

基于BNC架构的 随行私网技术创新与实践

Innovation and Practice of Mobile Private Network Technology Based on BNC Architecture

廖江, 薛强, 徐晓亮, 韩纬禧, 黄钟明(中国联通广东分公司, 广东 广州 510627)

Liao Jiang, Xue Qiang, Xu Xiaoliang, Han Weixi, Huang Zhongming (China Unicom Guangdong Branch, Guangzhou 510627, China)

摘要:

基于BNC架构(宽带核心网)构建随行私网,为中小企业和家庭用户提供安全、便捷、高速的私有网络服务。从技术架构、创新点、应用场景及未来发展方向等方面对随行私网进行了深入探讨,旨在展示其在推动数字化转型中的重要作用。

关键词:

随行私网;宽带核心网;5G固移融合;网络安全

doi:10.12045/j.issn.1007-3043.2025.10.012

文章编号:1007-3043(2025)10-0064-07

中图分类号:TN919

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

The mobile private network based on BNC (Broadband Core Network) provides secure, convenient, and high-speed private network services for small and medium-sized enterprises and home users. It delves into the technical architecture, innovation points, application scenarios, and future development directions of the mobile private network, aiming to demonstrate its important role in promoting digital transformation.

Keywords:

Mobile private network; Broadband core network; 5G fixed-mobile convergence; Network security

引用格式:廖江,薛强,徐晓亮,等. 基于BNC架构的随行私网技术创新与实践[J]. 邮电设计技术,2025(10):64-70.

0 引言

随着5G技术的广泛应用,社会数字化转型加速,家庭、个人和中小企业的数据资产快速累积,对网络的安全性、便捷性和高速性提出了更高要求。某省联通基于中国联通集团推出的BNC架构提出随行私网解决方案,通过打破传统网络固移独立的架构,实现

了固移网络的端到端融合,为用户提供了一种全新的网络体验。

1 需求及价值场景

1.1 智能家居市场前景分析

近些年来,随着AI等技术的发展,智能家居市场需求呈现出迅猛增长的态势。随着生活水平的提高和科技的不断进步,人们对便捷、舒适、高效生活的追求愈发强烈。消费者渴望通过智能家居实现远程控制家电、智能安防监控保障家庭安全以及智能化的能

通讯作者:薛强,xueqiang@chinaunicom.cn

收稿日期:2025-08-06

源管理以降低能耗。特别是年轻一代,他们对新技术的接受度高,期望智能家居能融入日常生活,提升生活品质。从家庭到办公场所,智能家居的需求正不断扩大,市场前景广阔。

根据艾瑞咨询测算(见图1),2025年中国智能家居市场规模为9 523亿元,其中以智能摄像机、智能门锁为代表的AI属性智能品类增速较快,并作为智能家居的入门级产品,将持续助推智能家居的市场渗透与智能水平的深化。

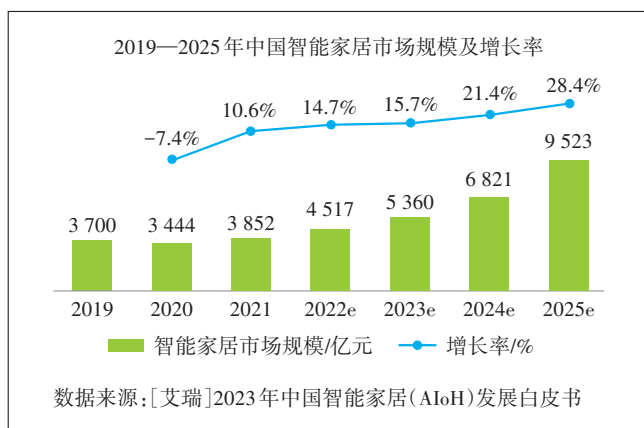


图1 中国智能家居市场规模机增长率预测

基于IDC在2023年1月的预测,2026年中国智能家居设备市场出货量将达3.9亿台,其中智能家电1.26亿台,视频娱乐设备0.42亿台,家庭安全监控0.79亿台,智能音箱0.28亿台,智能照明1.12亿台。

如何将这些设备有效地连接起来,实现智能化管理和控制,如何实现随时随地远程访问这些智能家居设备并获得高质量的数据传输服务,逐渐成为人们关注的问题。

1.2 远程访问家庭智能设备的场景

1.2.1 手机/车机和家庭安防远场互访

随着老龄化的加剧,社会中出现大量的独自居家养老的老人,他们的子女需要通过家庭摄像头及时监控老人的健康状态(见图2)。除此之外,留守儿童的监控场景、家庭防盗等安防场景、宠物监控等场景也都对远程访问家庭摄像头存在需求。

1.2.2 手机/车机和家庭网络存储服务器/打印机等远场互访

随着社会的发展,人们对于个人数据的保护意识不断增强。相比于公共存储服务,家庭网络存储服务器产品能提供更好的安全性和隐私性,这也催生了通



图2 手机/车机和家庭安防远场互访场景

过手机、车辆等移动设备远程访问家庭网络存储服务器产品的需求(见图3)。类似的场景还包括家庭打印机、家庭扫描仪等设备。

1.2.3 手机/车机和家庭PC文件远场互访

当用户出差时,或在工作环境中,需要临时访问家庭PC/平板获取文件。

1.3 “双千兆”催生远程访问家庭设备的市场需求

得益于三大运营商和设备厂商的共同努力,我国已建成全球规模最大、技术领先的“双千兆”网络基础设施。其中5G用户达8.51亿户,占移动电话用户的48.8%;固定互联网宽带接入用户规模达6.08亿户,其中有1.72亿用户已升级为千兆网络。

基于当前千兆家庭宽带,运营商引入FTTR(Fiber to the room),将超千兆的Wi-Fi网络无盲区覆盖到家庭的每个角落,家中处处是千兆。2023年国内FTTR发展用户数已达1 000万+。千兆及FTTR的中高端用户有通过高带宽、高安全性服务远程访问家庭智能设备的需求,此类用户发展空间广大。

虽然移动网络和家宽网络都发展迅速,达到了千兆速率,但是在通过移动端访问家宽网络下的智能家居设备时,会受到互联网带宽的限制,使人们无法享受真正的千兆体验(见图4)。

2 现有解决方案分析

当前主流家庭设备厂商以及远控服务提供商等,普遍基于通用NAT穿透技术(STUN)+中继代理技术(TURN),实现远程访问解决方案(见图5)。图5中的“中继服务”可以理解为采用STUN或TURN技术穿越NAT的服务的代称。

2个需要通信的设备通过访问网络中部署的



图3 手机/车机和家庭安防远场互访场景

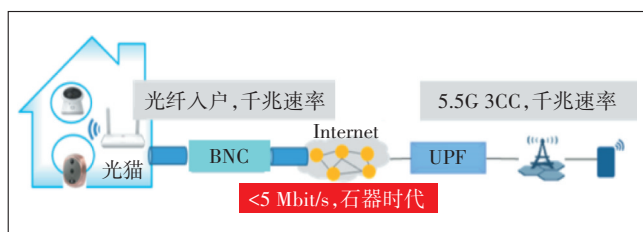


图4 移动端访问家庭设备带宽受限

STUN 服务器来判断自身是否在 NAT 之后,并获取 NAT 转换后自身的公网 IP 地址和端口号。设备还可以通过 STUN 服务器获取对端设备的公网 IP 地址和端口号。2 个设备都获得对端的公网 IP 地址和端口号之后就可以发起“打洞”消息,建立起它们之间的连接。对于对称型 NAT 来说,由于 NAT 对不同对端地址分配不同的公网地址和端口号,通信设备需要通过 TURN 服务器进行数据的代理转发,所有的数据都需要绕行,先发给 TURN 服务器,再由 TURN 服务器发给目的设备。出于安全考虑,大多数防火墙都采用对称型 NAT。现有解决方案存在以下痛点问题。

2.1 安全隐私风险

家庭用户内网隐私数据(安防视频/私照等)经过公有云互联网或者第三方网络(跨地域、跨国),导致出现互联网暴露面,有被黑客攻击的风险,一旦公网账号密码被攻破,用户隐私数据有泄漏的风险。

2.2 业务体验受限

a) 共享带宽速率受限。公网中继方式由于网络

架构为汇聚共享带宽模式,在用户连接数量较大的场景下,就会存在多连接共享有限的带宽和转发算力,导致每个用户连接的速度受限,在共享带宽高峰时段易拥塞,体验差,非单独付费的用户普遍的远场访问带宽在 1~5 Mbit/s。

b) 数据迂回时延高。公网中继服务一般集中部署,用户的手机和远场访问端的流量需要迂回汇聚到公网中继服务这个集中点,导致数据流量从互联网公网南北绕行,时延较高。

2.3 高成本抑制商业发展

家庭设备商需要持续投入资金租用公网中继服务(加解密转发算力、带宽),才能维持用户远程访问家庭内网设备的需求。如果家庭设备商将这部分成本转嫁到用户购买的设备价格上,会导致家庭设备价格过高,抑制用户使用需求。而且远程访问家庭设备是长期需求,很难通过一次性收费就保障持续提供后续服务。

3 随行私网解决方案及关键技术

3.1 随行私网解决方案

3.1.1 方案概述

基于 BNC 架构的随行私网解决方案是为用户提供手机高速、安全、极简、直连家庭内网的创新解决方案(见图 6)。该方案基于家庭 UPF,通过家庭扩展端可信接入、广域层三家庭组网技术,实现人、车、家灵活广域 Overlay 网络高速直连。家庭 UPF 作为移动网

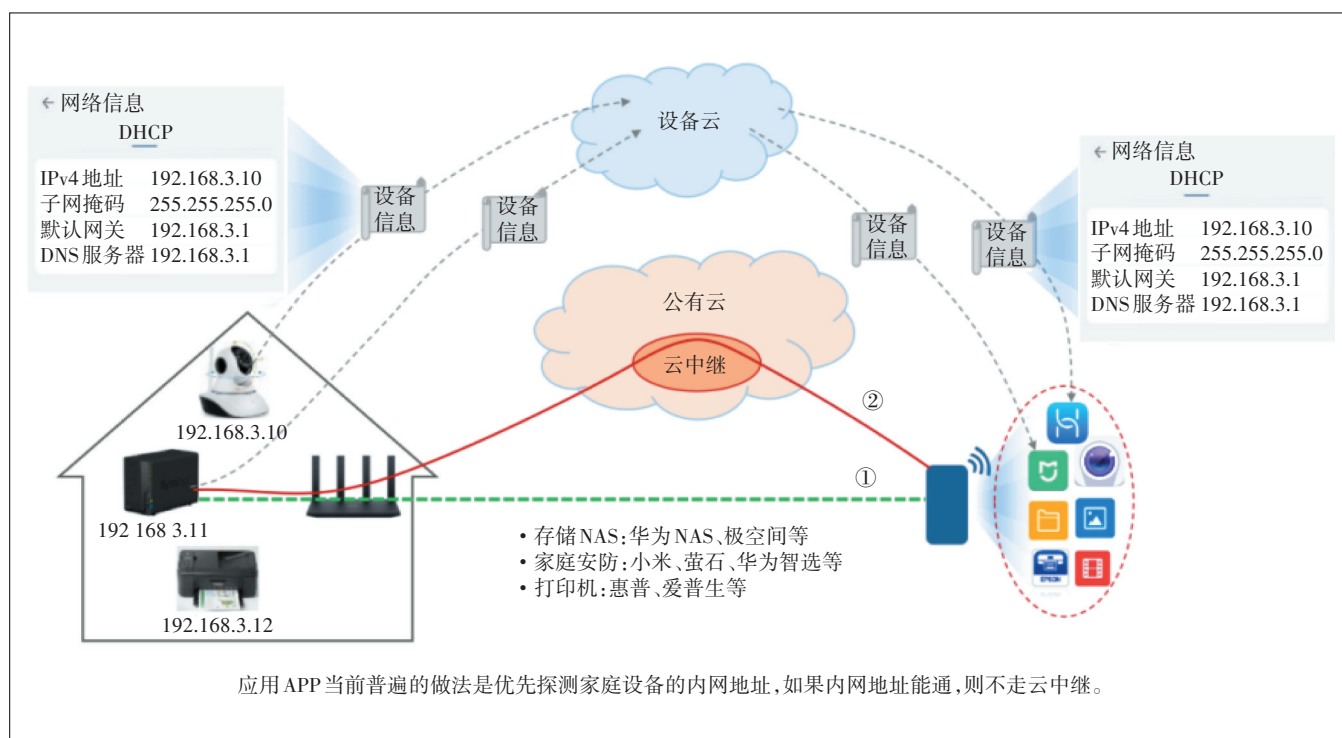


图5 移动端访问家庭智能设备现有解决方案

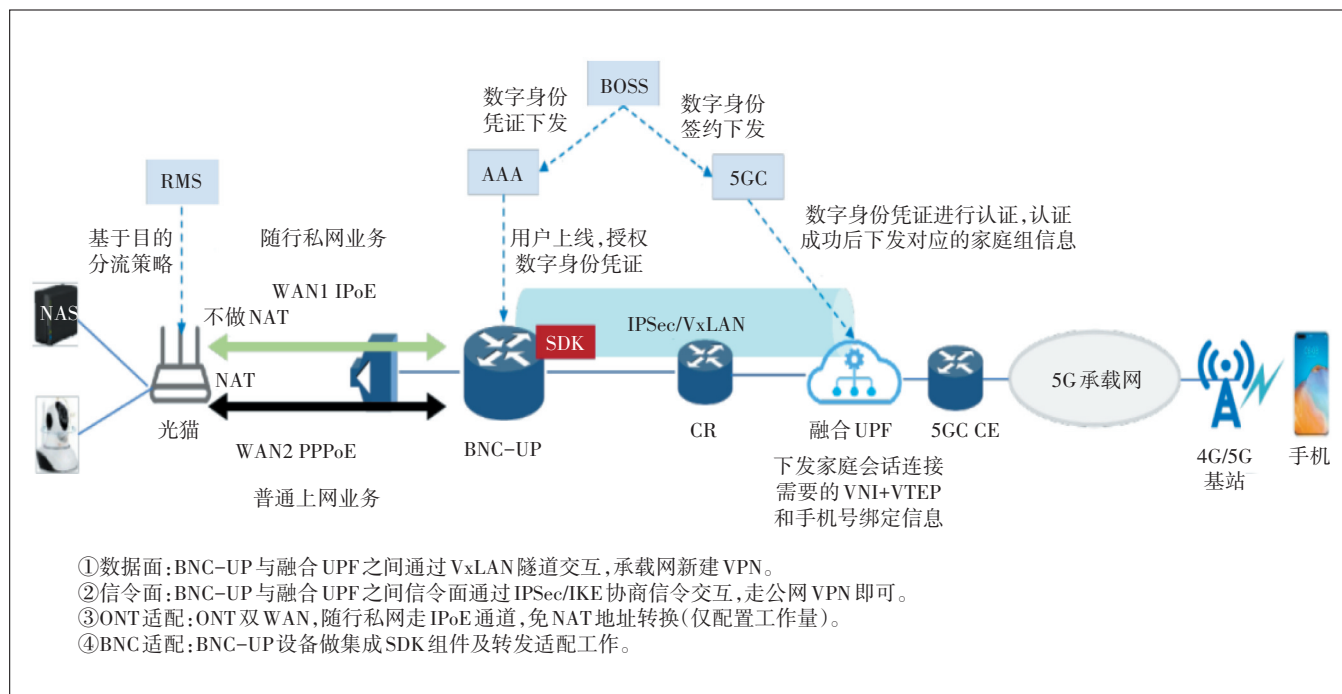


图6 随行私网解决方案

络中家庭设备的锚定点,负责和固网BNC中的家庭扩展端建立安全隧道,并帮助家庭扩展端完成鉴权接入流程。家庭扩展端发现家庭UPF并与之建立安全隧

道,在完成鉴权之后,负责转发家庭终端设备和远程手机之间的数据。手机在远场位置访问5GC网络,5GC网络建立从锚点UPF到家庭UPF、BNC-UP的转

发隧道,完成对家庭设备的访问。该方案部署简单,对生态友好,家庭扩展端即插即用,家庭设备即买即用,OTT生态零适配;打通固移终端业务互访,激发运营商网内东西流量,为客户赋能固移双网5G-A创新能力,开拓更广阔的toH/toB市场空间^[1]。

3.1.2 网络端侧关键技术

为了实现手机到家庭内网的IP直连互访,需要将普通家庭终端设备通过非可信Wi-Fi网络接入到5GC核心网。3GPP移动通信标准组织在R15中详细定义了终端非可信接入4G/5G核心网的方式,让带SIM卡的普通终端可以通过标准的IPSec/IKEv2/EAP鉴权认证协议接入到核心网。但对于当前市场上海量的不带SIM卡的终端来说,仍需要找到生态友好地接入到核心网的方法。

BNC集成随行私网适配功能需要具备的能力和机制如下。

a) 标准IPSec能力,支持IKEv2、EAP扩展鉴权认证协商能力,支持ESP传输模式加解密数据通道(AES/3DES等主流加密算法,SHA1/SHA256等主流摘要算法等)。

b) BNC适配功能软件在鉴权认证成功接入5GC核心网之后,需创建5GC业务地址段的策略路由。

3.1.3 随行私网移网侧关键技术

3.1.3.1 家庭设备安全接入5GC

对于拥有物理SIM卡的UE,3GPP定义了成熟完善的身份鉴权和安全接入方式以保障接入核心网的UE的真实可靠^[2]。在随行私网解决方案中,要实现手机用户随时随地安全访问家庭网络和业务,就需要家庭设备能够安全可信地接入5GC网络。手机用户作为家庭业务的业务主体和责任主体,可将BNC上的家庭扩展端视作可信家庭扩展端,家庭无SIM卡的设备可以通过该扩展端接入移动网络^[3]。

3.1.3.2 手机随行,跨域访问

家庭设备通过家庭可信扩展端接入移动网络后,远场手机(即在家庭局域网之外的UE)在任意地点通过蜂窝接入时,需要实现跨地域家庭业务互通,建立手机与BNC上家庭扩展端之间的内网连接,实现远场UE与家庭设备之间的互联互通。支持远场UE移动到任何位置,包括跨省市、跨大区、甚至跨国到家庭内网之间的互联互通访问。

3.1.3.3 灵活的业务管控

用户可实时查看网络状态,可自主控制实现家庭

业务开通、访问控制、内容管理等。随行私网业务主体(即随行私网业务开通人)需要管理随行私网成员组,包括添加成员、修改成员、删除成员等,并可定义每个成员可访问的家庭服务范围。同时,随行私网业务主体可灵活管理接入家庭网络域的内容服务实例,可灵活添加、删除家庭业务服务实例。

随行私网业务主体可随时查看端到端的随行私网状态,包括家庭成员与家庭业务服务实例之间的访问行为、流量状态,家庭接入端点状态等信息。

3.1.4 随行私网固网侧关键技术

3.1.4.1 BNC支持CU分离宽带核心网架构

BNC_UP作为家宽业务接入锚点设备,支持CU分离架构,UP池化部署,支持池内负载分担。当UP池内单台UP故障时,支持家宽业务、随行私网业务用户侧温备组/热备组倒换,同时支持网络侧IPSec/VxLAN隧道重建。同理,当网络侧故障时,可以联动用户侧温备组/热备组倒换,实现随行私网业务可靠性池化负载分担。

BNC_CP作为家宽业务接入控制节点,负责与AAA/DHCP等服务器通信,负责UP池管理和地址池、用户表项管理等。BNC_CP面异局址灾备1+1部署,当单CP故障时,随行私网场景支持CP面灾备倒换,随行私网用户session通过CP面控制下发用户表项到UP面(温备)或者CP指导UP池内热备倒换。

3.1.4.2 BNC_UP支持算力单板容器开放

BNC_UP作为宽带业务接入锚点,预留槽位支持算力板卡,算力板卡支持容器开放能力,CPU、内存、转发等资源通过标准接口向三方软件开放。

三方软件(例如固移融合适配功能、边缘云网关vSGW等网元)可以通过中间件方式部署于算力单板上。同时算力单板支持作为SAU单元配套中国联通集团CAM服务器,进行家宽用户质差分析、潜客挖掘、PCDN管控等,实现SAU单元和容器开放同板部署。

3.1.4.3 BNC_UP支持与家庭UPF鉴权建立IPSec隧道

固移融合适配功能(内置SDK)部署于BNC_UP算力单板,相比ONT,部署固移融合适配功能不用替换用户侧光猫,对接入网网元要求低。

固移融合适配功能负责与家庭UPF进行鉴权,并通过固网AAA授权的随行私网用户数字身份凭证,与家庭UPF进行IKE协商,协商内容为固移融合适配功能生成的FQDN信息(包含VxLAN隧道VTEP+VNI+MAC+数字身份ID),家庭UPF解析FQDN信息中数字

身份凭证并到移网AAA进行认证,认证通过后家庭SMF通知家庭UPF与BNC_UP分别建立IPSec隧道(控制面)和VxLAN隧道(转发面)^[4]。

3.1.4.4 ONT支持双WAN口区分随行私网业务

经过调研,现网主流厂家的ONT设备基本都支持双WAN口配置,一个WAN口为PPPoE家宽业务,一个WAN口为IPoE随行私网业务,且第2个WAN口不设置NAT为桥接模式。

主流厂家的ONT设备支持基于五元组的分流配置,即基于家庭UPF侧NAT后的地址,ONT设备上配置分流策略,区分网络侧双WAN口流量。

ONT的配置通过改造升级后的RMS下发配置,ONT设备无需支持VxLAN和IPSec隧道,无需安装固移融合适配功能。

3.2 随行私网解决方案优势

随行私网解决方案可以很好地解决业界当前的痛点问题,发挥网络原生能力,实现点到点、点到面的广域直连,提高用户内网穿透、远控业务体验,其关键特征包括以下几点。

3.2.1 电信级安全

家庭内网安全接入移动核心网,重用电信级安全接入能力,隐私数据在运营商内网东西向转发,不出运营商内网,没有公网暴露面,从而实现电信级安全的手机到家庭的直连网络。

随行私网实现了家庭成员与家庭内网之间的安全访问范围控制,即只有可信的家庭成员(SIM卡鉴权)才能够访问家庭内网;非家庭组成员禁止访问(基于SIM卡签约控制),做到可管可控可视。

3.2.2 超宽直连体验

运营商固移融合网络直连交互,保证手机到家庭内网的100%网络穿透,远场直连不经过第三方网络,运营商东西向内网传输上传下载速度可达业界普通中继服务带宽的50~100倍,极大提高了用户远场访问业务体验。

基于运营商的随行私网,可以轻松实现手机和手机之间,手机和家庭之间,家庭和家庭之间的全方位高带宽IP直连业务。

3.2.3 成本下降

运营商基于原生网络能力,建立手机到家庭的直连通道,从而降低OTT厂商公有云中继服务算力和带宽投资压力,南北流量转东西流量,减少数据迂回专线费用;手机用户通过购买运营商随行私网套餐,即

可享受手机远场通信业务,一次开通全家多个家庭设备共享带宽。运营商“修路”模式代替了OTT厂商各自“修路”模式,通过合作共享,让投资和回报更合理。

3.2.4 近场和远场操作极简

随行私网解决方案实现了手机到家庭内网的IP直连,即手机在蜂窝连接情况下,可以直接通过家庭内网IP访问家庭服务,保证手机用户在家里(Wi-Fi局域网)和户外(4G/5G蜂窝)访问家庭内网服务操作一致,体验一致。同时,家庭设备软件以及配套的APP应用无需任何改动,即可实现在Wi-Fi和蜂窝的任何连接下,都可以基于相同的内网IP进行访问,不影响已有手机终端生态。

3.3 方案对比

传统解决方案与随行私网解决方案的对比如表1所示。

表1 方案对比

领域	传统解决方案		随行私网解决方案	
	方案特点	评价等级	方案特点	评价等级
安全	安全性较差:隐私数据经过公有云或者3rd网络。从公有云/P2P网络中继服务中解密后转发(跨地域、跨国),存在隐私泄露风险	★★	电信级高安全:家庭内容安全接入移动核心网,重用电信级安全接入能力,家庭隐私数据不出运营商内网	★★★★ ★★
体验	体验差:带宽速度受限,数据迂回时延高。用户从互联网公网绕行,多用户共享带宽高峰时段易拥塞;业界NAT打洞技术针对“对称型”NAT穿透率只有约50%,导致用户连接不可靠	★	极致体验(高速100%互通):固移融合网络直连交互,实现100%网络穿透,远场直连不经过3rd网络,上传下载速度高	★★★★ ★★
成本	成本高,家庭设备OPEX高,抑制业务发展;当前租用公有云的中继云服务(算力+带宽)费用是折合到产品定价中的,随服务年限的增加,OPEX负担重	★★★★	更优成本和效率:减少公有云租用费用,减少数据迂回专线费用,用户开通手机远场通信业务,多个家庭设备均可使用	★★★★ ★
生态	使用复杂:每个IOT设备都要独立远程访问家庭内网方案,烟囱林立,手机侧每个APP远场登录方式不同,操作复杂	★★	极简使用:用户签约即开通,免配置接入核心网,构筑手机UE到家庭内网的“直连网线”;方案未来可支持手机、家庭、车远程通信一张网;家庭IOT应用0修改,0适配,近场、远场一致体验,无感直连家庭服务	★★★★

3.4 实践情况

随行私网方案经过不断的摸索与实践,最终确定了基于BNC架构的方案为目标方案。2024年初,采用专用防火墙设备,基于源IMSI到目标光猫IP之间的用户级访问控制策略实现了随行私网的初步功能,发展了7 000个用户,效果较好,但缺乏标准化手段,无法实现自动化,只能进行手工配置,限制了业务的规模化发展。2025年初,提出了UDM扩展“数字身份ID”统一鉴权,终端部署SDK建立独立长连接会话,端侧IOT设备生态0适配,应用无感知的方案,但涉及到现网大量ONT设备升级及维护的问题,经研究不宜大规模部署。

2024年底,随着中国联通集团BNC的大规模建设,BNC-UP的集中化部署为随行私网的大规模推广提供了集约化方案,由UP侧部署固移融合SDK实现数字身份认证,为IOT建立独立长连接会话,较好地解决了部署自动化与成本问题。目前该方案已完成UP侧SDK试验版本的开发,并完成实验室的测试验证,正在进行商用版本的开发,计划于2025年Q3进行小范围商用试点,Q4进行规模商用推广。

4 随行私网标准化研究

3GPP基于有线/无线融合的发展趋势,在SA1的R18版本定义了家庭网关(即随行私网解决方案中的家庭扩展端)接入5GC的场景需求,并具体研究了住宅环境(例如家庭和小型办公室)中的某些用例^[5],定义了主要用于接入5GC系统的家庭网关背后的智能终端(如手机)或non-3GPP末端设备的服务要求。然而,对于未来的智能家居服务,还有一些差距,例如:

a) 5GC系统支持的家庭业务有限,例如只支持末端设备的差异化QoS管控。

b) 对实际部署问题的考虑不足,例如家庭网关通常没有USIM,如何通过非3GPP接入5GC网络并获得服务。

因此,3GPP标准的R20版本推荐首先在SA1工作组推动家庭接入场景需求增强,研究智能家居用例,进行差距分析,并定义演进的家庭网关(无USIM)通过非3GPP接入5GC网络,获取5GC服务的潜在需求增强^[6],包括以下几点。

a) 身份验证和授权方面。基于运营商政策,5GC系统应支持无卡(无USIM)的家庭网关与用户的安全注册和认证^[7]。

b) 家庭网关(eRG)的标识(无USIM场景的标识定义)。

家庭接入场景需求增强已经获得3GPP标准组的认可(WID:Enhanced 5G Resident phase II),3GPP后续将继续在SA2工作组推动支持无卡接入,并支持跨境互通方案的研究,满足智能家居接入5GC的各项服务需求^[8]。

5 总结

随着技术的快速发展和我国人民生活水平的不断提高,智能家居设备的普及率将持续提高,AI技术的发展和普惠将更加深刻地改变人们的生活方式。随行私网技术以智能手机为中心,实现手机与家庭设备的互联协同,让使用者不受地域约束,始终享受高质量的业务体验。在实现“人”与“家”的互联后,该技术还有望扩展到移动办公、车辆等其他场景,创造智慧生活全场景随时随地全互联。

参考文献:

- [1] MAHALINGAM M, DUTT D, DUDA K, et al. Virtual eXtensible local area network (VxLAN): a framework for overlaying virtualized layer 2 networks over layer 3 networks; RFC 7348 [S/OL]. [2025-01-10]. <https://datatracker.ietf.org/doc/html/rfc7348>.
- [2] IMT-2020(5G)推进组. 5G网络技术架构白皮书[EB/OL]. [2025-01-10]. https://mp.weixin.qq.com/s/KqVlNOmG6dmuLH_uJe_bwg.
- [3] IMT-2020(5G)推动组. 家庭随身网络场景及关键技术研究[EB/OL]. [2025-01-10]. <https://www.fxbaogao.com/detail/4730240>.
- [4] FRANKEL S, KRISHNAN S. IP security (IPsec) and Internet key exchange (IKE) document roadmap; datatracker; RFC 6071 [S/OL]. [2025-01-10]. <https://datatracker.ietf.org/doc/html/rfc6071>.
- [5] 3GPP. System architecture for the 5G System (5GS); 3GPP TS 23.501 [S/OL]. [2025-01-10]. <https://www.3gpp.org/ftp/Specs/>.
- [6] 3GPP. Procedures for the 5G System (5GS); TS 23.502 [S/OL]. [2025-01-10]. <https://www.3gpp.org/ftp/Specs/>.
- [7] 3GPP. Security aspects of non-3GPP accesses; TS 33.402 [S/OL]. [2025-01-10]. <https://www.3gpp.org/ftp/Specs/>.
- [8] 3GPP. Architecture enhancements for non-3GPP accesses; TS 23.402 [S/OL]. [2025-01-10] <https://www.3gpp.org/ftp/Specs/>.

作者简介:

廖江,高级工程师,主要负责网络建设发展的管理工作;薛强,高级工程师,主要负责承载网、云池等的规划、创新工作;徐晓亮,高级工程师,主要负责无线、承载网等专业的管理工作;韩伟禧,工程师,主要负责各专业网络的规划工作;黄钟明,工程师,主要负责IP网络的规划与建设工作。