:端口→目的地址:端口 | 发起方/响应方报文数 | 剩余时间/老化时间/s |
|---|---|---|---|---|
| 39 | 2408:841d:fb00:3:702c:78b0:28a1:5f6b.46724→2408:871a:6010:a:3:3fe:443 | 2408:871a:6010:a:3:3fe:443→2408:841d:fb00:3:702c:78b0:28a1:5f6b.46724 | 11/15 | 1 743/1 800 |

## 5 结束语

IPv6单栈已经成为我国网络部署的重要目标，从双栈演进为IPv6单栈，不仅在战略上加速了互联网协议第6版（IPv6）的规模部署；在运维层面，也有效降低了网络管理成本，减少了运维工作量；在安全方面，更是通过减少协议暴露面，降低了安全风险。通过5G SA网络的IPv6单栈的部署测试，证明了该IPv6单栈总体技术方案能够实现过渡形态IPv6单栈，可以作为IPv6单栈的演进推进方案。

为了推动IPv6单栈的成熟和向终极形态IPv6演进，仍需要做好以下2方面工作：一是持续推动业务由IPv4向IPv6迁移；随着业务的逐步迁移，IPv6流量占比将持续提升。这将进一步加速推动IPv4协议彻底退网。二是加强IPv6网络安全领域研究，如IP地址溯源验证等关键技术等，以加速中国网络信息安全体系向IPv6单栈同步推进。

**参考文献：**

[1] 解冲锋，李星，李震，等.大规模网络向IPv6单栈演进的技术方案[J].中兴通讯技术，2022，28(1)：57-61.

[2] 余秀.邬贺铨：IPv6赋能行业专网助力上云转型[J].中国教育网络，2023(7)：27-29.

[3] ZHOU T R，FIOCCOLA G，LI Z B，et al. Enhanced alternate marking method：draft-zhou-ippm-enhanced-alternate-marking-04[R/OL].[2024-01-16]. https://datatracker. ietf. org/doc/draft-zhou-ippm-enhanced-alternate-marking/04/.

[4] GUICHARD J，SONG H Y，TANTSURA J，et al. Network service header（NSH）and segment routing integration for service function chaining（SFC）：draft-ietf-spring-nsh-sr-01[R/OL].[2024-01-16]. https://datatracker.ietf.org/doc/draft-ietf-spring-nsh-sr/01/.

[5] 3GPP. 3rd Generation partnership project；technical specification group services and system aspects；system architecture for the 5G system；stage 2：3GPP TS 23.501[S/OL].[2024-01-16]. ftp://ftp.3gpp.org/Specs/.

[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.

[7] FILSFILS C，CAMARILLO P，Cisco Systems，Inc.，et al. SRv6 network programming：draft-ietf-spring-srv6-networkprogramming-16[R/OL].[2024-01-16]. https://datatracker. ietf. org/doc/html/draft-ietf-spring-srv6-network-programming-16.

[8] IETF. IPv6 segment routing header（SRH）：RFC 8754[S/OL].[2024-01-16]. https://www.rfc-editor.org/rfc/rfc8754.

**作者简介：**
邢建兵，高级工程师，博士，主要从事智能终端、网络与应用相关技术研究工作；史春磊，高级工程师，硕士，主要从事5G网络的创新产品研发工作；高沛，工程师，学士，主要从事5G网络创新产品管理、解决方案工作；蔡超，毕业于西安电子科技大学，正高级工程师，硕士，主要从事5G网络的创新产品研发工作；邱佳慧，毕业于北京交通大学，正高级工程师，博士，主要研究方向包括车联网、5G通信、高精度定位等；屠礼彪，毕业于北京邮电大学，高级工程师，硕士，主要从事数据通信网络的规划、建设和管理等工作。