

团 体 标 准

T/XAZN xxx—2024

家庭物联网 Wi-Fi 的 IPv6 接入技术要求

Technical requirement for IPv6 access of Home IoT Wi-Fi

(征求意见稿)

2024 - xx - xx 发布

2024 - xx - xx 实施

雄安新区智能城市创新联合会 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 总体架构	2
6 通用要求	3
6.1 一般要求	3
6.2 Wi-Fi 要求	3
7 IPv6 接入要求	4
7.1 基本要求	4
7.2 接入流程	4
8 认证授权与访问控制	6
8.1 认证授权	6
8.2 访问控制	6
9 SLA 与 QoS 要求	6
10 安全要求	7
10.1 设备安全	7
10.2 传输安全	7
10.3 设备管理安全	7
10.4 安全审计	7
11 数据接口规范	7
11.1 通信协议	7
11.2 家庭物联网网关接口规范	7
11.3 家庭物联网设备接口规范	8

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由雄安睿哲科技有限公司提出。

本文件由雄安新区智能城市创新联合会（XAZN）归口。

本文件起草单位：雄安睿哲科技有限公司、睿哲科技股份有限公司、广东成德电子科技股份有限公司、广东奥马冰箱有限公司、中国电信集团有限公司河北雄安新区分公司、中国移动通信集团河北有限公司雄安新区分公司、中国联合网络通信有限公司河北雄安新区分公司、中国雄安集团数字城市科技有限公司。

本文件主要起草人：

家庭物联网 Wi-Fi 的 IPv6 接入技术要求

1 范围

本文件规定了家庭物联网设备 Wi-Fi 的 IPv6 接入的术语和定义、总体架构、通用要求、IPv6 接入要求、认证授权与访问控制、SLA 与 QoS 要求、安全要求、数据接口规范等技术要求。

本文件适用于家庭物联网终端、家庭网关等相关设备或系统的接入设计和开发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 25069—2022 信息安全技术 术语
- GB/T 28451—2023 信息安全技术 网络入侵防御产品技术规范
- GB/T 30246.1—2013 家庭网络 第1部分：系统体系结构及参考模型
- GB/T 30269.901—2016 信息技术 传感器网络 第901部分：网关：通用技术要求
- GB/T 33745—2017 物联网 术语
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- GB/T 41269—2022 网络关键设备安全技术要求 路由器设备
- GB/T 44810.1—2024 IPv6网络安全设备技术要求 第1部分：防火墙
- GB/T 44810.3—2024 IPv6网络安全设备技术要求 第3部分：入侵防御系统（IPS）
- GB 4943.1—2022 音视频、信息技术和通信技术设备 第1部分：安全要求
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification (IPv6协议规范)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4291 IP Version 6 Addressing Architecture (IPv6寻址结构)

3 术语和定义

GB/T 25069—2022、GB/T 30246.1—2013、GB/T 30269.901—2016、GB/T 33745—2017、GB/T 44810.1—2024、GB/T 44810.3—2024界定的以及下列术语和定义适用于本文件。

3.1

家庭物联网 Home IoT

利用物联网技术将家庭中的各种设备、设施、家居用品与互联网连接起来以实现家庭设备智能化的一种网络。

注：在本文件中家庭物联网仅指“通过Wi-Fi和IPv6技术而实现的家庭物联网”。

3.2

家庭物联网网关 Home IoT Gateway

家庭物联网中的一种设备，位于家庭物联网系统和外部系统之间，与家庭物联网中的设备实现互联，实现对家庭物联网的配置和管理，还可以连接到家庭外部网络。

注：在本文件中家庭物联网仅指“具有独立信道的无线路由器，可为家庭物联网设备提供快速接入IPv6网络，分配IPv6地址，支持认证授权和访问控制”。

4 缩略语

下列缩略语适用于本文件。

AAA：认证、授权与计费（Authentication, Authorization and Accounting）

ACL: 访问控制列表 (Access Control Lists)
AES: 高级加密标准 (Advanced Encryption Standard)
APN6: 应用感知型IPv6网络 (Application-aware IPv6 Networking)
CoAP: 受限应用程序协议 (Constrained Application Protocol)
DHCPv6: 互联网协议第六版动态主机配置协议 (Dynamic Host Configuration Protocol for IPv6)
DHCPv6-PD: DHCPv6前缀代理 (DHCPv6 Prefix Delegation)
DES: 数据加密标准 (Data Encryption Standard)
DSA: 数字签名算法 (Digital Signature Algorithm)
iFIT: 随流检测 (in-situ Flow Information Telemetry)
IoT: 物联网 (Internet of Things)
IP: 互联网协议 (Internet Protocol)
IPSec: 互联网安全协议 (Internet Protocol Security)
IPv6: 互联网协议第六版 (Internet Protocol Version 6)
MAC: 媒体访问控制 (Media Access Control)
MIMO: 多输入多输出 (Multiple-Input Multiple-Output)
MQTT: 消息队列遥测传输 (Message Queuing Telemetry Transport)
OFDM: 正交频分复用 (Orthogonal Frequency Division Multiplexing)
PPPoE: 以太网上的点对点协议 (Point-to-Point Protocol Over Ethernet)
PSK: 预共享密钥 (Pre-Shared Key)
QoS: 服务质量 (Quality of Service)
RSA: 非对称加密算法 (Rivest-Shamir-Adleman)
SLA: 服务水平协议 (Service Level Agreement)
SLAAC: 无状态地址自动配置 (Stateless Address Autoconfiguration)
SoftAP: 无线软路由模式 (Soft Access Point)
SRv6: IPv6段路由 (Segment Routing IPv6)
SSID: 服务集标识 (Service Set Identifier)
TLS: 传输层安全 (Transport Layer Security)
URPF: 单播反向路由查找 (Unicast Reverse Path Forwarding)
VPN: 虚拟专用网 (Virtual Private Network)
Wi-Fi: 无线保真 (Wireless Fidelity)
WPA: Wi-Fi网络安全接入 (Wi-Fi Protected Access)

5 总体架构

家庭物联网总体架构如图1所示,利用家庭宽带、Wi-Fi、IPv6与物联网技术,打造一个面向家庭场景的IPv6公众物联网接入网络,实现在住宅楼宇、社区中的各类智能城市联网设备、传感器等自动联网,实现更智能的使用和管理。家庭网络体系结构应符合GB/T 30246.1中的相关要求。

家庭物联网总体架构主要由运营商宽带接入服务器、AAA服务器、用户家庭网关、家庭物联网设备等部分组成。

宽带接入服务器负责为用户家庭宽带网络建立IPv6的PPPoE点对点链路,汇聚用户的流量;负责与AAA系统和客户管理系统及服务策略控制系统相配合实现用户接入的认证、计费和管理。点对点协议的规范使用符合RFC 2516的规定。

AAA服务器负责确认访问网络的用户的身份,判断访问者是否为合法的网络用户;对不同用户赋予不同的权限,限制用户可以使用的服务;收集和记录用户对网络资源的使用情况,实现针对时间、流量的计费需求。

用户家庭物联网网关是IPv6家庭物联网Wi-Fi接入点,负责为家庭物联网设备提供联网能力。北向连接宽带接入服务器,南向连接家庭物联网设备。网关通用技术要求应符合GB/T 30269.901中3.2和3.3的要求。

家庭物联网设备指家庭中具有联网功能的设备，包括数字家电、门禁、水电气热智能表具等。可分为直连设备和间联设备，直连设备指可直接连接家庭物联网网关的设备，间联设备指借助无线接入模块连接家庭物联网网关的设备。

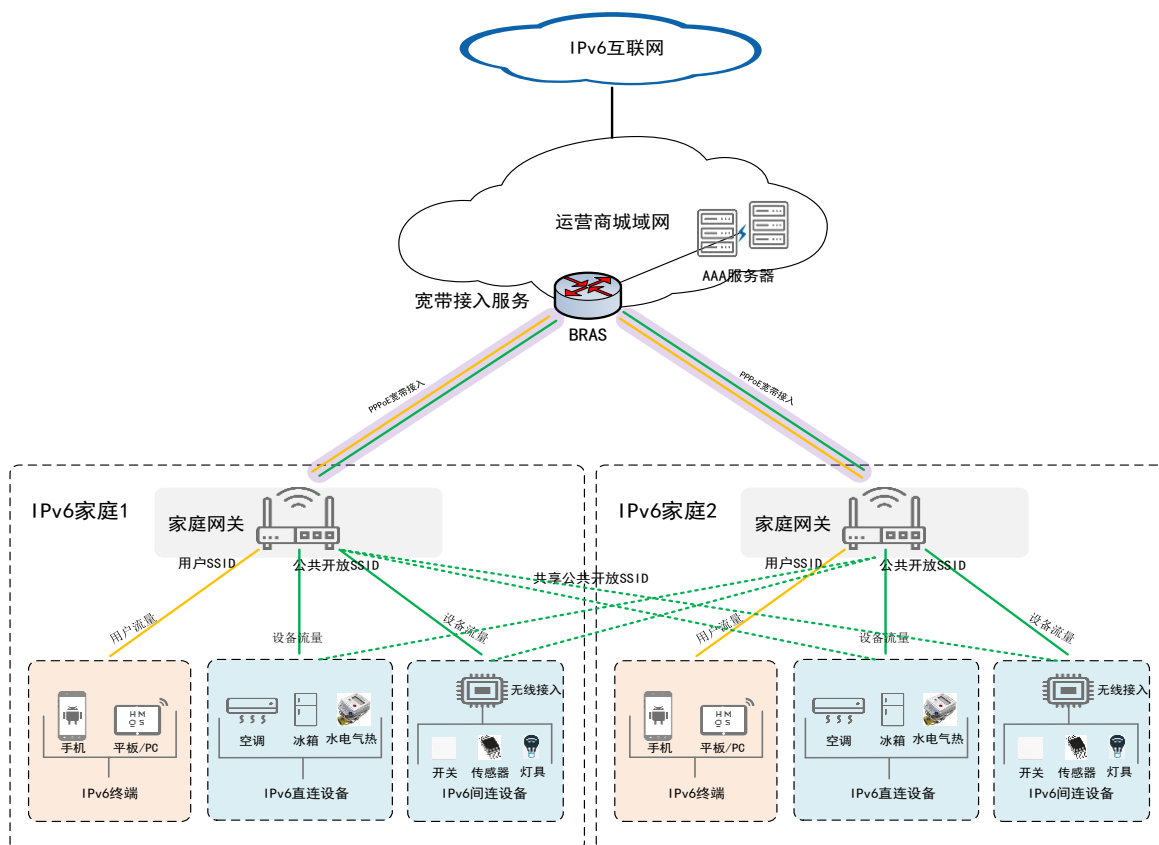


图 1 家庭物联网总体架构

6 通用要求

6.1 一般要求

家庭物联网一般要求如下：

- 家庭物联网应默认开启IPv6协议，宜采用IPv6单栈网络模式，IPv6报文结构符合RFC 2460的规定；
- 网络运营商应分配不少于2个/64的IPv6全球单播地址前缀，满足为物联网业务分配专属地址段需求；
- 家庭物联网的三层网络设备，宜支持SRv6、VPN+、iFIT、APN6等IPv6+特性，为IPv6网络提供更灵活的应用机制；
- 家庭物联网的网络传输比特速率应不低于100Mbit/s；
- 家庭物联网应支持所有可能的业务，包括会话型业务、消息/检索型业务和分配型业务等。

6.2 Wi-Fi 要求

家庭物联网Wi-Fi要求如下：

- 设备应支持IEEE 802.11ax协议，宜支持802.11be，兼容IEEE802.11ac/b/g/n协议；
- 设备应支持2.4GHz和5GHz频段，支持MIMO和OFDM技术；
- 设备应支持在特定频段内自动选择最佳频率，避免干扰；
- 设备应支持信道自动扫描功能和自动规避干扰，确保网络稳定性和性能；
- 设备应支持WPA2和WPA3加密标准；

- f) 在多个网关Wi-Fi接入点的Mesh组网模式下，支持无缝漫游；
- g) 设备运行内存宜不低于256 MB RAM，机身内存宜不低于128MB ROM；
- h) 设备应配有复位按键。

7 IPv6 接入要求

7.1 基本要求

家庭物联网IPv6基本要求如下：

- a) 家庭网关设备应支持SLAAC、DHCPv6协议，符合RFC 3315的规定；家庭网关应支持DHCPv6-PD自动配置网络前缀；
- b) 家庭网关应支持三层IPv6数据包的转发，确保用户设备能够正常访问互联网；
- c) 运营商应支持为家庭物联网分配专用于家庭物联网设备接入使用的带宽，且带宽应不少于50Mbps；
- d) 家庭网关应支持自动接入运营商宽带接入服务器，自动配置家庭物联网专用的IPv6地址前缀；
- e) 家庭网关应支持默认的SSID和共享密钥，允许设备自动搜索和连接；
- f) 家庭网关应支持为接入的家庭物联网设备分配专用的IPv6地址，IPv6地址格式与类型符合RFC 4291的规定；
- g) 家庭网关应支持IPv6+切片技术实现独立网络通道，隔离用户和设备流量；
- h) 家庭物联网设备应支持优先采用快速配网模式，自动搜索缺省SSID，并通过预置密钥信息完成接入认证流程，在快速配网模式不可用的情况下，应支持SoftAP手动配网模式；
- i) 家庭物联网设备宜支持通过CoAP或MQTT协议接入家庭物联网平台。

7.2 接入流程

家庭物联网IPv6接入参考流程见图2，家庭物联网设备配网流程见图3。

家庭物联网IPv6接入流程主要步骤如下：

- a) 家庭物联网网关启动，连接运营商宽带接入服务器，使用用户家庭宽带账号完成AAA认证，获取运营商下发的2个的IPv6地址前缀，一个用于传统宽带业务，一个用于家庭物联网业务；
- b) 家庭物联网网关开启默认的Wi-Fi SSID；
- c) 家庭物联网设备启动后，使用无线通信模块搜索预定义约定格式的Wi-Fi SSID，并使用出厂时预置的Wi-Fi密钥，通过WPA2或更高级别的加密协议与网关建立安全连接；
- d) 家庭物联网网关校验设备后，为设备分配子网和IPv6地址，确保地址的唯一性，避免地址冲突；
- e) 若家庭物联网设备无法搜索到相应家庭网关Wi-Fi SSID，应进入SoftAP配网模式，等待用户手动配网；
- f) 家庭物联网设备配网成功后，宜使用CoAP或MQTT协议接入家庭物联网平台，完成设备与平台间的高效、安全通信。

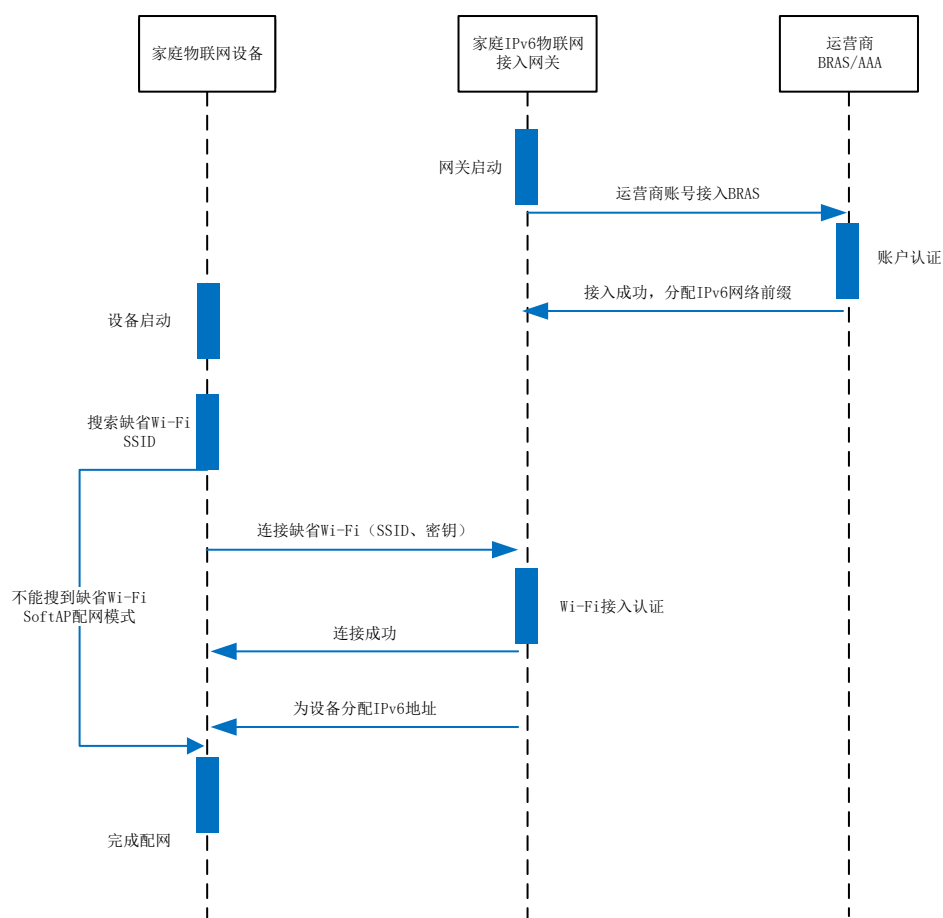


图 2 家庭物联网IPv6接入参考流程

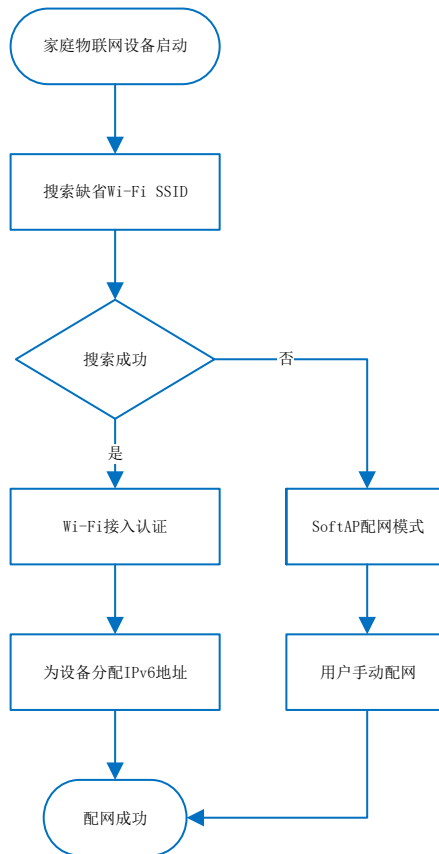


图 3 家庭物联网设备配网流程

8 认证授权与访问控制

8.1 认证授权

家庭物联网设备应支持以下认证授权要求：

- a) 家庭网关应支持基于密码的认证、MAC地址认证等认证方式；
- b) 家庭网关应支持设置认证类型、加密算法和共享密钥PSK，加密算法应支持AES；
- c) 共享密钥PSK应包含大小写字母、数字和符号，密钥长度应超过10个字符，不使用简单或易猜测的密码；
- d) 密钥管理应符合GB/T 39786中的3.7要求；
- e) 家庭网关宜支持为不同类型的设备分配不同的权限；
- f) 家庭物联网设备应支持通过预置密钥快速接入物联网业务平台。

8.2 访问控制

家庭物联网设备应支持以下访问控制要求：

- a) 家庭网关应支持IPv6网络的访问控制，允许设置ACL规则限制IPv6终端的连接和通信。支持基于源地址、目标地址和服务类型的ACL规则；
- b) 家庭网关应支持将传统家宽业务和家庭物联网业务隔离。

9 SLA 与 QoS 要求

家庭物联网设备应支持以下SLA与QoS要求：

- a) 应支持根据业务设置SLA，且默认家庭物联网业务的级别应优于传统家宽业务；
- b) 应支持为传统家宽业务和家庭物联网业务设置QoS，满足不同的服务质量要求。

10 安全要求

10.1 设备安全

家庭物联网设备应支持以下设备安全要求：

- a) 网关路由器应支持IPv6 Snooping功能，且默认开启，对接入设备流量的IPv6地址、MAC地址等进行校验，防止非法流量；
- b) 针对网络中IPv6源地址欺骗报文，可通过URPF技术来过滤这类报文，禁止其在网络中传播；网关路由器应支持严格URPF模式和松散URPF模式，可支持基于邻居的URPF功能；
- c) 设备应符合GB 4943.1—2022中的相关安全要求。

10.2 传输安全

家庭物联网设备应支持以下传输安全要求：

- a) 网关路由器应支持IPSec协议，在IP层提供数据机密性、数据源认证、数据完整性和抗重放等安全服务；
- b) 设备应支持TLS 1.2、TLS 1.3；
- c) 设备应支持AES、DES等常用的对称加密算法；支持RSA、DSA等非对称加密算法；宜支持国密算法；
- d) 家庭物联网传输安全应符合GB/T 25069中的3.82要求；
- e) 设备应支持数字签名、哈希算法等技术，防止传输数据被非法篡改；
- f) 家庭网关应支持记录数据传输日志，且日志保存时间应超过30天。

10.3 设备管理安全

家庭物联网设备应支持以下管理安全要求：

- a) 设备应具备自动更新功能，以修复可能存在的安全漏洞；设备制造商应定期发布设备相关协议的安全更新补丁；
- b) 网络入侵防御安全技术要求应符合GB/T 28451中6的要求；
- c) 设备加密密钥应定期更新，更新周期可以根据设备的重要性的和数据敏感度设定。

10.4 安全审计

家庭物联网网关设备应支持以下安全审计要求：

- a) 网关设备安全审计要求应满足GB/T 41269—2022中5.9的规定；
- b) 网关设备安全审计要求应支持IPv6协议，支持IPv6物联网设备的接入和安全日志审计。

11 数据接口规范

11.1 通信协议

家庭物联网设备应支持DHCPv6协议，宜支持请求响应、发布订阅模式，宜使用CoAP、MQTT协议，优先采用加密传输。

11.2 家庭物联网网关接口规范

11.2.1 接入日志

接入日志用于记录家庭物联网设备接入网关的相关信息，包括接入状态、时间、设备标识等，便于溯源分析和问题排查。

接入日志应符合表1给出的规范。

表 1 接入日志记录信息

参数名称	数据类型	说明
deviceId	string	设备唯一标识

gatewayId	string	家庭物联网网关唯一标识
method	string	设备接入方式
result	boolean	接入结果
resultDesc	string	接入结果描述
ipAddress	string	设备分配的IPv6地址
firmwareVersion	string	设备固件版本号
timestamp	long	设备接入时间戳

11.2.2 流量溯源

流量溯源接口用于记录和追踪家庭物联网中设备与网关或外部服务之间的流量信息,包含源、目标、通信方式、流量量化指标等,以便进行安全审计和异常行为分析。

数据访问记录应符合表2给出的规范。

表 2 数据访问记录信息

参数名称	数据类型	说明
sourceIp	string	流量发起方IPv6地址
sourcePort	int	流量发起方端口
destinationIp	string	流量目标方IPv6地址
destinationPort	int	流量目标方端口
protocol	string	传输协议
trafficSize	int	本次通信产生的流量大小,单位为字节

11.3 家庭物联网设备接口规范

11.3.1 请求消息通用格式

在请求/响应模式下,应遵循统一的数据接口格式,请求消息格式应符合表3给出的规范。

表 3 请求消息通用格式

参数名称	数据类型	说明
msgId	string	消息的唯一标识
businessType	string	业务类型
data	string	消息的详细数据,JSON格式
timestamp	long	消息的时间戳

11.3.2 响应消息通用格式

在请求/响应模式下,应遵循统一的数据接口格式,请求消息格式应符合表4给出的规范。

表 4 响应消息通用格式

参数名称	数据类型	说明
------	------	----

code	int	响应代码，“200”表示成功
msg	string	响应消息描述
data	string	响应数据类型，JSON格式

11.3.3 设备配网

接口描述：用于SoftAP配网模式，用户连接设备AP进行配网，使用CoAP协议。

接口地址：/set_wifi

请求参数：data数据应符合下表5给出的规范。

表 5 设备配网请求参数

参数名称	数据类型	说明
ssid	string	Wi-Fi的SSID
password	string	Wi-Fi的密码
shoapUrl	string	接入平台地址
appId	string	配网终端标识
userId	string	配网用户标识

返回参数：应符合表6给出的规范。

表 6 设备配网返回参数

参数名称	数据类型	说明
code	int	响应代码，“200”表示成功
msg	string	响应消息描述
data	string	响应数据类型，JSON格式

11.3.4 设备接入

接口描述：用于家庭物联网设备接入平台，使用MQTT协议，请求携带设备与证书信息，以供平台校验家庭物联网设备身份的合法性。

请求参数：data数据应符合表7给出的规范。

表 7 设备接入请求参数

参数名称	数据类型	说明
productId	string	产品标识
deviceId	string	设备标识
deviceSecret	string	设备密钥
ipv6Did	string	设备IPv6身份标识
appId	string	应用APP标识
userId	string	应用APP用户标识

返回参数：应符合表8给出的规范。

表 8 设备接入返回参数

参数名称	数据类型	说明
code	int	响应代码，“0”表示成功
msg	string	响应消息描述
data	string	响应数据类型，JSON格式