

保密等级：公开发放

中国电信集团公司 发布

2018-××-××实施

2018-××-××发布

中国电信智能家庭网关技术要求

Technical Specification for Smart Home Gateway of China Telecom

Q/CT 2603-2018

中国电信集团公司企业标准

目  次

[前  言 VI](#_Toc532477755)

[中国电信智能家庭网关技术要求 1](#_Toc532477756)

[1 范围 1](#_Toc532477757)

[2 规范性引用文件 1](#_Toc532477758)

[3 缩略语 2](#_Toc532477759)

[4 设备总体定义 4](#_Toc532477760)

[4.1 设备在网络中的位置 4](#_Toc532477761)

[4.2 接口定义 5](#_Toc532477762)

[4.3 设备形态 5](#_Toc532477763)

[5 物理接口要求 7](#_Toc532477764)

[5.1 网络侧接口要求 7](#_Toc532477765)

[5.2 用户侧接口要求 7](#_Toc532477766)

[5.3 视频外围设备要求（仅针对融合版） 8](#_Toc532477767)

[6 功能要求 9](#_Toc532477768)

[6.1 网络协议及数据转发功能要求 9](#_Toc532477769)

[6.2 WLAN AP功能要求 14](#_Toc532477770)

[6.3 设备发现功能要求 17](#_Toc532477771)

[6.4 业务控制功能要求 18](#_Toc532477772)

[6.5 语音功能处理要求 19](#_Toc532477773)

[7 安全要求 20](#_Toc532477774)

[7.1 网络访问的安全性 20](#_Toc532477775)

[7.2 用户侧WLAN接口安全性 21](#_Toc532477776)

[7.3 登录安全性 21](#_Toc532477777)

[7.4设备及系统安全性 21](#_Toc532477778)

[8 管理和维护要求 22](#_Toc532477779)

[8.1 基本要求 22](#_Toc532477780)

[8.2 本地UI管理和配置要求 23](#_Toc532477781)

[8.3 ITMS+远程管理和配置要求 30](#_Toc532477782)

[8.4 基于OAM的EMS远程管理和配置要求 33](#_Toc532477783)

[8.5 基于OMCI的EMS远程管理和配置要求 33](#_Toc532477784)

[8.6 基于智能网关及应用管理平台的管理配置要求 34](#_Toc532477785)

[8.7 机顶盒模块管理要求（仅针对融合版设备） 39](#_Toc532477786)

[9 性能要求 40](#_Toc532477787)

[9.1 转发性能要求 40](#_Toc532477788)

[9.2 WLAN无线性能要求 40](#_Toc532477789)

[9.3 可靠性要求 42](#_Toc532477790)

[10 运行环境要求 42](#_Toc532477791)

[10.1 供电及功耗要求 43](#_Toc532477792)

[10.2 环境要求 44](#_Toc532477793)

[10.3 抗电磁干扰能力 44](#_Toc532477794)

[10.4 设备本身产生的电磁干扰要求 44](#_Toc532477795)

[10.5 过压过流保护 44](#_Toc532477796)

[10.6 光接口安全性要求 44](#_Toc532477797)

[10.7 视音频信号电气性能要求（仅针对融合版设备） 45](#_Toc532477798)

[11 软硬件要求 45](#_Toc532477799)

[11.1 硬件要求 45](#_Toc532477800)

[11.2 软件要求 47](#_Toc532477801)

[11.3 版本号管理要求 49](#_Toc532477802)

[12 基本应用要求 49](#_Toc532477803)

[12.1 强制门户功能 49](#_Toc532477804)

[12.2 家庭存储 49](#_Toc532477805)

[12.3 IPTV 50](#_Toc532477806)

[13 设备外观及界面类要求 50](#_Toc532477807)

[13.1 设备外观要求 50](#_Toc532477808)

[13.2 智能家庭网关外壳标签要求 51](#_Toc532477809)

[13.3 界面要求 52](#_Toc532477810)

[附　录　A （规范性附录） DHCP报文扩展 53](#_Toc532477811)

[A.1 DHCPv4 Vendor class identifier格式 53](#_Toc532477812)

[A.2 DHCPv4 Vendor-Identifying Vendor-Specific Information Option要求 54](#_Toc532477813)

[A.3 DHCPv4认证（携带Option60、Option125字段）过程 56](#_Toc532477814)

[A.4 DHCPv6 Option字段携带说明 57](#_Toc532477815)

[附　录　B （规范性附录） 系统及数据安全性要求 60](#_Toc532477816)

[B.1 操作系统安全 60](#_Toc532477817)

[B.2 页面访问要求 60](#_Toc532477818)

[B.3 维护入口安全 60](#_Toc532477819)

[B.4 协议安全 61](#_Toc532477820)

[B.5 敏感数据安全 61](#_Toc532477821)

[B.6 日志安全 61](#_Toc532477822)

[B.7 代码安全 62](#_Toc532477823)

[B.8 设备安全 62](#_Toc532477824)

[附　录　C （规范性附录） 智能OS（基于嵌入式Linux智能OS）技术要求 63](#_Toc532477825)

[C.1 架构说明 63](#_Toc532477826)

[C.1.1 总体架构 63](#_Toc532477827)

[C.1.2 网关内部架构 64](#_Toc532477828)

[C.1.3 IPC Service 64](#_Toc532477829)

[C.2 系统要求 65](#_Toc532477830)

[C.2.1 系统软件要求 65](#_Toc532477831)

[C.2.2 系统分区及中间件集成要求 66](#_Toc532477832)

[C.3 预置软件配置要求 69](#_Toc532477833)

[C.3.1 DBus 69](#_Toc532477834)

[C.3.2 glib 70](#_Toc532477835)

[C.3.3 lxc 70](#_Toc532477836)

[C.3.4 DPI 70](#_Toc532477837)

[C.4 WEB要求 71](#_Toc532477838)

[C.4.1 权限分级界面 71](#_Toc532477839)

[C.4.2 插件配置下发记录的通知 71](#_Toc532477840)

[C.5 LXC容器技术要求 72](#_Toc532477841)

[C.6 DBus总体要求 72](#_Toc532477842)

[C.6.1 服务名 72](#_Toc532477843)

[C.6.2 兼容性 72](#_Toc532477844)

[C.6.3 效率 72](#_Toc532477845)

[C.7 扩展的DBus接口要求 72](#_Toc532477846)

[C.7.1 com.ctc.igd1.Properties 73](#_Toc532477847)

[C.7.2 com.ctc.igd1.ObjectManager 74](#_Toc532477848)

[C.8 系统服务及接口要求 74](#_Toc532477849)

[C.8.1 DBus接口 74](#_Toc532477850)

[C.8.2 DBus对象 115](#_Toc532477851)

[C.9 其它网关服务接口要求 118](#_Toc532477852)

[C.9.1 USB设备管理服务 118](#_Toc532477853)

[C.9.2 NAS服务 120](#_Toc532477854)

[C.9.3 VPN客户端服务 121](#_Toc532477855)

[C.9.4 DNS服务 123](#_Toc532477856)

[C.9.5 DDNS服务 124](#_Toc532477857)

[C.9.6 FTP服务 125](#_Toc532477858)

[C.9.7 Samba服务 126](#_Toc532477859)

[C.9.8 HTTP服务 127](#_Toc532477860)

[C.9.9 Telnet服务 127](#_Toc532477861)

[C.9.10 Beacon/Probe帧扩展Vendor-specific Information Element服务 128](#_Toc532477862)

[C.9.11 Roaming服务 132](#_Toc532477863)

[C.9.12 网关质量诊断服务 136](#_Toc532477864)

[C.10 DPI对网关接口要求 139](#_Toc532477865)

[C.10.1 会话信息 139](#_Toc532477866)

[C.10.2 插件识别信息 140](#_Toc532477867)

[C.10.3 流程处理接口 140](#_Toc532477868)

[C.10.4 报文处理接口 141](#_Toc532477869)

[C.10.5插件信息获取接口 143](#_Toc532477870)

[附　录　D （规范性附录） 告警信息 145](#_Toc532477871)

[D.1 告警编号规则 145](#_Toc532477872)

[D.2 设备告警信息列表 145](#_Toc532477873)

[附　录　E （规范性附录） 日志文件格式 148](#_Toc532477874)

[E.1 文件格式 148](#_Toc532477875)

[E.2 Syslog Message Severities 148](#_Toc532477876)

[附　录　F （规范性附录） 基于宽带识别码的设备首次认证用户提示信息 149](#_Toc532477877)

[F.1 基于宽带识别码的设备首次认证用户提示信息 149](#_Toc532477878)

[F.2 注册初始界面提示要求 150](#_Toc532477879)

[F.3 注册和业务下发过程中的提示规范要求 150](#_Toc532477880)

[附　录　G （规范性附录） 提供的服务及协议端口汇总 152](#_Toc532477881)

[G.1 网络侧协议及端口的开关要求 152](#_Toc532477882)

[G.2 用户侧协议及端口的开关要求 153](#_Toc532477883)

[附　录　H （规范性附录） 网关质量诊断信息收集要求 155](#_Toc532477884)

[H.1 方案架构 155](#_Toc532477885)

[H.2 网关质量诊断相关DBUS接口定义 157](#_Toc532477886)

[H.3 信息文件互斥 157](#_Toc532477887)

[H.4 服务器获取 157](#_Toc532477888)

[H.4.1 内核崩溃信息 158](#_Toc532477889)

[H.4.2 设备重启信息 158](#_Toc532477890)

[H.4.3 WIFI信息收集 158](#_Toc532477891)

[H.4.4 WIFI诊断 160](#_Toc532477892)

[H.4.5 断网检测 163](#_Toc532477893)

[H.4.6 网关进程资源监控 164](#_Toc532477894)

[H.4.7 插件异常监控信息（中间件实现） 165](#_Toc532477895)

[H.4.8 网关受控进程异常信息 166](#_Toc532477896)

[H.4.9 网关端口监测（网关质量插件实现） 167](#_Toc532477897)

[H.4.10 语音模块信息采集 167](#_Toc532477898)

[H.4.11 其它需要实现的接口 168](#_Toc532477899)

[H.4.12 补充要求 168](#_Toc532477900)

[附　录　I （资料性附录） 网关快联配网 169](#_Toc532477901)

[I.1 快联配网基础 169](#_Toc532477902)

[I.2 基于云平台认证的快联配网 169](#_Toc532477903)

[I.3 基于动态配网热点的快联配网 171](#_Toc532477904)

[I.4 Beacon/Probe帧中扩展Vendor-specific Information Element信息的快联配网 172](#_Toc532477905)

前  言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准是中国电信家庭网络终端及管理系统系列技术标准之一，该系列标准的结构及名称如下：

1. 中国电信家庭网关总体技术要求（Q/CT 2270-2014）
2. 中国电信家庭网关与增强型终端综合管理系统接口技术要求（Q/CT 2271-2014）
3. 中国电信增强型终端综合管理系统技术要求（Q/CT 2167-2013）
4. 中国电信家庭网络终端管理接口技术要求（Q/CT 2540-2012）
5. 中国电信智能家庭网关技术要求（Q/CT 2603-20XX）
6. 中国电信智能家庭网关与智能网关及应用管理平台接口技术要求（Q/CT 2604-2017）

中国电信智能家庭网关为了满足智慧家庭业务的发展需求，通过在e8-C家庭网关基础上提升硬件能力、引入智能OS和智能应用、扩展手机APP等智能操控能力而形成的智能化家庭宽带终端，是家庭的网络接入中心、设备管理中心和业务控制中心。

本标准是根据中国电信开展智慧家庭业务的实际情况而制定的，主要用于规范智能家庭网关的设备形态、接口、功能、管理、安全、性能、运行环境、设备软硬件和基本应用等内容。

本标准由中国电信集团公司提出并归口。

本标准由中国电信集团公司技术部组织制定，中国电信股份有限公司上海研究院起草。

本标准主要起草人：赵伟峰、刘文超、刘向辉、汤宪飞、侍芯蕊、胡冰松、陈健康、沈屹炜。

本标准于2014年9月发布试行标准，2015年7月发布正式标准，2017年2月第一次修订，本次为正式标准第二次修订。

中国电信智能家庭网关技术要求

1. 范围

本标准规定了智能家庭网关的设备形态、接口、功能、管理、安全、性能、运行环境、设备软硬件、基本应用和用户界面等要求。

本标准适用于中国电信网络中使用的智能家庭网关设备。

本标准中PON技术的名称参照《中国电信EPON设备技术要求1G-EPON/10G-EPON》、《中国电信GPON设备技术要求》和《中国电信XG-PON设备技术要求》，1G/1G-EPON称为1G-EPON；10G/1G-EPON和10G/10G-EPON统称为10G-EPON，1G-EPON和10G-EPON统称为EPON；EPON、GPON和XG-PON统称为PON。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

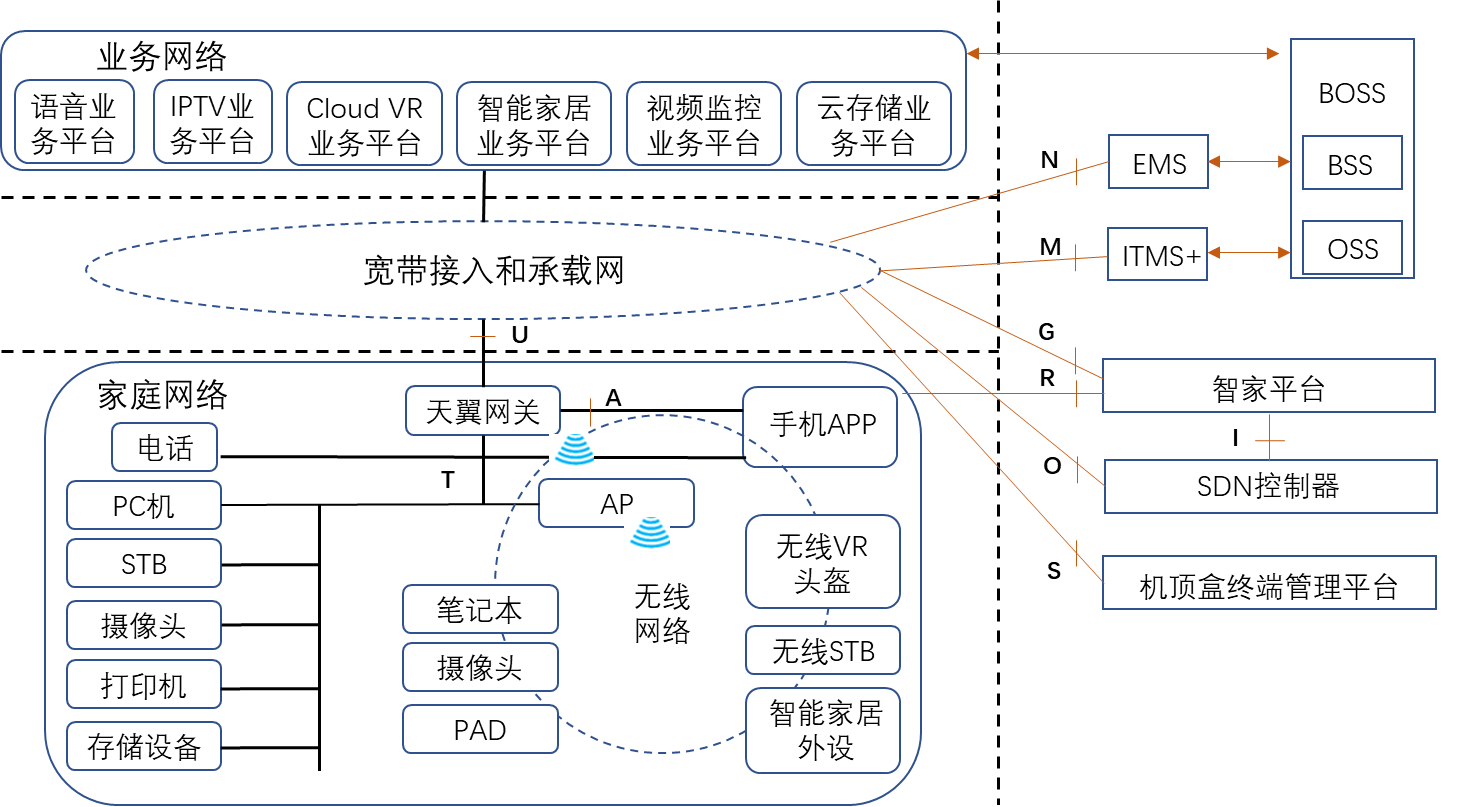
|  |  |
| --- | --- |
| YD/T 983-1998 | 通信电源设备电磁兼容性限值及测量方法 |
| Q/CT 1926-2007 | 中国电信IAD设备技术规范 |
| Q/CT 2085-2010 | 中国电信IMS网络IP Centrex业务技术要求 |
| Q/CT 2089-2010 | 中国电信IMS网络呼叫前转业务技术要求 |
| Q/CT 2090-2010 | 中国电信IMS网络呼叫保持业务技术要求 |
| Q/CT 2091-2010 | 中国电信IMS网络主叫识别显示/限制业务技术要求 |
| Q/CT 2094-2018 | 中国电信IMS网络SIP协议总体技术要求 |
| Q/CT 2270-2014 | 中国电信家庭网关总体技术要求 |
| Q/CT 2271-2014 | 中国电信家庭网关与增强型终端综合管理系统接口技术要求 |
| Q/CT 2360-2011 | 中国电信GPON设备技术要求 |
| Q/CT 2361-2017 | 中国电信EPON设备技术要求1G-EPON/10G-EPON |
| Q/CT 2460-2012 | 中国电信IMS SIP 硬终端技术要求 |
| Q/CT 2470-2017 | 中国电信智能机顶盒技术要求 |
| Q/CT 2604-2016 | 中国电信智能家庭网关与智能网关及应用管理平台接口技术要求 |
| Q/CT 2635-2017 | 中国电信XG-PON设备技术要求 |
| ITU-T G.9960 | 基于高速线路统一的家庭联网收发器——系统架构与物理层规范 |
| ITU-T G.9961 | 基于高速线路统一的家庭联网收发器——数据链路层规范 |
| IEEE 802.3 | CSMA/CD访问方式和物理层规范 |
| IEEE 802.11 | 无线局域网媒质访问控制层及物理层标准 |
| TR-069 | CPE WAN Management Protocol |
| TR-098 | Gateway Device Version 1.1 Data Model for TR-069 |
| TR-104 | Provisioning Parameters for VoIP CPE |
| UPnP IGD 1.0 | 通用即插即用标准（综合网关设备） |

1. 缩略语

下列缩略语适用于本标准：

|  |  |  |
| --- | --- | --- |
| 缩略语 | 英文全称 | 中文全称 |
| AP | Access Point | 无线接入点 |
| APP | Application | 应用 |
| BT | Blue Tooth | 蓝牙 |
| CPE | Customer Premise Equipment | 用户侧设备 |
| CPU | Central Processing Unit | 中央处理单元 |
| DDNS | Dynamic Domain Name Server | 动态域名解析 |
| DHCP | Dynamic Host Configuration Protocol | 动态主机配置协议 |
| DLNA | Digital Living Network Alliance | 数字生活网络联盟 |
| DMC | Digital Media Controller | 数位媒体控制器 |
| DMR | Digital Media Renderer | 数位媒体接收器 |
| DMS | Digital Media Server | 数字媒体服务器 |
| DNS | Domain Name Server | 域名服务器 |
| DSP | Digital Signal Processor | 数字信号处理器 |
| DS-Lite | Dual-Stack Lite | 轻型双栈 |
| EEE | Energy Efficient Ethernet | 高效节能以太网 |
| EMI | Electromagnetic Interference | 电磁干扰 |
| EMS | Element Management System | 网元管理系统 |
| EPON | Ethernet Passive Optical Networks | 以太网无源光网络 |
| FEC | Forward Error Correction | 前向纠错 |
| FTP | File Transfer Protocol | 文件传送协议 |
| GPON | Gigabit-Capable Passive Optical Network | 吉比特无源光网络 |
| GUI | Graphic User Interface | 图形化用户接口 |
| HTTP | Hyper Text Transfer Protocol | 超文本传输协议 |
| IGD | Integrated Gateway Device | 综合网关设备 |
| IP | Internet Protocol | 互联网协议 |
| IPTV | Internet Protocol Television | 交互式网络电视 |
| ITMS+ | Integrated Terminal Management System Plus | 增强型终端综合管理系统 |
| L2TP | Layer-2 Tunneling Protocol | 第二层穿隧协定 |
| LAN | Local Area Network | 局域网 |
| LXC | Linux Container | Linux容器 |
| LDPC | Low-density Parity-check | 低密度校验 |
| MAC | Media Access Control | 媒体访问控制 |
| MIMO | Multi-Input Multi-Output | 多输入多输出 |
| MIPS | Millions of Instructions Per Second | 百万条指令/秒 |
| MLD | Maximum-Likelihood Decoding | 最大似然解码 |
| NAT | Network Address Translation | 网络地址转换 |
| NTP | Network Time Protocol | 网络时间协议 |
| OAM | Operation, Administration &Maintenance | 操作、管理和维护 |
| OLT | Optical Line Terminal | 光线路终端 |
| OMCI | ONU Management and Control Interface | ONU管理控制接口 |
| ONU | Optical Network Unit | 光网络单元 |
| OUI | Organizationally Unique Identifiers | 组织唯一标识 |
| POTS | Plain Old Telephony Service | 传统电话服务 |
| PPPoE | PPP over Ethernet | 以太网上传送PPP协议 |
| QoS | Quality of Service | 服务质量 |
| RAM | Random Access Memory | 随机存储器 |
| SATA | Serial Advanced Technology Attachment | 串行高级技术附件 |
| SIP | Session Initiation Protocol | 初始会话协议 |
| SNMP | Simple Network Management Protocol | 简单网络管理协议 |
| SNTP | Simple Network Time Protocol | 简单网络时间协议 |
| SSID | Service Set Identifier | 服务集标志符 |
| STB | [set-top-box](http://suoxie.911cha.com/OXJv.html" \t "_blank) | 机顶盒 |
| STBC | Space-Time Block Coding | 时空块编码 |
| TCP | Transmission Control Protocol | [传输控制协议](http://baike.baidu.com/view/544903.htm" \t "_blank) |
| UDP | [User Datagram Protocol](http://www.networkdictionary.cn/?q=protocols/udp.php" \t "_blank) | 用户数据报协议 |
| UI | User Interface | 用户界面 |
| UPnP | Universal Plug and Play | 通用即插即用 |
| URL | [Uniform Resource Locator](http://suoxie.911cha.com/MTV4cQ==.html" \t "_blank) | [统一资源定位格式](http://suoxie.911cha.com/MTV4cQ==.html" \t "_blank) |
| USB | Universal Serial Bus | 通用串行总线 |
| VLAN | Virtual Local Area Network | 虚拟局域网 |
| VPN | Virtual Private Network | 虚拟专用网络 |
| WAN | Wide Area Network | 广域网 |
| WEP | Wired Equivalent Privacy | 有线等效加密 |
| WLAN | Wireless LAN | 无线局域网 |
| WPA | WiFi Protected Access | WiFi网络安全存取 |
| XG-PON | 10-Gigabit-capable Passive Optical Network | 10Gbit/s无源光网络 |
| XML | [eXtensible Markup Language](http://suoxie.911cha.com/cDJp.html" \t "_blank) | [可扩展标记语言](http://suoxie.911cha.com/cDJp.html" \t "_blank) |

1. 设备总体定义
   1. 设备在网络中的位置



1. 智能家庭网关在网络中的位置

天翼智能家庭网关是家庭网络和外部网络的接口单元，在网络中的位置如图1所示。

图1中，ITMS+（增强型终端综合管理系统）是家庭网关业务的部署和控制平台，也是家庭网关设备的远程管理平台，通过它既可以实现对家庭网关上的数据、语音、视频、QoS等功能进行部署、管理和控制；又可以实现对家庭网关的远程状态查询、故障管理、设备配置和软件升级。EMS（网元管理系统）用于PON上行家庭网关PON接口相关的物理层及链路层的配置及管理。手机APP、智家平台作为互联网操控体验的管理手段，为用户提供智能家庭网关及智能应用的全新配置管理方式。IPTV业务平台提供IPTV、终端桌面、应用市场、IPTV 增值业务、智能增值应用等服务。Cloud VR业务平台提供VR增值业务应用服务。

家庭网络内部各种终端通过智能家庭网关的用户侧接口与智能家庭网关进行通信，智能家庭网关对经过其的数据和应用进行转发、控制和管理，并通过网络侧接口与业务平台、ITMS+、智家平台、机顶盒终端管理平台进行交互，实现家庭网络和外部网络的通信，提供各种可管理、可控制的应用。

* 1. 接口定义

1. U接口

U接口是智能家庭网关和宽带接入网的接口，采用EPON、GPON、X-GPON等接入技术，同时传递接入认证、QoS适配等的控制信息。

1. T接口

T接口是智能家庭网关和各种应用终端或组网终端的接口，实现智能家庭网关对家庭应用终端的设备发现和统一管理。

1. M接口

M接口是智能家庭网关和ITMS+之间的远程逻辑接口，采用TR-069系列协议，可以实现对智能家庭网关的远程管理、配置、软件升级、性能统计、故障诊断等功能。

1. N接口

N接口是PON上行智能家庭网关和EMS之间的远程逻辑接口，采用OAM或OMCI系列协议，可以实现对智能家庭网关PON接口相关的物理层及链路层的配置及管理等功能。

1. G接口

G接口是智能家庭网关和“智家平台”之间的远程逻辑接口，可以实现对智能家庭网关以及加载应用的配置及管理等功能。

1. R接口

R接口是手机APP和“智家平台”之间的远程逻辑接口，可以通过“智家平台”实现对智能家庭网关以及加载应用的配置及管理等功能。

1. I接口

I接口是“智家平台”和“SDN控制器”之间的远程逻辑接口，用于“智家平台”和“SDN控制器”之间交互，实现“智家平台”操控“SDN控制器”向智能家庭网关下发OpenFlow流表。

1. O接口

O接口是智能家庭网关和“SDN控制器”之间的远程逻辑接口，可以实现SDN控制器接收智能家庭网关上SDN功能模块通过OpenFlow协议上报的用户报文信息，并对智能家庭网关上SDN功能模块的OpenFlow转发流表进行配置。

1. A接口

A接口是手机APP和智能家庭网关之间的本地逻辑接口，可以实现对智能家庭网关以及加载应用的配置及管理等功能。

1. S接口（仅针对融合版设备）

S接口是机顶盒模块的终端桌面客户端与机顶盒终端管理平台之间的逻辑接口，可以实现终端桌面的注册、终端桌面展现内容的配置及管理等功能。

* 1. 设备形态

智能家庭网关设备的主要形态如表1所示。

1. 智能家庭网关设备形态

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 项目 | | 单频版 | 双频版 | 双频WiFi6版 | 千兆版 | 融合版 | AP外置版 |
| 网络侧接口 | | 1G-EPON/GPON | | | 10G-EPON/XG-PON | EPON/GPON/以太网 | 网关组件：1G-EPON/GPON  外置AP：以太网（GE） |
| 用户侧接口 | 以太网接口 | 4个（其中至少1个GE口） | 4GE | 4GE | 4GE（其中宜支持至少一个2.5GE口） | 2个（其中至少1个GE口） | 网关组件：4个（其中至少1个GE口）  外置AP：至少1个GE口 |
| POTS接口 | 1个 | 1个 | 1个 | 1个 | 1个(PON上行设备为必选，以太网上行设备为可选) | 1个（网关组件提供） |
| WLAN接口 | 2.4GHz 802.11n（2X2） | 2.4GHz 802.11n（2X2）+ 5GHz 802.11ac（至少2X2） | 2.4GHz 802.11ax（2X2）+ 5GHz 802.11ax（2X2） | 2.4GHz 802.11ax（2X2）+ 5GHz 802.11ax（2X2） | 2.4GHz 802.11n（2X2） | 2.4GHz 802.11n（至少2X2）+ 5GHz 802.11ac（至少2X2）（由外置AP提供） |
|
| USB Host | 1个 | | | 1个 | 2个 |  |
| 视频接口 |  | | |  | HDMI2.0+MINICVBS |  |
| 红外IR |  | | |  | 1个 |  |
| TF卡 |  | | |  | 1个（可选） |  |
| 硬件指标 | 系统综合能力 | 不小于2000 DMIPS | | | 不小于3000DMIPS | * 网关模块：不小于2000DMIPS * 机顶盒模块：参照《中国电信智能机顶盒技术要求》5.1 | 网关组件：不小于2000 DMIPS |
| FLASH容量 | 不小于256MByte | | | 不小于256MByte | * 网关模块：不小于256MByte * 机顶盒模块：不小于8GByte ，建议 16GByte | 网关组件：不小于256MByte |
| RAM容量 | 不小于256MByte | 不小于512MByte | 不小于512MByte | 不小于512MByte | * 网关模块：不小于256Mbyte * 机顶模块：不小于1G Byte | 网关组件：不小于256MByte |
| 最大功耗 | 21W | 23W | 25W | 27W | 25W | 18W（仅网关组件） |
| 性能指标 | 整体吞吐量（见9.1） | T\_1 | | | T\_2 | T\_1 | 网关组件：T\_1 |
| WLAN吞吐量（见9.2） | W\_1 | 2.4G频段：W\_1 | 2.4G频段：W\_6 | 2.4G频段：W\_6 | W\_1 | 2.4G频段：至少W\_1 |
| 5G频段：至少W\_3 | 5G频段：W\_7 | 5G频段：至少W\_8 | 5G频段：至少W\_3 |

说明：

* 融合版设备同时包含网关模块和机顶盒模块。其中网关模块提供网络接入业务以及网关智能业务，机顶盒模块提供IPTV应用服务。
* AP外置版设备同时包含2个设备组件：无WiFi网关和外置AP。
* 系统综合能力是对智能家庭网关CPU处理能力、DSP处理能力及硬件加速能力的综合评价，每一部分的处理能力应和其承担的任务相匹配
* 智能家庭网关为应用插件预留的FLASH空间应在128MByte以上（对于融合版，本要求仅针对网络模块）
* 单频版、融合版（网络模块）为应用插件预留的RAM空间应在128MByte以上，双频版、双频WiFi6版和千兆版为应用插件预留的RAM空间应在256MByte以上
* 融合版设备的机顶盒模块要求RAM规格为32BIT DDR3 以上，且运行大型游戏时可提供 500MByte 空间（建议 2G Byte及以上）

1. 物理接口要求
   1. 网络侧接口要求
      1. 1G-EPON接口要求

应符合《中国电信EPON设备技术要求1G-EPON/10G-EPON》。

* + 1. 1G/10G-EPON接口要求

应符合《中国电信EPON设备技术要求1G-EPON/10G-EPON》。

* + 1. 10G/10G-EPON接口要求

应符合《中国电信EPON设备技术要求1G-EPON/10G-EPON》。

* + 1. GPON接口要求

应符合《中国电信GPON设备技术要求》。

* + 1. XG-PON接口要求

应符合《中国电信XG-PON设备技术要求》。

* + 1. 以太网接口要求

针对以太网上行融合版网关，上行接口应至少为FE口，宜为GE口。

FE口应是10/100 Base-T Ethernet接口，GE口应是100/1000 Base-T Ethernet接口。

应符合IEEE802.3标准，支持采用直连网线进行连接，支持自动校验连接网线的功能。

应符合IEEE 802.3az EEE标准。

* 1. 用户侧接口要求
     1. 用户侧以太网接口要求

FE口应是10/100 Base-T Ethernet接口， GE口应是100/1000 Base-T Ethernet接口。2.5G速率接口应是100M /1G/2.5G接口，应符合IEEE 802.3bz标准。

应符合IEEE802.3标准，支持采用直连网线进行连接，支持自动校验连接网线的功能。

应符合IEEE 802.3az EEE标准。

* + 1. WLAN接口要求

2.4GHz应符合IEEE 802.11n或802.11ax协议，5GHz应符合IEEE 802.11ac或802.11ax协议（详细要求见6.2）。应通过WiFi联盟互操作性认证。

* + 1. USB Host接口要求

至少应符合USB 2.0规范且支持Hi-Speed速率要求，宜支持USB3.0规范。

每个USB Host接口的最大工作电流应能达到1000mA。

USB Host接口支持USB Storage、USB转串口（含UART、ACM两种方式）、USB HID三种驱动模式。USB Storage模式下应支持USB Mass Storage类下定义的所有的子类及传输协议，应能识别并加载标准的USB Mass Storage类设备，应支持FAT、FAT32、NTFS的分区格式，宜支持exFAT的分区格式。

对于融合版设备，USB口宜支持网关模块和机顶盒模块共享使用。不支持USB口共享使用的融合版设备，2个USB接口应分别供网关模块和机顶盒模块使用。

* + 1. 用户侧电话接口要求

参见《中国电信家庭网关总体技术要求》5.2.4。

* + 1. 视频类接口要求（仅针对融合版）

视频接口（HDMI2.0、MINICVBS）、红外接口（含应支持通过红外接口、USB接口或耳机孔连接红外延长线）、TF卡接口应符合《中国电信智能机顶盒技术要求》5.2。

* 1. 视频外围设备要求（仅针对融合版）
     1. 普通遥控器

参见《中国电信智能机顶盒技术要求》5.4.1。

* + 1. 融合遥控器

参见《中国电信智能机顶盒技术要求》5.4.3。

* + 1. 摄像头

参见《中国电信智能机顶盒技术要求》5.4.4。

1. 功能要求
   1. 网络协议及数据转发功能要求

在网络侧，智能家庭网关设备应与网络设备配合，完成用户接入、网络地址分配、用户信息认证等管理控制功能，以支撑网络运营。

在用户侧，智能家庭网关设备应该能够支持家庭网络运行，提供如地址分配、地址解析等管理服务功能。

* + 1. IP协议要求

应支持IPv4/v6双栈协议：

1. 支持同时获取IPv4/v6地址的能力。支持建立一条支持IPv4/v6双栈的网络连接，同时获取IPv4、IPv6的地址，同时支持IPv4和IPv6的应用。
2. 能够根据获取IP地址的类型，自动使用相应的协议栈进行数据转发；对于同时获取到IPv4/v6地址的情况，优选使用IPv6地址。
3. 访问外网时，能够根据外网目的IP地址的类型，自动选择相应的网络连接或使用相应的协议栈进行外网访问；
4. IPv6协议应能够由ITMS+进行远程开启或关闭，缺省开启。
5. 在启用IPv4/v6双栈协议时，根据用户数据的协议（IPv4或IPv6）进行同协议类型的路由转发。
   * 1. 数据转发功能要求
6. 应支持路由工作模式、桥接工作模式,两种模式能同时工作，能够同时支持IPv4、IPv6报文的转发，应支持基于接口绑定、VLAN绑定两种绑定方式进行数据转发。在路由WAN模式下应支持根据网络连接的MTU值，最大匹配地限制所发起TCP连接或修改所承载TCP连接的MSS值。
7. 应支持静态路由。
8. 应支持基于流表的数据转发。
   * 1. DNS功能要求
9. 应支持DNS relay，支持家庭网络内部设备的DNS请求转发至DNS服务器，并将服务器的DNS响应转发至家庭内部网络设备。
10. 应支持IPv4和IPv6的DNS client，具备从外部DNS server同时获取同一域名IPv4/v6地址的功能，查询A记录时优先使用v4方式（如DHCPv4 option6）获得的DNS服务器，查询AAAA记录时优先使用v6方式（如DHCPv6 Option23）获得的DNS服务器。
11. 智能家庭网关在IPv4/v6双栈路由模式启用DNS proxy时，应根据用户侧设备DNS请求报文的IP地址类型（IPv4或IPv6）转发到IP地址类型相同的DNS server进行解析，在IP地址类型相同的DNS server不存在或没有响应时应转发到另一IP地址类型的DNS server进行解析。
12. 应支持每个WAN连接使用对应的DNS Server，智能家庭网关应支持自动获取、或在Static IP时手工配置DNS server信息。对于含有“Internet”属性的路由WAN链接，家庭网关应支持将指定的URL发送到特定DNS进行解析（未指定的URL仍使用WAN连接缺省DNS进行解析），指定URL列表及特定DNS地址由智家平台下发。
13. 应支持针对特定域名域的DNS解析请求报文在单位时间内向网络侧转发的数量进行限制，限定的域名域、限定阈值和越限处理策略由ITMS远程配置；对于超出限定阈值的DNS解析请求报文，需记录请求者的源IP地址及源MAC地址。
14. 应支持DDNS功能，宜支持多家DDNS服务商。DDNS功能应支持接受智家平台的配置控制（包括参数设置、启用、停止等相关操作）。
    * 1. IPv4地址管理及WAN连接管理功能要求
15. 家庭网关应支持DHCPv4 server，应具备为家庭网络提供至少253个可分配地址的能力。DHCPv4 server应支持在DHCP OFFER、DHCP ACK报文中携带Option125字段（符合附录A相关要求），具体要求为：
16. 在未启用全路由（缺省关闭全路由）、未启用基于VLAN绑定功能时，应至少包含以下选项内容：

* DHCP server的设备种类或分类（subopt-code值为2，sub-option-data值为HGW-CT）

1. 在启用了基于VLAN绑定功能时，应至少包含以下选项内容：

* DHCP server的设备种类或分类（subopt-code值为2，sub-option-data值为HGW-CT）
* 该端口所承载业务的VLAN ID（即需要用户应用设备携带的业务VLAN ID）：如上网类业务的VLAN ID（subopt-code值为10）、IPTV业务的VLAN ID（subopt-code值为11）、VOICE业务的VLAN ID（subopt-code值为13）等

1. 在启用了全路由功能且未启用基于VLAN绑定功能时，应至少包含以下选项内容：

* DHCP server的设备种类或分类（subopt-code值为2，sub-option-data值为HGW-CT-R）

1. 缺省所有LAN侧IP地址段为192.168.1.0/24。
2. 应同时支持用户侧端口数据携带或不携带VLAN ID。
3. 在WAN侧应支持静态配置IP地址、DHCPv4、PPPoE三种工作方式（遵循RFC2684/RFC2516）；当采用PPPoE工作方式时应支持自动重拨模式；当采用DHCPv4工作方式时，应支持以下DHCP option字段：
   * 1. Option60字段配置及上送，字段内容格式符合附录A的要求，Option60字段的具体内容能够由ITMS+进行配置
     2. Option125接收及检测，只接受Option125字段匹配的DHCP server报文，对于Option125字段不匹配的DHCP server报文不作回应，Option125字段的具体内容能够由ITMS+进行配置
4. 应支持至少16个WAN连接同时工作，应支持至少8个路由WAN连接同时工作。应至少支持8条VLAN同时连接，每条VLAN应支持5个WAN连接同时工作（每个WAN连接的模式应可任选桥接或路由模式）。
5. WAN连接建立及管理要求：
   * 1. 仅电信维护人员和TR069远程可配置WAN连接；
     2. 应自动生成WAN连接名称，且应符合“序号\_­关键字\_桥接或路由方式\_VLAN信息”的WAN连接名称组成规则，各组成部分具体定义如表2所示：
6. WAN连接名称定义

|  |  |  |
| --- | --- | --- |
| 内容 | 定义 | 含义 |
| 序号 | 数字：1～99 | WAN连接的数字标识，生成规则如下：按WAN连接生成顺序，序号依次递增，当前已使用的数字不应重复使用 |
| 关键字（即TR069、VOICE、INTERNET等业务属性或几个业务属性的组合） | TR069 | 表示此连接仅用于TR069 |
| INTERNET | 表示此连接仅用于上网等应用，但不支持TR069 |
| TR069\_INTERNET | 表示此连接同时用于TR069和上网等应用 |
| VOICE | 表示此连接仅用于语音 |
| TR069\_VOICE | 表示此连接仅用于TR069和语音应用 |
| VOICE\_INTERNET | 表示此连接仅用于上网和语音应用 |
| TR069\_VOICE\_INTERNET | 表示此连接仅用于TR069、上网和语音应用 |
| SPECIAL\_SERVICE\_1 | 表示此连接仅用于新增特定应用（如某智慧家庭应用） |
| SPECIAL\_SERVICE\_2 | 表示此连接仅用于新增特定应用（如某智慧家庭应用） |
| SPECIAL\_SERVICE\_3 | 表示此连接仅用于新增特定应用（如某智慧家庭应用） |
| SPECIAL\_SERVICE\_4 | 表示此连接仅用于新增特定应用（如某智慧家庭应用） |
| SPECIAL\_SERVICE\_VR | 表示此连接仅用于Cloud VR业务应用 |
| Other | 其它连接（除了以上的应用，都选Other，目前主要是STB会用Other这种方式） |
| 桥接或路由方式 | B | Bridge方式 |
| R | Router方式 |
| VLAN信息 | VID\_Z | VID\_Z中Z为实际VLAN\_ID值（对于untag的WAN连接，Z值为空且不出现在连接名称中） |

示例如下：

1\_TR069\_R\_VID\_46（表示此WAN连接的业务类型为TR069，工作方式为Router方式，VLAN ID为46）

2\_INTERNET\_R\_VID\_(表示此WAN连接的业务类型为INTERNET，工作方式为Router方式，VLAN ID为空)

3\_Other\_B\_VID\_45（表示此WAN连接的业务类型为Other，工作方式为Bridge方式，VLAN ID为45）

4\_INTERNET\_R\_VID\_2(表示此WAN连接的业务类型为INTERNET，工作方式为Router方式，VLAN ID为2)

5\_SPECIAL\_SERVICE\_1\_R\_VID\_21 (表示此WAN连接的业务类型为新增特定应用，工作方式为Router方式，VLAN ID为21)

* + 1. WAN连接配置可增加，可修改，可删除；
    2. WAN连接配置后立即启用，并按本地和远程配置的序号和名称进行显示；
    3. TR069、VOICE等本机业务应自动和对应关键字的WAN连接建立绑定关系；
    4. 数据绑定模式要求：

每个用户侧端口应支持以下数据绑定转发方式：

* 未进行绑定的用户侧端口:基于目的IP地址（目的IP地址和WAN连接的绑定关系由ITMS配置），查找绑定的WAN连接进行转发，未查找到WAN连接的，则由缺省WAN连接转发，未配置缺省WAN连接的则丢弃；
* 绑定单条WAN连接的端口：和指定某条WAN连接进行了绑定的用户侧端口，对应端口数据经由绑定的WAN连接收发；
* 绑定多条WAN连接的端口（基于VLAN）：按照配置的VLAN转换表进行转发，带有VLAN转换表中指定VLAN ID的数据经由指定的WAN连接收发，不携带VLAN ID的数据按照未进行绑定的用户侧端口进行处理 ；

每个端口的绑定方式可通过本地GUI及TR069进行配置，数据绑定的多项配置之间发生冲突时应以最新的配置为准，并应自动清除与之冲突的原有配置。

与带“INTERNET”属性WAN连接绑定（含缺省绑定）的终端应能够访问家庭网关WEB页面，各终端间应能相互访问。

TR069或VOICE专用WAN连接不应支持端口绑定功能。

* + 1. 关于缺省路由/缺省连接的确定：

带“INTERNET”属性的WAN连接（包括路由和桥接）为缺省WAN连接。

当存在多条带“INTERNET”属性的路由或桥接WAN连接时，终端自动选择其中生效的一条为缺省WAN连接，且优先选择生效的路由WAN连接。

* + 1. 默认IPv4 NAT模块启用要求：

新建路由WAN连接（TR069或VOICE专用WAN连接除外）时应默认自动起NAT。

* + 1. 默认DHCPv4 Server模块启用要求：

家庭网关用户侧应自动开启DHCP Server，只绑定了带“Other”关键字WAN连接的端口可除外。

* + 1. 多Router连接情况下上报ITMS+要求：

当家庭网关建立了一条以上路由WAN连接时，家庭网关向ITMS+上报的管理IP地址应是TR069通道的地址，上报的宽带帐号应是带“INTERNET”属性的WAN连接用的帐号。

* + 1. 多连接情况下的数据隔离要求：

当家庭网关建立了一条以上的WAN连接时，不同WAN连接之间的数据（包括DNS、ARP、管理应用数据等）应支持完全隔离。

在家庭网关用户侧私网段内，应屏蔽网络侧源IP地址或目的IP地址的ARP报文。

* + 1. 路由WAN透传PPPOE报文的要求：

当家庭网关建立一条Internet PPPoE路由WAN连接时，应支持LAN 侧终端 的PPPoE直接拨号功能，同时路由拨号和LAN侧终端直接拨号出现下列冲突场景时，需要优先保证网关的路由拨号功能；

* 因LAN侧终端先做PPPOE拨号导致BRAS对路由拨号拒绝服务。
* 路由拨号成功后断连重连或直接重连，因LAN侧终端拨号存在导致BRAS对路由拨号拒绝服务。
  + 1. IPv6地址管理及WAN连接管理功能要求

1. 路由、桥接、路由桥接混和模式下，家庭网关应支持SLAAC（无状态地址自动分配）和DHCPv6 server，可为家庭网络设备公告IPv6地址前缀。
2. 支持DHCPv6-PD机制，家庭网关能够接受DHCPv6通过IAPD（Identity Association for Prefix Delegation）下发LAN侧的地址前缀，并公告给家庭网络设备，支持根据给LAN侧的地址前缀设置LAN侧全局v6地址。
3. 应支持针对LAN侧IPv6路由器的DHCPv6-PD机制。
   * 1. 当家庭网关收到LAN侧设备发送的IA-PD请求时，应将网关WAN侧收到的delegated prefix中的一部分（至少一个，且和网关自身使用的PD前缀不同）通过DHCPv6响应b分配给LAN侧IPv6路由器，协助路由器为其下挂设备分配IPv6地址。
     2. 家庭网关应同时将WAN侧收到的preferred lifetime和valid lifetime值发送给LAN侧路由器。
     3. 当LAN侧有多个IPv6路由器时，家庭网关应保证分配给每个路由器的prefix的唯一性。
     4. 当网关WAN侧未分配到delegated prefix，或者delegated prefix的valid lifetime超时，网关应通过DHCP发送不带prefix的IA-PD通告，且通告中应包含NoPrefixAvail状态码。
4. 在WAN侧，应支持静态配置IP地址、DHCPv6、PPPoE三种工作方式；当WAN连接采用DHCPv6工作方式时，应支持以下DHCP option字段：
   * 1. Option16字段配置及上送，字段内容格式参照附录A，Option16字段的具体内容能够由ITMS+进行配置；
     2. Option17接收及检测，只接受Option17字段匹配的DHCP server报文，对于Option17字段不匹配的DHCP server报文不作回应，Option17字段的具体内容能够由ITMS+进行配置。
5. 家庭网关IPv6缺省本地管理地址为FE80::1。
6. 支持LAN侧设备的全局v6地址前缀和家庭网关所公告的地址前缀的一致性检查，对不一致的报文不进行处理或转发。
7. WAN侧IPv6地址前缀可通过SLAAC获取，即自动向WAN侧路由器请求地址前缀，并根据下发的前缀生成IPv6全局地址。
8. WAN侧支持启用DHCPv6 Client，使用DHCPv6报文请求地址前缀和其他配置，生成IPv6全局地址，并保存其它配置参数。
9. WAN侧支持RFC5072协议规范，支持PAP/CHAP认证，获取接口ID，IPv6全局地址前缀应使用SLAAC或DHCPv6获取。
10. 家庭网关在IPv6协议下应支持PMTU功能：
    * 1. 对不能处理的网络侧和用户侧超长报文，应向源设备发送类型为2的ICMPv6报文；
      2. 对接收到的网络侧或用户侧类型为2的ICMPv6报文，目的地址是家庭网关的，应根据报文中的MTU重新对所发数据流进行分片；目的地址不是家庭网关的，应遵循相应的网络连接数据转发机制进行路由、透传或丢弃处理。
11. WAN连接的命名和配置与6.1.4中的f)保持一致，9)和10)除外：
    * 1. 默认不启用IPv6 NAT功能；
      2. 默认启用SLAAC和DHCPv6 Server。
      3. IPv4 NAT
12. 应支持NAT，NAPT，符合RFC2663、RFC3022协议规范，支持的NAT数量不低于4000。
13. UDP穿越NAT，应支持STUN （RFC3489）的规定。
    * 1. IPv6 NAT

应支持IPv6 NAT功能。建议支持NPTv6，符合RFC6296协议规范，实现LAN侧终端IPv6地址前缀与指定WAN获取的IPv6地址前缀相互1:1转换。

* + 1. DS-Lite功能要求

智能家庭网关应支持DS-Lite功能，具体要求如下：

1. 支持通过ITMS+进行DS-Lite功能的独立开启和关闭，缺省关闭
2. DS-Lite功能只针对带有“INTERNET”关键字的路由WAN连接
3. 启动DS-Lite功能WAN连接，应支持如下功能：

* WAN侧自动关闭的IPv4协议栈，支持PPPv6(RFC5072)、NDRA/SLAAC(RFC4861/4862)和DHCPv6的Option5,23,25,26,24 (RFC3315/3646/3633/6334)，并能正确获得IPv6地址
* 支持通过DHCPv6协议动态获得IPv6 DNS地址、AFTR域名和用户侧接口的Prefix
* 对绑定的用户侧端口支持IPv4至IPv6的DNS代理，作为下接IPv4主机的DNS服务器，将主机发送的IPv4 DNS请求转换为IPv6 DNS请求向网络侧转发，收到网络侧IPv6 DNS响应后（A记录）再转换为IPv4 DNS响应回送给V4主机
* 支持IPv6流量的直接转发（无需经过隧道封装处理）
* IPv4流量应使用隧道封装的方式通过IPv6来承载，实现自动发起IPv4-in-IPv6隧道，隧道中的下行流量应解封装后发送到对应的IPv4地址上
* 同时对于上行IPv4流量，宜采用增大MTU方式来避免对数据的分段处理，否则，应实现报文的分段处理；对于下行IPv4流量，应支持对分段报文的重组
  + 1. 其它要求

1. 家庭网关应支持IPv4/IPv6 ALG功能，实现H.323、SIP、RTSP、L2TP、IPSEC、FTP、PPTP等的私网穿越的功能，每种ALG应提供单独的开关功能，ALG功能开关对开启NAT的IPv4和IPv6 WAN均有效。
2. 家庭网关应支持IGMP/MLD（Multicast Listener Discovery） SNOOPING、IGMP/MLD（Multicast Listener Discovery） PROXY功能，组播协议符合IGMP V2和MLD（Multicast Listener Discovery）V1版本协议要求；应具备将组播流转发到所有LAN接口和WLAN接口的能力。家庭网关缺省启用IGMP/MLD（Multicast Listener Discovery） SNOOPING，带“INTERNET”关键字的路由WAN连接缺省启用IGMP/MLD（Multicast Listener Discovery） PROXY。
3. 应支持IPv4 virtual server功能，实现外部网络对于家庭内部主机的访问。
4. 应支持SNTP，应支持NTP服务器和WAN连接的绑定；支持至少配置两个NTP服务器地址，多个NTP服务器采用主备工作模式，获取的时间作为设备统一时钟。家庭网关每次上电应和NTP服务器同步，持续上电时的同步间隔可配置，缺省为每24小时同步一次。
5. 应支持PPPoE间隔重拨。第一次拨号失败后等待5秒进行一次重拨，第二次仍然失败后等待10秒再进行一次重拨，第三次仍然失败后等待20秒再进行一次重拨，第四次仍然失败后等待40秒再进行一次重拨，第五次仍然失败后进入90秒固定间隔重拨模式（即每等待90秒进行一次重拨）。
6. 应支持增强的DHCP Client协议严谨性要求，家庭网关在构建DHCP报文（如DHCP DISCOVER、DHCP REQUEST、DHCP RELEASE）时，必须准确填写报文的参数信息（如IP地址等）；在处理接收到的DHCP OFFER、DHCP ACK报文时，应对报文中的Transaction ID、DHCP Server Identifier和Client MAC Address进行全匹配验证，任一项不匹配均不应当做可用答复。
7. 应支持DHCP Client获取地址失败时的间隔重试。第一次至第三次的重试间隔为10秒，第三次仍然失败后进入60秒固定间隔重试模式（即每等待60秒进行一次重试）。
   1. WLAN AP功能要求
      1. WLAN接口形式

根据工作频段及支持协议的不同，智能家庭网关WLAN接口具体可有如下形式：

* W1: 2.4GHz 802.11n（2条空间流）
* W2: 2.4GHz 802.11n（2条空间流）＋ 5GHz 802.11ac（2条空间流）
* W3：2.4GHz 802.11n（2条空间流）＋ 5GHz 802.11ac（3条空间流）
* W4：2.4GHz 802.11n（3条空间流）＋ 5GHz 802.11ac（3条空间流）
* W5: 2.4GHz 802.11ax（2条空间流）＋ 5GHz 802.11ax（2条空间流）
  + 1. WLAN基本功能要求

1. 应支持WLAN功能启用/禁用，默认为启用。
2. 2.4GHz频段应支持并符合IEEE 802.11n协议，应支持802.11b/g/n Mixed工作模式；5GHz频段应支持并符合IEEE 802.11ac协议，应支持802.11n/ac Mixed工作模式。对于支持Wi-Fi 6的设备，2.4GHz和5GHz频段应支持并符合802.11ax协议，并且保证前向兼容（2.4GHz频段兼容802.11b/g/n终端设备，5GHz频段兼容802.11ac/n终端设备）。
3. 频宽模式应可使用电信维护账号进行配置，并支持TR069远程配置：
   1. 2.4GHz频段应支持20MHz、40MHz、20/40MHz自适应的频宽模式，缺省为20MHz频宽；在20/40M频宽自适应模式下，智能家庭网关能够与各个关联无线客户端协商适当的频宽模式，并能根据外界干扰和业务实际带宽需求等动态改变信道特性。
   2. 5GHz频段应支持20MHz、40MHz、80MMHz的频宽模式，宜支持160MHz、80+80MHz的频宽模式，缺省为80MHz频宽模式。
4. 应支持多SSID功能：
5. 2.4GHz频段至少支持8个虚拟AP，每一虚拟AP应拥有自己的SSID（依次标识为2.4G-1、2.4G-2、2.4G-3等）、BSSID、发送队列、安全机制、配置参数（即对外看来每一虚拟AP和实际物理AP等同）。默认仅启用2.4G-1，其它SSID的启用和相关配置仅通过TR-069方式、DBus接口方式配置实现，不对电信维护人员及普通用户开放。
6. 5GHz频段至少支持8个虚拟AP，每一虚拟AP应拥有自己的SSID（依次标识为5G-1、5G-2、5G-3等）、BSSID、发送队列、安全机制、配置参数，即对外看来，每一虚拟AP和实际物理AP等同。默认仅启用5G-1，其他SSID的启用和相关配置仅通过TR-069方式、DBus接口方式配置实现，不对电信维护人员及普通用户开放。
7. 应支持单独设置每个SSID的隐藏及加密，应支持各SSID和WAN连接建立独立的绑定关系。

应支持自动速率调节。应支持SSID创建者、所承载业务名称、访问权限等属性的配置，具体参见附录C 8.1.12。每个SSID的开关状态变化应不影响无线模块的开关状态。

1. 应支持自动速率调节。
2. 应支持STA在节电模式下工作，能够识别STA进入节电状态，并缓存相关数据，能够通过Beacon信标帧唤醒STA，并发送已缓存的数据。对于支持Wi-Fi 6的设备，应支持TWT（Target Wake Time）功能， 应支持Individual TWT，允许和STA协商什么时候和多久会唤醒接收或者发送数据；宜支持Broadcast TWT。
3. 信道要求：
4. 2.4GHz频段，应支持13个工作信道（channel 1～13），信道范围符合802.11协议要求。
5. 5GHz频段，应支持13个工作信道（channel 36，40，44，48，52，56，60，64，149，153，157，161，165），信道范围符合802.11协议要求。信道52，56，60，64启用时应支持DFS功能，满足工信部无函〔2012〕620号“工业和信息化部发布5150-5350兆赫兹频段无线接入系统频率使用相关事宜的通知”的具体要求。
6. 应支持自动信道选择和手工配置两种方式，默认自动信道选择方式。自动信道选择方式要求如下：
7. 应支持在开机时刻自动选择干扰较小的信道。
8. 应支持根据DBus接口命令探测周边信道使用情况并反馈结果。
9. 应支持根据DBus接口命令触发自动信道选择。
10. 2.4GHz频段仅在channel 1～11做选择（优先选择channel 1、6、11）。
11. 应支持发射功率可调（电信维护账号、用户账号、ITMS和智家平台均可配置）。2.4GHz频段默认发射功率（包含天线增益）应达到95~100mW；5GHz频段默认发射功率（包含天线增益）应达到190~200mW，工作在5725~5850MHz最大发射功率宜达到400~500mW。
12. 应支持视频业务流组播转单播的功能要求。
13. 应提供统计功能，宜至少支持IEEE 802.11-1999 附录D MIB库中规定的“dot11Counters TABLE”中的所有统计项。
14. 智能家庭网关应具备和其它WLAN设备的良好兼容性，应通过WiFi联盟认证。对于支持Wi-Fi 6的设备应通过Wi-Fi联盟的Wi-Fi 6认证（Wi-Fi CERTIFIED 6™）。
15. 应支持802.11k/v/r要求，实现与周边AP设备以及不同频段之间的负载均衡，支持客户端设备在家庭网关与周边AP设备以及不同频段之间的无缝漫游。
16. 应支持数据帧汇聚 (Frame Aggregation)，支持把两个以上的帧组合成一个帧传输，减少协议开销，提高信道利用率。
17. 应支持块应答 (Block ACK)，支持对接收到的多个帧用一个帧回应，让发送方只重传没有接收成功的帧。对于支持Wi-Fi 6的设备，应支持C-BA（Compressed Block Ack）和M-BA（Multi-STA BlockAck）。
18. 2.4GHz频段宜支持隐式波束成型技术，且符合802.11n规范9.19中的规定。5GHz频段应支持显式，且符合802.11ac规范中的规定；宜支持隐式波束成型技术。对于支持Wi-Fi 6的设备，2.4GHz和5GHz频段都应支持波束成形技术，且符合802.11ax规范中的规定。
19. 应支持400ns、800ns两种保护间隔，保护间隔可使用电信维护账号进行配置，并支持TR069远程配置，5GHz频段默认使用400ns。
20. 2.4GHz频段可选支持802.11n规范STBC、LDPC功能，符合802.11n协议相关规定。5GHz频段应支持LDPC，符合802.11ac规范中的规定。对于支持Wi-Fi 6的设备，应支持LDPC，符合802.11ax规范中的规定
21. 2.4GHz频段应支持802.11n规范MLD（Maximum-Likelihood Decoding）功能，符合802.11n协议相关规定。
22. 5GHz频段应满足以下要求：
23. 应支持基于最大延迟时间的数据重传控制。尝试发送数据包若超过时间门限仍未成功则丢弃该数据包。超时门限值可使用电信维护账号进行配置，默认为20ms。
24. 宜支持业务服务质量管理。智能家庭网关对于多个5GHz频段客户端按照业务承载状态区分优先级，优先保障已连接的组播及点播视频业务质量。当一个客户端申请加入组播或点播时，不应该降低已在承载组播及点播业务客户端的服务质量。
25. 双频设备应支持BandSteering功能。在开启双频合一模式时，根据两个频段的信号质量及负载情况协同支持Band Steering的双频客户端进行频段切换：
26. 应支持自动识别并记录支持Band Steering的双频客户端。
27. 对于支持Band Steering双频客户端，基于以下策略引导其接入推荐的频段：
28. 在双频无线客户端连接家庭网关设备时，应引导其优先连接5G频段。
29. 在检测到5G频段下挂客户端信号强度低于所设定的阈值时，应引导其切换到2.4G频段。
30. 在检测到2.4G频段下挂客户端信号强度高于所设阈值且5G频段的信道负载低于所设阈值时，应引导其切换到5G频段。
31. 阈值应缺省预置，且可通过DBus接口命令进行修改。缺省阈值应具备冗余能力，避免乒乓效应。
32. 此策略仅针对2.4G-1和5G-1。
33. 对于支持Wi-Fi 6的设备还应该满足下列要求：
34. 2.4GHz和5GHz频段均应支持上行和下行OFDMA，基于RU调度STA，并且至少支持同时调度4/8个STA（2.4HzG频段4个STA，5GHz频段8个STA））。
35. 应支持Basic Triger触发帧格式。
36. 应支持Basic上下行多用户调度交互流程
37. 2.4GHz和5GHz频段均应支持1024QAM调制方式。
38. 应支持覆盖增强相关技术，包括DCM（Dual Carrier Modulation）和HE ER（Extended Range）
39. 宜支持下行MU-MIMO。
40. AP外置型网关应支持对外置AP模块的WLAN功能进行管理。
    * 1. 智能天线要求

应支持水平极化及垂直极化智能天线。

* + 1. PA及LNA增强要求

应支持在缺省配置的基础上，通过同时提升发射功率和接收灵敏度来改善无线覆盖效果。

* + 1. WPS功能要求

应支持WiFi Protected Setup（简称WPS）规范，支持Push Button的无线密钥协商及设备连接功能，具体要求如下：

1. 应支持根据智家平台下发命令进行以下操作（设备不应具有“WPS”的按键）：启动或停止WPS协商连接过程，上报协商状态及设备连接结果。
2. 能够和支持WPS Push-Button功能的无线客户端设备在2分钟内协商好加密算法，分发密钥，各自配置好相关参数，建立连接。相关配置自动保存，设备重启后应能保证已协商无线客户端设备的正常连接。
3. 正常工作状态下（无需设备重新启动），应能和多个无线客户端设备依次建立连接。
4. WPS过程不应影响已连接无线客户端设备的连接状态和数据传送。
5. WPS功能默认基于2.4G-1操作，应支持根据智家平台下发命令变更WPS所关联的SSID。
   * 1. Beacon/Probe帧扩展要求

应支持通过DBus接口Beacon/Probe帧扩展（具体要求详见附录C.9.10）：

1. 上报Probe Request帧中Vendor-specific Information Element字段。
2. 接收DBus接口的设置命令，在发送Beacon帧或Probe response帧中添加Vendor-specific Information Element字段。
   * 1. 漫游功能要求
3. 应支持采集STA到网关的RSSI值：
4. 应支持关联STA到网关的RSSI值的采集；
5. 应支持通过侦听方式对同信道非关联STA到网关的RSSI值的采集；
6. 应支持通过信道切换侦听方式对异信道非关联STA到网关的RSSI值的采集；
7. 应支持基于802.11k的Beacon测量方式，采集STA侧的RSSI值。
8. 应支持通过以下方式启动STA漫游（详见附录C 9.11）：
9. 根据DBus接口命令以802.11v BTM方式启动STA漫游；
10. 采用强制去关联的方式启动STA漫游。
11. 应支持WFA Multi-AP 的漫游功能（详见6.2.9）。
    * 1. 速率优先模式

应支持速率优先模式，具体要求如下：

1. 2.4GHz频段自动切换到纯802.11n模式（对于支持Wi-Fi 6的设备，切换到802.11ax/11n混合模式），不允许802.11b或802.11g方式接入，自动切换到20/40MHz自适应的频宽模式，禁止MCS3以下的设备接入。
2. 5GHz频段宜自动切换到纯802.11ac模式（对于支持Wi-Fi 6的设备，切换到802.11ax/11ac混合模式），不允许802.11n方式接入，宜禁止MCS3以下的设备接入。
3. 5GHz频段宜支持切换到160MHz或80+80MHz的频宽模式。
4. 速率优先模式的开启和关闭由智家平台控制，缺省关闭。
   * 1. WFA Multi-AP Agent功能要求

网关应支持WFA Multi-AP功能(符合WFA《Multi-AP specification version 1.0》规范),与其他支持Multi-AP协议的无线AP设备组成家庭Mesh网络。

对于具备WiFi接入能力的网关，Multi-AP功能应由2个逻辑实体：Controller和Agent配合来实现。其中Controller功能由部署在智能网关上的Multi-AP Controller插件完成，Agent功能由网关基础软件包负责实现。

对于AP外置型网关，Multi-AP功能仅包含Controller实体，由部署在网关上的Multi-AP Controller插件实现。

网关Multi-AP Agent功能的具体要求如下:

1. OnBoarding：
   1. 网关应作为existing agent，支持标准的基于PBC的OnBoarding，接受其他Multi-AP设备通过WiFi接入网络。
   2. 网关应支持其他Multi-AP设备通过Ethernet接口接入网络。
2. 自动发现

应支持自动发现流程，包含Service的发现，STA的关联和去关联通知。

应支持全网拓扑信息的自动发现。

1. 配置

应支持接收Controller发送的WiFi配置消息，实现WiFi参数的配置同步，包括对Fronthaul BSS 和Backhaul BSS的SSID、密码等属性配置，以及对steering策略和metrics报告策略的配置。

1. 信道选择

应支持信道选择和配置，支持上报preference信道以及在Controller协助下进行信道选择。

1. 能力信息上报

应支持能力信息上报，支持上报网关内置AP能力和已关联STA的能力。

1. 链路信息搜集

应支持链路信息搜集和上报，包括回传链路信息、AP metrics、已关联STA链路等信息搜集和上报， 可选支持非关联STA链路信息搜集和上报。

1. STA漫游

应支持controller控制下的STA漫游，包括：

* 1. 根据Controller 发送的Client Steering Request，当Request Mode bit 为0 时, 在漫游窗口期内根据收到的漫游策略（基于信号强度或信道利用率）来发起漫游。
  2. 根据Controller 发送的Client Steering Request，当Request Mode bit 为1时, 按照Steering Request TLV的要求，将指定的STA漫游到指定的BSS 上。

宜支持根据controller下发的漫游策略，由agent发起的STA漫游，包括：

1. 向controller上报AP能力时，声明支持Agent-initiated RCPI-based Steering能力。
2. 接收controller发来的Agent-initiated RCPI-based Steering漫游策略以及漫游门限规则。
3. 根据规则，当漫游条件满足时，agent触发STA漫游操作。
4. 应支持802.11帧的3地址转发和4地址转发。
   1. 设备发现功能要求

智能家庭网关对其连接设备进行自动发现后，对特定设备配置IPv4特定私网IP地址和特定参数（如QoS、Port Forwarding等）。

1. 支持UPnP IGD1.0协议，要求如下：
2. UPnP功能应支持启用/禁用，默认是禁用（disabled）。
3. 对于用户/应用接入智能家庭网关的操作，应支持配置为read-only，避免一些接入后的操作对智能家庭网关状态的更改。
4. 应支持NAT traversal启用/禁用。
5. 应支持用户做基于LAN IP地址的UPnP流量block。
6. 支持UPnP AV Media Server和DLNA DMS
7. 应支持UPnP AV Media server，应支持Media server的CDS（Content Directory Server）、Connetion Manager，可选支持Media server定义的AV Transport服务。
8. 应支持DLNA1.5的DMS设备功能，宜通过DLNA 1.5认证。DLNA功能缺省启用。
9. DMS功能只能通过ITMS+进行开启/关闭，缺省打开。DMS服务名称为“天翼网关”。
10. 应支持向家庭网络发布家庭网关连接的存储设备中的共享媒体内容，支持共享内容的读写。
11. 内容共享应支持FTP Server、SAMBA协议，支持共享访问的用户权限管理，可支持6个账户，每个账户均具有能够进行有效访问的根目录，账号可由ITMS+、智家平台进行修改，缺省账号为当前家庭网关用户账号。SAMBA功能缺省启用。
12. 具备支持索引1000个媒体文件的能力，能够生成并定期刷新维护共享内容的目录索引树，刷新的周期时间可设置。
    1. 业务控制功能要求

家庭网关应支持根据源/目的MAC、源/目的IP、协议（如TCP、UDP、RTP协议等）、源/目的端口号、Flow Label（仅针对IPv6的数据流）等信息，对用户数据流进行分类。

家庭网关应能够根据用户侧端口（包括有线及无线接口）、WAN连接、用户数据流分类结果对不同数据流进行QoS适配：

1. 优先级标识：
2. 根据数据分类结果，对特定的数据流（如RTP数据流）进行以下标识：

* 二层IEEE 802.1D标识
* 三层DSCP（RFC3260）标识
* 三层Flow Label标识（仅针对IPv6数据，可选支持）
* 三层Traffic Class标识（仅针对IPv6数据，可选支持)
* 三层TOS标识（仅针对IPv4数据，可选支持）

1. 对具有三层DSCP（RFC3260）标识的数据包进行二层IEEE 802.1D标识。
2. 策略转发：家庭网关可以根据用户侧端口（包括有线及无线接口）、WAN连接、用户数据流分类结果对数据进行队列划分，优先转发高优先级的数据包，要求如下：
3. 应至少支持8条不同优先级的队列（按优先级从高到低，队列号宜为1~8），应可配置队列长度。
4. 应支持将不同WAN连接映射到不同优先级的队列，缺省映射配置为：带TR069属性的WAN连接进最高优先级队列，带VoIP属性且不带TR069属性的WAN连接进次高优先级队列，Other属性WAN连接（一般承载IPTV业务）进第三高优先级队列，带SPECIAL\_SERVICE属性WAN连接进第三低队列，其它（如INTERNET属性WAN连接）进次低队列。
5. 应支持将不同类的数据流映射到不同优先级的队列里去。
6. 应支持队列的权重分配，宜支持WFQ等调度算法。
7. 宜支持WRED。
8. WLAN QoS功能要求：
9. 应支持WMM，支持流与WMM队列的映射，支持WMM定义的4种流类型（VOICE/VIDEO/BEST EFFORT/BACKGROUND）及其优先级调度规则，支持基于优先级的数据处理和转发。
10. 应保持WMM流分类和设备QoS策略的一致性。
11. 应支持基于数据流分类结果的带宽保障和限制机制。
12. 应支持基于WAN连接、用户侧物理端口、用户设备MAC地址进行数据流的双向限速，颗粒度至少为512Kbps。
13. 应支持对同一时间接入公网的用户TCP Session总数进行限制。
    1. 语音功能处理要求

应遵循《中国电信IAD设备技术规范》，并支持通过SIP（包括软交换SIP和IMS SIP）和H.248两种协议提供语音、传真应用。设备供货时可按需支持其中一种协议，并具备通过远程软件升级支持另一种协议的能力，协议类型的切换不能降低设备对本规范的支持能力。

本节要求除特殊说明外，同时适用于SIP（包括软交换SIP和IMS SIP）和H.248两种协议。

* + 1. 功能要求
       1. 呼叫处理要求

参见《中国电信家庭网关总体技术要求》6.5.1.1。

* + - 1. 语音处理要求

参见《中国电信家庭网关总体技术要求》6.5.1.2。

* + - 1. 在线保障要求

当家庭网关断电重启、本地恢复出厂设置或网络侧线路重新建链后，家庭网关应能自动发起至语音服务器（如BAC/软交换、IMS SIP服务器、H.248服务器等）的业务注册。

家庭网关应支持通过心跳消息与语音服务器之间进行连接性检查。

家庭网关应能配置备份软交换，在注册失败后，有序地向不同语音服务器进行注册，直到注册成功。

家庭网关应具备雪崩预防功能。

家庭网关配置H.248协议还应支持：

1. 家庭网关应能及时地向软交换报告由于重启、故障、设备恢复或维护管理而造成自身状态的改变，家庭网关应能自动通过H.248的ServiceChange消息将状态变化报告给软交换
2. 因异常事件而使家庭网关的某个终结点不能正常继续工作（例如模拟Z端口失效）时，家庭网关应向软交换请求释放该终结点并通告原因
   * + 1. 业务质量保证要求

参见《中国电信家庭网关总体技术要求》6.5.1.4。

* + 1. 业务要求

参见《中国电信家庭网关总体技术要求》6.5.2。

* + 1. 软交换SIP协议要求

参见《中国电信家庭网关总体技术要求》6.5.3。

* + 1. IMS SIP协议要求

家庭网关应支持IMS SIP协议，遵循《中国电信IMS网络SIP协议总体技术要求》、《中国电信IMS网络呼叫前转业务技术要求》、《中国电信IMS 网络主叫识别显示/限制业务技术要求》、《中国电信IMS网络呼叫保持业务技术要求》、《中国电信IMS网络PSTN仿真业务技术要求》、《中国电信IMS SIP 硬终端技术要求》相关规定。

家庭网关在支持IMS SIP协议时，应支持两个BAC的IP地址、单BAC 域名和双BAC 域名三种配置方式，并支持链路检测、轮询注册等功能，具体参照《中国电信IMS网络容灾技术要求》5.3.3.1中BAC容灾要求对SIP终端的相关规定。

家庭网关应支持隐式注册功能，当注册响应报文的P-Associated-URI头域中含有有效的公有用户标识时，取其中的第一个公有用户标识（即缺省的公有用户身份，参见中国电信《中国电信IMS网络SIP协议总体技术要求》）作为后续非注册会话过程中的用户标识。

家庭网关应支持video媒体，具备SIP协议4K大数据包的接收及处理能力。

家庭网关的媒体检测功能应符合《中国电信IMS网络SIP协议总体技术要求》，能对网络侧是否发送RTP媒体流进行判断，根据情况进行回铃音的播放，并符合如下补充要求：

* 对于没有早媒体（Early Media）的呼叫场景，即网关收到的180 ringing响应消息没有携带P-Early-Media和SDP参数，网关应播放本地回铃音。
* 对于有早媒体（Early Media）的呼叫场景，即网关收到的18\*响应消息中有携带P-Early-Media或SDP参数，若在3秒内收到被叫侧的RTP流，网关应透传被叫侧放音; 若在3秒内没有收到被叫侧的RTP媒体流，网关应播放本地回铃音。
* 对于183响应消息没有带SDP和P-Early-Media的情况，网关需一直等待后续的18\*响应消息，定时器为60秒(可以复用无应答定时器，也可另行定义)。在60秒内, 网关收到后续18\*时采用以上两种场景的处理机制进行处理; 在60秒内，如果网关没有收到以上两种场景的18\*响应消息，即使有收到网络侧的RTP媒体流，网关都不做处理，并且不播放本地回铃音。
  + 1. H.248协议要求

参见《中国电信家庭网关总体技术要求》6.5.5。

* + 1. 性能要求

参见《中国电信家庭网关总体技术要求》6.5.6。

* + 1. 诊断要求

智能家庭网关应支持回铃音检测、摘机检测、拨号检测、拨号音停止等信令事件的检测，应支持外线电压、振铃阻抗的测量，相关结果应能在UI上显示。

1. 安全要求
   1. 网络访问的安全性

家庭网关应提供基于IPv4/v6的接入控制能力、报文过滤能力、防DoS攻击能力、防端口扫描能力、防止非法报文攻击能力，并提供本地网络日志。具体要求如下：

1. 应支持DMZ。
2. 应支持SSL。
3. 应支持基于MAC地址的接入控制（包括LAN和WLAN），可支持到100条记录。
4. 应支持基于URL的控制（包括HTTP和HTTPS），接入控制以黑白名单形式提供，黑名单和白名单不能同时启用，可支持到100条纪录。
5. 应支持IP层协议报文过滤功能，宜支持应用层报文过滤，宜支持SPI（Stateful Packet Inspection）。
6. 应能够提供防DoS攻击能力，能够防止LAND、Ping of Death、SYN Flooding、ICMP Redirection、Smurf、Winnuke等类型的攻击。
7. 应能够提供防端口扫描功能。
8. 应能够提供防非法报文攻击能力。
9. 应支持日志功能，本地提供至少存储500条日志的能力。
10. 应支持防火墙功能，支持对防火墙等级的设置，支持对防火墙规则的配置，并支持基于以下规则对报文进行过滤：

* 支持根据源MAC地址、目的MAC地址进行报文过滤；
* 支持根据源IP地址及范围段、目的IP地址及范围段进行报文过滤；
* 支持根据IP源端口及范围段、目的端口及范围段进行报文过滤；
* 支持根据IP包的传输层协议类型进行报文过滤，要求有TCP/UDP/ICMP/TCP+UDP/ANY的选项；
* 支持对匹配规则的报文进行处理模式的选择，对匹配规则的报文的处理模式，有允许和禁止2种，默认为禁止模式。

1. 应支持防止用户做源的组播，禁止用户端口发出的IGMP Query和组播数据报文。
2. 应能够对特定协议的广播/多播包（例如DHCP，ARP，IGMP等）进行抑制，并能对其它二层广播报文进行速率限制。
   1. 用户侧WLAN接口安全性

对于带有WLAN用户接口的家庭网关，应支持以下无线安全协议或功能：

1. 2.4G-1、5G-1默认应使用中国电信提供的SSID标识（字符范围为0-9、a-z、A-Z，且排除“0 /o/ O、B/8、1/ l/ I”等易混淆字符）及密钥，并在家庭网关外壳上加以标注。默认2.4G-1名称为ChinaNet-XXXX（XXXX为4位随机ASCII字符），用户可修改为长度1~32字节的任意字符串
2. 应支持Open System和Shared Key两种链路层认证方式，且应自动适应STA的认证方式。
3. 应支持WPA-PSK、WPA2-PSK、WPA-PSK/WPA2-PSK混和模式，应支持AES加密，建议不再使用WEP、TKIP加密，2.4GHz频段默认启用WPA-PSK/WPA2-PSK混和模式，5GHz频段默认启用WPA2-PSK模式。
4. 对于支持Wi-Fi 6的设备，应支持WPA3-SAE、WPA3-SAE Transition模式，2.4GHz&5GHz频段默认启用WPA3-SAE Transision模式。
5. 应支持国家无线局域网安全标准。
   1. 登录安全性
      1. 登录安全基本要求

智能家庭网关有两个不同的权限的帐号：电信维护帐号、智能家庭网关用户帐号。用户需使用密码登录（智能家庭网关不进行用户名验证，只根据密码直接匹配账号），才能对智能家庭网关设备进行配置或管理。

1. 每个帐号同时只允许一个用户登录；应拒绝第二个用户登录。
2. 用户登录后连续5分钟无操作，智能家庭网关自动退出登录状态。
3. 密码输入连续错误3次，则再次密码验证应在1分钟以后。
4. 每种权限仅有一个帐号生效，帐号权限不能因为密码的修改或操作过程而改变。
   * 1. 电信维护帐号

智能家庭网关只有一个电信维护帐号，由电信维护人员使用，只允许在私网登录，初始用户名为“telecomadmin” 。

电信维护帐号可进行全部的参数设置，并可强行修改智能家庭网关用户帐号的密码。

在以下场景，应通过ITMS+修改电信维护帐号的密码：

1. 当智能家庭网关第一次连接ITMS+时。
2. 当电信维护人员在在维护完成后通过WEB页面的“维护结束”按键后，智能家庭网关需确保成功通知ITMS+修改密码，即：如果由于网络原因设备未能连接到ITMS+，智能家庭网关需记录“维护结束”事件，智能家庭网关在能够连接平台时应通知ITMS+修改密码。
   * 1. 智能家庭网关用户帐号

智能家庭网关只有一个智能家庭网关用户帐号，由智能家庭网关设备的用户使用，只允许在私网登录，默认用户名为“useradmin” ，初始密码应使用中国电信提供的密码，标记在产品标识上。

登录本地WEB界面可使用的功能与应用：

1. 可进行部分的参数设置；
2. 可修改智能家庭网关用户帐号密码。

智能家庭网关用户帐号的用户名不能修改，密码的修改方式如下：

1. 通过电信维护帐号登录本地WEB界面强行修改；
2. 通过智能家庭网关用户帐号登录本地WEB界面，校验原密码后再进行修改。
   1. 设备及系统安全性

应符合符合YD/T 965-1998 《电信终端设备的安全要求和试验方法》中的相关规定。

应符合附录B的要求。

1. 管理和维护要求
   1. 基本要求
      1. 功能要求

智能家庭网关提供如下三种管理模式：

1. 本地UI管理：由电信维护人员或智能家庭网关用户对智能家庭网关设备进行的常规管理和维护。
2. 远程TR069/EMS管理（PON上行的家庭网关同时支持ITMS+和EMS的远程管理，ITMS+用于进行业务层的管理及配置，EMS用于进行和PON接口相关的物理层及链路层的管理及配置）：
3. 支持由ITMS+通过TR069方式对智能家庭网关设备进行全面管理和维护；
4. 支持EMS通过OAM方式对智能家庭网关设备进行PON接口远程管理（仅针对EPON上行的家庭网关）；
5. 支持EMS通过OMCI方式对智能家庭网关设备进行PON接口远程管理（仅针对GPON/XG-PON上行的家庭网关）。
6. 手机APP管理：由电信维护人员或智能家庭网关用户通过手机APP、智家平台对智能家庭网关设备进行本地及远程的智能应用管理和维护。
   * 1. 协议要求

对于智能家庭网关的管理应遵循以下协议：

1. 远程TR069/EMS管理：
2. 应支持TR-069协议进行远程配置和管理，应支持HTTP/XML/SOAP协议，宜支持FTP/TFTP client。
3. 对EPON上行的智能家庭网关，应支持通过OAM实现对设备的远程管理。
4. 对GPON/XG-PON上行的智能家庭网关，应支持通过OMCI实现对设备的远程管理。
5. 本地UI管理：应支持Web配置管理方式，可支持telnet 配置管理。
6. 手机APP管理：应支持《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》定义的协议及接口要求，实现手机APP、智家平台对设备的本地及远程配置管理。
   * 1. 日志要求
7. 家庭网关应支持日志记录，内容包括帐号登录记录、管理配置操作记录、外部攻击记录、告警信息记录等，其中告警信息应符合附录D规定。
8. 日志文件应应支持如下要求：
9. 日志文件要求是txt文本文件；
10. 本地日志文件提供至少存储500条日志的能力；
11. 所有日志文件要求保存在本地，保证断电不丢失；
12. 日志文件可以应ITMS+要求上传至ITMS+服务器，上传使用HTTP Post或HTTP Put方式，上传后可以删除/清空；
13. 日志文件格式应符合附录E规定。
    * 1. 设备标识要求

智能家庭网关设备标识是唯一标识设备的参数，主要用途如下：

1. 终端综合管理系统唯一标识设备；
2. 智能家庭网关设备外壳标签标识。

智能家庭网关设备标识定义见表3：

1. 家庭网关设备标识定义

|  |  |
| --- | --- |
| **设备标识格式** | **示例** |
| <OUI> "-" <SerialNumber> | 00D09E-01234567890123456 |

其中<OUI>和 <SerialNumber> 域应和Inform中的DeviceIdStruct结构中的参数匹配，参见TR-069规范附录A。

具体的设备标识由中国电信生成并提供给厂商。

* + 1. 配置文件备份要求

配置文件应支持双备份，每个配置文件应具备CRC校验码进行合法性校验，配置文件应位于flash的两个不同块中，配置文件更新时应同时更新两个配置文件，读取配置时应使用CRC校验合法的那个配置文件。配置文件内容在设备内应加密保存。

* + 1. 设备注册认证功能

对于PON上行的家庭网关，当业务下发状态为初始值或下发失败（即Internet­Gateway­Device.X\_CT-COM\_UserInfo.Result值为99或2），并且用户在PC上启动网页浏览器访问网站时，家庭网关自动启动基于宽带识别码的设备首次认证功能：

1. 向用户PC强制推送宽带识别码设备首次认证页面。
2. 检查认证重试次数（Internet­Gateway­Device.X\_CT-COM\_UserInfo.Times）是否超出限制（Internet­Gateway­Device. X\_CT-COM\_ UserInfo.Limit）：
3. 如果未超出限制，则按以下流程进行认证：

* 引导用户输入宽带识别码。
* 利用该宽带识别码根据OLT的要求进行注册/激活。对于EPON上行的家庭网关，具体流程应符合《中国电信EPON设备技术要求1G-EPON/10G-EPON》；对于GPON上行的家庭网关，具体流程应符合《中国电信GPON设备技术要求》；对于XG-PON上行的家庭网关，具体流程应符合《中国电信XG-PON设备技术要求》。
* 在向OLT注册/激活成功并连接到ITMS+后，自动向ITMS+发起基于宽带识别码的设备首次认证流程（Internet­Gateway­Device.X\_CT-COM\_UserInfo.UserName的赋值等同LOID，将Internet­Gateway­Device.X\_CT-COM\_UserInfo.UserId的赋值等同Password）。

1. 如果已超出限制次数，则显示本功能不可用的原因，不允许进行宽带识别码输入，并建议用户联系10000号。

基于宽带识别码的设备首次认证功能的用户提示信息要求参见附录F，认证流程的具体要求参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》附录F.22。认证过程中认证重试次数超出限制3分钟后自动清零，以允许用户重新进行认证。

在输入宽带识别码后，只要未注册成功，终端应在每次上电后向ITMS+发起基于宽带识别码的设备首次认证流程。

PON上行家庭网关在用户每次修改宽带识别码后，应自动重新向OLT发起注册（可采取重启家庭网关设备或只重启PON部分等方式），具体应符合《中国电信EPON设备技术要求1G-EPON/10G-EPON》、《中国电信GPON设备技术要求》和《中国电信XG-PON设备技术要求》。

宽带识别码（包括LOID和Password）初始值为空，宽带识别码的修改在且仅在以下情况下被长期保存（其它情况下的修改仅在当次上电期间有效）：

1. 在OLT或ITMS+首次注册成功前进行的任何修改
2. 首次注册成功后，通过本地界面等方式修改宽带识别码且新的宽带识别码在OLT或ITMS+上注册成功（对于融合版设备，此时应清空机顶盒模块的接入账号和业务账号）
3. 由ITMS+进行的远程修改
   1. 本地UI管理和配置要求
      1. 本地UI管理基本要求
4. 支持通过PC实现用户级配置管理，应提供良好的用户UI，应至少支持IE、360、Firefox、chrome、qq、windows edge、safari等浏览器主流版本；
5. 应支持Web管理方式，并且提供安装配置的向导服务；
6. 应提供良好的中文界面，应提供良好的中文帮助信息；
7. 应支持用户分级管理，具体要求参见本规范7.3；
8. 对于融合版，同时应支持通过遥控器及电视屏幕进行设备状态的查看及配置管理。终端支持通过电视界面显示网关信息，包括：网络连接状态、业务状态、平台连接状态、软件版本等，终端支持通过电视界面进行逻辑ID注册，终端支持通过电视界面进行网关WiFi的配置。
   * 1. 系统信息管理

系统信息管理主要包括对智能家庭网关的设备状态和设备日志的管理。

根据用户分级管理的要求，电信维护人员和智能家庭网关用户都具有以下管理项目的操作权限（特别标注者除外）。

1. 网关侧信息管理
2. 设备状态

设备状态显示智能家庭网关的总体设备信息和工作状态：

* 设备信息：应包含设备型号、设备标识号、硬件版本、软件版本。
* 网络侧连接信息：
* 智能家庭网关公共信息：显示网络侧连接状态、IP地址、子网掩码、默认网关、DNS服务器等信息。
* PON信息（仅针对有PON上行接口的设备）：

基本信息：显示智能家庭网关的EPON链路连接状态（注册、认证的阶段及是否成功）

* 高级信息（仅提供给电信维护人员）：显示FEC使能/禁止状态、加密模式（三重搅动开启与关闭）、链路的性能统计、告警信息，光模块信息（如来自OLT的下行光功率，智能家庭网关的发送光功率）
* 用户侧信息：
* WLAN接口信息：仅显示2.4G-1、5G-1的WLAN的连接状态（接入设备的IP地址和MAC地址、收发包数等）、SSID名称、信道、加密状态信息。
* 用户侧以太网接口连接状态：显示接入设备的设备名称、设备类型（如手机/平板/电脑/机顶盒等）、品牌名、操作系统、MAC地址、IP地址、收发包数等。家庭网关应支持基于数据检测功能或第三方插件提高对下挂设备的识别能力；在基于数据检测的识别结果和其它识别方式（如DHCP的Option60）有差异时，以基于数据检测的的识别结果为准。
* 网关的DHCP server地址池中已分配的地址情况，包括客户端设备的设备名称、MAC地址、IP地址、剩余租借期等。
* 语音信息：显示连接状态、注册信息、用户号码等。
* 插件信息：通过加载智家平台提供的应用中心页面显示当前安装的所有插件名称及运行状态（已卸载插件无需显示）。

1. ITMS平台远程管理状态（仅提供给电信维护人员）

ITMS平台远程管理状态显示智能家庭网关与ITMS平台之间的远程连接建立状态和业务下发状态：

* 远程连接建立状态：
* 主动上报Inform状态：显示智能家庭网关主动向ITMS+发Inform的情况，具体要求如下：
* 未上报（####）：指家庭网关未发起向ITMS+的TCP连接请求，其中“####”代表未未发起向ITMS+的TCP连接请求的原因（如家庭网关正在启动、无远程管理WAN连接、远程管理WAN连接未生效、无管理通道DNS信息、无ACS配置参数、ACS域名解析失败等），示例如下：家庭网关上电后的最初状态显示为“未上报（家庭网关正在启动）
* 上报无回应：家庭网关发起了向ITMS+的TCP连接请求，但连接建立失败
* 上报过程中断：家庭网关向ITMS+的TCP连接建立成功，但上报Inform过程未完成
* 上报成功：上报Inform过程成功完成
* 接受ITMS+连接请求情况，包括未收到远程连接请求、ITMS+发起的远程连接过程中断、ITMS+发起的远程连接过程成功等
* 业务配置下发状态，根据ITMS+对参数InternetGatewayDevice.X\_CT-COM\_UserInfo.Result的赋值，具体显示为“ITMS未下发远程业务配置状态”、“正在接受ITMS的远程业务配置”、“业务配置成功”、“业务配置失败”，当家庭网关未接收到ITMS+设置的下发结果信息时，应不影响正常的业务配置流程

1. 智能网关及应用平台远程管理状态（仅提供给电信维护人员）

智能网关及应用平台远程管理状态显示智能家庭网关与智家平台之间的远程连接建立状态和业务下发状态：

* 智家平台的连接状态，示例如下：
* BSS平台连接情况：显示智能家庭网关连接BSS平台的情况（只针对本次上电过程），具体要求如下：
* 未连接：指家庭网关本次上电后未曾连接BSS平台
* 连接结束：指家庭网关已成功建立和BSS平台的连接，且连接已经正常结束
* ####，等待\*\*秒后连接：指家庭网关向BSS平台连接失败，并且会在\*\*秒之后重新尝试连接BSS平台。其中####表示详细的失败原因，包括以下原因:

未收到平台响应报文

TCP连接断开

平台域名解析失败

创建套接字失败

* 等待WAN连接建立，\*\*秒后尝试连接：指家庭网关WAN没有没有连上，家庭网关会等待WAN连接信号连接平台，如果一直没有信号的话多长时间后尝试连接平台
* 能力平台连接情况：显示智能家庭网关连接能力平台情况（只针对本次上电过程），具体要求如下：
* 未连接：指家庭网关本次上电后未曾连接能力平台
* 等待WAN连接建立，\*\*秒后尝试连接：指家庭网关WAN没有连上，家庭网关会等待WAN连接信号连接平台，如果一直没有信号的话多长时间后尝试连接平台
* 激活中：指家庭网关获取挑战码成功（还没激活），正尝试激活设备
* 连接中：指家庭网关获取挑战码成功（已经激活），正尝试连接能力平台
* 心跳保活中：指家庭网关成功连接上能力平台
* ####，等待\*\*秒后连接：家庭网关已发起向能力平台的连接，但目前连接失败,并且家庭网关会在\*\*秒之后重新尝试连接能力平台。其中####表示详细的失败原因，包括以下原因：

未收到平台响应报文

TCP连接断开

平台域名解析失败

创建套接字失败

备注：具体根据通信协议提示信息进行调整。

* 插件配置下发状态

显示本次上电后，运营平台所下发或配置的插件：如“下发\*\*\*\*\*、\*\*\*\*\*插件”、“启动\*\*\*\*\*插件”、“卸载\*\*\*\*插件”等。

1. 设备日志

显示智能家庭网关的登录记录、管理配置操作记录、外部攻击记录、告警信息记录等。

1. 机顶盒模块信息（仅针对融合版）
2. 针对融合版显示机顶盒模块信息（仅提供给电信维护人员，在网关本地管理界面“状态”菜单下增加“机顶盒模块信息”子菜单）

* 机顶盒模块版本信息：操作系统版本、系统软件版本、各应用软件版本等；
* 网络信息：机顶盒模块的MAC、IP、子网掩码、默认网关、DNS 服务器等；
* 服务器信息：机顶盒终端管理平台地址、NTP 地址等。

1. 基于电视屏幕呈现的系统状态信息（仅提供给电信维护人员，在机顶盒模块本地管理界面“系统信息”菜单下增加“网关信息”子菜单）

* 网络连接状态：光纤（如：连通、断开、光信号低等）、OLT认证状态、IPTV WAN连接状态（如：未配置、断开、正常等）
* 业务状态：上网业务状态（如：未配置、断开、正常等）、语音业务状态（如：未配置、注册失败、正常等）
* 平台连接状态：包括ITMS连接状态、智家平台连接状态等
* 告警状态：包括CPU负载告警、CPU温度告警等
  + 1. 基本配置

智能家庭网关的基本配置包含网络侧和用户侧的参数配置。

根据用户分级管理的要求，电信维护人员和家庭网关用户都具有以下配置项目的操作权限（特别标注者除外）。

1. 网络侧配置（缺省仅提供给电信维护人员）

家庭网关应支持以下参数配置：

* VLAN的设置（包括公共组播VLAN的设置）；
* 应支持路由桥接模式的选择，支持路由模式下PPPoE、DHCP、静态IP的选择及配置；在PPPoE模式下应支持用户名、密码的设置。

1. 用户侧配置

用户侧配置包括用户侧网络参数配置和接口参数配置：

1. 用户侧网络参数配置

* 应支持家庭网关设备本身（用户侧）IP地址的配置；
* 应支持用户侧DHCP的打开和关闭。

1. 用户侧WLAN接口参数配置（仅针对具有WLAN用户接口的设备）

* WLAN功能的打开和关闭、信道选择、频宽模式选择、发射功率调节、5GHz频段保护间隔（家庭网关用户仅可设置发射功率）；
* 2.4G-1设置：名称、加密/认证配置、广播取消；
* 5G-1设置（仅针对支持双频段无线的设备）：名称、加密/认证配置、广播取消。

1. 融合版专用配置（仅提供给电信维护人员）
2. 机顶盒模块应支持以下 3 种IPv4/v6 双栈的网络连接方式的配置：

* PPPoE：当选择此种方式时，要求支持设置PPPoE 用户名及密码
* DHCP(及扩展)：当选择此种方式时，支持选择是否启用 OPTION60 及扩展，在启用扩展的情况下应允许设置 DHCP 用户名及密码，其中用户名长度不应超过 36 位； 支持 OPTION125
* 静态 IP：当选择此种方式时，支持设置静态 IP、子网掩码、默认网关及 DNS 服务器(主备)；

1. 应支持基于电视屏幕进行配置：

* 逻辑ID配置：配置逻辑ID后应可选择启动设备注册认证过程（参见8.1.6）并显示业务开通过程（政企场景下，注册过程中不显示无线的修改界面）。界面入口在机顶盒模块本地管理界面中“基本设置”菜单下添加的“逻辑ID注册”子菜单。
* 无线2.4G-1基本信息配置（仅针对公客场景）：开关、名称、密码、加密模式等。界面入口在机顶盒模块本地管理界面中“基本设置”菜单下添加的“无线配置”子菜单。
* 机顶盒模块专用配置：应符合《中国电信智能机顶盒技术要求》6.10.1和6.10.2要求（在“基本设置”菜单下，取消“连接方式”子菜单）
  + 1. 高级配置

高级配置实现对家庭网关的一些特殊功能进行配置管理，仅对电信维护人员开放（特别标注者除外）。

1. DDNS配置

应支持DDNS参数（服务商、域名、用户名、密码）的配置。

1. DMZ配置

应支持需要打开DMZ功能的LAN侧IP地址的配置。

1. 安全配置

应支持过滤器、防火墙和攻击保护等配置：

* 过滤器配置

应支持URL、MAC地址的过滤参数的配置，生成过滤器规则，并可删除过滤器规则。

* 防火墙配置

应支持防火墙功能的开关配置。

* 攻击保护配置

应支持防攻击保护功能的开关配置。

1. UPnP配置

应支持UPnP功能的开关配置。

1. 虚拟主机配置（电信维护人员和家庭网关用户都具有该操作权限）

应支持外部端口的访问映射到家庭内部不同的IP地址或主机名的配置，并且映射的目的端口可配。用户可选择常见协议（如FTP、HTTP等）进行Virtual Server配置。

1. ALG配置

应支持对ALG功能的开关设置。

1. 语音设置

在支持SIP时，维护员管理界面应支持软交换SIP、IMS SIP协议的选择。

维护员管理界面应支持主、备用Server/Proxy的域名、IP地址、端口号，用户帐号、密码等相关参数的配置。

1. ITMS+服务器配置

应支持ITMS+服务器参数（如域名/IP地址、端口等）的设置。

1. 逻辑ID的配置（电信维护人员和家庭网关用户都具有该操作权限）

支持逻辑ID的配置，应支持从本地管理页面上启动基于逻辑ID的设备注册认证功能（功能要求见8.1.6）。

1. NTP配置

应支持NTP服务器的地址（域名或IP地址）、绑定的WAN连接、同步间隔的设置。

* + 1. 设备管理

设备管理实现智能家庭网关的用户管理、日志文件管理、软件升级、设备重启、恢复出厂设置功能。

根据用户分级管理的要求，电信维护人员和智能家庭网关用户都具有以下管理项目的操作权限（特别标注者除外）。

1. 用户管理

应支持智能家庭网关用户账号的密码的强制修改（仅提供给电信维护人员）；

应支持智能家庭网关用户账号的密码验证后修改（先验证原密码，仅提供给智能家庭网关用户）。

1. 日志文件管理

应支持日志文件写入等级设置，只有日志等级高于此限制的信息才记入到日志文件（仅提供给电信维护人员）。

1. 软件升级

智能家庭网关软件不能提供Web等方式的本地升级，仅能通过ITMS或智家平台进行远程升级。

1. 设备重启

应支持智能家庭网关的重新启动。

1. 恢复出厂设置

应支持通过手动按键恢复出厂配置，按键持续时间短于10秒执行短按本地恢复出厂设置，按键持续时间达到10秒立即执行长按本地恢复出厂设置。按键持续时间达到2秒时，所有指示灯（电源灯可除外）开始以2秒为周期闪烁。

短按本地恢复出厂设置时，智能家庭网关应具备保留关键参数能力，各关键参数值以最后保存配置的为准，短按恢复出厂设置后第一次Inform上报不发”0 boot”。短按本地恢复出厂设置的关键参数包括（本地GUI恢复出厂设置要求与短按本地恢复出厂设置相同）：

* ITMS+ URL
* 智能家庭网关和ITMS+间双向Digest认证用户名/密码信息
* 电信维护帐号的用户名/密码
* TR069 使用的WAN连接及绑定关系（包含VLAN、绑定、路由等设置）
* 其它WAN连接相关配置（包含VLAN、LAN/WLAN绑定关系、VLAN绑定及全路由设置、桥接/路由等设置、PPPoE用户名/密码）
* 接入用户数相关参数
* 2.4G-2～2.4G-8相关参数
* 5G-2～5G-8相关参数（仅针对支持双频段无线的设备）
* 语音Server/Proxy的域名、IP地址、端口号、用户帐号、密码
* 端口映射相关参数
* 设备认证状态（Internet­Gateway­Device.X\_CT-COM\_UserInfo.Times、Internet­Gateway­Device.X\_CT-COM\_UserInfo.Limit、Internet­Gateway­Device.X\_CT-COM\_UserInfo.Status、Internet­Gateway­Device. X\_CT-COM\_UserInfo.Result）
* 宽带识别码（包括LOID和Password）
* 远程链路维持相关参数
* NTP相关参数：服务器的地址（域名或IP地址）、绑定的WAN连接、同步间隔的设置
* 《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》规定的其它应保留参数，包括接口开放权限、错误页面重定向配置、WAN侧L2TP VPN通道配置、插件访问权限、智能OS资源权限
* 插件（含出厂预装插件）相关配置（包含存储应用相关的FTP、SAMBA配置）
* 机顶盒模块相关配置（仅针对融合版设备）

长按本地恢复出厂设置时，智能家庭网关应具备保留关键参数能力，各关键参数值以最后保存配置的为准，长按恢复出厂设置后第一次Inform消息中包含X CT-COM LONGRESET事件号。关键参数包括：

* ITMS+ URL
* 智能家庭网关和ITMS+间双向Digest认证用户名/密码信息
* 电信维护帐号的用户名/密码
* TR069 使用的WAN连接及绑定关系（包含VLAN、绑定、路由等设置）
* 宽带识别码（包括LOID和Password）
* 机顶盒模块相关配置（仅针对融合版设备）
  + 1. 网络及设备诊断

根据用户分级管理的要求，仅电信维护人员具有以下管理项目的操作权限。

家庭网关应支持在选定的WAN连接下PING及Trace route测试，测试的目的地址支持IP地址和域名两种方式，测试结果清晰易读。

家庭网关宜支持在选定的WAN连接下DNS QUERY、HTTP GET等故障检测操作。

家庭网关应支持手动的Inform上报，手动Inform上报的状态显示要求与主动Inform上报相同。

家庭网关应支持手动重启及暂停Framework，暂停周期可选3分钟、10分钟、30分钟和120分钟，设备重启时当前暂停周期应保持，Framework重启时当前暂停周期应终止。

融合版设备的机顶盒模块应支持《中国电信智能机顶盒技术要求》6.12所列的本地诊断功能。

* 1. ITMS+远程管理和配置要求
     1. 远程管理基本要求

1. 应支持远程管理和维护操作：参数配置、软件升级、故障诊断、家庭网关统计信息及状态查询等。
2. 应支持TR-069 / TR-098 / TR-104参数模型，及中国电信扩展的业务相关的参数模型，扩展参数模型参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》。
3. 应支持《中国电信家庭网关与增强型终端综合管理系统接口技术要求》定义的接口和功能。
4. 应支持Digest双向认证，家庭网关认证平台的初始用户名/密码为：itms/itms，平台认证家庭网关的初始用户名/密码为：hgw/hgw；家庭网关应支持SSL。
5. 应提高远程管理过程中的响应速度，一个交互过程中每次ITMS+平台断开连接到终端主动发起连接的平均间隔时间应低于0.4秒。
6. 通过ITMS+配置参数后，如果设备需要重启生效，则需要上报ITMS+，由ITMS+命令设备重启后再重启，需要重启生效的参数范围应不超出WAN连接相关参数；家庭网关应优化启动（包括重启）流程，尽量缩短启动时间，并支持所有配置业务功能全部成功下发后一次性重启生效。
   * 1. 远程参数配置和性能监测

家庭网关能够接受ITMS+对其进行远程的配置以及设备信息、状态参数的远程读取。具体需要实现的功能如下：

1. 家庭网关设备信息

家庭网关应支持设备信息（设备型号、设备标识号、硬件版本、软件版本等）的查询。

1. 网络侧参数配置和查询
2. 网络侧连接方式的配置和查询

* PPP方式的参数设置和查询；
* IP方式的参数设置和查询。

1. PON上行参数配置和性能检测

* PON线路物理层参数的查询（如来自OLT的下行光功率，智能家庭网关的发送光功率）。

1. 用户侧参数配置和查询
2. 用户侧网络参数配置和性能监测

* LAN设备地址分配参数的配置和查询；
* LAN地址信息的配置和查询。

1. 以太网参数的配置和查询

* 以太网物理端口的参数配置和查询；
* 以太网端口的性能监测（收发字节等）。

1. WLAN参数的配置和查询

* 家庭网关WLAN部分的基本参数和安全参数的配置和查询；
* WLAN所连接设备的状态查询。

1. 语音应用的配置和查询
2. 应支持语音业务的激活/去激活；
3. 应支持SIP、H.248各种参数的配置和查询（具体参见TR-104要求）；
4. 在支持SIP时，支持软交换SIP、IMS SIP协议的选择；
5. 配置SIP协议支持远程配置的Digital Map。
6. DDNS功能的参数配置：参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》。
7. UPnP功能的参数设置：参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》。
8. 防火墙参数的配置和查询：参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》。
9. 根据URL、IP地址、协议、端口数据包过滤的参数配置和查询；
10. 攻击保护的参数配置和查询；
11. 安全级的参数配置和查询。
12. QoS配置

家庭网关提供和业务相关的QoS配置模板，ITMS+能够根据业务的开通情况选择相适应的QoS配置模板。

QoS配置模板中应包括以下功能的设置（具体参见TR-069 和TR-098要求）：

1. 应支持数据流的分类参数源/目的MAC、源/目的IP、源/目的端口号、协议、Flow Label等的配置（其中Flow Label仅针对IPv6数据）；
2. 应支持基于物理端口的QoS配置；
3. 策略路由的配置，支持数据流到队列的映射；
4. 支持根据数据流分类进行标识的配置，包括802.1D、DSCP、TOS（仅针对IPv4数据，可选）、Traffic Class（仅针对IPv6数据，可选）、Flow Label（仅针对IPv6数据，可选）；
5. 应支持根据应用划分数据流参数的配置；
6. 应支持CAR参数的配置；
7. 应支持队列参数的配置。
8. 公网接入用户数管理

应支持家庭网关路由方式下公网接入用户数的配置。

1. 强制门户功能的配置和查询
2. 应支持强制门户功能的开启和关闭；
3. 应支持针对不同终端（包括电脑、手机、机顶盒等）的强制门户URL的设置和查询。
4. 端口映射功能的配置和查询

应支持家庭监控等应用所需端口映射功能的设置和查询。

1. 业务统计功能

应根据具体业务需求，与网络侧配合，提供业务管理所需的业务统计功能。

1. NTP配置

应支持NTP服务器的地址（域名或IP地址）、绑定的WAN连接、同步间隔的设置。

* + 1. 远程故障诊断功能

智能家庭网关能配合ITMS+实现如下的远程故障诊断功能：

1. 远程重启和恢复出厂设置

智能家庭网关能够接受ITMS+的远程控制，执行设备重启和恢复出厂设置的操作。

远程恢复出厂设置应具备保留关键参数能力（各关键参数值以最后保存配置的为准），其余配置应恢复成出厂预配置，关键参数包括：

* 宽带识别码（包括LOID和Password）
* 《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》第8章所列的智能网关及应用管理平台接口可配置参数（即可写参数）中，《中国电信家庭网关与增强型终端综合管理系统接口技术要求》未涉及的相关参数
* 插件（含出厂预装插件）相关配置（包含存储应用相关的FTP、SAMBA配置）
* 机顶盒模块相关配置（仅针对融合版设备）

远程恢复出厂设置后智能家庭网关第一次Inform上报应发”0 boot”。

1. PING测试功能

智能家庭网关能够接受ITMS+的远程控制和相关参数配置，发起PING测试。

智能家庭网关能够接受ITMS+的远程参数配置，使能/禁止响应网络侧设备发起的PING测试。

1. Trace route测试功能

智能家庭网关能够接受ITMS+的远程控制和相关参数配置，发起Trace route测试。

1. PON线路参数查询

智能家庭网关能够接受ITMS+的远程查询，上报PON线路参数（如错帧率、误码率等）。

1. 环路检测功能

智能家庭网关能够接受ITMS+的远程控制和相关参数配置，对用户侧是否存在环路进行检测并记录各用户侧接口的检测结果。具体要求如下：

当开启环路检测功能时，家庭网关应支持根据配置的环路检测时间间隔，向用户侧接口发送指定VLAN及以太类型的环路检测报文（报文目的地址为广播地址）。当指定有多个VLAN时，家庭网关应依次发送携带不同VLANID的环路检测报文。当检测到存在环路故障时，家庭网关应关闭相应故障端口。

对检测到环路并已关闭的端口，家庭网关应支持对其进行环路解除检测，根据配置的环路解除检测时间间隔，临时开启端口并发送环路检测报文以判断环路是否解除。如果检测到环路解除，家庭网关应自动恢复端口的正常工作状态。如果还存在环路故障，应继续关闭端口。

1. 语音仿真测试及话机连接性检查

家庭网关能够接受ITMS+的远程控制，进行语音业务的主叫/被叫仿真测试及话机连接性检查。

* + 1. 设备告警功能

家庭网关应支持设备告警的功能，能够在ITMS+的控制下上传设备的告警信息，告警信息的定义参见附录D。

* + 1. 远程链路维持功能

智能家庭网关应具有链路维护的功能，在ITMS+的控制下，家庭网关能够通过持续的PING操作配合实现网络链路的维持（参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》C.2.1.28）。远程链路维持功能应和PING测试功能互不影响。远程链路维持功能缺省关闭。

* + 1. 软件远程管理

智能家庭网关能够接受ITMS+的远程控制，进行软件版本升级。智能家庭网关升级软件时应具有容错校验功能，如果升级失败，应能恢复到原来的软件版本或者连接ITMS+接受再次升级。当智能家庭网关本地软件发生故障或遭到破坏的时候应能够连接ITMS+接受软件下载。

智能家庭网关软件升级时应基于配置文件双备份等机制实现配置信息的继承、更新及增减，从而支持通过软件升级实现业务预配置信息、TR069远程参数等配置内容的条目增减或定义变更。

智能家庭网关应可选择使用以下方式支持软件升级的异常恢复：

1. 小型软件升级核方式：家庭网关在包含普通的软件Image之外，配置小型软件升级核，小型软件升级核可以连接ITMS+平台、智家平台，支持ITMS+、智家平台对普通的软件Image的升级功能。当家庭网关普通的软件Image不能正常工作时，能够自动启动小型软件升级核运行。
2. 双Image备份方式：家庭网关支持软件的双Image备份功能，在一个Image出现异常时，能够切换到另一个Image运行。

智能家庭网关在根据ITMS命令进行软件升级时，不得损害与智家平台的连接配置信息，并应支持对已加载插件的继承或清除：

1. 对于新软件架构仍能支持的已加载插件，家庭网关应保障相关插件的生命周期及运行状态在网关软件升级前后不变
2. 对于新软件架构放弃支持的已加载插件，家庭网关软件升级过程中应实现对相关插件的全面清除
   * 1. 业务部署和控制

家庭网关应接受ITMS+下发的命令请求，实现业务参数配置、业务状态查询和业务参数调整：

1. 上网应用的参数配置和状态查询
2. IPTV应用承载WAN连接的参数配置和状态查询
3. 语音应用的参数配置和状态查询
4. 家庭存储应用的参数配置和状态查询
   1. 基于OAM的EMS远程管理和配置要求

EPON上行智能家庭网关除支持8.3节的 ITMS+远程管理和配置要求外，还应支持本节的基于OAM的EMS远程管理和配置要求。

* + 1. 标准OAM管理要求

EPON上行的家庭网关需要支持IEEE 802.3-2005中规定的标准属性和操作，应支持的属性和操作如表4所示。对这些标准的属性（Attributes）和操作（Actions）的variable discriptor/container的格式应符合IEEE 802.3-2005的规定。

1. 应支持的标准属性（Attributes）和操作(Actions)

|  |  |  |  |
| --- | --- | --- | --- |
| **属性/操作** | **功能描述（Description）** | **Get** | **Set** |
| aFECAbility | FEC能力查询（IEEE 802.3 Clause 30.5.1.1.13） | ○ |  |
| aFECmode | 双向FEC功能的打开/关闭（IEEE 802.3 Clause30.5.1.1.14） | ○ | ○ |

应具有通过OAM的Dying Gasp功能将自身掉电事件通知OLT的能力。

* + 1. 扩展OAM管理要求

支持《中国电信EPON设备技术要求（V3.0）》所规定的扩展OAM功能。

应支持的扩展属性如表5所示。

1. 应支持的扩展属性（Attributes）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **属性名称（Attribute）** | **描述（Description）** | **Get** | **Set** | **说明** |
| ONU SN | ONU的标识符 | ○ |  | 使用向中国电信申请家庭网关设备标签数据时提供的设备MAC地址 |
| FirmwareVer | ONU MAC芯片的固件版本 | ○ |  |  |
| Chipset ID | ONU的PON芯片厂商和版本 | ○ |  |  |
| ONU Capabilities-2 | ONU支持的端口类型和基本功能 | ○ |  |  |
| ONU Capabilities-3 | ONU支持的端口类型和基本功能 | ○ |  |  |
| OpticalTransceiverDiagnosis | ONU光模块的重要参数检测和链路诊断 | ○ |  |  |
| HoldoverConfig | Holdover属性配置 | ○ | ○ |  |
| Active PON\_IFAdminstate | ONU的PON接口的管理 | ○ | ○ | 仅针对支持类型c或d的光链路保护的EPON上行家庭网关 |
| Service SLA | ONU上每个业务队列的SLA及上行队列调度管理 | ○ | ○ | 支持Serive SLA的HGU必选 |
| Group Num Max | ONU或端口同时支持的组播组数量 | ○ | ○ |  |
| aFastLeaveAbility | 查询ONU端口的组播Fast Leave能力 | ○ |  |  |
| aFastLeaveAdminState | 查询ONU端口的组播Fast Leave状态 | ○ |  |  |
| LLIDQueueConfig | LLID与队列的绑定关系管理 | ○ | ○ | 具备多LLID能力的EPON上行家庭网关必选，否则可选 |
| ONUTxPowerSupplyControl | 设置ONU PON口光模块电源的关断和开启 |  | ○ | 可选支持 |
| ONU power saving capabilities | 描述ONU是否支持节能模式和提前醒来功能 |  |  |  |
| ONU power saving config | 描述OLT查询/配置ONU节能模式中的提前醒来功能及最大刷新时间 |  |  |  |
| ONU Protection Parameters | 查询/配置光链路保护机制中ONU的Optical LoS和MAC LoS的时间 |  |  |  |
| Performance Monitoring Status | OLT查询/设置ONU PON接口和SFU UNI接口的数据包性能统计状态和统计周期 | ○ | ○ |  |
| Performance Monitoring Data Current | OLT查询/设置ONU PON接口和SFU UNI接口当前统计周期的性能统计数据 | ○ | ○ |  |
| Performance Monitoring Data History | OLT查询/ ONU PON接口和SFU UNI接口前一统计周期的性能统计数据 | ○ |  |  |

应支持的扩展操作如下（具体要求参见《中国电信EPON设备技术要求（V3.0）》）：

* RebootONU
* Sleep Control
* acMultiLLIDAdminControl（具备多LLID能力的HGU必选）
* acFastLeaveAdminControl
  1. 基于OMCI的EMS远程管理和配置要求

GPON/XG-PON上行家庭网关除支持8.3节的ITMS+远程管理和配置要求外，还应支持本节的基于OMCI的EMS远程管理和配置要求。

GPON/XG-PON上行家庭网关应支持OLT通过OMCI实现终端光链路相关内容的的配置管理。

GPON/XG-PON上行家庭网关缺省创建一条用于OLT配置和管理的OMCI的T-CONT连接（其Alloc ID=ONU ID），该OMCI T-CONT的ME不应在MIB UPLOAD时候进行上报。

GPON/XG-PON上行家庭网关应支持OLT使用PLOAM消息设置管理通道的PortID值。

GPON/XG-PON上行家庭网关应支持Virtual Ethernet Interface Point（VEIP）作为OMCI管理域和TR069管理域（如TR069、SNMP等）在数据平面的分割点：

* 该ME仅可以通过OMCI进行管理；
* VEIP下面所有业务及功能模块仅接受非OMCI管理域管理；
* 每个家庭网关中应仅创建一个VEIP。

GPON/ XG-PON 上行家庭网关应支持1：MP bridge-map-filtering的GEM连接方式，应支持的ME如表6所示：

1. 智能家庭网关应支持的ME

| **ME Class** | **ME名称** |
| --- | --- |
| 2 | ONT Data |
| 5 | Cardholder |
| 6 | CircuitPack |
| 45 | MAC Bridge Service Profile |
| 46 | MAC Bridge Configuration Data |
| 47 | MAC Bridge Port Configuration Data |
| 50 | MAC Bridge Port Bridge Table Data |
| 84 | VLAN Tagging Filter Data |
| 130 | 802.1p Mapper Service Profile |
| 131 | OLT-G |
| 171 | Extended VLAN Tagging Operation Configuration Data |
| 256 | ONU-G |
| 257 | ONU2-G |
| 262 | T-CONT |
| 263 | ANI-G |
| 264 | UNI-G |
| 266 | GEM IWTP |
| 268 | GEM Port Network CTP |
| 277 | Priority Queue-G |
| 278 | Traffic Scheduler-G |
| 281 | Multicast GEM IWTP |
| 329 | Virtual Ethernet Interface Point |
| 65530 | LOID Authentication |
| 65531 | Extended Multicast Operation Profiles |

OMCI的具体要求应符合G.988、《中国电信GPON设备技术要求（V2.0）》和《中国电信XG-PON设备技术要求》的规定。

GPON 上行家庭网关应支持OLT对设备的认证功能，应符合《中国电信GPON设备技术要求》。

XG-PON 上行家庭网关应支持OLT对设备的认证功能，应符合《中国电信XG-PON设备技术要求》。

* 1. 基于智能网关及应用管理平台的管理配置要求
     1. 智能网关及应用管理平台基本管理要求

智能家庭网关应存在含INTERNET属性的路由WAN连接（非按需拨号模式），应遵循《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》和智家平台、手机APP进行连接和交互，且应满足如下要求：

1. 和智家平台的交互

* 和智家平台及相关文件/数据服务器（如升级软件服务器、插件业务数据服务器等）的交互只能通过含INTERNET属性的路由WAN连接承载（含INTERNET属性的路由WAN连接同时获得IPv4和IPv6地址时，优先使用IPv4协议）
* 智能家庭网关只接受/响应协议格式和源IP地址均正常的智家平台报文
* 典型交互的处理时限应满足表7要求

1. 典型交互时限要求

|  |  |  |
| --- | --- | --- |
| 交互计时起点 | 交互计时终点 | 最大时限 |
| 上网业务能通 | 发首个BSS平台域名解析请求包 | 200毫秒 |
| 收到BSS平台域名解析结果 | 发出首个向BSS平台注册包 | 200毫秒 |
| 收到BSS平台所发指派能力平台的报文 | 发首个能力平台域名解析请求包 | 200毫秒 |
| 收到能力平台域名解析结果 | 发出首个向能力平台注册包 | 200毫秒 |
| 收到获取下挂信息的命令报文 | 发送出所有设备信息响应报文 | 200毫秒 |
| 收到关闭或打开WLAN的命令报文 | 操作成功并发送出响应报文 | 2000毫秒 |
| 收到调整WLAN发射功率的命令报文 | 调整成功并发送出响应报文 | 1000毫秒 |
| 收到关闭或打开指示灯的命令报文 | 操作成功并发送出响应报文 | 200毫秒 |
| 收到设置或取消黑名单的命令报文 | 操作完成并发送出响应报文 | 200毫秒 |

1. 和手机APP的交互

* 智能家庭网关只能通过家庭局域网和手机APP进行交互
* 智能家庭网关只接受/响应协议格式和源IP地址均正常的手机APP报文

1. 家庭网关与智家平台的接口交互及处理分发功能应模块化实现，支持以模块升级的方式实现对通讯协议（如UDP、TCP、HTTP）、能力封装接口、交互流程（如增加主动上报参数、变更验证字段等）等的升级。
   * 1. 智家平台具体配置及功能要求

智能家庭网关应配合智家平台、手机APP实现《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》规定的配置及功能，其中主要的配置及功能如下：

1. WiFi控制

通过Web管理配置页面和智家平台两种配置方式，家庭网关应均能实现以下WiFi控制功能：

* 1. WiFi开启/关闭；
  2. 调节WiFi发射功率（百分比）；
  3. 查询当前环境WiFi信道占用情况，进行设备WiFi信道切换；
  4. 实现WiFi定时开关，包括：
* 定时设置的内容包括：该设置是否使能（使能/禁止）、针对的SSID、所设置的时间点、所设置的动作（打开/关闭）、以星期为周期（周一至周日）的重复性
* 支持定时设置的添加、修改、删除
* 可设置不少于6个定时
  1. WiFi快联配网的设置：包括WiFi黑白名单的设置, WiFi网络访问权限的配置，基于VSIE(Vendor Specific Information Element)的快联功能配置；
  2. WiFi漫游功能的设置。

家庭网关应采用“开关状态单次反转或无缝延续”的方式实现WiFi每次的开启/关闭控制或定时控制，应支持WiFi控制相关配置信息在设备重启时不丢失。

1. 网关休眠控制

家庭网关应支持休眠/唤醒功能，休眠时应关闭除网络侧上网业务连接、语音、TR069、时钟之外的其它功能（如WiFi、存储、LAN口、指示灯等）。休眠期间，网关应正常响应ITMS、智家平台的各种管理配置命令。

家庭网关应支持如下的休眠/唤醒控制方式：

1） 由智家平台远程下发休眠/唤醒命令

2） 通过Web管理配置页面、智家平台进行定时休眠/唤醒的设置，包括：

* 定时设置的内容包括：该设置是否使能（使能/禁止）、所设置的时间点、所设置的动作（休眠/唤醒）、以星期为周期（周一至周日）的重复性
* 支持定时设置的添加、修改、删除
* 可设置不少于6个定时

3） 通过外部操作对休眠状态的家庭网关进行唤醒，包括：

* 重启家庭网关设备

家庭网关应采用“状态单次反转或无缝延续”的方式实现每次的休眠/唤醒控制（含休眠/唤醒控制定时控制），应支持休眠控制相关配置信息在设备重启时不丢失。

针对融合终端，当网关模块休眠时，机顶盒模块应同步进入待机状态；网关模块从休眠状态恢复时，机顶盒模块维持现有状态不变；机顶盒模块唤醒时，网关模块若处于休眠状态应同步唤醒。

1. 指示灯开关

支持通过Web管理配置页面、智家平台两种方式控制网关指示灯开关。

家庭网关应支持指示灯开关相关配置信息在设备重启时不丢失。在指示灯关闭的情况下出现设备重新启动时，启动过程中指示灯应按状态进行正常指示，启动结束后再匹配到当前的实际设置要求。

1. 设备信息读取及修改

通过Web管理配置页面、智家平台两种配置方式，家庭网关应均能实现设备名称的读写，并可实现以下设备信息的读取：

* 网关硬件型号、网关软件版本号、硬件能力（FLASH容量、RAM容量、wifi支持协议）、MAC地址（PON上行设备指上报给OLT的MAC）
* 路由上网业务的WAN侧IP地址、DNS服务器地址、局域网管理IP地址
* LAN口是否正常、WiFi模块是否正常、语音模块是否正常、存储模块是否正常、存储设备容量使用情况、指示灯模块是否正常
* 网关本次工作时长、已安装插件数目
* 宽带上行是否正常、网关Telnet访问是否开启
* 加载应用的生命周期状态

1. WAN连接上下行带宽监测

应支持对各条WAN连接的上下行实际使用带宽进行监测，监测结果能在本地界面显示，并可通过响应智家平台的查询请求进行上报。带宽监测功能可通过本地界面、智家平台进行开启及关闭，缺省关闭。家庭网关应支持WAN连接上下行带宽监测相关配置信息在设备重启时不丢失。

各条WAN连接的上下行实际使用带宽的计量及限制单位为kbps。计量周期缺省为1秒，并可通过本地界面、智家平台进行修改。

1. 下挂设备上下行带宽监测及限制

应能对每一个下挂设备的上下行实际使用带宽的进行监测，监测结果能在本地界面显示，并可通过响应智家平台的查询请求进行上报。带宽监测功能缺省关闭，可通过本地界面、智家平台进行开启及关闭。家庭网关应支持下挂设备上下行带宽监测及限制相关配置信息在设备重启时不丢失。

应能对每一个下挂设备的上下行实际使用带宽的进行限制（颗粒度应不大于512Kbps），限制值可通过本地界面、智家平台进行配置。带宽限制功能可通过本地界面、智家平台进行开启及关闭，缺省关闭。

下挂设备的上下行实际使用带宽的计量及限制单位为kbps，不用区分局域网和公网流量。计量周期缺省为1秒，可通过本地界面、智家平台进行修改。

1. 下挂终端接入权限

家庭网关能够根据智家平台的配置要求，基于MAC地址对指定的终端进行接入权限限制，限制内容包括：

* 家庭网络接入限制：不允许接入家庭网络（同时控制对家庭局域网络和外网的访问）
* 外网访问限制：（仅控制对外网的访问，不影响对家庭局域网络的访问）
* 可否本地访问存储设备（不影响对家庭局域网络和外网的访问）

家庭网关应支持下挂终端接入权限相关配置信息在设备重启时不丢失。

1. 下挂设备信息识别

智能家庭网关应支持下挂设备的识别管理功能（可通过集成第三方插件实现）：

* 应能识别由以太网口和WLAN接入的设备，根据智家平台的控制提供以下信息：设备名称、设备类型（如手机/平板/电脑/机顶盒等）、品牌名、操作系统、MAC地址、IP地址、本次连接在线时长
* 对于首次接入智能家庭网关的设备（指家庭网关首次上电或上次恢复出厂设置以来，第一次使用其MAC地址接入到家庭网关的设备），应将设备名称和MAC地址主动上报智家平台
* 应支持智家平台、本地GUI对设备名称的修改

1. L2TP/PPTP VPN功能

应支持L2TP和PPTP VPN客户端功能，实现特定目的地址、特定源MAC的数据流通过VPN进行转发。

家庭网关应根据智家平台下发的配置信息，自动识别需要VPN承载的数据流，并按以下要求进行承载：

* 对于同时匹配了多条VPN通道关联条件的数据流，优先选择高优先级VPN通道，优先级相同时任选一条可正常工作的VPN通道，如果所选VPN通道失败应尝试其它可选通道
* 检查所需VPN通道是否已处于正常工作状态，如未处于正常工作状态应立即进行创建（建立动态账号的VPN通道时应先向平台申请本次连接的帐号）
* 将识别出的数据流通过VPN通道承载
* 不能正常建立VPN时，识别出的数据流通过正常上网通道承载

家庭网关应支持VPN通道的空闲自动断开，该功能的启用及断开前空闲等待时间由智家平台远程配置。

家庭网关应支持响应智家平台下发的命令，上报VPN通道承载的数据流次数统计。

家庭网关应支持VPN相关配置信息在设备重启时不丢失。

1. 业务平台参数设置

家庭网关能够根据智家平台的配置，更新智家平台URL、远程访问端口、网关和智家平台之间的心跳、手机APP客户端本地访问端口等信息，相关配置信息在设备重启时不丢失。

1. 设置接口开放权限

家庭网关能够根据智家平台的配置，设置相应API的接口开放权限，相关配置信息在设备重启时不丢失。

1. 故障诊断

家庭网关能够根据手机APP或智家平台的控制，进行以下设备故障诊断：

1) Ping诊断：在选定WAN连接下发起Ping诊断测试并返回诊断结果。

2) Traceroute诊断：在选定WAN连接下发起Traceroute诊断测试并返回诊断结果。

3) Inform诊断：家庭网关能够根据要求，发起向ITMS的Inform诊断并返回诊断结果。

4) 控制网关PPP拨号：使用特定账号驱动网关进行拨号，并返回拨号状态、拨号失败原因等信息。当测试完成后，网关应该自动恢复原有账号并重新拨号。

1. 网络测速

家庭网关能够根据手机APP或智家平台的控制和相关参数配置，发起HTTP或FTP下载进行测速，并根据要求返回WAN连接接收字节总数的统计结果。家庭网关应支持测速下载地址配置信息在设备重启时不丢失。

EPON/GPON网关网络测速能力应不低于500Mbps，10G-EPON/XG-PON网关网络测速能力应不低于1000Mbps。

1. 设备管理

家庭网关能够根据手机APP或智家平台的控制，进行以下设备管理：

* 1. 网关重启：家庭网关能够根据要求进行重启操作。
  2. 恢复非关键参数：将以下参数恢复成出厂预设值（家庭网关执行该操作时应不重启）：
* 《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》第8章所列的智能网关及应用管理平台接口可配置参数（即可写参数）中，《中国电信家庭网关与增强型终端综合管理系统接口技术要求》未涉及的相关参数
* 网关下挂终端接入控制相关参数
  1. 固件升级：到指定的URL地址下载固件并进行升级操作，并应符合8.3.6中的升级异常恢复、升级前后配置文件及插件的保障等技术要求。
  2. 模块化升级：对智能OS、应用插件、基本软件能力接口、APP管理平台命令处理分发模块等进行模块化升级。升级时应支持对升级压缩包（如tar.gz包）进行自动解压。当对C-code的模块进行软件升级时，网关在下载了新的软件模块后应在更新Flash相关模块前先加载运行新模块（不改变模块实际的启动/停止状态），新模块加载运行正常后再进行Flash相关模块的替换并上报升级成功。
  3. 网关校时：同步当前家庭网关时间。
  4. 上报恢复出厂设置操作的类型：当网关进行恢复出厂设置操作时，应在下次向智能网关及应用平台注册时上报所进行恢复出厂设置操作的类型。
  5. 设置FTP、SAMBA的服务开放范围（内网、外网）及账号权限。
  6. 上报设备当前支持的设备规范、与ITMS平台接口规范、与智家平台接口规范的版本情况。
  7. 清除家庭网关的DNS缓存。
  8. 上报设备运行状态，记录上报和智家平台的交互记录，记录上报DBUS接口交互记录。

1. DNS解析结果重定向

家庭网关能够根据智家平台的控制和相关参数配置，下载DNS解析结果重定向配置文件，并根据其中的策略执行DNS解析结果重定向操作：当家庭网关侦测到网络侧返回的DNS解析结果为文件中指定的IP地址或解析失败时，应将配置文件中的相应重定向IP地址作为解析结果返回给用户端设备，实现DNS解析结果重定向功能。

DNS解析结果重定向配置参数掉电不可丢失。

DNS解析结果重定向功能的相关操作（如接受智家平台的重定向配置文件下发命令、下载重定向配置文件、实现重定向等）均应记入日志文件（为日志文件最高记录等级内容）。

1. 关联数据流到指定DNS解析

家庭网关能够根据智家平台的控制和相关参数配置，关联匹配的数据流到指定的DNS进行解析。当家庭网关接收到关联数据流到指定DNS解析命令（CmdType：ATTACH\_WAN\_DNS\_ TUNNEL）时，应立即清空自身的DNS缓存。

关联数据流到指定DNS解析的配置参数掉电不可丢失。

关联数据流到指定DNS解析的相关操作（如接受智家平台的指定DNS配置下发命令、实现定向解析等）均应记入日志文件（为日志文件最高记录等级内容）。

1. 设备注册

家庭网关能够根据手机APP的控制和相关参数配置，启动基于宽带识别码的设备注册认证功能。

* 1. 机顶盒模块管理要求（仅针对融合版设备）

1. 应支持通过机顶盒终端管理平台实现对机顶盒模块的远程管理，且符合《中国电信智能机顶盒技术要求》6.10.3要求。
2. 应支持机顶盒模块软件单独升级，且符合《中国电信智能机顶盒技术要求》6.6要求。
3. 应支持机顶盒模块发起IPPING及 Trace route等远程诊断功能，且符合《中国电信智能机顶盒技术要求》6.12要求。
4. CEC控制要求：
   * 开启CEC且电视机控制机顶盒模式：默认电视机开机时同步开启机顶盒；电视机关机/待机时，通过设置项来配置同步、1小时、3小时、自定义时间，确定机顶盒待机。
   * 关闭CEC且电视机控制机顶盒模式
   * 开启CEC且机顶盒控制电视机模式：默认机顶盒待机时通过CEC同步发送电视机待机指令，机顶盒开机时同步唤醒电视机。
   * 关闭CEC且机顶盒控制电视机模式
5. 性能要求
   1. 转发性能要求
      1. 整体吞吐量

智能家庭网关整体吞吐量指标等级要求见表8，不同形态智能家庭网关应支持的整体吞吐量指标等级见4.3。

1. 多种业务同时承载的整体吞吐量指标等级要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标等级 | 上网 | IPTV | 远程管理 | 语音 |
| T\_1 | 上下行总流量（路由方式）应不低于600Mbps，宜不低于800Mbps | 下行流量（桥接方式）应不低于90Mbps | 1条TR069数据流 | 1条语音流 |
| T\_2 | 上下行总流量（路由方式）应不低于1500Mbps，宜不低于3000Mbps | 下行流量（桥接方式）应不低于200Mbps |

吞吐量指标等级应符合如下条件：

* + IPv4、IPv4/v6双栈（含DS-Lite应用场景）、IPv6协议下均应满足相关指标要求
  + 上网、IPTV、语音（仅针对包含语音口的设备）、远程管理数据流同时承载，其中2.4GHz频段承载的无线上网上下行流量应均不低于35Mbps，5GHz频段承载的无线上网上下行流量应均不低于100Mbps
  + 启用预装插件
    1. 地址学习

MAC地址学习数量应不少于128个。

* + 1. 缓存大小

应支持1518字节包长的80个数据包的缓存能力，以支持少量突发性数据业务。

* + 1. 并发处理要求

应支持在64字节、512字节、1024字节、1518字节下UDP的session数不低于4000个，10G-EPON和XG-PON网关宜不低于8000个。

打开防火墙、ACL、NAT之后，设备支持的每秒新建TCP Session数应不低于400个，10G-EPON和XG-PON网关宜不低于800个。

打开防火墙、ACL、NAT之后，设备支持的最大并发TCP Session数应不低于4000个，10G-EPON和XG-PON网关宜不低于8000个。

* 1. WLAN无线性能要求
     1. WLAN吞吐量性能要求

智能家庭网关的WLAN吞吐量指标等级要求见表9，不同形态智能家庭网关应支持的WLAN吞吐量指标等级见4.3。

1. WLAN吞吐量要求

|  |  |  |  |
| --- | --- | --- | --- |
| 指标等级 | 频段（Hz） | 频宽设置（Hz） | 吞吐量要求不低于（Mbps） |
| W\_1 | 2.4G（2X2） | 20M | 85 |
| 40M | 140 |
| W\_2 | 2.4G（3X3） | 20M | 130 |
| 40M | 220 |
| W\_3 | 5G（2X2） | 20M | 85 |
| 40M | 180 |
| 80M | 400 |
| 160M | 800 |
| 80+80M | 800 |
| W\_4 | 5G（3X3） | 20M | 130 |
| 40M | 280 |
| 80M | 600 |
| 160M | 1200 |
| 80+80M | 1200 |
| W\_5 | 5G（4X4） | 20M | 170 |
| 40M | 360 |
| 80M | 750 |
| 160M | 1500 |
| 80+80M | 1500 |
| W\_6 | 2.4G（2X2）  11ax | 20M | 160 |
| 40M | 300 |
| W\_7 | 5G（2X2）  11ax | 20M | 160 |
| 40M | 300 |
| 80M | 750 |
| 160M | 1000 |
| 80+80M | 1000 |
| W\_8 | 5G（2X2）  11ax | 20M | 160 |
| 40M | 300 |
| 80M | 750 |
| 160M | 1600 |
| 80+80M | 1600 |

WLAN吞吐量指标等级应符合如下条件：

* + WLAN覆盖的范围内仅有1个终端，且为网关和WLAN终端无阻挡无干扰的室内短距离传播环境
  + 采用Chariot Throughput等脚本，测试时间应固定，例如5分钟、0.5小时、1小时等
  + 同时进行上下行吞吐量测试时，要求任一方向吞吐量不能低于总吞吐量的40％
  + 单pair/多pair/多pair上下行混和的情况下，均应满足相关指标要求
  + 对于支持双频的设备，应同时测试2.4G和5G两个频段
    1. WLAN覆盖性能要求

典型无干扰覆盖场景下（覆盖范围内仅有1个终端）的WLAN承载性能应不低于表10的要求。

1. WLAN覆盖性要求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 频宽设置 | 发射功率 | 室内可视距离100米 | 间隔1道混凝土墙 | 间隔2道普通砖墙 | 相邻的两个楼层 | 说明 |
| 默认 | 默认 | 1（Mbps） | 1（Mbps） | 1（Mbps） | 1（Mbps） | 上、下行分别考核TCP承载速率 |
| 默认 | 最大（针对支持PA及LNA的设备） | 5（Mbps） | 5（Mbps） | 5（Mbps） | 5（Mbps） |

* + 1. WLAN接收灵敏度要求

智能家庭网关的WLAN接收灵敏度应符合表11的要求。

1. WLAN接收灵敏度要求

|  |  |  |
| --- | --- | --- |
| 频段（Hz） | 模式 | 接收灵敏度 |
| 2.4G | 缺省模式 | 1M:-95dBm  11M:-86dBm  54M:-72dBm  HT20\_MCS7:-69dBm  HT40\_MCS7:-67dBm  HE20\_MCS11: -62dBm  HE40\_MCS11: -59dBm |
| PA及LNA增强模式 | 1M:-97dBm  11M:-88dBm  54M:-75dBm  HT20\_MCS7:-73dBm  HT40\_MCS7:-70dBm  HE20\_MCS11: -63dBm  HE40\_MCS11: -60dBm |
| 5G | 缺省模式 | HT20\_mcs8nss1:-66dBm  HT40\_mcs9nss1:-60dBm  HT80\_mcs9nss1:-59dBm  HE20\_mcs11nss1: -61dBm  HE40\_mcs11nss1: -58dBm  HE80\_mcs11nss1: -55dBm  HE160\_mcs11nss1: -54dBm |
| PA及LNA增强模式 | HT20\_mcs8nss1:-66dBm  HT40\_mcs9nss1:-61dBm  HT80\_mcs9nss1:-59dBm  HE20\_mcs11nss1: -62dBm  HE40\_mcs11nss1: -59dBm  HE80\_mcs11nss1: -56dBm  HE160\_mcs11nss1: -55dBm |

* + 1. WLAN设备接入能力

支持32个无线客户端设备同时在线，每秒支持16个无线客户端设备进行接入操作。

同时连接16个无线客户端设备(包括手机、PAD、PC等)时，家庭网关的WLAN吞吐量应不低于连接单个无线客户端设备指标的50%。

对于支持Wi-Fi 6(11ax)的设备，上下行应分别支持至少4/8个无线客户终端设备（2.4G频段支持4终端，5G频段支持8终端）的同时调度(DL/UL-OFDMA)。4/8个无线终端设备并发业务情况下的WLAN的吞吐量不低于单个无线终端吞吐量的60%。

* + 1. WLAN网络时延和抖动的要求

对于支持Wi-Fi 6的设备，在4/8个无线客户终端同时工作的情况下，WLAN的网络时延应该满足在80%的情况下不超过20ms。

* 1. 可靠性要求

MTBF（平均无故障工作时间）应达到30000小时以上，长时间运行时不应出现业务中断或性能下降。

网关设备在开启防火墙、NAT，10条ACL，每秒新建TCP Session数和流量均为指标要求60%的情况下，7×24小时内的会话成功率在99.999%以上。

网关设备应在超负荷运行（如用户发起的每秒新建TCP Session数及占用的WAN口带宽均超过设备实际最大能力）时不死机，负荷解除后可恢复到正常工作状态。

针对融合版，应同时满足《中国电信智能机顶盒技术要求》5.5和8的要求。

1. 运行环境要求
   1. 供电及功耗要求

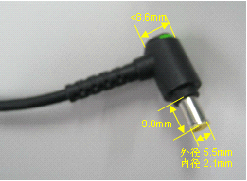
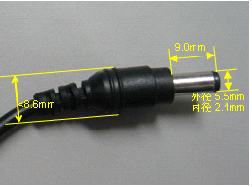
智能家庭网关（或其电源适配器）应支持本地交流供电方式，输入交流电压及其波动范围要求为：单相220V，变化范围为100～240V，频率50Hz，变化范围为5%，线电压波形畸变率小于5%。设备在此范围内应正常工作。

在正常情况下，设备的金属外壳与电源线间的绝缘电阻应不小于50MΩ。

对于使用电源适配器的家庭网关，设备自身的电源接口和电源适配器直流输出端接口应为统一的国际标准圆接口。电源适配器应符合YD/T 983的EMC要求，可选支持电力线通信功能，直流输出端电源线可选具备EMI吸收磁环，并应符合以下要求：

1. 输出电压：直流＋11.4V～＋12.6V
2. 输出端接口尺寸：

* 金属部分内径： Φ2.1±0.1mm
* 金属部分外径： Φ5.5±0.1mm
* 金属部分长度： 9.0±0.1mm
* 塑胶部分直径小于8.6mm，如图2所示。



1. 电源适配器输出端接口示意图
2. 输入端接口管脚定义：

* 内：输出正极
* 外：输出负极

1. EMI吸收磁环要求（如图3所示）：

* 磁环直径<18mm
* 磁环到插头距离<25mm



<18mm

<25mm



<25mm

<18mm

1. 电源适配器输出电缆EMI吸收磁环示意图
2. 电力线通信功能：具体参见《中国电信家庭网关总体技术要求》附录H。
3. 其它要求：

* 限流范围：1.8~3A
* 带容性负载能力不小于3000uF
* 输出纹波噪声小于120mV
* 雷击：差模±4KV，共模±4KV（B级标准）
* 静电：符合IEC61000-4-2标准，接触放电±4KV，空气放电±8KV（B级标准）
* 电压稳定度≤5%、负载稳定度≤5% (IL=20%~100%)
* 具有过流、过压（14V~16V）和短路保护能力
* 应满足LPS、RoHS要求，宜满足ErP V要求

智能家庭网关（包括电源适配器）的最大功耗要求见4.3。

* 1. 环境要求

设备应在表12所列环境条件下正常工作，且整机外壳任意点相对于环境的温度升高应不大于20℃。

1. 环境要求

|  |  |  |
| --- | --- | --- |
| **温度(℃)** | **相对湿度(％)** | **大气压力（KPa）** |
| -5~45 | 10~95 | 86~106 |

* 1. 抗电磁干扰能力

应符合YD/T 968-2002 电信终端设备电磁兼容性要求和测量方法》的要求。

* 1. 设备本身产生的电磁干扰要求

应符合YD/T 968-2002 电信终端设备电磁兼容性要求和测量方法》的要求。

* 1. 电磁兼容性

应满足YD/T1082-2000《接入网设备过电压过电流防护及基本环境适应性技术条件》规定的要求。

* 1. 过压过流保护

电源适配器应满足GBT 17626.5-2008《电磁兼容试验和测量技术 浪涌(冲击)抗扰度试验》附录A.1中安装类别4的试验等级要求，且具备4KV（差模和共模）的防护能力。

用户侧及网络侧接口应具备0.5KV（差模和共模）的防护能力。

* 1. 光接口安全性要求

对带有光接口的智能家庭网关，光接口安全性应符合IEC 60825-2中的Class 1激光安全性要求。

* 1. 视音频信号电气性能要求（仅针对融合版设备）

参见《中国电信智能机顶盒技术要求》5.5。

1. 软硬件要求
   1. 硬件要求
      1. 硬件基本要求

智能家庭网关的硬件设计应稳定可靠，能够全面满足本标准所提出的性能指标要求，并且具有良好的扩展性。

* + 1. 硬件能力要求

智能家庭网关应满足的硬件要求见4.3。

融合版设备的机顶盒模块同时应满足《中国电信智能机顶盒技术要求》5.1.1-5.1.4（含AVS2.0）。

* + 1. Flash存储空间规划要求

智能家庭网关Flash存储空间划分为8个区域，如表13所示。

1. Flash存储空间规划

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 引导区（可能包含小型软件升级核） | 终端软件（image 1） | 终端软件（image 2） | 参数区  （可选） | 文件系统 | Framework分区1（16MB） | Framework分区2（16MB） | 插件分区  (不小于96MB) |

说明：

1. 在引导区支持小型软件升级核处理升级异常恢复的情况下，双image备份要求可选，否则必选；
2. 参数区（可选）主要用以存放终端运行时所需的各种参数；
3. 文件系统可用于存放配置文件、用户数据、设备日志等；
4. Framework分区要求双备份；
5. 插件分区用于存放插件、插件应用数据及相关日志等。
6. 融合版设备的机顶盒模块同时应满足：
   * Flash类型不低于EMMC
   * 存储空间应至少包括系统分区、应用分区、恢复分区、额外分区等分区。建议系统分区在 700M至1G(Android4.4 版本)，应用分区在 1G Byte 以上，恢复分区在100M Byte 以上，额外分区（用于存放账号数据，挂载目录为/backup/，挂载权限为 system 级别）不少于 30MB。
   * 具备CTC分区，且大小不少于256MB。CTC分区应用支持自升级，恢复出厂后CTC分区应用不会回退。
     1. 指示灯要求

智能家庭网关应具有足够的指示灯，用以简单明了地指示各部分的运行状态，具体要求如表14所示。

1. 指示灯要求

|  |  |  |
| --- | --- | --- |
| **指示灯名称** | **标识文字** | **显示功能** |
| 电源状态灯 | 电源 | * 熄灭：表示网关未上电或指示灯被关闭 * 常亮：表示网关上电启动完成，已处于正常运行状态 * 闪烁（亮灭各0.25秒）：网关上电启动中 |
| PON状态灯（仅针对PON上行的设备） | 光纤 | * 熄灭：尚未OLT注册或授权成功 * 长亮：已经OLT注册或授权成功 * 闪烁：正在进行OLT注册 |
| 光信号灯（仅针对PON上行的设备） | 光信号 | * 熄灭：光信号接收正常 * 红色闪烁：光信号低于光接收机灵敏度 * 红色长亮：PON口光模块电源关断 |
| WAN口状态灯（仅针对以太网上行的设备） | 网络L | * 常亮：表示上行网口已连接，但无数据传输 * 熄灭：表示系统未上电或上行网口未连接 * 闪烁：表示有数据传输 |
| 上网状态灯 | 宽带 | * 熄灭：未配置带“INTERNET”关键字的WAN连接，或配置了但未生效，或指示灯被关闭 * 常亮：带“INTERNET”关键字的WAN连接正常生效（桥接WAN连接配置已生效、路由WAN连接已正常获取IP地址及DNS等信息） |
| WLAN口状态灯（仅针对AP内置型设备） | 无线 | * 熄灭：表示系统未上电，或无线接口（2.4GHz和5GHz）均被禁用，或指示灯被关闭 * 常亮：表示2.4GHz或5GHz无线接口已启动 * 闪烁：表示2.4GHz或5GHz无线接口有数据传输 |
| 存储状态灯 | 存储 | * 熄灭：表示系统未上电，或未连接任何存储设备（即USB和SATA均未连接存储设备），或指示灯被关闭 * 常亮：表示连接了存储设备（即USB或SATA连接了存储设备），但无数据传输 * 闪烁：表示与存储设备有数据传输 |
| 语音状态灯 | 电话 | * 熄灭：表示系统未上电或者无法注册到软交换机； * 常亮：表示已经成功注册到软交换机，但无业务流； * 闪烁：表示有业务流传输。 |
| IPTV状态灯(仅针对融合版) | iTV | * 常亮：机顶盒模块网络正常 * 红色常亮（可选）：机顶盒模块网络故障 * 熄灭：机顶盒模块待机状态 |
| 遥控器指示灯(仅针对融合版) | 红外 | * 闪烁：机顶盒模块响应遥控器操作 |

说明：

a) 所有指示灯应采用中文标识（除iTV外）；

b) PON状态灯应为蓝色，光信号灯应为红色，其它灯建议蓝色；

c) PON状态灯、光信号灯可以集成至一个灯位（标识为“光纤”），且应保持各自的颜色及显示功能。

d) 对于融合版，存储指示灯依据网关模块的状态进行显示，遥控器指示灯可以并入到IPTV状态灯中。

* + 1. 开关与按钮

应具有整机恢复出厂设置按钮，标识为“复位”，用以复位重启设备。

* + 1. 环保性要求

应满足SJ/T 11363对其有毒物质的限制和管理要求。

* 1. 软件要求
     1. 软件基本要求

软件系统应稳定，功能软件具有明显的层次结构。

Linux操作系统版本应不低于3.18，宜不低于4.4。

Linux系统内核应支持Relay和DebugFS。

应支持中文文件操作（包括中文文件名及中文文件内容），支持大于4G字节的文件的读写（即支持64位文件位置指针、文件长度等）。

宜不开启Linux系统网卡的GRO（Generic receive offload）功能。

融合版设备机顶盒模块应满足的软件基本应符合《中国电信智能机顶盒技术要求》6.1-6.6,6.9-6.16,7.1-7.15的要求。

* + 1. 操作系统软件要求
       1. 智能OS要求

智能家庭网关应支持智能OS（具体要求见附录C），支持与智家平台、手机APP的交互和管理，能够提供对外能力开放，支持插件（如ko、so和专用业务插件）的动态加载、生命周期控制（包括安装、启动、卸载、更新、停止等）、资源管理和安全管理，支持对智能OS、专用功能模块（如基本软件能力接口模块、APP管理平台接口模块等）的软件升级。

* + - 1. Linux文件系统结构要求

智能家庭网关的Linux系统根文件系统的顶层目录建议包含以下目录：

* /bin 必要的用户命令（二进制文件）
* /dev 设备文件和其它特殊文件
* /etc 系统配置文件，包括启动文件
* /lib 必要的链接库
* /mnt 安装点，用于暂时安装文件系统
* /proc 提供内核与进程信息的虚拟文件系统
* /sbin 必要的系统管理员命令（二进制文件）
* /usr 在第二层包括智能家庭网关应用程序，中间件模块以及中间件管理程序
* /var 监控程序和工具程序所存放的可变数据
* /var/local/tmp 目录用于PF\_UNIX类型socket通信的文件路径
* /webs WEB界面访问文件
  + - 1. Linux系统命令要求

Linux可执行命令存放的目录包括/bin、/sbin、 /usr/bin，在这些目录下只允许包含以下两类命令：

1. 用于当telnet服务被允许时由操作维护人员使用，用于对系统进行初步维护的系统命令：ls、ps、iptables、ping。
2. 用于实现网关业务能力的应用软件，厂商需要对所包含的应用软件进行详细技术说明。
   * + 1. 要求提供的服务

除上网业务、IPTV业务、语音业务、TR069管理、智家平台管理、加载插件所需的服务之外，家庭网关应提供FTP服务、 SAMBA服务、HTTP服务和Telnet登录服务，不应提供其它服务（参见附录G）。

FTP服务和SAMBA服务默认为仅本地开启状态；服务的开放范围（内网、外网）配置、服务端口的配置、用户名与密码的设置等只能通过ITMS+、智家平台进行。

HTTP服务默认为仅本地开启状态，不可修改。

Telnet服务默认为关闭状态；服务的启动和关闭只能通过ITMS+、智家平台进行，服务端口的配置、用户名与密码的设置等只能通过ITMS+进行。

* + 1. 插件加载要求
       1. 插件预装要求

智能家庭网关应支持电信统一开发插件（包括数据检测插件、智能组网插件、网关质量诊断插件、网络质量诊断插件、统一上报插件、云客户端扩展插件等）的出厂预装，出厂预装插件默认启动。

当执行长按恢复出厂设置时，预装插件作为非关键参数，无论是否已经被卸载或升级，都应恢复成出厂预装时的版本及状态（即清空所有的用户私有参数配置并默认启动）。

对于数据检测插件，家庭网关除满足本规范要求的插件处理机制之外，在以下场景下应保障数据检测插件安装文件夹的data子文件夹原样具有网关当前固件包中数据检测插件子文件夹MyPlugin下的所有文件（包括config、m01-b01-us、m01\_prog.tgz、m01\_sig.tgz、md5.txt）：

* 出厂预装时
* 网关固件升级，网关上的数据检测插件被升级成新固件内的数据检测插件版本时
* 长按恢复出厂设置时
* 恢复数据检测插件默认配置时

网关质量诊断插件的支持要求参见附录H。

* + - 1. 插件生命周期控制

智能家庭网关应支持根据智家平台下发的命令，对插件进行加载、启动、停止、更新、卸载等操作，详细要求如下：

1. 加载：加载后的插件自动启动
2. 启动：若插件处于停止状态，则启动插件并回应平台；若插件处于启动状态，则直接回应平台；若插件处于其它状态，则向平台报错
3. 停止：若插件处于启动状态，则停止插件并回应平台；若插件处于停止状态，则直接回应平台；若插件处于其它状态，则向平台报错
4. 更新：若插件存在，则更新插件并回应平台，同时需保持插件的生命周期状态不变（原来启动的仍启动，原来停止的仍停止）；若不存在该插件，则向平台报错
5. 卸载：若存在插件，则卸载插件并回应平台；若不存在该插件，则向平台报错
   * + 1. 插件资源及协议端口管理要求

当插件是user权限时，要求网关为每个C插件创建单独的用户运行，并根据C插件配置文件中的CPU、VirtualRam、Socket数值进行相应的资源限制。

网关应启动一个监控进程定时监控每个插件占用的FLASH存储空间大小：缺省每10分钟检查一次；当发现某个插件占用的FLASH存储空间达到其MaxStorageSize的70%时，开始每3分钟对该插件检查一次；当发现某个插件占用的FLASH存储空间超过其MaxStorageSize值时，立即停止该插件，同时将该操作及原因记入网关日志文件。

智能家庭网关应支持根据智家平台下发的命令，只允许插件在许可的协议及端口上进行网络侧、用户侧、家庭网关设备内部的数据侦听及服务提供。

家庭网关设备内部允许插件使用的端口范围为9000-9500（TCP/UDP）。

* 1. 版本号管理要求

家庭网关的硬件、软件、可单独升级软件模块（如智能OS、基本软件能力接口模块、APP管理平台接口模块等）应支持严格定义的版本号管理，应能够标识或区分所有软硬件设计及功能变化。具体要求如下：

* 版本号采用分段式设计
* 格式应为VXX.XX.################，其中“XX”代表1到2位的数字，“################”代表0~16位的数字、字母及下划线的组合
* 版本号前面两段（即“VXX.XX”段位）定义为“集中运营基线版本号”。凡是对智能网关集中运营相关功能（包括与智家平台的连接、APP管理、预装及加载插件等）产生或可能产生影响的软硬件变化（如toolchain、kernal版本更改、linux container相关模块更新等），都应变更“集中运营基线版本号”（即“VXX.XX”段位）；凡是不影响集中运营相关功能的版本变化，应只变更“集中运营基线版本号”后面的段位（即“################”段位）
* 举例：V1.0.0（集中运营基线版本号为V1.0）、V3.12.16TS\_IMSSIP\_03（集中运营基线版本号为V3.12）
  1. 上报机顶盒管理平台的设备型号要求（仅针对融合版）

机顶盒模块上报机顶盒管理平台的设备型号必须包含“CTMix-P”字符。

* 1. 上报机顶盒管理平台的硬件版本号要求（仅针对融合版）

机顶盒模块上报机顶盒管理平台的硬件版本号具体规则要求如下：

* 6位厂家OUI+6位芯片型号代码（2位为芯片厂商代码+4位芯片代码，可确认芯片型号及解码能力）+4位序号（表示同一设备型号下的硬件版本时间和顺序）+8位“厂家自定义”，共计24位
* 芯片厂商代码：由电信统一分配
* 4位芯片代码：需要芯片厂商上报对应的芯片型号及解码能力
* 4位序号：前2位为年份，后2位为当年设备硬件版本序号。如1701指2017年第一个硬件版本。

1. 基本应用要求
   1. 强制门户功能

家庭网关在路由模式下应支持强制门户功能。家庭网关应能够识别不同终端（电脑、手机、机顶盒等），在以下情况时家庭网关应强制链接到家庭门户的相关页面：

* 强制门户功能每次使能后，每个用户终端首次发送公网HTTP请求时
* 强制门户功能每次使能后，每个终端每次关联（开机连接、插拔网线及重新连接无线都视为一次关联）到家庭网关首次发送公网HTTP请求时
  1. 家庭存储

智能家庭网关应能够识别外接或内置USB/Sata存储设备的基本信息（包括设备类型、设备总容量、剩余空间），应支持不同的存储设备的命名，应支持SAMBA、DLNA等存储应用对各存储设备内容的访问。

智能家庭网关应支持FTP Server及Client。

智能家庭网关应支持基于本地UI选择具体的USB/Sata存储设备，按物理文件系统进行文件和文件夹的创建、读取、写入、修改、删除、移动和重命名等操作。

家庭网关应支持下挂存储设备（U盘、移动硬盘等）的名称管理，要求如下：

* 具有卷标的存储设备：家庭网关应使用其卷标作为该存储设备的名称
* 没有卷标的存储设备：家庭网关应根据其所连接的接口为其自动编号（从1开始）命名（如USB\_disc1）
  1. IPTV

智能家庭网关支持将公共组播VLAN内的下行视频数据流及IGMP控制报文转发到IPTV应用设备，公共组播VLAN内不应传输上行数据（包括IGMP报文）。

对于融合版设备应集成支持IPTV业务，具体要求如下：

* IPTV应用应符合《中国电信智能机顶盒技术要求》的“第7章及6.2-6.5、6.7-6.9、6.10.4、6.11、6.13-6.16、附录C-附录F”的要求。
* 应支持将机顶盒模块视作一个虚拟网口（名称缺省为“inter-iTV”）自动绑定IPTV业务所用WAN连接（如接口绑定、VLAN绑定等）。
* 融合版设备上电开机时，机顶盒模块应默认处于开机模式。在网关模块启动过程中，网络连接状态应显示“网络正在连接中，请稍候┄┄”。

应支持无STB承载IPTV业务的功能，具体要求如下：

* 应支持接受DMR的媒体请求报文，并过滤出IPTV节目源地址及协议（截取DMR媒体请求报文中GET之后第一个“/”和第二个“/”之间的内容，如“IGMP:x.x.x.x:xxxx””），向IPTV服务端请求媒体数据；
* 应支持对接收到的媒体流进行协议类型转换，将组播流转换为DLNA数据流使用的HTTP协议，并转发给DMR设备；
* 网关请求加入组播组之后，在HTTP流持续期间应主动响应WAN侧的query报文；在HTTP流中止后应向服务器发起leave报文。

1. 设备外观及界面类要求
   1. 设备外观要求
      1. 外观要求

智能家庭网关设备应易于安装、放置稳固，支持后背壁挂、盘纤和外置天线。针对外置AP型，外置天线由外置AP组件支持。

* + 1. 设备外壳标识要求

智能家庭网关设备表面应有各种端口的标识信息，其中各种端口的标识应和WEB管理页面一致，且符合表15的要求。

1. 端口标识要求

|  |  |  |
| --- | --- | --- |
| 端口 | 标识文字 | 说明 |
| 电源接口 | 直流12伏 |  |
| 网络口（针对EPON上行的设备） | 光纤E | 除非设备无需任何软硬件及配置变动就能够自动适应EPON和GPON线路，否则不可标识为“光纤E/G” |
| 网络口（针对GPON上行的设备） | 光纤G | 除非设备无需任何软硬件及配置变动就能够自动适应EPON和GPON线路，否则不可标识为“光纤E/G” |
| 网络口（针对10G EPON上行的设备） | 光纤E\_10G | 除非设备无需任何软硬件及配置变动就能够自动适应10G EPON和XG-PON线路，否则不可标识为“光纤E/G\_10G” |
| 网络口（针对XG-PON上行的设备） | 光纤G\_10G | 除非设备无需任何软硬件及配置变动就能够自动适应10G EPON和XG-PON线路，否则不可标识为“光纤E/G\_10G” |
| 网络口（针对以太网上行的设备） | 网络L |  |
| 用户侧以太网口 | * 4网口（均为GE口）设备：千兆口1、iTV、千兆口3、千兆口4 * 4网口（仅网口1为GE口）设备：千兆口、iTV、百兆口2、百兆口3 * 2网口（均为GE口）设备：千兆口1、千兆口2 * 2网口（仅网口1为GE口）设备：千兆口、百兆口 |  |
| USB口 | USB |  |
| USB口（融合版机顶盒模块专用） | USB（iTV） |  |
| 语音口 | 电话 |  |
| HDMI口 | HDMI |  |
| TF卡接口 | TF |  |
| MINI CVBS端子 | AV |  |

* 1. 智能家庭网关外壳标签要求

智能家庭网关设备表面应有相关的设备信息标识，至少包括：

1. 设备类型；
2. 设备型号；
3. 设备标识号；
4. 2.4G-1缺省名称和密钥信息；
5. 5G-1缺省名称和密钥信息（仅针对支持双频段无线的设备， 5G-1缺省名称为2.4G-1缺省名称加“-5G”后缀，5G-1缺省密钥和2.4G-1缺省密钥相同）；
6. 缺省LAN侧默认配置IP地址；
7. 缺省智能家庭网关用户帐号的用户名与密码；
8. 相关信息（客户端下载网址、缺省2.4G-1名称和密钥、缺省用户帐号的密码、设备型号、设备标识号等）的二维码。
9. 机顶盒模块编号、MAC地址等相关信息（仅针对融合版设备，要求参见《中国电信智能机顶盒技术要求》附录B）。
10. Wi-Fi6标识（仅针对支持Wi-Fi 6的设备）。
    1. 外包装要求

融合终端设备外包装应符合电信统一要求，具体参见《中国电信智能网关用户WEB管理页面及ID设计规范》。 应在外包装上标明网关设备类型。

多个带有包装盒的融合终端设备集中运输时所使用的外包装箱，应在侧面黏贴标贴，其上印刷包装箱内所有设备的设备标识条形码。

* 1. 界面要求
     1. 用户界面分类

智能家庭网关根据登录帐号（电信维护帐号或智能家庭网关用户帐号）的权限不同显示不同的管理配置界面。电信维护人员和智能家庭网关用户的具体管理配置权限参见“8.2本地UI管理和配置要求”。

* + 1. 界面整体风格要求

电信维护人员界面应整洁大方、功能区域分隔清晰、字体美观并清晰、色彩简洁清爽。

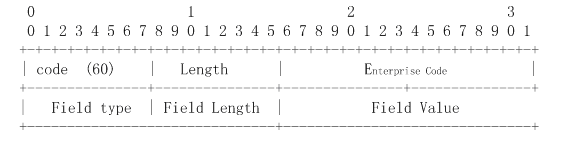
智能家庭网关用户界面应简洁明了、体验良好，方便用户浏览和使用，应符合《中国电信智能网关用户WEB管理页面及ID设计规范》的要求。

1. （规范性附录）  
   DHCP报文扩展

本附录定义家庭网关应支持的DHCP报文扩展字段，涵盖以下两种应用情形：

1. 家庭网关作DHCP Server时，在与家庭网络内的DHCP Client（如IP摄像机、机顶盒等）交互中的Option字段处理
2. 家庭网关配置DHCP认证方式的WAN连接时，作为DHCP Client与网络侧的DHCP Server交互中的Option字段处理
   1. DHCPv4 Vendor class identifier格式

DHCPv4 Vendor class identifier（Option 60）应符合RFC 2132的要求，格式如图A.1所示。



**图A.1 DHCPv4 Option 60 格式**

其中：

1. Length为Enterprise Code和Field字段（包括FieldType、Field Length、Field Value）数据的总的字节数；
2. 中国电信的企业码（Enterprise Code）：待定，暂用0x0000；
3. Field字段（包括FieldType、Field Length、Field Value）的定义见表A.1。

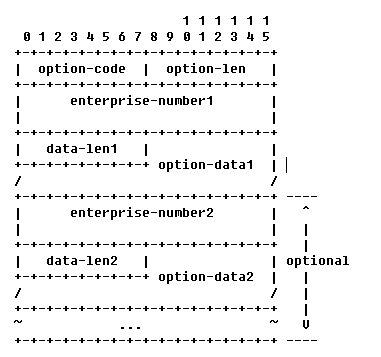
**表A.1 Field字段定义**

| Field  Type | Field  Length | Field  Value | Description |
| --- | --- | --- | --- |
| 1 | 1-32 | 设备的生产厂商名称 | 字符串格式，宜使用英文或拼音 |
| 2 | 1-32 | 设备种类 | 字符串格式，如：   * HGW * STB * Camera * Computer * Phone   …… |
| 3 | 1-32 | 设备型号 | 字符串格式，如STB-8000 |
| 4 | 1-32 | 设备的软/硬件版本号 | 字符串格式，如2.00/1.30 |
| 5 | 4n（n=1~10，n对应需映射的端口的数量） | 端口映射的协议及端口 | 一条端口映射规则使用4个字节十六进制数表示：   * 前2个字节表示协议类型：   ——0：UDP  ——1：TCP  ——2：TCP & UDP（两种协议映射同一端口）  ——其它数值：保留   * 后2个字节表示端口号，范围：1~65535 * 主要用于应用终端主动向家庭网关报告所需的端口映射配置 |
| 6～30 |  |  | 保留 |
| 31 |  | 机顶盒设备专用认证 | 具体要求参见机顶盒设备相关技术规范 |
| 32 | 11 | CTCDHCP0001 | * IPTV机顶盒在DHCP申请过程中携带的认证鉴权信息 * 全路由模式下，家庭网关在承载IPTV业务且认证方式为DHCP的路由WAN连接申请地址时应携带的认证鉴权信息 |
| 33 |  |  | 保留给机顶盒设备使用 |
| 34 | 35~73 | 设备信息及语音账号上报 | * 具体要求参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》F.40 * 家庭网关用于带“VOICE”关键字且认证方式为DHCP的WAN连接 |
| 35 | 35~73 | 设备信息及Cloud VR账号上报 | * 具体要求参见《中国电信家庭网关与增强型终端综合管理系统接口技术要求》F.40 * 智能网关用于开展Cloud VR业务且认证方式为DHCP的WAN连接 |
| 36~60 |  |  | 保留 |
| 61～255 |  |  | 待定 |

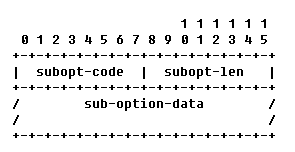
说明：一个Option60报文可以携带多个Field字段，但所携带Field字段的总字节数不应超过253。

* 1. DHCPv4 Vendor-Identifying Vendor-Specific Information Option要求

1. DHCPv4 Vendor-Identifying Vendor-Specific Information Option（Option 125）应符合RFC 3925要求， 格式如图A.2、A.3所示。



**图A.2 DHCPv4 Option 125 格式**



**图A.3 DHCPv4 Option 125的option-dataN 格式**

1. Option125特定字段内容定义

enterprise-number1：待定，暂用0x0填充。

option-data1：DHCP SERVER特定信息（根据需要添加，总字节数不可超过250），具体要求见表A.2。

**表A.2 Option 125 option-data1字段定义**

|  |  |  |  |
| --- | --- | --- | --- |
| subopt-code | Subopt  -len | sub-option-data | Description of sub-option-data |
| 1 | 1-32 | 设备的生产厂商名称 | 字符串格式，宜使用英文或拼音 |
| 2 | 1-32 | DHCP server的设备种类或分类 | 字符串格式，如：   * HGW-CT * HGW-CT-R * STB DHCP SERVER * DHCP SERVER No.5 |
| 3 | 1-32 | DHCP server的设备型号 | 字符串格式，如DS-8000 |
| 10 | 2 | 上网类业务的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 11 | 2 | IPTV业务的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 12 | 2 | ITMS+业务的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 13 | 2 | VOICE业务的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 15 | 2 | 专用业务1的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 16 | 2 | 专用业务2的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 17 | 2 | 专用业务3的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 18 | 2 | 专用业务4的VLAN ID | 2个字节十六进制数（高字节在前），值0x2000表示untag |
| 14、19～60 |  |  | （预留） |
| 65~90 |  | 保留 | * 原有IPTV通道DHCP server专用 * 全路由模式下，家庭网关应保存承载IPTV业务且认证方式为DHCP的路由WAN连接申请地址时获取的IPTV平台侧的Option 125信息，并在给机顶盒分配地址时进行原样携带（不进行TLV格式的转换） |
| 其它 |  |  | （待定） |

* 1. DHCPv4认证（携带Option60、Option125字段）过程

DHCP过程中可根据要求携带Option 60、Option 125字段，并应分别符合A.1、A.2的要求，具体过程如图A.4所示（以同时携带Option 60、Option 125为例）。

（广播包）

（广播包）

DHCP DISCOVER (Option 60)

**DHCP Client**

**DHCP Server**

DHCP OFFER (Option 125)

DHCP REQUEST (Option 60)

DHCP ACK (Option 125)

**图 A.4 携带Option 60、Option 125字段的DHCP过程**

具体描述如下：

1. DHCP Client（如应用终端或配置了DHCP WAN连接的1FE+1POTS SFU/家庭网关）上电或重启时，向网络广播一个 DHCP DISCOVER 封包以寻找DHCP Server，封包的源地址为0.0.0.0，目的地址为255.255.255.255，并携带所需的Option 60信息。
2. DHCP Server接收到来自DHCP Client的DHCP DISCOVER信息，验证Option 60信息后发出DHCP OFFER响应报文，其中包括可分配的IP地址等相关信息，并可携带所需的Option 125信息。
3. DHCP Client可能会收到多个DHCP OFFER报文，最终DHCP Client应依据DHCP OFFER报文中的Option 125信息选择匹配的DHCP Server。
4. DHCP Client将广播一个DHCP REQUEST封包，其中包含了自己所选的server信息，并携带与DHCP DISCOVER 封包相同的Option 60信息。
5. DHCP Server收到DHCP REQUEST封包后，将依据其中的Option 60信息及DHCP Client的MAC地址等信息查询DHCP Server内部的策略表，给予相应的DHCP ACK响应报文，并携带与DHCP OFFER封包相同的Option 125信息。
6. DHCP Client收到DHCP ACK报文后，从中获取自动配置信息，DHCP建立过程结束。
7. DHCP Client在断开时应该主动给DHCP Server发送DHCP RELEASE报文，DHCP Server也将释放分配给 DHCP Client的资源。
   1. DHCPv6 Option字段携带说明

DHCPv6的过程与DHCPv4相同，仅需对使用的Option代码及封包的格式进行变更：

1. DHCPv6使用Option代码16替代DHCPv4的Option代码60，封包格式应遵循RFC3315要求，如图A.5所示。

+1 2 3 +

+0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Code=16   | length|

+---------------+---------------+-------------------------------+

| enterprise-number |

+---------------+---------------+-------------------------------+

| vendor-class-len  | vendor-class-data…|

+---------------+---------------+-------------------------------+

**图 A.5 DHCPv6 Option 16 格式**

其中：

* Length为Enterprise-number、vendor-class-len和vendor-class-data字段数据的总的字节数；
* enterprise-number：待定，暂用0x0填充；
* vendor-class-len为vendor-class-data字段数据的总的字节数
* vendor-class-data字段的内容为1个或多个Field字段，该Field字段定义与DHCPv4的Option 60中的Field字段相同（包括FieldType、Field Length和Field Value的长度及含义，具体参见表A.1）。

1. DHCPv6使用Option代码17替代DHCPv4的Option代码125，封包格式应遵循RFC3315要求，如图A.6所示。

+1 2 3 +

+0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Code=17   | length|

+---------------+---------------+-------------------------------+

| enterprise-number |

+---------------+---------------+-------------------------------+

| opt-code | opt-len |

+---------------+---------------+-------------------------------+

| opt-data |

+---------------+---------------+-------------------------------+

**图 A.6 DHCPv6 Option 17 格式**

其中：

* Length为Enterprise-number、opt字段（包括opt-code、opt-len、opt-data）数据的总的字节数；
* enterprise-number：待定，暂用0x0填充；
* opt-code、opt-len、opt-data的数值定义分别等同于DHCPv4的Option125中的subopt-code、subopt-len、subopt-data（参见表B.2），opt-code和opt-len的自身字节长度应遵循RFC3315要求；
* 一个DHCPv6 Option 17报文可包含多个opt字段（包括opt-code、opt-len、opt-data）。

1. （规范性附录）  
   系统及数据安全性要求
   1. 操作系统安全

嵌入式Linux系统需使用主线长期演进Linux kernel版本。

操作系统应及时修复高危风险漏洞，版本发布时需提供业界主流工具的扫描报告（如Nessus等工具），不允许存在高风险漏洞，需提供相关安全漏洞分析或者修复报告。

* 1. 页面访问要求

对于每一个需要授权访问的页面的请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作，网页的CGI操作是否过滤通配符命令，以防止URL越权，防止XSS(Cross Site Script Execution跨站攻击)，CSRF(Cross-site request forgery跨站请求伪造)等攻击。

不应存在超出规范要求范围的配置或显示页面（含隐藏页面）。

使用Web安全扫描软件（如AppScan等工具）扫描Web服务器和Web应用，不存在高风险的漏洞；每个版本发布时，都需要进行安全扫描，提供扫描报告。

* 1. 维护入口安全

针对正式供货的终端版本，要求

1. 不保留开发调试用的串口连接，默认关闭调试通道；
2. 不保留开发调试用的隐藏页面；
3. Telnet/SSH的远程和本地端口默认全部关闭；
4. Telnet/SSH登陆需认证账号和密码，需具备防爆破功能：
   1. 同时只允许一个用户登录，应拒绝第二个用户登录；
   2. 用户登录后连续5分钟无操作，家庭网关自动退出登录状态；
   3. 密码输入连续错误3次，则再次密码验证应在1分钟以后。
5. Telnet/SSH不可采用root权限账号直接登陆，需采用普通账号登陆，且普通账号默认只提供有限且必要的Linux命令行供现场调试以及收集日志需要的shell环境。该shell环境下应该支持以下的命令：
   1. 网络相关的命令，如ip, ping, route, ifconfig, ifstatus, nslookup等；
   2. 进程状态察看相关的名字，如ps, top等；
   3. 不支持D-BUS以及中间件相关的命令；
   4. 厂商特有的命令，如查看包加速器状态和统计的命令等。
6. 对于系统维护相关的账户的默认密码，每台供货网关应随机生成。
7. Telnet/SSH端口开启后24小时，强制自动关闭，重启后重新计算。
8. 存在对外报文交互的进程禁止拥有root权限，包括web、tr069、telnet等。由此涉及的系统访问问题，提供如下参考：
   1. 将业务功能与对外交互分离，分别在单独的进程中实现；
   2. 对于必要的文件访问，可修改文件属性，使对外交互进程所在组具备该文件的访问权限；
   3. 对于root权限系统调用，借用linux内核自身机制，找到替代方法。
   4. 协议安全

开放端口列表必须符合附录G的要求，应通过端口检测工具（如NMAP工具）检测。

家庭网关应提供一定的防DoS攻击能力，满足以下要求：

* 应涵盖LAND、Ping of Death、SYN Flooding、ICMP Redirection、Smurf、Winnuke等攻击类型；
* 受到攻击时网关应不重启、不死机；
* 攻击结束后网关的功能和性能应自动恢复正常，自动恢复的延迟时间应低于30秒。

支持对防火墙规则的配置，并支持基于以下规则对报文进行过滤：

* 支持根据源MAC地址、目的MAC地址进行报文过滤；
* 支持根据源IP地址及范围段、目的IP地址及范围段进行报文过滤；
* 支持根据以太网包的传输层协议类型进行报文过滤，要求有IP/PPPoE/ARP的选项
* 支持根据IP源端口及范围段、目的端口及范围段进行报文过滤；
* 支持根据IP包的传输层协议类型进行报文过滤，要求有TCP/UDP/ICMP/TCP+UDP/ANY的选项；
* 支持对匹配规则的报文进行处理模式的选择，对匹配规则的报文的处理模式，有允许和禁止2种，默认为禁止模式。

支持IPv6 Session访问防火墙，等同IPv4 NAT访问功能，需先由内网发起访问，外网IPv6会话才能内网。

支持访客WiFi和家庭LAN网络隔离

支持配网模式和其他家庭LAN网络隔离

FTP功能，必须严格控制在权限目录下，不允许访问网关的其他目录。

SAMBA功能，必须严格控制在权限目录下，不允许访问网关的其他目录。

* 1. 敏感数据安全

口令在代码和flash系统中应该加密保存：

* 对于不需要还原口令的场景，应使用不可逆算法加密。
* 对于需要还原口令的场景，应使用分组密码算法AES128或者密钥长度更长的AES算法。

产品安全敏感数据（如：个人用户使用的口令、操作维护用途的口令、用于网络通信协议协商的身份认证Key等）不得在日志中明文记录。

产品的软件（包含软件包/补丁包），需具备数字签名完整性保护机制，在升级过程中对产品的软件（包含软件包/补丁包）进行完整性验证。

* 1. 日志安全

设备日志应支持对所有用户的登录/登出进行记录。记录内容包括用户登录使用的账号，登录是否成功，登录时间，用户使用的IP地址。

日志记录需涵盖管理面上所有的操作指令，包括：

1. 对系统配置参数的修改；
2. 对系统进行启动、重启、恢复；
3. 对业务的加载、卸载；
4. 软件的升级操作，包括远程升级和本地升级；
5. 对业务数据的创建、删除、修改；

日志记录需涵盖管理面上所有的用户活动，包括：

1. 登录和注销；
2. 用户属性（口令）的变更；
3. 用户的锁定和解锁，禁用和恢复；
4. 系统相关安全配置的变更；

设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如FTP等。

设备管理员应能够设置查看日志信息。

提供至少存储500条日志的能力。

* 1. 代码安全

对开源和自研代码进行安全扫描和修复，提交相关的扫描和分析报告。每个版本发布时，都需要进行安全扫描，提供扫描报告。

* 1. 设备安全

支持协议控制报文高优先级处理

1. 支持PPPoE的LCP、IPCP、IPv6CP等控制报文入高优先级队列优先处理
2. 支持DHCPv4/v6等协议报文进高优先级队列，系统保证优先处理
3. 支持管理报文入高优先队列不脱管，如TR-069，本地WEB管理报文，在泛洪攻击场景下，设备不脱管。

支持CPU过载保护机制

1. 网络泛洪或攻击场景下，CPU不过载，语音/IPTV等业务不受影响
2. 网络攻击CPU繁忙时，设备不脱管，TR-069和WEB可访问

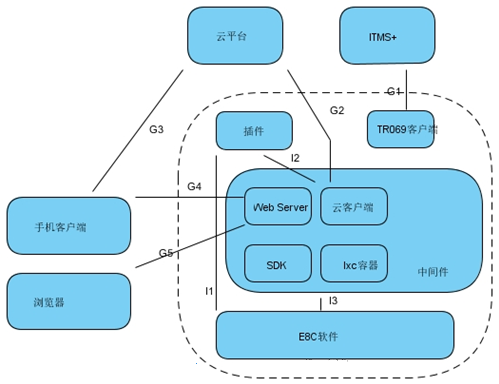
支持智能插件资源管理

1. 智能插件运行在非特权容器模式
2. 智能插件使用资源受控（CPU，线程，socket，内存，flash）

外部交互进程（DHCP，PPPoE，DNS，CWMP，WEB Server等）必须非root运行，防止交互进程被攻破后，只能获取非root权限，从而防止破坏者获取更多权限和资源

支持安全启动（参见附录M），网关软件版本签名由设备厂家签发。

1. （规范性附录）  
   智能OS（基于嵌入式Linux智能OS）技术要求
   1. 架构说明
      1. 总体架构

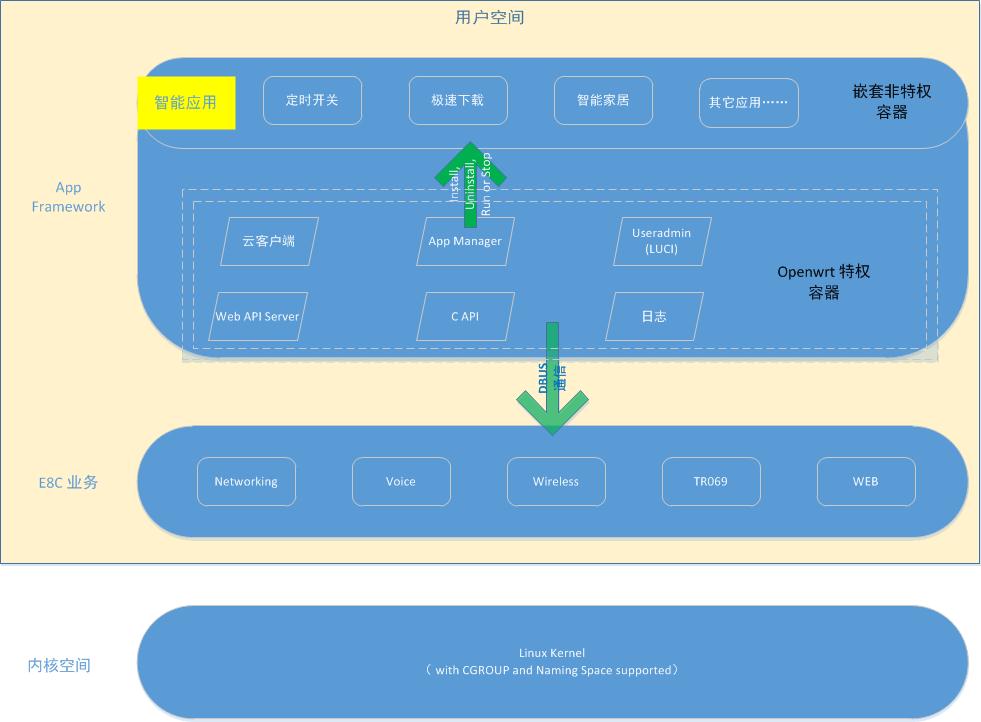
****

**外部接口**

* 网关和ITMS接口（G1）
  + 业务开通、设备诊断等
* 网关和云平台接口（G2）
  + 网关配置和信息查询
  + 平台能力开放接口，如用户认证鉴权、消息推送等
* 手机客户端和网关接口（G4）
  + 手机客户端上部分功能通过G4接口直接和网关交互
* 浏览器和网关接口（G5）
  + Telecomadmin管理界面
  + Useradmin管理界面，包括网关的简单配置界面，以及第三方插件的管理界面

**内部接口**

* 插件和中间件接口（I2）
  + 中间件对插件的生命周期进行管理。
  + 插件调用API，调用云平台的能力。
  + 插件在Web API Server中嵌入Luci脚本，实现插件的管理界面。
* 中间件和DBus间的接口（I3）
  + DBus接口将网关能力集暴露给中间件。
  + 插件通过中间件提供的API，设置或获取网关能力。
* I1接口已经集成在中间件中，不需要再单独列出。
  + 1. 网关内部架构



Framework由中国电信提供，内核和E8C业务（含电信维护账号页面）由网关厂商提供。

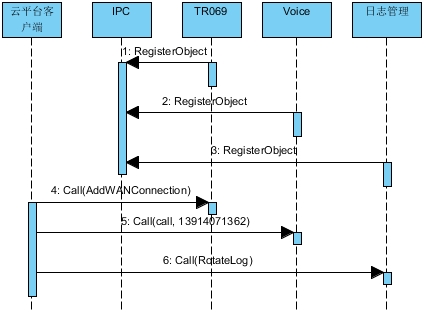
网关厂家将E8C业务封装成DBus的服务(名为com.ctc.igd1)。

Framework和E8C业务之间通过DBus总线通信，通信过程要遵循标准的和电信扩展的DBus协议。

* + 1. IPC Service

IPC Service模块将网关的业务能力封装成IPC对象和接口，注册到DBus总线上，云平台客户端或APP通过IPC接口可以实现远程调用网关能力。

下图是网关能力的向IPC注册，云平台客户端远程调用的过程：



1. TR069启动时，向IPC模块注册接口，暴露TR069部分业务能力
2. Voice模块启动时，向IPC模块注册接口，暴露语音模块底层能力
3. 日志管理模块启动时，向IPC模块注册接口，暴露日志管理能力
4. 云平台要增加一个WAN连接，云平台客户端收到请求后，IPC调用TR069模块的AddWANConnection接口。
5. 云平台要呼叫一个号码，云平台客户端收到请求后，IPC调用Voice模块的call接口，带上被叫号码作为参数。
6. 云平台要回滚设备的日志，云平台客户端收到请求后，IPC调用日志管理模块的RotateLog接口。
   1. 系统要求
      1. 系统软件要求

对操作系统要求如下：

1）应使用Linux内核，版本应不低于3.18，宜不低于4.4。当版本不支持LXC时，应将LXC相关代码移植到所用的版本。

2）内核必须支持overlayfs。

3）按照下图要求，打开所有lxc选项。

|  |
| --- |
| \* General setup  \* Control Group support  -> Namespaces cgroup subsystem  -> Freezer cgroup subsystem  -> Cpuset support  -> Simple CPU accounting cgroup subsystem  -> Resource counters  -> Memory Resource Controller for Control Groups  \* Group CPU scheduler  -> Basis for grouping tasks (Control Groups)  \* Namespaces support  -> UTS namespace  -> IPC namespace  -> User namespace  -> Pid Namespaces  -> Network namespace  \* Device Drivers  \* Character devices  -> Support multiple instances of devpts  \* Network device support  -> MAC-VLAN support  -> Virtual ethernet pair device  \* Networking  \* Networking options  -> 802.1d Ethernet Bridging  \* Security options  ->File POSIX Capabilities |

4）要求使用不低于musl-libc1.1.22版本的C库，应不修改musl-libc的代码，如果使用glibc，版本不应该低于2.22。

* + 1. 系统分区及中间件集成要求
       1. 中间件的更新能力

中间件平台支持三种形式的更新:

1. 中间件系统固件升级 (Framework Upgrade)

中间件系统更新，核心程序框架发上较大程度的更新，譬如, 资源框架，安全模型等核心组件的升级，这时会需要中间件固件的升级。这种升级的频度往往相对是比较低的。

1. 中间件的系统更新 (Framework Update)

中间的的系统更新，往往是中间件的某些功能模块发生了升级更新，譬如，云平台客户端的升级更新，功能库的增加及升级等。

1. 插件安装及升级

第三方插件的升级，这个是高频度的升级更新行为，而且用户对于这类的更新是可控的。

* + - 1. 中间件对系统分区及文件系统的要求

1. 设备系统应满足如下分区要求:

* Framework 系统分区

用于存放中间件的核心系统，分区以只读方式挂载到/opt/upt/framework1 挂载点上，防止系统文件被误删除。

* Framework 系统备份分区

实现framework的双备份机制，防止中间件系统固件升级时，如果发生不可预知的掉电行为，网关还能启动升级之前的中间平台运行。

* Framework apps 分区

用于保存动态安装的插件，以及中间件的系统更新。

1. 应支持如下文件系统要求:

* 只读文件系统（用于Framework 系统分区及系统备份分区）:

Squash FS 4.0 以上（含4.0）, 要求支持xz 压缩算法。

* 可读写文件系统 (用于Apps 分区)

Ubifs, 要求使用zlib压缩算法。

1. 应支持如下分区大小要求：

* 至少提供128MB给中间件平台使用。

Framework1: 16M.

Framework2: 16M.

Apps: >=96M

* + - 1. 中间件集成要求

1. framework. squashfs文件 (squash FS image)

设备厂家需要将此image烧录到Framework1 MTD 分区中。

1. Dbus 工具(包含dbus配置文件的需求)

设备厂家需要将此 DBus 工具集成进各自的软件里面，包含配置文件的存放路径。

1. SAF启动程序 (Smart Application Framework)

将saf程序放置于网关的启动脚本中去

并且需要将三个mtd分区的名字传递过去

saf-xxx service a b c（a,b,c分别对应framework1，framework2和apps的mtd分区号）

应对saf-xxx启动的进程具备守护措施，保证进程死掉后可以自动恢复。

1. 设备厂家需要在跟文件系统里面准备好一下相应的挂载点

/opt/upt/framework

/opt/upt/apps

1. 终端产品固件要求:

终端产品固件必须支持两种形态，一种是包含中间件的形态，一种是不包含中间件的形态。

包含中间件的固件升级的时候，请烧录到中间件备份分区。

终端产品固件升级（包括通过ITMS、智家平台发起的升级）时，应先暂停中间件的运行。

* + - 1. 中间件管理接口及升级流程要求

1. 应支持如下中间件管理接口:

服务名: com.ctc.saf1

对象路径: /com/ctc/saf1

接口: com.ctc.saf1.framework

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| SAFVersion | STRING(31) | read | 无 | SAF 版本号 | 1.0 |
| FrameworkVersion | STRING(63) | read | 无 | 中间件版本号 | 1.0 |
| BackupFrameworkVersion | STRING(63) | read | 无 | 备份中间件版本号 | 1.1 |
| CloudClientVersion | STRING(63) | read | 无 | 云客户端版本号 | 1.0 |
| BackupMTD | BYTE | read | 无 | 中间件备份分区MTD号 | 1.0 |
| ActiveMTD | BYTE | read | 无 | 中间件活动分区MTD号 | 1.0 |

方法：

* UpdateMTDInfo(OUT UINT32 result)

更新分区信息

result = 0, 表示更新成功。

* Pause(IN UINT32 interval, OUT UINT32 result)

暂停Framework

interval: 表示暂停的时间，单位是分钟，如果是0, 表示重启。

result = 0, 表示操作成功。

* Upgrade(IN STRING filename, OUT UINT32 result)

升级Framework

* Switch(OUT UINT result)

切换到另外一个中间件运行

* Restore(OUT UINT result)

恢复到初始设置

1. 应支持如下中间件升级流程:
2. 暂停framework

bus-send --system --print-reply --dest=com.ctc.saf1 /com/ctc/saf1 com.ctc.saf1.framework.Pause uint32:"10"

1. 获取备份分区

dbus-send --system --print-reply --dest=com.ctc.saf1 /com/ctc/saf1 com.ctc.igd1.Properties.Get string:"com.ctc.saf1.framework" string:"BackupMTD"

1. 将Framework烧录到该备份分区。
2. 切换活动分区信息

dbus-send --system --print-reply --dest=com.ctc.saf1 /com/ctc/saf1 com.ctc.saf1.framework.Switch

1. 重新启动中间件

dbus-send --system --print-reply --dest=com.ctc.saf1 /com/ctc/saf1 com.ctc.saf1.framework.Pause uint32:"0"

1. 长按恢复出厂设置的时候，应支持恢复插件到预置状态：

通过调用com.ctc.saf1.framework接口中的Restore方法实现。

* + - 1. 获取平台地址和连接状态

服务名: com.ctc.cloudclient1

对象路径: /com/ctc/cloudclient1

接口: com.ctc.cloudclient1

方法：

* GetPlatformServers(OUT STRING ServerStatus, OUT UINT result)

返回JSON格式平台信息

{

"BSS平台": {

"Server": "bss.189cube.com:12112",

"Status": “连接结束"

},

"主能力平台": {

"Server": "101.95.49.44:60002",

"Status": "心跳保活中"

}

}

* 1. 预置软件配置要求
     1. DBus
* 介绍

dbus开发包包括dbus-daemon消息路由程序，dbus协议库libdbus，一些dbus工具(如dbus-monitor/dbus-send/dbus-uuidgen)。

* SDK

DBus的工具和动态库由电信统一提供，要求集成安装到固件中，供固件，中间件和APP使用。

* + 1. glib
  + 介绍

glib是一个通用的是linux下通用的C语言库，其中的gio实现了dbus协议，取名为gdbus，可以方便的实现dbus的服务端server和客户端client。

在网关的开发中，要求dbus的客户端和服务端都使用glib下的gdbus来开发，而不是使用C.3.1中的libdbus。

* 版本号

建议使用2.56.1版本。

* Configure 选项

--enable-shared \

--enable-static \

--enable-debug=no \

--disable-selinux \

--disable-fam

* Make选项

无

* 安装文件

库文件（libgio/libgobject/libgthread/libglib/libgmodule）安装到/usr/lib/glib-2.0目录

Gdbus程序安装到/usr/bin目录

* 默认配置

无

* 启动

无

* SDK

Glib相关头文件安装到SDK中，供中间件厂商和APP使用。

* + 1. lxc
* 介绍

lxc(linux container)，用来创建和管理linux下的系统或应用容器，提供了一系列的用户态的工具，如lxc-start、lxc-stop、lxc-execute等。

* SDK

电信提供的中间件基于容器技术, 集成了lxc组件,厂商需要集成中国电信提供的中间件启动及管理程序(SAF)到固件中。

* + 1. DPI

支持DPI插件的网关接口要求参见<C.10 DPI对网关接口要求>

* 1. WEB要求
     1. 权限分级界面

政企场景的Telecomadmin Web管理界面和Useradmin Web管理界面，均沿用E8C的原有界面。

公客场景的Telecomadmin Web管理界面，还是沿用E8C的现有界面，默认8080端口。

公客场景的Useradmin Web管理界面，由电信定制开发，使用OpenWrt的Luci作为其web框架，默认80端口。

用户输入网关默认地址后，默认展现80端口的Useradmin Web管理界面，页面在提交请求时判断用户密码，如果是telecomadmin的正确密码，则采用POST请求跳转到8080端口对应的E8C管理页面；如果不是telecomadmin的正确密码，则由Useradmin Web管理界面处理。

1）telecomadmin对应的CGI URI：http://hostip:8080/login.cgi

2）POST里面的报文包含两个form item, 分别是username & psd

发送POST的参考代码如下：

HTML代码如下：

<form method="post" id="argform">

<input type="hidden" name="username" id="username" value="telecomadmin" />

<input type="hidden" name="psd" id="psd" value="" />

<input type="submit" style="display:none"/>

</form>

JS实现代码如下，

if (Valid\_TA\_PW)

{

document.getElementById("argform").action = location.protocol + "//" + location.host.split(":")[0] + ":8080/login.cgi";

document.getElementById("psd").value = $("#login\_password").val();

document.getElementById("argform").submit();

}

* + 1. 插件配置下发记录的通知

Framework将插件配置下发的记录文件保存在/tmp/plugin.log文件中，供Telecomadmin UI显示插件配置下发状态。

文件格式示意如下:

2016-07-15 08:00:00 安装xxxx插件。

2016-07-15 08:10:00 升级xxxx插件。

2016-07-15 08:20:00 卸载xxxx插件。

2016-07-15 08:30:00 配置xxxx插件。

2016-07-15 08:40:00 启动xxxx插件。

2016-07-15 08:50:06 停止xxxx插件。

2016-08-31 12:01:00 系统已使用内存超过MemLimit，停止低优先级插件。

2016-08-31 13:00:01 插件xxxx占用flash超过插件设置xxxx，已停止该插件。

* 1. LXC容器技术要求
  2. DBus总体要求
     1. 服务名
     + 系统软件提供的DBus服务，命名为com.ctc.igd1。
     + saf提供的DBus服务，命名为com.ctc.saf1。
     + Appframework提供DBus服务，命名为com.ctc.appframework1。
     + 云客户端提供的DBus服务，命名为com.ctc.cloudclint1。
     + App提供的DBus服务，按照DBus服务命名规则命名com.<公司名>.<模块名+版本号>，保证不冲突即可。
     1. 兼容性
* 在定义DBus服务时，服务名、接口名、Object Path中，要求都嵌入了同样的版本号信息，比如DBus接口名com.ctc.igd1，其中1即为版本号。
* 当接口定义升级，并且无法向后兼容时，版本号+1。
* 一般情况下，接口定义升级尽量保持向后兼容，即不允许删除现有DBus接口、不允许修改现有DBus接口签名，只允许增加新的DBus接口。
* App在Manifest文件中声明依赖的服务名，比如com.ctc.igd1。服务名可以为多个，比如com.ctc.igd1, com.ctc.igd2，表示App在支持这两个服务的设备中，均可运行。

当这个服务名和网关提供的服务名不匹配时，平台应拒绝网关下载App，App Framework应拒绝安装App。

当网关升级后，重新校验依赖关系，如果服务名不匹配，应删除App。

* App应在Manifest文件中声明其提供的DBus服务名及依赖的服务名，平台可以据此推送正确的版本给客户进行安装。
  + 1. 效率
  + DBus服务的实现必须支持并发访问。
  + DBus接口的响应时间一般不应超过200ms。
  + 要求DBus服务和DBus-Deamon具备守护措施（间隔应小于15秒），进程死掉后应恢复。
  1. 扩展的DBus接口要求

要求所有注册到DBus总线的对象都要支持两个DBus标准接口：org.freedesktop.DBus.Peer和org.freedesktop.DBus.Introspectable。

另外，要求所有注册到DBus总线的对象都要实现电信扩展的两个Dbus接口：com.ctc.igd1.Properties和com.ctc.igd1.ObjectManager。

* + 1. com.ctc.igd1.Properties

本接口是对org.freedesktop.DBus.Properties接口的扩展，接口包含如下方法：

com.ctc.igd1.Properties.Get(in STRING interface\_name,

in STRING property\_name,

out VARIANT value);

com.ctc.igd1.Properties.Set (in STRING interface\_name,

in STRING property\_name,

in VARIANT value);

com.ctc.igd1.Properties.GetAll (in STRING interface\_name,

out DICT<STRING,VARIANT> props);

com.ctc.igd1.Properties.SetMulti (in STRING interface\_name,

in DICT<STRING,VARIANT>props);

Get/Set/GetAll接口和DBus规范定义一致。

* + G\_DBUS\_ERROR\_SET\_FAILED = 8100, /\* Set Error \*/

新增的方法是SetMulti，用于一次设置多个Property，减少交互次数，提高服务端的处理效率。

本接口的信号为com.ctc.igd1.Properties.PropertiesChanged，和Dbus规范标准信号org.freedesktop.DBus.Properties.PropertiesChanged作用类似，本文中所有对象要求都必须实现本接口。

本接口的实现要求具备原子性，即属性要么全部设置成功，要么全部设置失败。不允许出现部分属性设置成功，部分属性设置失败的情况。

本接口的实现要考虑效率，尽可能一次性将属性设置到系统软件中，减小本接口的响应时间。

对有Enable属性的接口，当Enable为0时，调用Set/SetMulti进行设置，可以立即生效，也可以等到Enable为1时生效，由实现者决定。

当Enable为1，或者没有Enable属性时，设置应立即生效。

SetMulti方法GDBusErrorEntry的定义：

* + {G\_DBUS\_ERROR\_SETMULTI\_FAILED , "org.freedesktop.DBus.Error.SetMultiError"},
  + {G\_DBUS\_ERROR\_SETMULTI\_ROLLBACK\_FAILED"org.freedesktop.DBus.Error.SetMultiRollbackError"},

SetMulti方法Error Code：

* + G\_DBUS\_ERROR\_SETMULTI\_FAILED = 8000, /\* SetMulti Error \*/
  + G\_DBUS\_ERROR\_SETMULTI\_ROLLBACK\_FAILED = 8001, /\* SetMulti Rollback Error \*/

如果SetMulti调用失败，ErrorName按照上述统一为“org.freedesktop.DBus.Error.SetMultiError”及“org.freedesktop.DBus.Error.SetMultiRollbackError”。

Error Message 部分，原则上能把出错的参数表达出来即可。

* + 1. com.ctc.igd1.ObjectManager

本接口是对org.freedesktop.DBus.ObjectManager的扩展，包含方法如下：

com.ctc.igd1.ObjectManager.GetManagedObjects(outDICT<OBJPATH,DICT<STRING,DICT<STRING,VARIANT>>>objpath\_interfaces\_and\_properties);

com.ctc.igd1.ObjectManager.AddObject(out OBJPATH objpath);

com.ctc.igd1.ObjectManager.DeleteObject(in OBJPATH objpath);

com.ctc.igd1.ObjectManager.RemoveAllObjects();

新增的方法是AddObject, DeleteObject和RemoveAllObjects，用于增加和删除和清空下面的所有对象。RemoveAllObjects方法要求具备原子性，要么全部删除，要么返回失败，并且原来对象保持不变。

本接口的信号为com.ctc.igd1.ObjectManager.InterfacesAdded和com.ctc.igd1.ObjectManager.InterfacesRemoved，和DBus规范一致。

* 1. 系统服务及接口要求

本章节定义系统软件需要实现的DBus接口和对象。

这些接口和对象涵盖了《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》中定义的平台接口，《中国电信智能家庭网关技术要求》中定义的网关本地接口。同时根据useradmin管理界面的需求，对接口进行了扩充。

所有的时间格式的对象属性，统一按照格式“YYYY-MM-DD HH:MM:SS”, 例如“2016-07-11 08:00:00”。如果没有特殊说明，所有时间为GMT+8时间。

所有MAC地址参数的格式，统一定义为12字节的十六进制ASCII码，并且字母应大写，如"048D3A750406"。

5G无线属性及相应的频段切换等功能接口仅需双频无线设备支持。

* + 1. DBus接口
       1. **com.ctc.igd1.DeviceInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| BusinessStatus | BYTE | read | 有 | 业务下发状态，1 – 成功，0 – 失败 | 1.0 |
| Manufacturer | STRING(63) | Read | 无 | 设备厂商 | 1.0 |
| MAC | STRING(12) | read | 无 | 设备MAC，格式为0123456789AB | 1.0 |
| SWVersion | STRING(63) | read | 无 | 软件版本号 | 1.0 |
| HDVersion | STRING(63) | read | 无 | 硬件版本号 | 1.0 |
| ITMSProtocolVersion | STRING(63) | read | 无 | 表示当前和ITMS通信协议的版本号；格式为“A|B“。其中：   * A为集团正式发布的网关接口规范编号，如“2014 SX-013”或” Q/CT 2271-2014 “ * B为增补编号，具体格式为“a“+增补编号，如”a1.0“，无增补要求时为空且省略前置分隔符“|” | 1.0 |
| SpecVersion | STRING(63) | read | 无 | 表示符合智能网关技术规范版本号；格式为"A|B"。其中：   * A为集团正式发布的网关技术规范编号，如" Q/CT 2603-2016” * B为增补编号，具体格式为"a"+增补编号，如“a1.0”，无增补要求时为空且省略前置分隔符“|” | 1.0 |
| DBusInterfaceVersion | STRING(16) | read | 无 | 表示DBus接口的版本号  当前版本号为1.2 | 1.0 |
| ProductClass | STRING(63) | read | 无 | 网关型号 | 1.0 |
| CPUClass | STRING(63) | read | 无 | CPU型号（主芯片厂商+主芯片完整型号） | 1.0 |
| DevType | STRING(127) | read | 无 | 设备型号（OUI-SN） | 1.0 |
| DevType1 | STRING(8) | read | 无 | 设备类型（X\_CT-COM\_DeviceType） | 1.0 |
| DevType2 | STRING(127) | read | 无 | 设备类型（用于Web UI页面的设备类型显示，如：“EPON天翼网关(4口单频)”，具体参考《中国电信智能网关用户WEB管理页面及ID设计规范》） | 1.0 |
| Capability | STRING(63) | read | 无 | 设备能力（X\_CT-COM\_Capability） | 1.0 |
| FlashSize | UINT32 | read | 无 | Flash大小，单位byte | 1.0 |
| RamSize | UINT32 | read | 无 | RAM大小，单位byte | 1.0 |
| DevName | STRING(127) | readwrite | 有 | 设备名称（可供用户修改）, 最长为128, UTF8编码，初始为空 | 1.0 |
| CPUUsage | BYTE | read | 无 | CPU占用率，百分比表示，如80表示80% | 1.0 |
| MEMUsage | BYTE | read | 无 | 内存占用率，百分比表示 | 1.0 |
| FlashUsage | BYTE | read | 无 | Flash占用率 | 1.0 |
| SysDuration | UINT32 | read | 无 | 系统上电运行时间，单位为秒 | 1.0 |
| HGWSleep | BYTE | read | 无 | 表示网关休眠当前状态，0：当前状态为休眠模式；1：当前状态为正常模式； | 1.0 |
| DevStyle | STRING(32) | Read | 无 | 网关扩展形态标识  空：没有该属性或属性为空，表示标准的公客网关；  “Mix2018”：表示融合网关公客网关（只有两个LAN口）；  “MixEnterprise2018”：表示融合网关政企网关（只有两个LAN口，无useradmin管理页面，不预装组网插件，不可绑定手机客户端）；  zw\_auto：表示标准的公客网关，且组网插件一键配置打开；  Mix2018\_zw\_auto：表示融合网关公客网关（只有两个LAN口），且组网插件一键配置打开；  MixEnterprise2018\_zw\_auto：表示融合网关政企网关（只有两个LAN口，无useradmin管理页面，不可绑定手机客户端），且组网插件一键配置打开。 | 1.12 |

* + - 1. **com.ctc.igd1.NetworkInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| UPLink | UINT32 | read | 无 | 上行方式（X\_CT-COM\_ UPLink） | 1.0 |
| IPv6 | BYTE | read | 无 | 是否支持IPv6双栈能力其中0：不支持IPv6；1：支持IPv6，2：支持IPv6及DS—lite | 1.0 |
| VLANbind | BYTE | read | 无 | 是否支持VLAN绑定能力，0：不支持，1：支持 | 1.0 |
| WiFiMode | STRING(127) | read | 无 | WiFi模式：802.11a /802.11g/802.11n/802.11ac（要求列出网关支持的所有WiFi模式，以/分割） | 1.0 |
| PONDuration | UINT32 | read | 无 | PON注册授权成功持续时间，单位为秒（从PON线路的逻辑ID认证成功开始计时） | 1.0 |
| PPPOEDuration | UINT32 | read | 无 | PPPOE拨号成功持续时间，单位为秒 | 1.0 |
| LAN1Status | BYTE | read | 有 | LAN1链路状态，0 – 未连接，1 – 已连接 | 1.0 |
| LAN2Status | BYTE | read | 有 | 同上 | 1.0 |
| LAN3Status | BYTE | read | 有 | 同上 | 1.0 |
| LAN4Status | BYTE | read | 有 | 同上 | 1.0 |
| LAN1TXByte | UINT64 | read | 无 | LAN1接口发送字节数，单位为byte | 1.0 |
| LAN1RXByte | UINT64 | read | 无 | LAN1接口接收字节数，单位为byte | 1.0 |
| LAN2TXByte | UINT64 | read | 无 | LAN2接口发送字节数，单位为byte | 1.0 |
| LAN2RXByte | UINT64 | read | 无 | LAN2接口接收字节数，单位为byte | 1.0 |
| LAN3TXByte | UINT64 | read | 无 | LAN3接口发送字节数，单位为byte | 1.0 |
| LAN3RXByte | UINT64 | read | 无 | LAN3接口接收字节数，单位为byte | 1.0 |
| LAN4TXByte | UINT64 | read | 无 | LAN4接口发送字节数，单位为byte | 1.0 |
| LAN4RXByte | UINT64 | read | 无 | LAN4接口接收字节数，单位为byte | 1.0 |
| WANLinkStatus | STRING(8) | read | 有 | WAN链路状态，0 – 未连接，1 – 已连接 | 1.0 |
| WIFIModuleStatus | STRING(8) | read | 有 | 0 – WiFi模块关闭，1 – WiFi模块开启 | 1.0 |
| WANConnectionStatus | STRING(63) | read | 有 | Internet WAN IPv4连接状态，对应TR098 WANIPConnection.{i}.ConnectionStatus和WANPPPConnection.{i}.ConnectionStatus | 1.0 |
| PPPoEDialReason | STRING(63) | read | 无 | PPPoE连接拨号失败原因  WANPPPConnection.{i}.LastConnectionError | 1.0 |
| IPv6\_WANConnectionStatus | STRING(63) | read | 有 | Internet WAN IPv6连接状态 | 1.0 |
| IPv6\_PPPoEDialReason | STRING(63) | read | 无 | PPPoE连接拨号失败原因  和V4可能不一样，需要再查一下 | 1.0 |
| LANIPAddr | STRING(15) | read | 有 | LAN侧IPv4管理地址 | 1.0 |
| LANIPv6Addr | STRING(45) | read | 有 | LAN侧IPv6管理地址 | 1.1 |
| WANIPAddr | STRING(15) | read | 有 | Internet WAN IPv4地址 | 1.0 |
| WANIPv6Addr | STRING(45) | read | 有 | Internet WAN IPv6地址 | 1.0 |
| WiFiBytes | UINT64 | read | 无 | WiFi接口发送接收字节数，单位为byte | 1.0 |
| WiFiTxBytes | UINT64 | read | 无 | WiFi接口发送字节数，单位为byte | 1.0 |
| WiFiRxBytes | UINT64 | read | 无 | WiFi接口接收字节数，单位为byte | 1.0 |
| WANBytes | UINT64 | read | 无 | Internet连接发送接收字节数，单位为byte | 1.0 |
| WANTxBytes | UINT64 | read | 无 | Internet连接发送字节数，单位为byte | 1.0 |
| WANRxBytes | UINT64 | read | 无 | Internet连接接收字节数，单位为byte | 1.0 |

* + - 1. **com.ctc.igd1.WANConnectionInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Index | STRING(8) | read | 无 | WAN的序号 | 1.0 |
| WANName | STRING(63) | read | 无 | WAN连接名称命名方式：序号\_关键字\_桥接或路由方式\_VID\_数字 | 1.0 |
| IfName | STRING(32) | read | 无 | 接口名称 | 1.0 |
| ServiceList | STRING(32) | read | 有 | WAN连接承载的业务列表，目前定义：“TR069”,“INTERNET”,“VOIP”,“OTHER” | 1.0 |
| ConnectionType | STRING(32) | read | 无 | 连接类型 | 1.0 |
| VLANID | UINT32 | read | 无 | VLANID号（值0x2000表示untag） | 1.0 |
| VLAN8021P | UINT32 | read | 无 | 8021p优先级 | 1.0 |
| Protocol | STRING(32) | read | 无 | 使用协议类型 | 1.0 |
| ConnectionStatus | STRING(32) | read | 有 | 连接状态 | 1.0 |
| IPAddress | STRING(15) | read | 有 | IP地址 | 1.0 |
| SubnetMask | STRING(15) | read | 有 | 子网掩码 | 1.0 |
| Gateway | STRING(15) | read | 有 | 网关地址 | 1.0 |
| PPPoEPassthrough | BOOLEAN | read | 无 | 是否开启路由桥接混合模式 | 1.2 |
| SpeedLimit\_UP | UINT32 | read | 无 | 基于WAN接口限速（上行），数值为”n”, 表示限速为n\*512kbps, 0表示不限速，默认值为0 | 1.2 |
| SpeedLimit\_DOWN | UINT32 | read | 无 | 基于WAN接口限速（下行），数值为”n”, 表示限速为n\*512kbps, 0表示不限速，默认值为0 | 1.2 |
| DNS1 | STRING(15) | read | 有 | 首选DNS | 1.0 |
| DNS2 | STRING(15) | read | 有 | 备选DNS | 1.0 |
| IPv6\_ConnectionStatus | STRING(32) | read | 有 | IPv6连接状态 | 1.0 |
| IPv6\_IPAddress | STRING(45) | read | 有 | IPv6的IP地址 | 1.0 |
| IPv6\_PrefixLength | STRING(8) | read | 有 | IPv6的前缀长度 | 1.0 |
| IPv6\_Gateway | STRING(45) | read | 有 | IPv6的网关地址 | 1.0 |
| IPv6\_DNS1 | STRING(45) | read | 有 | IPv6的首选DNS | 1.0 |
| IPv6\_DNS2 | STRING(45) | read | 有 | IPv6的备选DNS | 1.0 |
| IPv6\_Prefix | STRING(45) | read | 有 | IPv6协商前缀 | 1.0 |
| NATv6Enable | BOOLEAN | read | 无 | NATv6功能是否启用，默认值：false | 1.2 |
| RxBytes | UINT64 | read | 无 | 接收字节数 | 1.0 |
| TxBytes | UINT64 | read | 无 | 发送字节数 | 1.0 |
| RxPkts | UINT64 | read | 无 | 收包个数 | 1.0 |
| TxPkts | UINT64 | read | 无 | 发包个数 | 1.0 |
| IPv6\_AddressOrigin | STRING(32) | read | 无 | X\_CT-COM\_IPv6IPAddressOrigin  地址分配机制，取值范围有：  AutoConfigured：通过RA通告自动获取  DHCPv6：默认值  Static  None | 1.1 |
| IPv6\_PrefixOrigin | STRING(32) | read | 无 | X\_CT-COM\_IPv6PrefixOrigin  前缀地址分配机制：  PrefixDelegation：默认值;  Static  None | 1.1 |
| IPv6\_PrefixPltime | UINT32 | read | 无 | X\_CT-COM\_IPv6PrefixPltime  公告前缀的preferred lifetime，单位：秒 | 1.1 |
| IPv6\_PrefixVltime | UINT32 | read | 无 | X\_CT-COM\_IPv6PrefixVltime  公告前缀的valid lifetime，单位：秒 | 1.1 |
| DSLite\_Enable | BOOLEAN | read | 无 | 是否启用DS-lite功能，缺省值：false | 1.1 |
| DSLite\_AftrMode | BYTE | read | 无 | AFTR配置模式，0：为自动获取方式。1：为配置方式，缺省值：0 | 1.1 |
| DSLite\_Aftr | STRING(63) | read | 无 | 当X\_CT-COM\_AftrMode值为1时，需要配置的AFTR地址。可为域名方式或者IP地址方式。 | 1.1 |
|  |  |  |  |  |  |

* + - 1. **com.ctc.igd1.WANConnectionDb**

**方法**

* GetWANConnByName(IN STRING name, OUT OBJECT\_PATH path, OUT UINT32 result，OUT STRING errdesc);

根据WAN接口名字（对应com.ctc.idg1.WANConnectionInfo中的WANName属性）获取对应WANConnectionInfo对象的路径，索引用于查询连接详细信息，对应QUEYR\_WAN\_INFO接口

result：0（成功）/1（失败）。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* GetInternetConnIndex(OUT OBJECT\_PATH path, OUT UINT32 result，OUT STRING errdesc);

获取Internet路由正常上网连接的对象路径（根据com.ctc.idg1.WANConnectionInfo中的 ServiceList返回对应的Internet路由正常上网连接对应的com.ctc.idg1.WANConnectionInfo路径）

result： 0（成功）/1（失败）

errdesc：若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.WiFiInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本号 |
| Enable2G | BOOLEAN | readwrite | 有 | 是否启用2.4无线模块（false表示未启用，true表示启用） | 1.1 |
| Enable5G | BOOLEAN | readwrite | 有 | 是否启用5G无线模块（false表示未启用，true表示启用） | 1.1 |
| WiFiMode | STRING(63) | read | 无 | WiFi模式：802.11a /802.11g/802.11n/802.11ac/802.11ax（要求列出网关支持的所有WiFi模式，以/分割）同NetWorkInfo属性 | 1.0 |
| DualBand | BOOLEAN | read | 无 | 是否支持双频段WiFi：true表示支持，false表示不支持 | 1.0 |
| SameSSIDStatus | BOOLEAN | read | 有 | 是否开启SameSSID | 1.0 |
| RxBytes | UINT64 | read | 无 | 接收字节数 | 1.0 |
| RxPkts | UINT64 | read | 无 | 收包个数 | 1.0 |
| RxErrorPkts | UINT64 | read | 无 | 发送错误包个数 | 1.0 |
| RxDropPkts | UINT64 | read | 无 | 发送丢包个数 | 1.0 |
| TxBytes | UINT64 | read | 无 | 发送字节数 | 1.0 |
| TxPkts | UINT64 | read | 无 | 发包个数 | 1.0 |
| TxErrorPkts | UINT64 | read | 无 | 发送错误包个数 | 1.0 |
| TxDropPkts | UINT64 | read | 无 | 发送丢包个数 | 1.0 |
| RatePriority | BOOLEAN | readwrite | 有 | 2.4G WiFi速率优先模式开启true/关闭false，默认false | 1.0 |
| RatePriority5G | BOOLEAN | readwrite | 有 | 5G WiFi速率优先模式开启true/关闭false，默认false | 1.0 |
| ChannelScanStatus | BYTE | readwrite | 有 | 0:2.4G信道质量扫描未开始或未完成  1：2.4G信道质量扫描完成  缺省值为0，当插件（或APP）调用ChannelCollectionRequest()，网关开始扫描，扫描完成以后网关将该值设置为1。此时插件（或APP）来读取ChannelScanScore的值，读取完成以后，由插件（或APP）重新把该值设置为0 | 1.1 |
| ChannelScanFinishTime | STRING（32） | read | 无 | 最近一次2.4G信道扫描完成时间。 | 1.1 |
| ChannelScanScore | ARRAY<STRING> | read | 无 | 2.4G信道质量扫描结果。其中STRING格式为“channel:score” | 1.1 |
| ChannelScanStatus5G | BYTE | readwrite | 有 | 0:5G信道质量扫描未开始或未完成  1：5G信道质量扫描完成  缺省值为0，当插件（或APP）调用ChannelCollectionRequest()，网关开始扫描，扫描完成以后网关将该值设置为1。此时插件（或APP）来读取ChannelScanScore5G的值，读取完成以后，由插件（或APP）重新把该值设置为0 | 1.1 |
| ChannelScanFinishTime5G | STRING(32) | read | 无 | 最近一次5G信道扫描完成时间。 | 1.1 |
| ChannelScanScore5G | ARRAY<STRING> | read | 无 | 5G信道质量扫描结果。其中STRING格式为“channel:score” | 1.1 |

**方法**

* KickOutDevice(IN STRING MAC, IN STRING SSIDIndex, OUT UINT32 result，OUT STRING errdesc);

根据设备的MAC地址，将该设备从SSIDIndex对应的WiFi上断开无线连接。

备注：本方法主要用于智能组网中设备的WiFi切换。

* SetSameSSID(IN STRING SSIDIndex24, IN STRING SSIDIndex58, OUT UINT32 result，OUT STRING errdesc);

如果网关支持双频，则支持此项功能，将2.4G和5G的SSID、密码和相关配置统一为2.4G对应的配置，返回设置下发成功失败结果；开启后，2.4G和5G会使用同一名称，建议路由器会自动为终端设备选择最佳WiFi网络，并将SameSSIDStatus设置为true。

* CancelSameSSID(OUT UINT32 result，OUT STRING errdesc);

如果网关支持双频，则支持此项功能：2.4G的SSID名称保持不变，5G的SSID名称更新为2.4G的SSID名称后增加”-5G”；密码和其它相关配置不变；返回设置下发成功失败结果，并将SameSSIDStatus设置为false。

* ChannelSwitch(IN STRING Band, OUT UINT32 result,OUT STRING errdesc);

在指定的Band上进行进行信道切换，终端设备选择WiFi最佳信道。

备注：本方法主要用于智能组网中设备的WiFi信道切换。

* ChannelCollection(IN STRING Band,OUT STRING ChannelScore, OUT UINT32 result, OUT STRING errdesc);

获取指定Band的WiFi信道评分值

备注：本方法主要用于智能组网中设备的WiFi信道切换参数参考。

ChannelScore：

描述返回的当前所有信道的评分值，格式为：

channelindex1:percent,channelindex2:percent

举例：1:10,2:90:3:100,4:10,5:90:6:100,7:10,8:90:9:100,10:10,11:90…

* ChannelCollectionRequest(IN STRING Band, OUT UINT32 result，OUT STRING errdesc);

请求获取指定Band的WiFi信道评分值，ChannelCollection的异步调用方式

备注：STA获取所有信道的评分值，可能需要消耗一定的时间，为避免调用进程长时间阻塞，此接口通知底层开始获取信道评分即返回。底层获取完所有信道的评分后，再通知调用者结果。

* + - 1. **com.ctc.igd1.PONInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| LOID | STRING(63) | read | 无 | 逻辑ID | 1.0 |
| Password | STRING(63) | read | 无 | 密码 | 1.0 |
| Temperature | DOUBLE | read | 无 | 光模块温度（单位：摄氏度，取值：0到95） | 1.0 |
| Voltage | DOUBLE | read | 无 | 电压，单位：V | 1.0 |
| Current | DOUBLE | read | 无 | 电流，单位：mA | 1.0 |
| TXPower | DOUBLE | read | 无 | 发送光功率，单位：dBm | 1.0 |
| RXPower | DOUBLE | read | 无 | 接收光功率，单位：dBm | 1.0 |
| SupportPONStatusQuery | BOOLEAN | read | 无 | 设备是否支持PON注册状态查询，false – 不支持，PONStatus字段无效，true – 支持 | 1.0 |
| PONStatus | STRING(63) | read | 无 | PonStatus =%s表示注册状态。  PonStatus的具体含义:  PonStatus =“PON\_STATUS\_NO\_REG\_NO\_AUTH”未注册未授权；  PonStatus =“PON\_STATUS\_REG\_NO\_AUTH”已注册未授权；  PonStatus =“PON\_STATUS\_REG\_AUTH”已注册已授权； | 1.0 |
| Bytes­Sent | UINT64 | read | 无 | PON口发送的字节数 | 1.1 |
| BytesReceived | UINT64 | read | 无 | PON口接收的字节数 | 1.1 |
| Packets­Sent | UINT64 | read | 无 | PON口发送帧个数 | 1.1 |
| Packets­Received | UINT64 | read | 无 | PON口接收帧个数 | 1.1 |
| FECError | UINT64 | read | 无 | PON口接受的FEC错误帧数 | 1.1 |
| DropPackets | UINT64 | read | 无 | PON口发送方向丢帧数 | 1.1 |

备注：当未接入光纤时，光功率返回-100dBm。

* + - 1. **com.ctc.igd1.VoIPInfo**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| VoIPName1 | STRING(63) | read | 有 | 第一路的电话号码；当为H.248协议时，应返回终端的物理标示 | 1.0 |
| VoIPName2 | STRING(63) | read | 有 | 第二路的电话号码 | 1.0 |
| Line1Status | STRING(32) | read | 有 | VOIP注册状态 | 1.0 |
| Line2Status | STRING(32) | read | 有 | VOIP注册状态 | 1.0 |

* + - 1. **com.ctc.igd1.LANHostManager**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| EnableStats | BOOLEAN | readwrite | 有 | 是否启用LAN侧设备流量统计功能 | 1.0 |
| LANHostMaxNumber | UINT32 | readwrite | 有 | 默认64个 | 1.0 |
| LANHostNumber | UINT32 | read | 有 | 当前LANHost多实例中的实例个数 | 1.0 |
| ControlListMaxNumber | UINT32 | readwrite | 有 | 默认32个 | 1.1 |
| ControlListNumber | UINT32 | read | 有 | 当前LANHost多实例中受控制的实例个数（ControlStatus =true） | 1.0 |

**方法**

* GetOnlineDevicesSnapShot (OUT DICT<OBJPATH,DICT<STRING,DICT<STRING,VARIANT>>> objpath\_interfaces\_and\_properties, OUT UINT32 result, OUT STRING errdesc);

获取所有在线设备的基本信息，DICT<STRING, VARIANT>包含的值：MAC, DevName, InternetAccess, DevType, IP, ConnectionType, Port, OS, OnlineTime, Brand。

* GetOnlineDeviceList(OUTDICT<OBJPATH,DICT<STRING,DICT<STRING,VARIANT>>> objpath\_interfaces\_and\_properties, OUT UINT32 result, OUT STRING errdesc);

获取所有在线设备的列表,包含所有属性。

* GetLANHostPathbyMAC(IN STRING mac, OUTOBJECT\_PATH path, OUT UINT32 result, OUT STRING errdesc )

根据MAC获取对应LANHost对象的路径，索引用于查询或者设置LANHost的属性，对应接口SET\_ATTACH\_DEVICE\_NAME, SET\_ATTACH\_DEVICE\_BANDWIDTH,

GET\_ATTACH\_DEVICE\_BANDWIDTH,GET\_ATTACH\_DEVICE\_RIGHT,

SET\_ATTACH\_DEVICE\_RIGHT, QUERY\_ATTACH\_DEVICE\_REALRATE

result：0（成功）/1（失败）。

errdesc：若为NULL或者函数成功，则不用赋值；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.LANHost**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC | STRING(12) | read | 无 | 指网关下挂设备的MAC信息，格式为"0123456789AB" | 1.0 |
| HostName | STRING(63) | read | 无 | 表示下挂设备的HostName | 1.1 |
| DevName | STRING(63) | readwrite | 有 | 表示下挂设备别名 | 1.0 |
| ControlStatus | BOOLEAN | read | 有 | 表示下挂设备当前是否处于受控状态（true为正处于受控状态，计入ControlListNumber统计；false为未处于受控状态，不计入ControlListNumber统计。默认false） | 1.0 |
| InternetAccess | BYTE | readwrite | 有 | 是否允许接入和访问Internet（"0"-不允许接入；"1"-允许接入但禁上网；"2"-允许接入并且可以上网，默认为2）  当设置为0、1时，ControlStatus设置为true； | 1.0 |
| StorageAccess | BOOLEAN | readwrite | 有 | 是否允许访问USB/SATA存储（true为允许，false为不允许，默认为true）  当设置为false时，ControlStatus设置为true | 1.0 |
| MaxUSBandwidth | UINT32 | readwrite | 有 | 表示下挂设备上行最大带宽，0表示不限，单位为kbps，默认为0  当设置为非0时，ControlStatus设置为true | 1.0 |
| MaxDSBandwidth | UINT32 | readwrite | 有 | 表示下挂设备下行最大带宽，0表示不限，单位为kbps，默认为0  当设置为非0时，ControlStatus设置为true | 1.0 |
| DevType | STRING(16) | readwrite | 无 | 下挂设备类型（phone/Pad/PC/STB/ROUTER/SMTDEV/AP/PLC/CloudVR/OTHER） | 1.0 |
| IP | STRING(16) | read | 无 | 下挂设备IP地址 | 1.0 |
| IPv6 | STRING(45) | read | 无 | 下挂设备IPv6地址 | 1.13 |
| ConnectionType | BYTE | read | 无 | ConnectionType为下挂终端和网关的连接形式（0：有线/1：无线） | 1.0 |
| Port | BYTE | read | 无 | 当ConnectionType=0时，1：lan1口连接，2：lan2口连接，3：lan3口连接，4：lan4口连接；  当ConnectionType=1时，表示SSIDIndex | 1.0 |
| Brand | STRING(63) | readwrite | 无 | 下挂设备品牌名 | 1.0 |
| Model | STRING(63) | readwrite | 无 | 下挂设备型号 | 1.0 |
| OS | STRING(63) | readwrite | 无 | 下挂设备操作系统 | 1.0 |
| Active | BOOLEAN | read | 有 | 下挂设备是否在线，在线=true，离线=false | 1.0 |
| LatestActiveTime | STRING(32) | read | 有 | 下挂设备的最新的上线时间 | 1.0 |
| LatestInactiveTime | STRING(32) | read | 有 | 下挂设备的最新的下线时间 | 1.0 |
| OnlineTime | UINT32 | read | 无 | 下挂设备在线时长 | 1.0 |
| RxBytes | UINT64 | read | 无 | 单位byte | 1.0 |
| TxBytes | UINT64 | read | 无 | 单位byte | 1.0 |
| PowerLevel | INT32 | read | 无 | 只在ConnetionType=1时有意义，表示此终端连接上的信号强度，单位dbm；  当ConnectionType=0时，设置为0。 | 1.0 |
| DeviceOnlineNofication | BOOLEAN | readwrite | 无 | 下挂设备是否上报，默认值为false. | 1.0 |
| NegoRate | UINT32 | read | 无 | 网关与下挂设备协商速率，包括有线和无线，单位kbps  1Mbps=1000kbps  1Gbps=1000Mbps | 1.01 |

接口说明：

1. LANHost保存下挂设备信息，包括在线、离线、拉黑(InternetAccess =0)、限制(InternetAccess =1)的所有下挂设备；
2. LANHost合计最多保存LANHostMaxNumber个实例；
3. 实例数已经达到或超过LANHostMaxNumber时，有新设备接入应允许上线，如存在不受控（ControlStatus=false）的离线设备实例，则覆盖最早离线的不受控离线设备实例；如无不受控的离线设备，新上线设备可以不在LANHost实例中体现。
4. InternetAccess、SotrageAccess、带宽限制，都没有限制的时候，ControlStatus需要设置为false。

操作说明：

1. 设备拉黑操作，设置LANHost接口中InternetAccess=0，该设备无法接入网关，拉黑成功；
2. 设备拉黑操作，网关该接口要实现Acitve以及LatestInactiveTime的更新；
3. 设备拉黑操作，最多支持ControlListMaxNumber个，超过将设置失败；
4. 设备取消拉黑操作，设置LANHost接口中InternetAccess=2，设备可以上网。
5. 设备限制操作，设置LANHost接口中InternetAccess=1，该设备禁止上网，限制成功；
6. 设备取消限制操作，设置LANHost接口中InternetAccess=2，设备可以上网；
7. 设备限制操作，网关该接口不需要实现Acitve以及LatestInactiveTime的更新。

属性说明：

1. DevType、Brand、Model、OS可结合DPI插件实现；
2. LatestInactiveTime要求误差不超过5分钟。
   * + 1. **com.ctc.igd1.HttpDownloadTest**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Status | UINT32 | read | 有 | Status=0表示成功；Status=1表示失败 | 1.0 |
| Result | STRING(256) | read | 有 | 表示字节数；（单位Kbyte），数据类型应为整数 | 1.0 |
| URL | STRING(1023) | readwrite | 无 | URL表示设置进行下载的URL地址；地址内容应包括协议类型（如：HTTP、FTP等），如果是多个测速地址，应该以“|”区隔 | 1.0 |

**方法**

* StartTest(IN UINT32 time, OUT UINT32 result, OUT STRING errdesc);

开始满负载下载测试，time为持续时间

* + - 1. **com.ctc.igd1.WPS**

本接口对应业务管理平台如下接口：

* WPS\_ON

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 有 | Enable：true，Disable：false | 1.0 |
| WPSStatus | BYTE | read | 有 | WPSStatus =0表示已进入WPS配置状态，但设备尚未与网关进行WPS交互  WPSStatus =1表示WPS启动失败  WPSStatus =2表示已有设备通过WPS接入网络  WPSStatus =3表示WPS超时关闭，未有设备连接  WPSStatus=4 表示WPS未开启 | 1.0 |
| DevInfo | ARRAY<STRING> | read | 无 | 表示本次通过WPS接入网络的设备信息。默认填写该设备的IP地址，并可扩展支持设备的其它信息（如设备的MAC地址、设备类型、设备名称等），格式要求为“IP:X.X.X.X;MAC:XXXXXXXXXXXX;……” 参数之间以“;”隔开 | 1.0 |

**方法**

* SetWPS(IN INT32 on1OrOff0, IN UINT32 time, OUT UINT32 result, OUT STRING errdesc);

触发开启或关闭WPS

* + - 1. **com.ctc.igd1.WLANConfiguration**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本号 |
| SSID | STRING(32) | readwrite | 有 | SSID名称 | 1.0 |
| Enable | BOOLEAN | readwrite | 有 | 表示此SSID是否启用（true表示启用，false表示不启用）； | 1.0 |
| Channel | UINT32 | readwrite | 有 | 设置WLAN模块所在信道，其中：  0：表示自动选择信道（网关自动选择的信道值通过ChannelsInUse读取）  1～255：实际信道值 | 1.0 |
| ChannelInUse | UINT32 | read | 有 | WLAN模块实际工作信道 | 1.0 |
| BeaconType | STRING(32) | readwrite | 有 | 加密安全模式，取值范围如下：  “None” （不加密，对应的BasicAuthenticationMode＝OpenSystem）  “Basic” （对应WEP加密，对应的BasicAuthenticationMode默认值为Both）  “WPA”  “WPA2”  “WPA/ WPA2”  “WPA2/ WPA3”  “WPA3”  “11i” (Optional) | 1.0 |
| Standard | STRING(15) | readwrite | 无 | 802.11工作模式：  “b”  “g”  “n”  “b,g,n” (802.11b/g混和模式)“ac”  “ax” | 1.0 |
| WEPEncryptionLevel | STRING(63) | readwrite | 无 | WEP密钥长度：  “40-bit”  “104-bit” | 1.0 |
| BasicAuthenticationMode | STRING(15) | readwrite | 无 | 基本认证模式：  “OpenSystem”)  “SharedKey”  “Both“ （包含上面两者） | 1.0 |
| WPAEncryptionModes | STRING(31) | readwrite | 有 | WPA/WPA2加密方式：  “TKIPEncryption”  “AESEncryption”  “TKIPandAESEncryption” | 1.0 |
| SSIDHide | BOOLEAN | readwrite | 有 | SSID是否隐藏, 取值范围(true,false) | 1.0 |
| RFBand | UINT32 | readwrite | 无 | 对应无线模块的无线频段，0：表示2.4GHz，1：表示5GHz，缺省为0（最低要求：创建实例后可修改一次） | 1.0 |
| ChannelWidth | UINT32 | readwrite | 无 | 对应无线模块的频宽，支持20MHz频宽、40MHz频宽、20/40M频宽自适应、80MHz频宽、160MHz频宽模式,其中0：20MHz。1：40MHz。2：20、40MHz。3：80MHz，4:160MHz，5：80MHz+80MHz。  2.4GHz频段默认为20MHz频宽。5GHz频段默认为80M频宽自适应模式 | 1.0 |
| GuardInterval | UINT32 | readwrite | 无 | 对应无线模块的保护间隔，对5GHz频段，无线保护间隔设置，支持400ns、800ns两种保护间隔，其中0：400ns;1:800ns, 默认0 | 1.0 |
| RetryTimeout | UINT32 | readwrite | 无 | 对应无线模块的超时，对5GHz频段，支持基于最大延迟时间的数据重传控制，尝试发送数据包若超过时间门限仍未成功则丢弃该数据包，单位为毫秒，默认20ms | 1.0 |
| Powerlevel | UINT32 | readwrite | 无 | 以百分比表示无线模块功率大小：   * 默认发射功率对应的Powerlevel取值为100，取值0~100对应发射功率从0增大至默认发射功率，并可以此顺延 * 与ITMS管理参数X\_CT-COM\_Powerlevel的对应关系：通过ITMS设置时，X\_CT-COM\_Powerlevel的1-5等级分别与取值100，80，60，40，20对应；通过ITMS读取时，取值大于90对应X\_CT-COM\_Powerlevel的1等级，不大于90且大于70对应2等级，不大于70且大于50对应3等级，不大于50且大于30对应4等级，其它对应5等级 | 1.0 |
| PowerValue | UINT32 | read | 无 | 无线模块发射功率能力最大值（单位：dBm） | 1.0 |
| PWD | STRING(5:63) | readwrite | 有 | SSID密码； | 1.0 |
| RxBytes | UINT64 | read | 无 | 接收字节数 | 1.0 |
| RxPkts | UINT64 | read | 无 | 收包个数 | 1.0 |
| RxErrorPkts | UINT64 | read | 无 | 发送错误包个数 | 1.0 |
| RxDropPkts | UINT64 | read | 无 | 发送丢包个数 | 1.0 |
| TxBytes | UINT64 | read | 无 | 发送字节数 | 1.0 |
| TxPkts | UINT64 | read | 无 | 发包个数 | 1.0 |
| TxErrorPkts | UINT64 | read | 无 | 发送错误包个数 | 1.0 |
| TxDropPkts | UINT64 | read | 无 | 发送丢包个数 | 1.0 |
| SSIDAlias | STRING(30) | read | 无 | 别名，按照创建顺序标记为2.4G-1，2.4G-2……5G-1，5G-2…… | 1.1 |
| Owner | STRING(30) | readwrite | 有 | SSID创建者，选项：ITMS（IMTS创建）、APP（智能管理平台及插件创建），缺省ITMS | 1.1 |
| Service | STRING(30) | readwrite | 有 | 占用该SSID的业务名称，选项：  Internet（2.4G与5G的第一个SSID的缺省属性）、IPTV、Voice；  中间件和插件创建的根据业务自定义（如：Guest、IOT等）  TR069创建的SSID需网关赋值且需根据业务联动：承载业务包含Internet的均填“Internet”，仅承载IPTV的填“IPTV”，仅承载VOICE的填“VOICE”，缺省为“Internet”  中间件和插件创建的SSID，网关接收并保存中间件和插件对其的设置和更改 | 1.1 |
| MACAccessMode | UINT32 | readwrite | 有 | MAC黑白名单无线接入控制模式  0：不启用黑白名单  1：启动黑名单  2：启用白名单 | 1.1 |
| AccessRule | UINT32 | readwrite | 有 | 0：WAN连接缺省权限  1：只能通过带Internet属性的WAN连接访问公网，隔离本地网络（主要针对访客wifi场景）2：只能访问固定IP地址的固定端口（网关提供的DHCP除外，主要针对快联配网场景） | 1.1 |
| AllowedIPPort | STRING(256) | readwrite | 无 | 在AccessRule的2的情况下，可以访问的IP和端口（如：192.168.1.1:8888,192.168.1.1:9999,……） | 1.1 |
| USBandwidth | UINT32 | readwrite | 无 | 访客上行带宽限制，单位kbps，0表示不限制 | 1.1 |
| DSBandwidth | UINT32 | readwrite | 无 | 访客下行带宽限制，单位kbps，0表示不限制 | 1.1 |

多SSID说明：

1. 仅预先创建2.4G和5G的第一个SSID；

2）2.4G 和5G的第一个SSID，不能通过DBus接口DeleteObject删除。

3）“双频合一”配置模式，默认仅针对2.4G和5G的第一个SSID。

* + - 1. com.ctc.igd1.WiFiBandSteering

**属性**（单频设备无需支持）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 无 | 是否启用无线BandSteering功能（false表示未启用，true表示启用） | 1.1 |
| Capability | BOOLEAN | read | 无 | 是否支持BandSteering功能（false表示不支持，true表示支持） | 1.1 |
| RSSIThreshold | INT32 | readwrite | 无 | 接收信号强度阈值，当2.4G频段检测到某一下挂STA接收到的信号强度高于此阈值并持续时间大于SteeringDetectInterval后，网关应检测5G 频段信道状况（ChannelUtilization5G）及当前客户端的负载状况，如果满足要求（ChannelUtilization5G<ChannelUtilizationThreshold5G, 下挂双频STA流量< STALoadThreshold2G），将当前双频STA切换至5G频段。单位：dbm.默认值-40  取值范围（-100~0） | 1.1 |
| RSSIThreshold5G | INT32 | readwrite | 无 | 5G接收信号强度阈值，当双频客户端首次连接或者当前工作在5G频段时，检测到某一下挂双频STA接收到的信号强度低于此阈值并持续时间大于SteeringDetectInterval，将下挂双频客户端切换至2.4G频段。单位：dbm.默认值 -80  取值范围（-100~0） | 1.1 |
| ChannelUtilization5G | UINT32 | read | 无 | 5G信道利用率（综合考虑当前信道下周边WiFi以及网关自身的负载），单位：百分比（%），取值范围0-100 | 1.1 |
| ChannelUtilizationThreshold5G | UINT32 | readwrite | 无 | 5G信道利用率参考阈值（STA是否从2.4G切换到5G的判断条件之一）。单位：百分比（%），0：不参考此阈值，默认值80  取值范围0-100 | 1.1 |
| STALoadThreshold2G | UINT32 | readwrite | 无 | 2.4G下挂双频STA终端的流量参考阈值（STA是否从2.4G切换到5G的判断条件之一）。  单位：kbps，默认值75。  0：不参考此阈值。 | 1.1 |
| SteeringDetectInterval | UINT32 | readwrite | 无 | Steering状态持续时间，在满足steering的阈值而且持续时间大于此时间后才开始进行频段切换动作，单位：秒，默认值30 | 1.1 |

* + - 1. com.ctc.igd1.WiFiTimer

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| StartTime | STRING(6) | readwrite | 有 | Wifi开机的时间 | 1.0 |
| EndTime | STRING(6) | readwrite | 有 | Wifi关机的时间 | 1.0 |
| ControlCycle | STRING(6) | readwrite | 无 | 表示控制周期；  可以取值范围为  DAY | 1.0 |
| Enable | BOOLEAN | readwrite | 有 | Wifi定时开关启用/关闭功能；FALSE表示功能关闭，TRUE表示功能开启。 | 1.0 |
| SSIDMask | UINT32 | readwrite | 有 | 表示受定时器控制的SSIDIndex位码。例如0x01（二进制…00000001）表示SSIDIndex1, 0x03（二进制…00000011）表示SSIDIndex1和SSIDIndex2。  备注：DBUS1.0中类型为BYTE | 1.1 |

说明：WiFi定时器仅针对SSIDMask指定的SSID。

* + - 1. **com.ctc.igd1.WiFiTimer1**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| WeekDay | ARRAY<STRING> | readwrite | 有 | 表示Wifi开机的重复周期，取值1～7。如：1代表星期一、2代表星期二 | 1.0 |
| Time | STRING(6) | readwrite | 有 | 表示Wifi开/关机的时间，如：19:30 | 1.0 |
| Active | STRING(2) | readwrite | 有 | 表示定时器启用/关闭，0表示关闭，1表示启用 | 1.0 |
| Enable | BOOLEAN | readwrite | 有 | 表示Wifi定时开关启用/关闭功能，FALSE表示功能关闭，TRUE表示功能开启 | 1.0 |
| SSIDMask | UINT32 | readwrite | 有 | 表示受定时器控制的SSIDIndex位码。例如0x01（二进制…00000001）表示SSIDIndex1, 0x03（二进制…00000011）表示SSIDIndex1和SSIDIndex2。  备注：DBUS1.0中类型为BYTE | 1.1 |

说明：WiFi定时器仅针对SSIDMask指定的SSID。

* + - 1. **com.ctc.igd1.LED**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Status | STRING(4) | readwrite | 有 | 设置LED灯状态；  取值范围OFF关闭，ON开启 | 1.0 |
| StartTime | STRING(6) | readwrite | 有 | 表示LED指示灯开机的时间，如：9:30 | 1.0 |
| EndTime | STRING(6) | readwrite | 有 | 表示LED指示灯关机的时间，如：21:20 | 1.0 |
| ControlCycle | STRING(6) | readwrite | 无 | 表示控制周期；  可以取值范围为  DAY | 1.0 |
| Enable | BOOLEAN | readwrite | 有 | 表示LED定时开关启用/关闭功能；  TRUE表示成功，FALSE表示失败 | 1.0 |

* + - 1. **com.ctc.igd1.SleepTimer**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Day | ARRAY<STRING> | readwrite | 有 | 休眠开机的重复周期，取值0～7。如：1代表星期一、2代表星期二；如果为0，表示立即开启或者关闭休眠功能 | 1.0 |
| Time | STRING(6) | readwrite | 有 | 表示休眠开/关的时间，如：19:30 | 1.0 |
| Active | STRING(2) | readwrite | 有 | 表示定时器启用/关闭，0表示关闭，1表示启用 | 1.0 |
| Enable | BOOLEAN | readwrite | 有 | 表示休眠定时开关启用/关闭功能，FALSE表示功能关闭，TRUE表示功能开启 | 1.0 |

* + - 1. **com.ctc.igd1.SysCmd**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本号 |
| UpgradeStatus | BYTE | read | 有 | 表示固件升级状态  0: 没有升级任务  1：下发到网关的版本不正确；  2：下载失败；  3：网关空间不够；  4：当前已经是目标升级版本；  5：其他错误  6: 正在升级中  7: 升级成功 | 1.0 |
| UpgradeSWVersion | STRING(63) | read | 无 | 表示新升级的固件版本号（用于在升级不重启的情况下，向平台返回所升级的版本） | 1.0 |
| RestoreStatus | BYTE | read | 有 | 表示终端的恢复设置状态，  缺省为0：  0：未进行恢复出厂设置；  1：长按设备的复位按钮；  2：短按设备的复位按钮；  3：点击本地界面上的复位按钮；  4：通过ITMS恢复出厂设置；5：通过"智家平台"恢复出厂设置。 | 1.0 |
| Province | STRING(8) | read | 无 | 省份编码  省份编码定义请参考智能网关及应用管理平台接口规范要求 | 1.0 |
| MemAlarm | BYTE | readwrite | 无 | 内存告警阈值，默认值是80。  如果当前系统已使用内存大于等于MemAlarm并且小于MemLimit, 发送SysMemControl信号, 信号内容请参考下面本接口SysMemControl信号规范。 | 1.0 |
| MemLimit | BYTE | readwrite | 无 | 内存限制阈值，默认值是90。  如果当前系统已经使用内存大于等于MemLimit, 发送SysMemControl信号，信号内容请参考下面本接口SysMemControl信号规范。 | 1.0 |

**方法**

* SetLOID(IN STRING loid, IN STRING password, IN STRING province, OUT UINT32 result, OUT STRING errdesc);

设置宽带注册码和密码

当province为空(即为””)时，表示不修改省份编码。

* RegisterLOID(OUT UINT32 result, OUT STRING errdesc);

发起宽带识别码注册

* CheckLOID(OUT UINT32 result, OUT STRING errdesc);

检测宽带识别码注册状态

* SetDateTime(IN STRING time, OUT UINT32 result, OUT STRING errdesc);

设置设备时间

* Reboot(OUT UINT32 result, OUT STRING errdesc);

重启设备

* Restore(OUT UINT32 result, OUT STRING errdesc);

恢复非关键参数（基于“智家平台的恢复非关键参数命令”方式进行恢复）

* LocalRecovery(OUT UINT32 result, OUT STRING errdesc);

恢复出厂设置（基于“点击本地界面上的复位按钮”方式进行恢复）

* Upgrade(IN STRING url, IN UINT32 mode, IN UINT32 method, IN BOOLEAN needreboot, OUT UINT32 result, OUT STRING errdesc);

系统固件升级

下发升级任务后，须将UpgradeStatus置为6，表示正在升级。

如果升级不需要重启，则需要将值设置为上述定义的状态，并且发送变更通知。

如果升级需要重启，在重启之后，保持UpgradeStatus值，不需要发送变更通知。

* ClearUpgradeStatus(OUT UINT32 result, OUT STRING errdesc);

恢复UpgradeStatus初始状态(0)，表示该升级任务结果已经上报平台。

* ClearRestoreStatus (OUT UINT32 result, OUT STRING errdesc)

恢复RestoreStatus初始状态，表示已经将该状态上报平台，要求回复到初始状态。

* CheckUAPasswd(IN STRING pass, OUT UINT32 result, OUT STRING errdesc);

检查useradmin密码是否正确

* SetUAPasswd(IN STRING pass, OUT UINT32 result, OUT STRING errdesc);

设置useradmin密码

* CheckTAPasswd(IN STRING pass, OUT UINT32 result, OUT STRING errdesc);

检查telecomadmin密码是否正确

* UploadTroubleLocatingInfo(IN STRING uploadurl,IN STRING faultcategory, OUT UINT32 result, OUT STRING errdesc);

一键故障信息收集，参见智能网关及应用管理平台接口规范要求

* StartCollectionDebugInfo(IN STRING uploadurl,IN STRING category , IN UINT16 timeout,OUT UINT32 result, OUT STRING errdesc);

启动调试信息搜集, 参见智能网关平台接口规范要求

* GetTAPasswd(OUT STRING pass, OUT UINT32 result, OUT STRING errdesc);

获取telecomadmin 密码

* GetUAPasswd(OUT STRING pass, OUT UINT32 result, OUT STRING errdesc);

获取useradmin 密码

result：0 on success, 1 on fail

errdesc: If errdesc is NULL or method success, do nothing; otherwise fill with error description

CheckLOID(OUT UINT32 result, OUT STRING errdesc)返回值说明

说明：

result，表示返回的状态代码分类

2xx，表示注册成功

4xx, 表示已知原因的错误

5xx, 表示未知原因的错误

errdesc，表示注册状态的详细参数

合成规则: key1=value1&key2=value2…

详细描述如下:

|  |  |  |
| --- | --- | --- |
| **result** | **errdesc** | **说明** |
| 401 | “RegisterStatus=REGISTER\_DEFAULT” | 表示初始设备未注册状态 |
| 402 | “RegisterStatus=REGISTER\_REGISTED” | 表示设备为已注册状态,不需要再次注册 |
| 403 | “RegisterStatus=REGISTER\_TIMEOUT” | 表示注册超时失败 |
| 404 | “RegisterStatus=REGISTER\_NOMATCH\_NOLIMITED&RETRY\_COUNT=N” | 表示逻辑ID与密码不匹配，N表示剩余尝试次数 |
| 405 | “RegisterStatus=REGISTER\_NOMATCH\_LIMITED“ | 表示逻辑ID与密码不匹配 |
| 406 | “RegisterStatus=REGISTER\_NOACCOUNT\_NOLIMITED&RETRY\_COUNT=N“ | 密码不存在，N表示剩余尝试次数 |
| 407 | “RegisterStatus=REGISTER\_NOACCOUNT\_LIMITED“ | 密码不存在 |
| 408 | “RegisterStatus=REGISTER\_NOUSER\_NOLIMITED&RETRY\_COUNT=N” | 逻辑ID不存在，N表示剩余尝试次数 |
| 409 | “RegisterStatus=REGISTER\_NOUSER\_LIMITED“ | 逻辑ID不存在 |
| 410 | “RegisterStatus=REGISTER\_OLT\_FAIL“ | 注册OLT失败 |
| 200 | “RegisterStatus=REGISTER\_OK&BUSINESS\_NUMBER=N&BUSINESS\_NAME=INTERNET+VOIP+IPTV” | 表示注册成功，BUSINESS\_NUMBER表示下发了几个业务，BUSINESS\_NAME表示下发的业务名字的或组合（组合用+连接在一起） |
| 201 | “RegisterStatus=REGISTER\_OLT&PERCENTAGE=xx” | 正在注册OLT，PERCENTAGE=xx表示注册的进度值百分比，典型可取：20表示正在注册OLT，30表示在OLT授权成功，提示 “正在获取管理IP”，40表示TR069 的WAN连接获得IP地址，提示“已获得管理IP，正在连接ITMS” |
| 202 | “RegisterStatus=REGISTER\_OK\_DOWN\_BUSINESS&PERCENTAGE=xx&BUSINESS\_NAME=%s” | 表示注册成功，正在下发业务，实现中可取：PERCENTAGE =50，表示注册成功，等待ITMS下发业务；PERCENTAGE取值60-99，表示平台开始下发业务；BUSINESS\_NAME取值INTERNET, VOIP, IPTV 及OTHER，表示平台正在下发业务的名字 |
| 203 | “RegisterStatus=REGISTER\_OK\_NOW\_REBOOT&BUSINESS\_NUMBER=N&BUSINESS\_NAME=INTERNET+VOIP+IPTV” | 表示注册成功，业务下发成功，网关需要重启, BUSINESS\_NUMBER表示下发了几个业务，BUSINESS\_NAME表示下发的业务名字的或组合（组合用+连接在一起） |
| 204 | "RegisterStatus=REGISTER\_POK" | 表示注册成功，但是业务下发失败 |
| 500 | 空字符串 | 表示非以上原因的注册失败 |

**信号**

* SysMemControl(STRING signaltype), 表示系统内存控制信号。

用于Framework触发内存控制机制.

参数: s

内存控制信号类型:

“MemAlarm”表示系统已使用内存大于或等于属性MemAlarm且小于属性MemLimit；

“MemLimit”表示系统已使用内存大于或等于属性MemLimit；

“MemResumeNormal”表示系统已使用内存从报警或者限制状态恢复到正常稳定状态，例如当系统已使用内存在持续一分钟时间内均不大于 (MemAlarm – 10)%时发送此信号，通知中间件恢复到正常运行状态（例如中间件不再关闭低优先级的插件）。

* + - 1. **com.ctc.igd1.PPPoE**

本接口只提供给云客户端和特别授权的插件使用，不提供给普通插件使用。

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| PPPoEUserName | STRING(63) | read | 有 | PPPoE拨号用户名 | 1.0 |

* + - 1. **com.ctc.igd1.DHCPServer**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 有 | DHCP Server使能 | 1.0 |
| MinAddress | STRING(15) | readwrite | 有 | 地址分配起始地址 | 1.0 |
| MaxAddress | STRING(15) | readwrite | 有 | 地址分配结束地址 | 1.0 |
| IPAddr | STRING(15) | readwrite | 有 | LAN IP地址，如：192.168.1.1 | 1.0 |
| SubnetMask | STRING(15) | readwrite | 有 | 子网掩码 | 1.0 |
| LeaseTime | UINT32 | readwrite | 有 | 租约时间，单位为秒 | 1.0 |

* + - 1. **com.ctc.igd1.PortMapping**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 有 | 是否开启，TRUE开启，FALSE关闭 | 1.0 |
| LeaseDuration | UINT32 | readwrite | 有 | 租约时间，0表示static，具体参考TR-098 | 1.0 |
| RemoteHost | STRING(63) | readwrite | 有 | 外部主机，具体说明请参考TR-098 | 1.0 |
| ExternalPort | UINT32 | readwrite | 有 | 外部端口 | 1.0 |
| InternalPort | UINT32 | readwrite | 有 | 内部端口 | 1.0 |
| PortMappingProtocol | STRING(6) | readwrite | 有 | 协议类型，取值范围为”UDP”, “TCP” and “BOTH” | 1.0 |
| InternalClient | STRING(15) | readwrite | 有 | 设备在网关下的地址 | 1.0 |
| Description | STRING(32) | readwrite | 有 | 该PortMapping的描述说明 | 1.0 |

备注：PortMapping默认配置在带“INTERNET”属性的缺省路由WAN连接上。

* + - 1. **com.ctc.igd1.PlatformService**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Appmodel | BYTE | Read | 有 | 云客户端模块开关，0：模块关闭；1：模块开启；缺省：1；中间件在收到关闭或开启的变更通知后，更新云客户端的运行状态（参考平台接口的智能网关TR098扩充参数说明） | 1.0 |
| InitUAPwd | STRING(32) | Read | 无 | Useradmin的初始密码 | 1.0 |
| InitSSID | STRING(32) | Read | 无 | SSID1的初始名称 | 1.0 |
| InitSSIDPwd | STRING(63) | Read | 无 | SSID1的初始密码 | 1.0 |
| DistAddr | STRING(32) | readwrite | 有 | 分发平台地址, 缺省为189cube.com | 1.0 |
| Port | UINT32 | readwrite | 有 | 分发平台端口，缺省为12112 | 1.0 |
| Heartbeat | UINT32 | readwrite | 无 | 终端和运营平台心跳，缺省是60，单位是秒 | 1.0 |
| Ability | UINT32 | readwrite | 有 | 网关封装接口能力是否向本地开放，0：开放，1：不开放，缺省：0 | 1.0 |
| LocalPort | UINT32 | readwrite | 有 | 网关内部为客户端本地访问的TCP端口，缺省：17998 | 1.0 |
| Version | STRING(16) | readwrite | 无 | 网关通信接口版本号（缺省：3.0） | 1.0 |
| SSN | STRING(63) | readwrite | 无 | 和平台交互验证码，长度和sn保持一致，缺省为：null。  该参数的访问权限要求：只对于网关通信接口模块有读的权限；只对特定的APP插件"com.chinatelecom.XXX（厂商简名的拼音全拼）.smartgateway.ssncheck"有读写的权限。  如果该参数为null，网关与智能网关平台交互，仍然用拼接的sn进行交互，如果SSN非空，网关与智能网关平台的交互中，凡是涉及到sn的，应统一由SSN来替代 | 1.0 |
| DistStatus | BYTE | readwrite | 无 | 分发平台连接情况  1: 未连接  2: 正在尝试连接分发平台  3: 与分发平台保持连接中  4: 与分发平台连接结束  5: 尝试连接分发平台失败 | 1.0 |
| DistErrorMsg | STRING(63) | readwrite | 无 | 当DistStatus=5时,用于描述失败原因，如”上网WAN连接未生效“、”无分发平台配置参数“、”分发平台域名解析失败“、”TCP连接无法建立”、“未收到平台响应报文”等 | 1.0 |
| OperAddr | STRING(32) | readwrite | 无 | 运营平台地址 | 1.0 |
| OperStatus | BYTE | readwrite | 无 | 运营平台连接情况  1: 未连接  2: 正在尝试连接  3: 向运营平台注册中  4: 向运营平台心跳保活中  5: 与运营平台等待下一次心跳中  6: 尝试连接运营平台失败 | 1.0 |
| OperErrorMsg | STRING(63) | readwrite | 无 | 当OperStatus=6时，用于描述错误的原因，如“上网WAN连接未生效”、”无运营平台注册中心配置参数”、”运营平台注册中心域名解析失败”、”TCP连接无法建立”、”未收到平台响应报文”等 | 1.0 |
| PluginAddr | STRING(32) | readwrite | 无 | 插件中心地址 | 1.0 |
| PluginStatus | BYTE | readwrite | 无 | 插件中心连接情况  1: 未连接  2: 正在尝试连接  3: 向插件中心注册中  4: 向插件中心心跳保活中  5: 与插件中心等待下一次心跳  6: 尝试连接插件中心失败 | 1.0 |
| PluginErrorMsg | STRING(63) | Readwrite | 无 | 当PluginStatus = 6是，用于描述错误的原因，如”上网WAN连接未生效”、”无运营平台插件中心配置参数”、”运营平台插件中心域名解析失败”、”TCP连接无法建立”、”未收到平台响应报文”等 | 1.0 |
| BSSAddr | STRING(63) | readwrite | 有 | BSS分发平台地址（含端口），适用于天翼网关3.0协议；网关超级用户界面可通过云客户端com.ctc.cloudclient1接口获取当前连接情况。 | 1.1 |

说明：分发平台、运营平台、插件中心等的相关地址和状态码由Framework和云客户端负责更新，网关设备的超级用户界面可以通过访问这些属性，获取当前网关与平台的连接情况。

* + - 1. **com.ctc.igd1.IncomingFilter**

方法

* AddIncomingEntry(IN STRING remoteIP, IN BYTE protocol, IN UINT32 port，IN BYTE interface, OUT UINT32 result, OUT STRING errdesc)

添加并打开插件开端口

remoteIP: 远端HOST IP地址, 如果为“”表示任何IP

protocol: 0 表示TCP, 1表示UDP, 2 表示TCP&UDP

port: 端口, 0-65535

interface: 接口，0表示WAN侧, 1 表示LAN侧

* DelIncomingEntry(IN STRING remoteIP, IN BYTE protocol, IN UINT32 port, IN BYTE interface, OUT UINT32 result, OUT STRING errdesc)

删除并关闭插件开放端口

remoteIP: 远端HOST IP地址, 如果为“”表示任何IP

protocol: 0 表示TCP, 1表示UDP, 2 表示TCP&UDP

port: 端口, 0-65535

interface: 接口，0表示WAN侧, 1 表示LAN侧

* + - 1. **com.ctc.igd1.QoS**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Mode | STRING(32) | readwrite | 无 | 规定家庭网关需要对下列业务或组合进行QoS：“VOIP”, “TR069”, “IPTV”,“INTERNET”,“OTHER”.缺省值：“TR069, VOIP, IPTV, INTERNET”  优先级按照前后次序递减，如“VOIP, TR069, IPTV”，则VOIP具有最高的优先级，TR069次之，IPTV最低 | 1.1 |
| Enable | BOOLEAN | readwrite | 无 | QoS启用, 0禁用, 1启用 | 1.1 |
| Bandwidth | UINT32 | readwrite | 无 | 设定上传的流量，0是不限制，单位为Kbps,缺省值：0 | 1.1 |
| Plan | STRING(16) | readwrite | 无 | 设定QOS机制为加权优先级、严格优先级、承诺访问速率，其中：  权重：weight，  优先级：priority  承诺访问速率：car | 1.1 |
| EnableForceWeight | BOOLEAN | readwrite | 无 | 设定强制带宽，这是用在权重的QoS机制，是强制各个队列的上传带宽，即使沒有其他队列在上传，也不能超过他所设定的带宽比例，缺省值：false | 1.1 |
| EnableDSCPMark | BOOLEAN | readwrite | 无 | 是否启用DSCP标志,缺省值：false | 1.1 |
| Enable8021P | UINT32 | readwrite | 无 | 是否启用802-1\_P标志，缺省值：0, 其中，0表示不启用，1表示保持原来的标志位值，2表示重写802-1\_P标志位值,缺省值：0 | 1.1 |

* + - 1. **com.ctc.igd1.QoSClassification**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ClassQueue | UINT32 | readwrite | 无 | 有8个队列可选：1，2，3，4，5，6，7，8，缺省值：1 | 1.1 |
| DSCPMarkValue | UINT32 | readwrite | 无 | DSCP值 | 1.1 |
| VLAN8021PValue | UINT32 | readwrite | 无 | 802.1p值 | 1.1 |

* + - 1. **com.ctc.igd1.QoSClassificationType**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Type | STRING(63) | readwrite | 无 | 设定队列的条件类型,取值范围为：“SMAC(源MAC地址)”，“8021P”，“SIP（源IP地址）”，“DIP（目的IP地址）”，“SPORT（源端口号）”，“DPORT（目的端口号）”，“TOS”，“DSCP”，“WANInterface(设置WAN连接的QOS,其中Max，Min值为WAN连接索引)”，“LANInterface(设置LAN连接的QOS，其中Max，Min值为LAN连接索引)” 、“TC”、“FL” | 1.1 |
| Max | STRING(512) | readwrite | 无 | 最大取值 | 1.1 |
| Min | STRING(512) | readwrite | 无 | 最小取值，可以和Max取值一样 | 1.1 |
| ProtocolList | STRING(20) | readwrite | 无 | 队列符合哪些协议，以逗号分割，包括：“TCP”，“UDP”，“ICMP”，“RTP” | 1.1 |

* + - 1. **com.ctc.igd1.QoSPriorityQueue**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 无 | 启用队列 | 1.1 |
| Priority | UINT32 | readwrite | 无 | 优先级,取值范围1，2，3，4，5，6，7，8，要求和队列实例号保持一致 | 1.1 |
| Weight | UINT32 | readwrite | 无 | 设定权重的百分比，只有当计划选择为权重的时候才能填，并且所有启用队列的权重加起来要是100 | 1.1 |
| Car | INT32 | readwrite | 无 | 设置承诺访问速度阈值，只有在选择为承诺访问速度时有效，单位是Kbps。  -1表示不限制，0表示完全限制 | 1.1 |

* + - 1. **com.ctc.igd1.QoSApp**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| AppName | STRING(16) | readwrite | 无 | 有三个可选:“” ,“VOIP”, “TR069”缺省为：“” | 1.1 |
| ClassQueue | UINT32 | readwrite | 无 | 有8个队列可选：1，2，3，4，5，6，7，8，缺省值：1 | 1.1 |

* + - 1. **com.ctc.igd1.DNSSpeedLimit**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Domain | STRING(1023) | readwrite | 无 | 按照“m1/n1,m2/n2”格式设置，其中:  “m”为限速的一级域名域，如“sttri.com”。值为“ALL”表示对所有DNS域进行限速，值为“NULL”则表示不对任何DNS域进行限速。缺省值为“NULL”  “n”为相对于所设域名域家庭网关每分钟许可正常处理的DNS请求数量阈值，缺省值为1200 | 1.1 |
| LimitAction | STRING(32) | readwrite | 无 | 越限控制策略，可选值及相应要求如下：   * “Alert” * “Drop”：超出阈值的DNS请求被直接丢弃（无需向ITMS告警） | 1.1 |
| HgwInfo | STRING(63) | read | 无 | 网关WAN侧IP地址及MAC地址，以“|”分隔； | 1.1 |
| DeviceInfo | STRING(1023) | read | 有 | 当有域名域的DNS请求超过阈值时，记录请求相关越限域名域的源设备的IP地址及MAC，格式为“m1/IP1/MAC1,m1/IP2/MAC2,m2/IP3/MAC3”，其中“IP1/MAC1”为域名域“m1”对应的第一台源设备的IP地址及MAC，“IP2/MAC2”为域名域“m1”对应的第二台源设备的IP地址及MAC，以此类推 | 1.1 |

说明：DNS限速配置最大支持16条记录

* + - 1. **com.ctc.igd1.IPTV**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| IGMPEnable | BOOLEAN | read | 无 | IPTV是否启用，只是用作IPTV业务查询，没有实质的作用，缺省值：false（IGMP Proxy，IGMP Snooping缺省启用） | 1.1 |
| ProxyEnable | BOOLEAN | readwrite | 无 | 缺省值：true | 1.1 |
| SnoopingEnable | BOOLEAN | readwrite | 无 | 缺省值：true | 1.1 |
| STBNumber | UINT32 | read | 无 | 家庭网关自动发现机顶盒的数目 | 1.1 |
| iTVLineStatus | UINT32 | read | 有 | 当前线路状态，包括：  0：有组播流  1：有流量、无组播流  2：无流量 | 1.1 |
| NoStbEnable | boolean | read | 无 | 是否启用无STB承载IPTV业务功能，取值范围(true,false)，缺省值：false  当NoStbEnable开启时，带“other”关键字的路由WAN连接缺省作为承载IPTV业务的WAN连接 | 1.2 |

**方法**

* StartDetectiTVLineStatus(IN UINT32 duration, OUT UINT32 result，OUT STRING errdesc);

开始IPTV线路诊断，诊断前先将iTVLineStatus更新成默认值，诊断后将结果更新到iTVLineStatus属性

duration:单位：秒，范围：2~60秒，诊断持续最长时间。

result：0（成功）/1（失败）。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.IADDiagnostics**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| RegistResult | UINT32 | read | 有 | 注册是否成功，0：成功，1：失败 | 1.1 |
| Reason | UINT32 | read | 有 | 失败原因，取值范围：1：IAD模块错误，2：访问路由不通，3：访问服务器无响应，4：帐号错误，5：未知错误。如果注册成功，值为默认值99 | 1.1 |

**方法**

* StartIADDiagTest(IN UINT32 TestServer, OUT UINT32 result, OUT STRING errdesc);

开始VOIP IAD Diagnositcs测试

TestServer: 取值范围：1：主用服务器，2：备用服务器。

result：0（成功）/1（失败）。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.VoicePoorQualityStats**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| StatTime | STRING(16) | read | 无 | 生成记录的时间，UTC时间 | 1.1 |
| TxPackets | UINT64 | read | 无 | 发送包数 | 1.1 |
| RxPackets | UINT64 | read | 无 | 接收包数 | 1.1 |
| MeanDelay | UINT32 | read | 无 | 平均时延 | 1.1 |
| MeanJitter | UINT32 | read | 无 | 平均抖动 | 1.1 |
| FractionLoss | UINT32 | read | 无 | 丢包率，单位：%，取值，0-100 | 1.1 |
| LocalIPAddress | STRING(15) | read | 无 | 本端IP地址 点分十进制形式 | 1.1 |
| LocalUDPPort | UINT32 | read | 无 | 本端端口，0-65535 | 1.1 |
| FarEndIPAddress | STRING(15) | read | 无 | 远端IP地址 点分十进制形式 | 1.1 |
| FarEndUDPPort | UINT32 | read | 无 | 远端端口，0-65535 | 1.1 |
| MosLq | UINT32 | read | 无 | Mos值,单位0.1 | 1.1 |
| Codec | STRING(16) | read | 无 | 编解码:  “G.711MuLaw”  “G.711ALaw”  “G.729”  “G.722”  “T.38” | 1.1 |

默认预置10个实例，循环写入统计信息

* + - 1. **com.ctc.igd1.VOIPSimulateTest**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| CalledNumber | STRING(32) | Readwrite | 无 | 叫仿真时的被叫号码 | 1.1 |
| DialDTMFConfirmEnable | BOOLEAN | Readwrite | 无 | 拨号确认是否开启  是指接通主叫或被叫仿真后，另一侧的测试人员可以通过拨号确认其听到测试提示音清晰与否来确认通话是否OK | 1.1 |
| DialDTMFConfirmNumber | STRING(32) | Readwrite | 无 | 拨号确认的号码  只能是\*#0-9的字符 | 1.1 |
| DialDTMFConfirmResult | BYTE | Read | 有 | 拨号确认结果，  True:0  False:1  缺省:99 | 1.1 |
| Status | STRING(32) | Read | 有 | 仿真当前状态：  Idle 端口空闲  Off-hook 摘机  Dialtone 放拨号音  Receiving 收号  ReceiveEnd 收号完成  Ringing-back听回铃音  Connected通话状态  Testend 测试结束 | 1.1 |
| Conclusion | BYTE | Read | 有 | 仿真结果  0成功  1失败  缺省：99 | 1.1 |
| CallerFailReason | STRING(32) | Read | 有 | 主叫仿真失败原因  NoDailTone主叫无拨号音  OffhookRelease主叫摘机释放  DialingRelease主叫拨号时释放  AfterDialRelease主叫拨号后释放  NoAnswer主叫拨号后未通话  key error 按键与测试设定不一致 | 1.1 |
| CalledFailReason | STRING(32) | Read | 有 | 被叫仿真失败原因  NoIncomingCall未接收到呼叫  OffhookRelease被叫摘机释放  NoAnswer被叫未通话 | 1.1 |
| FailedResponseCode | UINT32 | Read | 有 | 仿真失败时接收到的错误码  0表示无错误码 | 1.1 |

**方法**

* StartTest(IN UINT32 TestType, OUT UINT32 result, OUT STRING errdesc);

开始语音仿真测试

TestType仿真测试类型：2：主叫仿真 1：被叫仿真 0：取消仿真

result：0（开始成功）/1（开始失败）。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.PhoneConnectivity**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| PhoneConnectivity | BOOLEAN | read | 有 | 是否连接了话机,true:有话机连接，false:无话机连接 | 1.1 |
| OffHookAlarmStatus | BOOLEAN | read | 有 | 是否处在长时间异常未挂机状态，true:是，false: 否 | 1.1 |

**方法**

* StartTest(OUT UINT32 result, OUT STRING errdesc);

开始语音话机连接性测试

result：0（成功）/1（失败）。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. **com.ctc.igd1.IPv6LANConfig**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| LocalAddress | STRING(45) | readwrite | 有 | IPv6管理地址 | 1.1 |
| ConfigType | STRING(32) | readwrite | 有 | DNS来源：HGWProxy, WANConnection, Static | 1.1 |
| DNSWAN | STRING(127) | readwrite | 有 | ConfigType为WANConnection时，WAN的DBUS绝对路径 | 1.1 |
| Servers | STRING(256) | readwrite | 有 | ConfigType为Static时，DNS服务器地址 | 1.1 |
| PrefixMode | STRING(32) | readwrite | 有 | 前缀来源：WANDelegated, Static | 1.1 |
| DelegatedWAN | STRING(127) | readwrite | 有 | PrefixMode为WANDelegated时，默认上网Internet WAN的DBUS绝对路径 | 1.1 |
| Prefix | STRING(45) | readwrite | 有 | PrefixMode为Static时，前缀地址 | 1.1 |
| PreferredLifeTime | UINT32 | readwrite | 有 | PrefixMode为Static时，前缀首选期 | 1.1 |
| ValidLifeTime | UINT32 | readwrite | 有 | PrefixMode为Static时，前缀合法期 | 1.1 |

* + - 1. **com.ctc.igd1.DHCPv6Server**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 有 | DHCPv6 Server使能 | 1.1 |
| MinAddress | STRING(45) | readwrite | 有 | 地址分配起始地址(IP地址的后64位)，格式为：“xxxx:xxxx:xxxx:xxxx” | 1.1 |
| MaxAddress | STRING(45) | readwrite | 有 | 地址分配结束地址(IP地址的后64位),格式为：“xxxx:xxxx:xxxx:xxxx” | 1.1 |
| PreferredLifeTime | UINT32 | readwrite | 有 | 单位为秒 | 1.1 |
| ValidLifeTime | UINT32 | readwrite | 有 | 单位为秒 | 1.1 |
| Option16Enable | BOOLEAN | readwrite | 有 | 是否检测Option16，缺省值：true | 1.1 |
| Option17Enable | BOOLEAN | readwrite | 有 | 是否检测Option17，缺省值：true | 1.1 |

* + - 1. **com.ctc.igd1.RouterAdvertisement**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 有 | RA使能 | 1.1 |
| MaxRtrAdvInterval | UINT32 | readwrite | 有 | 最大自动发送时间  缺省600秒 | 1.1 |
| MinRtrAdvInterval | UINT32 | readwrite | 有 | 最小自动发送时间  缺省200秒 | 1.1 |
| AdvManagedFlag | BOOLEAN | readwrite | 有 | RA M位  缺省 FALSE | 1.1 |
| AdvOtherConfigFlag | BOOLEAN | readwrite | 有 | RA O位  缺省 TRUE | 1.1 |

* + - 1. **com.ctc.igd1.CWMP**

**方法**

* AddObject(IN STRING ObjectName, OUT UINT32 InstNum, OUT UINT32 result, OUT STRING errdesc)
  + ObjectName：需要增加的TR069对象路径全称，例如：InternetGatewayDevice.WANDevice.1.WANConnectionDevice.
  + InstNum：非0，表示增加成功的实例号，等于0表示增加对象失败
  + result：0表示添加对象成功，1表示添加对象失败
  + errdesc：根据TR069相关返回内容
* DeleteObject(IN STRING ObjectName, OUT UINT32 result, OUT STRING errdesc)
  + ObjectName：需要删除的TR069对象路径全称，例如：InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1
  + result：0表示删除对象成功，1表示删除对象失败
  + errdesc：根据TR069相关返回内容
* SetParameterValues(IN a(ss) List, OUT UINT32 result, OUT STRING errdesc)
  + List：需要设置的的TR069参数路径全称及数值列表

[

('InternetGatewayDevice.ManagementServer.Username', 'itms'),

('InternetGatewayDevice.ManagementServer.Password', 'itms')

]

* + result：0表示设置成功，1表示设置失败
  + errdesc：根据TR069相关返回内容
* GetParameterValues(IN as List, OUTa(ss)ValueList, OUT UINT32 result, OUT STRING errdesc)
  + List：需要获取的TR069参数路径全称，如果路径以.结尾，表示获取对象下所有属性的取值

['InternetGatewayDevice.ManagementServer.Username','InternetGatewayDevice.X\_CT-COM\_UserInfo.']

* + ValueList：返回结果
  + result：0表示获取成功，1表示获取失败
  + errdesc：根据TR069相关返回内容
* GetParameterNames(IN STRING ObjectName, IN BOOLEANNextLevel, OUT a(sb) ParameterList, OUT UINT32 result, OUT STRING errdesc)
  + ObjectName：需要查询的TR069对象路径全称，例如：InternetGatewayDevice.WANDevice.1.WANConnectionDevice.
  + NextLevel：参考TR069对应参数
  + ParameterList：返回参数TR069路径
* [
* ('InternetGatewayDevice.ManagementServer.Username', 'false' ),
* ('InternetGatewayDevice.ManagementServer.Password', 'false')
* ]

前面是参数路径，后面表示是否可写

* + result：0表示获取成功，1表示获取失败
  + errdesc：根据TR069相关返回内容
    - 1. **com.ctc.igd1.MACBlackList**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC | STRING(12) | readwrite | 无 | STA的MAC地址 | 1.1 |
| Name | STRING(63) | readwrite | 无 | STA的别名 | 1.1 |
| BlockedTimes | UINT32 | read | 无 | 拦截该MAC的次数  当Enable置0时，BlockedTimes需清零 | 1.1 |

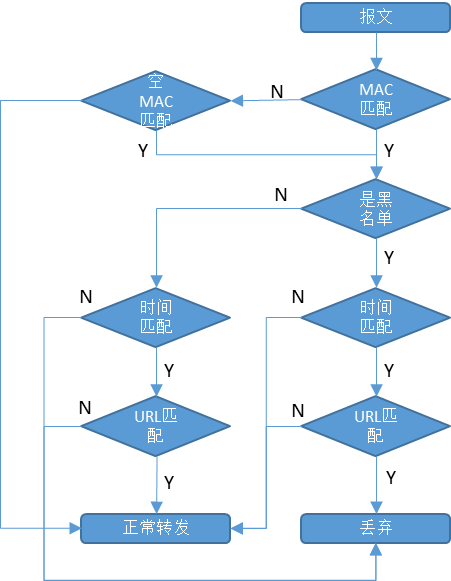
* + - 1. **com.ctc.igd1.MACWhiteList**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC | STRING(12) | readwrite | 无 | STA的MAC地址 | 1.1 |
| Name | STRING(63) | readwrite | 无 | STA的别名 | 1.1 |

* + - 1. **com.ctc.igd1.URLFilter**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
|  |  |  |  |  |  |
| Enable | BOOLEAN | readwrite | 无 | 是否使能  0：去使能  1：使能 | 1.1 |
| URL | STRING(255) | readwrite | 无 | URL地址, 格式:  <http://host:port>  支持模糊匹配，如baidu.com匹配所有baidu域名；  \*表示匹配所有域名。 | 1.1 |
| MAC | STRING(259) | readwrite | 无 | 对应的下挂设备的MAC，如果为空，此规则对应所有的下挂设备，该规则优先级最低。 | 1.1 |
| Name | STRING(63) | readwrite | 无 | 规则名称 | 1.1 |
| BlockedTimes | UINT32 | read | 无 | 拦截该URL的次数  当Enable置0时，BloeckedTimes需清零 | 1.1 |
| Mode | BYTE | readwrite | 无 | 黑白名单模式。  0：黑名单，默认模式；若报文匹配URLList的某项或者匹配URL字段，且匹配时间字段（WeekDays+ Time），则丢弃报文，否则正常转发；  1：白名单，若报文匹配URLList的某项或者匹配URL字段，且匹配时间字段（WeekDays+ Time），则正常转发，否则丢弃报文； | 1.2 |
| URLList | ARRAY<STRING(255)> | readwrite | 无 | URL列表，ARRAY内容的最大条目数为99。格式:  http://host:port  支持模糊匹配，如baidu.com匹配所有baidu域名 | 1.2 |
| WeekDays | STRING(31) | readwrite | 无 | 一个星期中哪几天该规则生效。如果是多天，采用英文逗号“,”分开，如：1,2,3,7表示星期一，星期二，星期三，星期天；为空等同于1,2,3,4,5,6,7，即每天生效。 | 1.2 |
| Time | STRING(63) | readwrite | 无 | 一天中该规则生效时间段。24小时格式，格式如00:00-08:00，多个时间段采用英文逗号“,”分开，最多允许3个时间段，时间段之间不允许有交集；时间段00:00-00:00表示全天生效。为空等同于00:00-00:00，即全天生效。 | 1.2 |

备注：当同时存在DNSSpeedLimit和URLFilter两类规则时，应先执行DNSSpeedLimit操作。至少支持32个MAC地址设备做过滤，各表项MAC地址不能冲突，即一个MAC只能配置一次，每个设备最多可以配置100条过滤规则，URL和URLList两个字段都有效；针对路由模式上行有效。URL详细匹配参考流程如下：



* + - 1. **com.ctc.igd1.DNSFilter**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 无 | 是否使能  0：去使能  1：使能 | 1.1 |
| Name | STRING(63) | readwrite | 无 | 规则名称 | 1.1 |
| Hostname | STRING(255) | readwrite | 无 | 需要过滤的Hostname，  支持模糊匹配，如baidu.com匹配所有baidu域名；  \*表示匹配所有域名。 | 1.1 |
| Action | BYTE | readwrite | 无 | 对于hostname DNS请求的处理。  0：不处理，不代理该DNS请求；  1：回复网关LAN IP地址；  2：DNS回复Name Error。 | 1.1 |
| MAC | STRING(12) | readwrite | 无 | 对应的下挂设备的MAC.  如果为空，此规则对应所有的下挂设备，该规则优先级最低。 | 1.1 |
| BlockedTimes | UINT32 | read | 无 | 拦截该DNS查询的次数  Action值修改后，BlockedTimes需重新计数  当Enable置0时，BloeckedTimes需清零 | 1.1 |
| Mode | BYTE | readwrite | 无 | 黑白名单模式。  0：黑名单，默认模式；当前DNS请求的URL如果能匹配Hostname 或者HostNameList的某项，且匹配时间字段（WeekDays+ Time），则按照Action动作执行，否则正常转发；  1：白名单，当前DNS请求的URL如果匹配Hostname 或者HostNameList的某项，且匹配时间字段（WeekDays+ Time），则正常转发，否则按照Action动作执行。 | 1.2 |
| HostNameList | ARRAY<STRING(255)> | readwrite | 无 | DNS域名列表，ARRAY内容的最大条目数为99。 | 1.2 |
| WeekDays | STRING(31) | readwrite | 无 | 一个星期中哪几天该规则生效。如果是多天，采用英文逗号“,”分开，如：1,2,3,7表示星期一，星期二，星期三，星期天；为空等同于1,2,3,4,5,6,7，即每天生效。 | 1.2 |
| Time | STRING(63) | readwrite | 无 | 一天中该规则生效时间段。24小时格式，格式如00:00-08:00，多个时间段采用英文逗号“,”分开，最多允许3个时间段，时间段之间不允许有交集；时间段00:00-00:00表示全天生效。为空等同于00:00-00:00，即全天生效。 | 1.2 |

说明：DNSFilter最大条数暂定100。至少支持32个MAC地址设备做过滤，各表项MAC地址不能冲突，即一个MAC只能配置一次，每个设备最多可以配置100条过滤规则，Hostname和HostNameList两个字段都有效；http和https都能过滤；针对路由模式上行有效。

* + - 1. **com.ctc.igd1.SpeedTestFF**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| TestingStatus | BOOLEAN | read | 有 | 测速的状态（true表示正在测试，false表示测速结束） | 1.1 |
| Result | UINT32 | read | 无 | Result =0表示成功；  Result =1表示失败 | 1.1 |
| Ticket | STRING(80) | readwrite | 无 | 测速门票取值64 | 1.1 |
| SpeedType | BYTE | readwrite | 无 | 测速类型：1-下行测速鉴权、2-上行测速鉴权、3-上、下行测速鉴权 | 1.1 |
| URL | STRING(1023) | readwrite | 无 | URL表示设置进行下载的URL地址，如果是多个测速地址，应该以“|”区隔（格式：http://IP:端口号，网关在处理时，需要过滤掉“http://”，采用通信协议为TCP）  取值1024 | 1.1 |
| DW\_SPEED\_MAX\_RATE | STRING(16) | read | 无 | 下载峰值速率（KB） | 1.1 |
| DW\_SPEED\_RATE | STRING(16) | read | 无 | 下载平均速率（KB） | 1.1 |
| UP\_SPEED\_MAX\_RATE | STRING(16) | read | 无 | 上传峰值速率（KB） | 1.1 |
| UP\_SPEED\_RATE | STRING(16) | read | 无 | 上传平均速率（KB） | 1.1 |
| BEGIN\_TIME | STRING(32) | read | 无 | 测速起始时间（yyyy-MM-dd HH:mm:ss） | 1.1 |
| END\_TIME | STRING(32) | read | 无 | 测速结束时间（yyyy-MM-dd HH:mm:ss） | 1.1 |

**方法**

* StartTest(IN UINT32 time, OUT UINT32 result, OUT STRING errdesc);
* 启动测速。
* time为持续时间，如果SpeedType=3，则上下行时间均为time秒。
* 开始正式测试前，应清除DW\_SPEED\_MAX\_RATE、DW\_SPEED\_RATE、UP\_SPEED\_MAX\_RATE、UP\_SPEED\_RATE、BEGIN\_TIME、END\_TIME的属性值。
* 测速结束后，更新相关测速状态和测试结果。
* 请注意测速前后的TestingStatus状态和变更通知。
  + - 1. **com.ctc.igd1.FeatureFlag**

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| H248 | BOOLEAN | read | 无 | 当前网关是否实际使用H248业务，TRUE:在用FALSE:未使用 | 1.2 |
| PortBind | BOOLEAN | read | 无 | 当前网关是否实际使用端口绑定业务，TRUE:在用FALSE:未使用 | 1.2 |
| VlanBind | BOOLEAN | read | 无 | 当前网关是否实际使用VLAN 绑定业务，TRUE:在用 FALSE:未使用 | 1.2 |
| OnDemondDialin | BOOLEAN | read | 无 | 当前网关是否实际使用按需拨号业务，TRUE:在用FALSE:未使用 | 1.2 |

* + - 1. **com.ctc.igd1.CLOUDVR**

属性

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | read | 有 | Cloud VR是否启用，缺省值：false | 1.2 |
| UserID | STRING | read | 无 | Cloud VR用户账号信息，缺省为空 | 1.2 |
| Password | STRING | read | 无 | Cloud VR用户密码信息，缺省为空 | 1.2 |

* + 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口名 | 权限 |
| /com/ctc/igd1 |  |  |
| /com/ctc/igd1/Config/DHCPServer | com.ctc.igd1.DHCPServer | DHCP服务配置 |
| /com/ctc/igd1/Config/IncomingFilter | com.ctc.igd1.IncomingFilter | 插件端口配置 |
| /com/ctc/igd1/Config/IPV6/DHCPV6S | com.ctc.igd1.DHCPV6Server | DHCPV6服务器配置 |
| /com/ctc/igd1/Config/IPV6/LAN | com.ctc.igd1.IPV6LANConfig | IPV6 LAN配置 |
| /com/ctc/igd1/Config/IPV6/RA | com.ctc.igd1.RouterAdvertisement | IPV6 RA配置 |
| /com/ctc/igd1/Config/LANHosts | com.ctc.igd1.LANHostManager com.ctc.igd1.ObjectManager | 查看内网设备信息（不要求AddObject方法，但应支持对不受控的离线设备实例进行DeleteObject操作） |
| /com/ctc/igd1/Config/LANHosts/{i} | com.ctc.igd1.LANHost | 查看内网设备信息 |
| /com/ctc/igd1/Config/Peripheral/LED | com.ctc.igd1.LED | LED控制 |
| /com/ctc/igd1/Config/PortMapping | com.ctc.igd1.ObjectManager | 端口映射配置 |
| /com/ctc/igd1/Config/PortMapping/{i} | com.ctc.igd1.PortMapping | 端口映射配置 |
| /com/ctc/igd1/Config/Power/SleepTimers | com.ctc.igd1.ObjectManager | 休眠控制 |
| /com/ctc/igd1/Config/Power/SleepTimers/{i} | com.ctc.igd1.SleepTimer | 休眠控制 |
| /com/ctc/igd1/Config/WLAN/BandSteering | com.ctc.igd1.WiFiBandSteering | Wifi BandSteering 配置 |
| /com/ctc/igd1/Config/WLAN/Devices | com.ctc.igd1.ObjectManager | WiFi配置 |
| /com/ctc/igd1/Config/WLAN/Devices/{i} | com.ctc.igd1.WLANConfiguration | WiFi配置，注意{i}须和SSIDIndex保持一致 |
| /com/ctc/igd1/Config/WLAN/Devices/{i}/WPS | com.ctc.igd1.WPS | WiFi配置 |
| /com/ctc/igd1/Config/WLAN/ExTimers | com.ctc.igd1.ObjectManager | WiFi配置 |
| /com/ctc/igd1/Config/WLAN/ExTimers/{i} | com.ctc.igd1.WiFiTimer1 | WiFi配置 |
| /com/ctc/igd1/Config/WLAN/Timer | com.ctc.igd1.WiFiTimer | WiFi配置 |
| /com/ctc/igd1/Diagnostics/HttpDownload | com.ctc.igd1.HttpDownloadTest com.ctc.igd1.SpeedTestFF | 设备诊断 |
| /com/ctc/igd1/Diagnostics/IADTest | com.ctc.igd1.IADDiagnostics | IAD诊断 |
| /com/ctc/igd1/Diagnostics/VoiceSimulateTest | com.ctc.igd1.VOIPSimulateTest | 语音测试 |
| /com/ctc/igd1/Info/Device | com.ctc.igd1.DeviceInfo | 查看设备信息 |
| /com/ctc/igd1/Info/Network | com.ctc.igd1.NetworkInfo | 查看网络信息 |
| /com/ctc/igd1/Info/Network/WANConnectionDb | com.ctc.igd1.WANConnectionDb com.ctc.igd1.ObjectManager | 查看网络信息（不要求AddObject和 DeleteObject方法） |
| /com/ctc/igd1/Info/Network/WANConnectionDb/{i} | com.ctc.igd1.WANConnectionInfo | 查看网络信息 |
| /com/ctc/igd1/Info/PhoneConnectivity | com.ctc.igd1.PhoneConnectivity | 电话状态 |
| /com/ctc/igd1/Info/PON | com.ctc.igd1.PONInfo | 查看PON信息 |
| /com/ctc/igd1/Info/Voice/PoorQualityStats | com.ctc.igd1.ObjectManager | 语音异常统计，不需要支持AddObject和DelObject方法 |
| /com/ctc/igd1/Info/Voice/PoorQualityStats/{i} | com.ctc.igd1.VoicePoorQualityStats | 语音异常统计，不需要支持AddObject和DelObject方法 |
| /com/ctc/igd1/Info/VoIP | com.ctc.igd1.VoIPInfo | 查看电话信息 |
| /com/ctc/igd1/Info/WiFi | com.ctc.igd1.WiFiInfo | 查看WiFi信息 |
| /com/ctc/igd1/Info/FeatureFlag | com.ctc.igd1.FeatureFlag | 查看已有功能是否使用信息 |
| /com/ctc/igd1/Network/DNSFilter | com.ctc.igd1.ObjectManager | DNS过滤 |
| /com/ctc/igd1/Network/DNSFilter/{i} | com.ctc.igd1.DNSFilter | DNS过滤 |
| /com/ctc/igd1/Network/DNSSpeedLimit | com.ctc.igd1.DNSSpeedLimit | DNS限速 |
| /com/ctc/igd1/Network/IPTV | com.ctc.igd1.IPTV | IPTV配置 |
| /com/ctc/igd1/Network/MACBlackList | com.ctc.igd1.ObjectManager | MAC黑名单配置 |
| /com/ctc/igd1/Network/MACBlackList/{i} | com.ctc.igd1.MACBlackList | MAC黑名单配置 |
| /com/ctc/igd1/Network/MACWhiteList | com.ctc.igd1.ObjectManager | MAC白名单配置 |
| /com/ctc/igd1/Network/MACWhiteList/{i} | com.ctc.igd1.MACWhiteList | MAC白名单配置 |
| /com/ctc/igd1/Network/QoS | com.ctc.igd1.QoS | QoS配置 |
| /com/ctc/igd1/Network/QoS/App | com.ctc.igd1.ObjectManager | QoS配置 |
| /com/ctc/igd1/Network/QoS/App/{i} | com.ctc.igd1.QoSApp | QoS配置 |
| /com/ctc/igd1/Network/QoS/Classification | com.ctc.igd1.ObjectManager | QoS配置 |
| /com/ctc/igd1/Network/QoS/Classification/{i} | com.ctc.igd1.QoSClassification | QoS配置 |
| /com/ctc/igd1/Network/QoS/Classification/{i}/Type | com.ctc.igd1.ObjectManager | QoS配置 |
| /com/ctc/igd1/Network/QoS/Classification/{i}/Type/{i} | com.ctc.igd1.QoSClassificationType | QoS配置 |
| /com/ctc/igd1/Network/QoS/PriorityQueue | com.ctc.igd1.ObjectManager | QoS配置，不需要支持AddObject和DelObject方法 |
| /com/ctc/igd1/Network/QoS/PriorityQueue/{i} | com.ctc.igd1.QosPriorityQueue | QoS配置 |
| /com/ctc/igd1/Network/URLFilter | com.ctc.igd1.ObjectManager | URL过滤 |
| /com/ctc/igd1/Network/URLFilter/{i} | com.ctc.igd1.URLFilter | URL过滤 |
| /com/ctc/igd1/Telecom/CWMP | com.ctc.igd1.CWMP | TR098参数配置 |
| /com/ctc/igd1/Telecom/PlatformService | com.ctc.igd1.PlatformService | 平台服务相关 |
| /com/ctc/igd1/Telecom/PPPoE | com.ctc.igd1.PPPoE | 电信配置 |
| /com/ctc/igd1/Telecom/System | com.ctc.igd1.SysCmd | 电信配置 |

* 1. 其它网关服务接口要求
     1. USB设备管理服务

为了支持USB Dongle以及USB存储业务，厂家需按照本章节规范，封装DBus服务，提供给开发者，实现所插USB设备（含通过USB HUB下挂的设备）的控制和访问。

对于非存储类设备，在/com/ctc/igd1/Storage/usb/devices/{i}下只需要com.ctc.igd1.usb.Device接口，不需要com.ctc.igd1.usb.FileSystem接口。

* + - 1. DBus接口
         1. com.ctc.igd1.usb.Device

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| DeviceType | UINT16 | read | 无 | CtUsbDevType | 1.0 |
| DeviceId | INT32 | read | 无 |  | 1.0 |
| DeviceName | STRING(63) | read | 无 |  | 1.0 |
| Vendor | STRING(63) | read | 无 | 厂商名字, 例如SanDisk | 1.0 |
| Model | STRING(63) | read | 无 | USB 型号，例如: U3 Cruzer Micro | 1.0 |
| WriteProtection | BOOLEAN | read | 无 | 写保护：true，没有写保护：false | 1.0 |

* + - * 1. com.ctc.igd1.usb.FileSystem

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MountPoint | STRING(127) | read | 无 | 挂载点 | 1.0 |
| TotalSize | UINT64 | read | 无 | 单位byte | 1.0 |
| UsedSize | UINT64 | read | 无 | 单位byte | 1.0 |
| FreeSize | UINT64 | read | 无 | 单位byte | 1.0 |
| Label | STRING(127) | read | 无 | 标签名称 | 1.0 |

**方法**

* Mount(IN a{sv} options, OUT s mount\_path, OUT UINT32 result，OUT STRING errdesc);

挂载文件系统

* Unmount{IN a{sv} options, OUT UINT32 result，OUT STRING errdesc };

卸载文件系统

* SetLabel(IN s label, OUT UINT32 result，OUT STRING errdesc);

设置Label

* Format(IN a{sv} options, OUT UINT32 result，OUT STRING errdesc);

格式化USB设备

result：0 on success, 1 on fail

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description。

备注：  
Mount/Unmount命令的参数中，有部分是带短号的，比如’-t’，也有不带短号的，比如mount的路径。对{sv}现在统一定义如下：

1）所有的带短号的，都作为这里的STRING，短号后面的参数则作为GVariant。也有部分带短号的option是不带参数的，比如’-r’，’-w’等，碰到这种情况GVariant的内容就用字符串”NULL”来填充；

2）对于不带短号的参数，把STRING部分用字符串”NULL”来填充，Gvariant的内容就用参数内容即可；

3）{sv}可以为mount里面’-o’的内容，也可以指其它的参数。

比如’mount -t smbfs –r -o username=guest,password=guest /dev/sdb1 /mnt/mydir’这命令，转化后就是这样的：

{ <string:”-t”, variant:string:”smbfs”>,

 <string:”-r”, variant:string:”NULL”>,

 <string:”-o”, variant:string:”username=guest,password=guest”>,

<sting:”NULL”, variant:string:”/dev/sdb1”>,

<sting:”NULL”, variant:sting:”/mnt/mydir”>}

/dev/sdb1 指Com.ctc.igd1.usb.Device 里面的DeviceId 或者DeviceName 参数；

/mnt/mydir指Com.ctc.igd1.usb.FileSystem的MountPoint参数。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Storage/usb |  | USB控制 |
| /com/ctc/igd1/Storage/usb/devices | com.ctc.igd1.ObjectManager | USB控制（不要求AddObject、DeleteObject方法） |
| /com/ctc/igd1/Storage/usb/devices/{i} | com.ctc.igd1.usb.FileSystem  com.ctc.igd1.usb.Device | USB控制 |

* + 1. NAS服务
       1. DBus接口
          1. com.ctc.igd1.NASAccess

**方法**

* GetFileNum(IN STRING folderName, OUT UINT32 fileNum, OUT UINT32 result, OUT STRING errdesc);
* ListFolder(IN STRING folderName, IN UINT32 StartIndex, IN UINT32 EndIndex, OUT ARRAY<STRUCT<STRING, STRING, BOOLEAN, UINT64, STRING>> FileList, OUT UINT32 result, OUT STRING errdesc);

*FileList: FileName – STRING, PhysicalFolderName – STRING, IsFolder – BOOLEAN, FileSize – UINT64, ModifiedTime – STRING.*

* CreateFolder(IN STRING folderName, OUT UINT32 result, OUT STRING errdesc);
* Rename(IN STRING oldName, IN STRING newName, OUT UINT32 result, OUT STRING errdesc);
* Remove(IN STRING name, OUT UINT32 result, OUT STRING errdesc);
* Move(IN STRING filename, IN STRING destFolderName, OUT UINT32 result, OUT STRING errdesc);
* Copy(IN STRING name, IN STRING destFolderName, OUT UINT32 TransactionId, OUT UINT32 result, OUT STRING errdesc);
* GetCopyProgress(IN UINT32 TransactionId,OUT UINT32 Percent, OUT UINT32 result, OUT STRING errdesc);

result：0 on success, 1 on fail

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description

备注：

1、ListFolder方法只需查询当前路径的文件及文件夹，不需要递归查询；

2、StartIndex从1开始。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 备注 |
| /com/ctc/igd1/Storage/nas | com.ctc.igd1.NASAccess | NAS控制 |

* + 1. VPN客户端服务
       1. DBus接口
          1. com.ctc.igd1.VPNConnection

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| vpn\_type | STRING(15) | readwrite | 无 | VPN的类型：l2tp或pptp | 1.0 |
| tunnel\_name | STRING(63) | readwrite | 无 | VPN通道的名称 | 1.0 |
| user\_id | STRING(63) | readwrite | 无 | 由平台分配，用于区分VPN业务的提供者，标识VPN通道 | 1.0 |
| vpn\_enable | BYTE | readwrite | 无 | 1表示使能，0表示去使能 | 1.0 |
| vpn\_status | BYTE | read | 无 | Vpn通道的状态，  0表示正常，1表示不正常 | 1.0 |
| vpn\_mode | STRING(15) | readwrite | 无 | VPN模式，代表该VPN是否采用动态账号；  参数包括：  random：动态账号，每次重连时需要向平台请求账号；  steady：账号恒定； | 1.0 |
| vpn\_priority | STRING(7) | readwrite | 无 | VPN的优先级，取值0—7，值越小优先级越高； | 1.0 |
| vpn\_idletime | STRING(15) | readwrite | 无 | VPN自动断开前需等待的时间，单位为秒。默认值：0，代表不断开； | 1.0 |
| account\_proxy | STRING(63) | readwrite | 无 | VPN获取动态账号密码的地址；仅当vpn\_mode为random时生效； | 1.0 |
| vpn\_addr | STRING(63) | readwrite | 无 | VPN连接的地址 | 1.0 |
| vpn\_account | STRING(63) | readwrite | 无 | VPN账号 | 1.0 |
| vpn\_pwd | STRING(63) | readwrite | 无 | VPN密码 | 1.0 |
| vpn\_port | STRING(5) | readwrite | 无 | VPN端口 | 1.0 |
| attach\_mode | STRING(3) | readwrite | 无 | 0（默认值）；同时支持按目的地址和按源MAC地址；  1：按目的地址；  2：按源MAC地址。 | 1.0 |
| domains | ARRAY<STRING(63)> | readwrite | 无 | 加速域名，ARRAY内容的最大条目数为2048。attach\_mode为0或1时，该参数生效，网关以新配置内容覆盖原有配置 | 1.0 |
| ips | ARRAY<STRING(63)> | readwrite | 无 | 加速IP，ARRAY内容的最大条目数为2048。attach\_mode为0或1时，该参数生效，网关以新配置内容覆盖原有配置 | 1.0 |
| terminal\_mac | ARRAY<STRING(20)> | readwrite | 无 | 加速MAC，ARRAY内容的最大条目数为64。attach\_mode为0或2时生效，网关以新配置内容覆盖原有配置 | 1.0 |

说明：

当vpn\_mode参数为random时，网关建立VPN前需向平台获取VPN账号（由网关底层实现），具体要求参见《中国电信智能家庭网关与智能网关及应用管理平台接口技术要求》。

* + - * 1. com.ctc.igd1.VPNConnectionStats

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| data | ARRAY<STRING(63)> | read | 无 | domain@count: 关联的域名@次数或  ip@count:关联的ip@次数 | 1.0 |

**说明：**

目的地址是特定的domain或者IP的封包被VPN处理的次数,  比如有100个封包通过VPN发往 domain [www.amazon.com](http://www.amazon.com/), 则返回100。

” domain@count”或者” ip@count”中的domain和ip按照下发的规则进行上报：下发的域名带通配符，则上报也按照有通配符的格式，若下发的IP是掩码格式，则上报也是掩码格式。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 备注 |
| /com/ctc/igd1/Network /VPN /Connection | com.ctc.igd1.ObjectManager | VPN客户端控制 |
| /com/ctc/igd1/Network/VPN /Connection/{i} | com.ctc.igd1.VPNConnection | VPN客户端控制 |
| /com/ctc/igd1/Network/VPN/Connection/{i}/Stats | com.ctc.igd1.VPNConnectionStats | VPN客户端控制统计 |

* + 1. DNS服务
       1. DBus接口
          1. com.ctc.igd1.DNSServerConfig

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Server1 | STRING(23) | readwrite | 有 | 首选DNS服务器 | 1.0 |
| Server2 | STRING(23) | readwrite | 有 | 备选DNS服务器 | 1.0 |

**方法**

* FlushDNS(OUT UINT32 result，OUT STRING errdesc);

清除DNS缓存。

* + - * 1. com.ctc.igd1.DNSTunnel

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ServerIP | STRING(23) | readwrite | 无 |  | 1.0 |
| DomainName | ARRAY<STRING(63)> | readwrite | 无 |  | 1.0 |

* + - * 1. com.ctc.igd1.DNSv6ServerConfig

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Server1 | STRING(63) | readwrite | 有 | 首选DNS服务器 | 1.0 |
| Server2 | STRING(63) | readwrite | 有 | 备选DNS服务器 | 1.0 |

**方法**

* FlushDNS(OUT UINT32 result，OUT STRING errdesc);

清除DNS缓存。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Network/dns | com.ctc.igd1.ObjectManager  com.ctc.igd1.DNSServerConfig | DNS服务配置 |
| /com/ctc/igd1/Network/dns/{i} | com.ctc.igd1.DNSTunnel | DNS服务配置 |
| /com/ctc/igd1/Network/dnsv6 | com.ctc.igd1.DNSv6ServerConfig | DNSv6服务配置 |

* + 1. DDNS服务
       1. DBus接口
          1. com.ctc.igd1.DDNSServerConfig

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| DDNSCfgEnabled | BOOLEAN | readwrite | 无 | 启动DDNS功能开  关量，取值范围(true,false)，缺省值：false | 1.0 |
| DDNSStatus | BTYE | read | 无 | DDNSStatus表示此DDNS的当前的运行或错误状态（0表示正常运行,1表示未启用,2请填写服务端口,3表示连接DDNS服务商平台失败,4表示DDNS帐号在服务商平台认证失败, 5请填写DDNS用户名,6请填写DDNS密码,7请填写DDNS域名,8请填写DDNS主机名,9表示其它错误,错误码xxx,10 DDNS服务商拒绝服务,错误码xxx，11表示正在向DDNS服务商认证，12表示认证成功，正在解析） | 1.0 |
| DDNSProvider | STRING(63) | readwrite | 无 | 服务提供商 | 1.0 |
| DDNSUsername | STRING(31) | readwrite | 无 | DDNS用户名 | 1.0 |
| DDNSPassword | STRING(31) | readwrite | 无 | DDNS密码 | 1.0 |
| ServicePort | UINT32 | readwrite | 无 | 服务端口（花生壳默认6060） | 1.0 |
| DDNSDomainName | STRING(63) | readwrite | 无 | DDNS域名 | 1.0 |
| DDNSHostName | STRING(63) | readwrite | 无 | DDNS主机名 | 1.0 |
| DDNSIP | STRING(15) | read | 无 | DDNS解析到的公网IP | 1.1 |
| DDNSErrMsg | STRING(63) | read | 无 | 当DDNSStatus的值为9或10时，请描述详细错误信息 | 1.1 |

说明：本接口默认对应Internet WAN连接下。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Network/ddns | com.ctc.igd1.ObjectManager | DDNS服务配置 |
| /com/ctc/igd1/Network/ddns/{i} | com.ctc.igd1.DDNSServerConfig | DDNS服务配置 |

* + 1. FTP服务
       1. DBus接口
          1. com.ctc.igd1.FTPServer

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BYTE | readwrite | 有 | 网关FTP服务是否开启，其中0：表示服务关闭；1：表示本地开启，远程关闭；2：表示本地关闭，远程开启；3;表示本地、远程开启 | 1.0 |
| AllowAnonymous | BOOLEAN | readwrite | 有 | 是否允许匿名访问 | 1.0 |
| Port | UINT32 | read | 无 | FTP服务端口取值范围0-65535 | 1.0 |

* + - * 1. com.ctc.igd1.FTPAccount

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| UserName | STRING(47) | readwrite | 有 | FTP用户名 | 1.0 |
| Password | STRING(47) | readwrite | 有 | FTP密码 | 1.0 |

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 备注 |
| /com/ctc/igd1/Storage/Ftpserver | com.ctc.igd1.FTPServer | FTP服务配置 |
| /com/ctc/igd1/Storage/Ftpserver/Accounts | com.ctc.igd1.ObjectManager | FTP服务配置 |
| /com/ctc/igd1/Storage/Ftpserver/Accounts/{i} | com.ctc.igd1.FTPAccount | FTP服务配置 |

* + 1. Samba服务
       1. DBus接口
          1. com.ctc.igd1.SambaServer

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BYTE | readwrite | 有 | 表示网关Samba服务是否开启，其中0：表示服务关闭；1：表示本地开启，远程关闭；2：表示本地关闭，远程开启；3：表示本地、远程开启 | 1.0 |
| AllowAnonymous | BOOLEAN | readwrite | 有 | 是否允许匿名访问 | 1.0 |

* + - * 1. com.ctc.igd1.SambaAccount

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| UserName | STRING(47) | readwrite | 有 | Samba用户名 | 1.0 |
| Password | STRING(47) | readwrite | 有 | Samba密码 | 1.0 |

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Storage/SambaServer | com.ctc.igd1.SambaServer | Samba服务器配置 |
| /com/ctc/igd1/Storage/SambaServer/Accounts | com.ctc.igd1.ObjectManager | Samba服务器配置 |
| /com/ctc/igd1/Storage/SambaServer/Accounts/{i} | com.ctc.igd1.SambaAccount | Samba服务器配置 |

* + 1. HTTP服务
       1. DBus接口
          1. com.ctc.igd1.HTTPServer

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| AdminPassword | STRING(47) | read | 有 | telecomadmin密码 | 1.0 |

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 备注 |
| /com/ctc/igd1/Network/HTTPServer | com.ctc.igd1.HTTPServer | HTTP服务器配置 |

* + 1. Telnet服务
       1. DBus接口
          1. com.ctc.igd1.TelnetServer

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BYTE | readwrite | 无 | 网关Telnet服务是否开启，其中0：表示服务关闭；1：表示本地开启，远程关闭；2：表示本地关闭，远程开启；3：表示本地、远程开启 | 1.0 |
| LANPort | UINT32 | read | 无 | LAN侧Telnet服务端口取值范围0-65535 | 1.0 |
| WANPort | UINT32 | read | 无 | WAN侧Telnet服务端口取值范围0-65535 | 1.0 |

说明：Telnet服务开启时，未限定LAN侧或WAN侧服务端口在LAN侧、WAN侧同时生效。

* + - * 1. com.ctc.igd1.TelnetAccount

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| UserName | STRING(47) | read | 无 | Telnet用户名 | 1.0 |
| Password | STRING(47) | read | 无 | Telnet密码 | 1.0 |
| Type | STRING(7) | read | 无 | Telnet服务类型，取值范围LAN/WAN/BOTH | 1.0 |

说明：Telnet用户创建时，服务类型默认为BOTH。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 备注 |
| /com/ctc/igd1/Network /Telnetserver | com.ctc.igd1. TelnetServer | Telnet服务配置 |
| /com/ctc/igd1/Network/Telnetserver/Accounts | com.ctc.igd1.ObjectManager | Telnet服务配置（不要求AddObject、DeleteObject方法） |
| /com/ctc/igd1/Network/Telnetserver/Accounts/{i} | com.ctc.igd1. TelnetAccount | Telnet服务配置 |

* + 1. Beacon/Probe帧扩展Vendor-specific Information Element服务
       1. DBus 接口
          1. com.ctc.igd1.VSIE.BeaconTxVSIEManager

属性

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAM | readwrite | 无 | 功能开启 | 1.1 |
| MaxEntryNum | UINT32 | readwrite | 无 | 最大实例条目，默认值为8 | 1.1 |
| CurrentEntryNum | UINT32 | read | 无 | 当前实例条目 | 1.1 |
| MaxConcurrentTask | UINT32 | read | 无 | 最大的并行发送任务数，不得低于3。 | 1.1 |

**方法**

* GetBeaconTxVSIEByServiceName(IN STRING ServiceName, OUT OBJECT\_PATH path, OUT UINT32 result，OUT STRING errdesc);

获取ServiceName（对应com.ctc.igd1.VSIE.BeaconTxVSIE的ServiceName）的对应/com/ctc/igd1/VSIE/BeaconTxVSIE/{i}对象的路径名。result: 0 表示成功, 1 表示失败，2表示系统忙（当CurrentEntryNum等于MaxEntryNum时）。

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description

* + - * 1. com.ctc.igd1.VSIE.BeaconTxVSIE

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ServiceName | STRING(63) | readwrite | 无 | 服务名称 | 1.1 |
| Status | BYTE | readwrite | 有 | 0表示成功，1表示失败, 2表示忙，3表示被停止 | 1.1 |
| SSIDIndex | BYTE | readwrite | 无 | 对应的SSID Index | 1.1 |
| Duration | UINT32 | readwrite | 无 | 发送时间，默认值为0，表示没有发送  取值范围0-300 | 1.1 |
| IEData | ARRAY<BYTE> | readwrite | 无 | 发送的Vendor-specific Information Element内容 | 1.1 |
| LenofIEData | UINT32 | readwrite | 无 | IEData的长度 | 1.1 |

**方法**

* StartBeaconTxVSIE( OUT UINT32 result, OUT STRING errdesc);
* StopBeaconTxVSIE(OUT UINT32 result, OUT STRING errdesc);

result: 0 表示成功, 1 表示失败，2表示系统忙

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description

说明：

1. Duration为发送持续时间，单位为秒，允许0-300，当为0时，表示中止当前发送；
2. IEData包含完整的Vendor-specific Information Element，LenOfIEData为IEData的长度；
3. 一个ServiceName只允许在Beacon帧中发送一个Vendor-specific Information Element，固件需对插件发送的内容进行合法性检查。
4. 在发送期间，插件能调用StopBeaconTxvSIE方法来终止发送任务；
5. 系统需最多同时支持不低于3个ServiceName发送Vendor-specific Information Element。当达到3个ServiceName在发送中时，调用返回busy，插件应等待5秒重试。
6. 服务名称跟插件的DBus服务名称保持一致。插件正常退出时，应删除添加的/com/ctc/igd1/VSIE/ProbeRxVSIE/{i}实例，该实例如果没有插件使用，中间件也会定期删除。
   * + - 1. com.ctc.igd1.VSIE.ProbeRxVSIEManager

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| Enable | BOOLEAN | readwrite | 无 | 服务是否开启 | 1.1 |
| MaxEntryNum | UINT32 | read | 无 | 支持最大的条目数，要求不得小于3条。 | 1.1 |
| CurrentEntryNum | UINT32 | read | 有 | 当前条目的数量 | 1.1 |

**方法**

* GetProbeRxVSIEByServiceName(IN STRING ServiceName, OUT OBJECT\_PATH path, OUT UINT32 result，OUT STRING errdesc);

获取ServiceName（对应com.ctc.igd1.VSIE.ProbeRxVSIE的ServiceName）的对应/com/ctc/igd1/VSIE/BeaconTxVSIE/{i}对象的路径名。当插件退出时，应删除该路径的对象。

result: 0 表示成功, 1 表示失败，2表示系统忙（当CurrentEntryNum等于MaxEntryNum时）。

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description.

* + - * 1. com.ctc.igd1.VSIE.ProbeRxVSIE

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ServiceName | STRING(63) | readwrite | 无 | 服务名称 | 1.1 |
| ProbeBand | BYTE | readwrite | 无 | 0表示2.4G，1表示5G，2表示2.4G和5G | 1.1 |
| OUI | ARRAY<BYTE> | readwrite | 无 | OUI，二进制格式，数组大小是3. | 1.1 |

* + - * 1. com.ctc.igd1.VSIE.ProbeRxVSIERecordManager

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| RecordNum | UINT32 | read | 无 | ProbeRxVSIERecord的条目, 系统支持的最大条目数不得小于10条。 | 1.1 |

**方法**

* FlushProbeRxVSIERecord(OUT UINT32 result，OUT STRING errdesc);

清空所有该对象下面的RxVSIERecord实例。

Result: 0 on success, 1 on fail

errdesc: If errdesc is NULL or function success, do nothing; otherwise fill with error description

* + - * 1. com.ctc.igd1.VSIE.ProbeRxVSIERecord

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC | STRING(12) | read | 无 | STA的MAC | 1.1 |
| VSIE | ARRARY(BYTE) | read | 无 | Vendor specific Information Element内容 | 1.1 |
| BAND | BYTE | read | 无 | 无线频段，0表示2.4g, 1表示5G | 1.1 |

说明：此接口对应的多实例对象中，不得出现重复内容的对象实例。

* + - * 1. com.ctc.igd1.VSIE.ProbeRspTxVSIE

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC | STRING(12) | readwrite | 无 | STA的MAC | 1.2 |
| Band | BYTE | readwrite | 无 | 0表示2.4G，1表示5G | 1.2 |
| IEData | ARRAY<BYTE> | readwrite | 无 | 发送的Vendor-specific Information Element内容 | 1.2 |
| LenofIEData | UINT32 | readwrite | 无 | IEData的长度 | 1.2 |

* + - * 1. com.ctc.igd1.VSIE.ProbeRspTxVSIEManager

**属性**

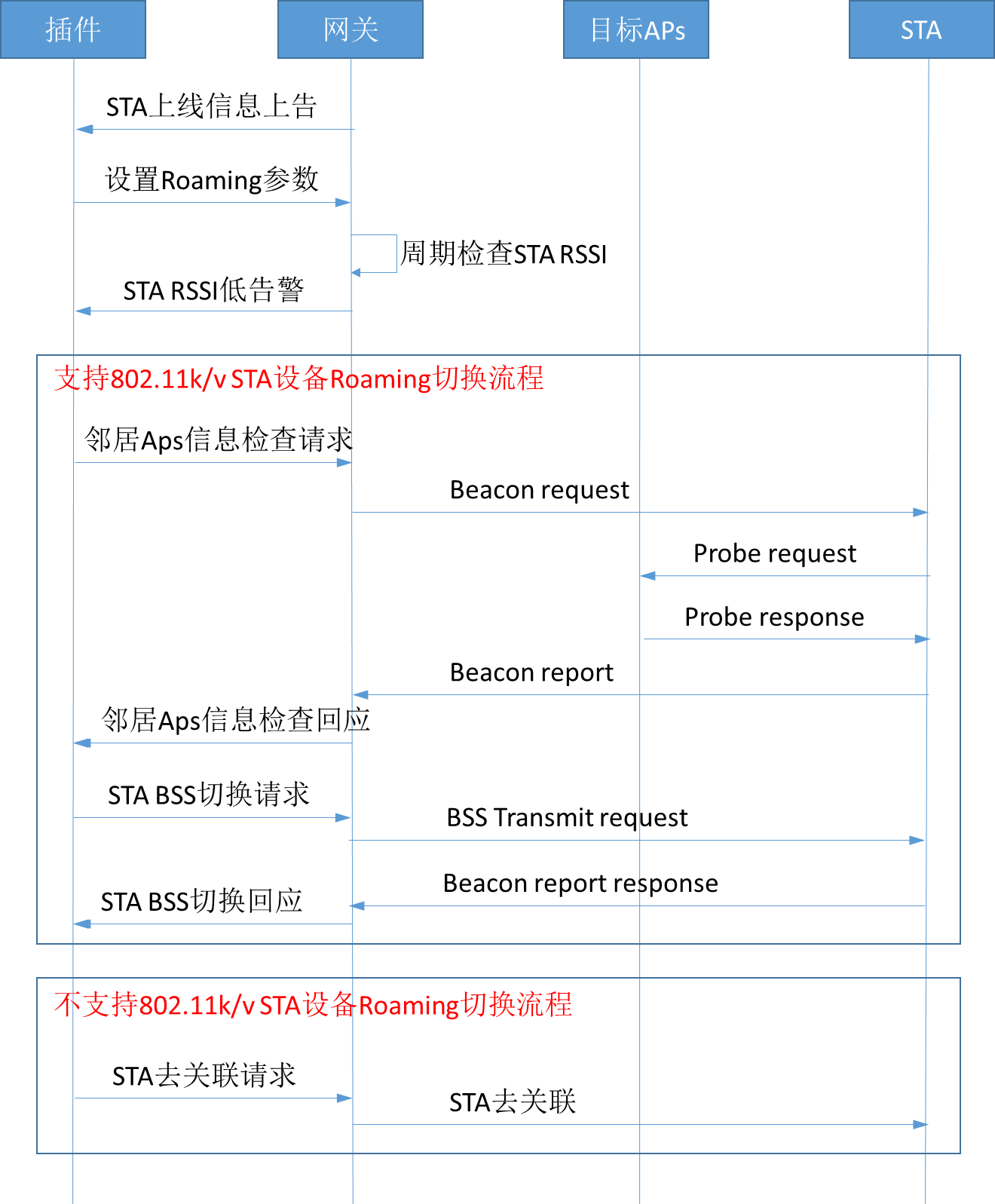
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MaxEntryNum | UINT32 | read | 无 | 支持最大的条目数，要求不得小于3条。 | 1.2 |
| CurrentEntryNum | UINT32 | read | 有 | 当前条目的数量 | 1.2 |

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/VSIE/BeaconTxVSIE | com.ctc.igd1.VSIE.BeaconTxVSIEManager  com.ctc.igd1.ObjectManager | VSIE服务配置 |
| /com/ctc/igd1/VSIE/BeaconTxVSIE/{i} | com.ctc.igd1.VSIE.BeaconTxVSIE | VSIE服务配置 |
| /com/ctc/igd1/VSIE/ProbeRxVSIE | comctc.igd1.ProbeRxVSIEManager  com.ctc.igd1.ObjectManager | VSIE服务配置 |
| /com/ctc/igd1/VSIE/ProbeRxVSIE/{i} | com.ctc.igd1.VSIE.ProbeRxVSIE | VSIE服务配置 |
| /com/ctc/igd1/VSIE/ProbeRxVSIE/{i}/Records | com.ctc.igd1.VSIE.ProbeRxVSIERecordManager  com.ctc.igd1.ObjectManager | VSIE服务配置  不需要支持AddObject和DelObject方法 |
| /com/ctc/igd1/VSIE/ProbeRxVSIE/{i}/Records/{i} | com.ctc.igd1.VSIE.ProbeRxVSIERecord | VSIE服务配置 |
| /com/ctc/igd1/VSIE/ProbeRspTxVSIE | comctc.igd1.ProbeRspTxVSIEManager  com.ctc.igd1.ObjectManager | VSIE服务配置 |
| /com/ctc/igd1/VSIE/ProbeRspTxVSIE/{i} | com.ctc.igd1.VSIE.ProbeRspTxVSIE | VSIE服务配置 |

* + 1. Roaming服务
       1. Roaming切换流程

1. 当网关设备启动时，运行于ONT的第三方插件设置网关的Roaming策略参数，控制Roaming功能的开启/关闭，以及Rssi告警门限等；
2. 当STA接入网关时，网关获取STA 的802.11k/v能力，并上告第三方插件；
3. 网关在Roaming参数设置的Start\_time时间之后，周期性检查关联的STA RSSI信号强度，当RSSI低于Roaming RSSI切换门限，主动上告STA RSSI低告警给第三方插件；当STA RSSI高于门限时，主动上告告警恢复；
4. 第三方插件检查STA对802.11k/v的支持能力，当STA支持802.11k/v能力时，从步骤5执行；当STA设备不支持802.11k/v能力时，跳转到步骤9执行；
5. 第三方插件启动该STA到周边邻居APs信息的查询，指明需要查询的信道、邻居APs列表；
6. 网关按照第三方插件要求，向STA发起Beacon request检测请求，STA返回Beacon report检测结果给网关，网关汇总所有被检查邻居APs信息后，上告邻居APs信息Report给第三方插件；
7. 第三方插件收到邻居APs信息查询回应后，从中选择合适的目标AP，发起STA BSS切换流程请求；
8. 网关向STA发起BSS切换流程，并把STA的切换结果返回第三方插件，结束Roaming切换流程。
9. 当STA不支持802.11k/v能力时，第三方插件在收到STA RSSI低告警通知后，根据其内部策略，周期性查询关联和非关联STA 到AP的RSSI，决定是否需要向STA发送去关联消息；
10. 当网关收到第三方插件的去关联请求后，向STA发送去关联消息，由STA自行决定需要关联的目标AP设备，并重新上线，结束Roaming切换流程。



* + - 1. DBus接口
         1. com.ctc.igd1.Roaming

设置及获取Roaming参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| BSSID | STRING | read | 无 | AP的MAC | 1.1 |
| Enable | BOOLEAN | readwrite | 无 | 是否启动漫游 | 1.1 |
| Start\_time | UINT32 | readwrite | 无 | 当某个STA的关联时间大于start\_time，开启判断逻辑 | 1.1 |
| Threshold1\_RSSI | INT32 | readwrite | 无 | 当STA到AP的RSSI低于该门限，上报RSSI低告警。只上报一次，低告警清除后再重新上报。 | 1.1 |
| Threshold2\_RSSI | INT32 | readwrite | 无 | 当STA到AP的RSSI高于该门限，上报RSSI低告警清除。只上报一次，低告警清除后再重新上报。 | 1.1 |

方法：

* StartAPRSSIQuery（IN STRING MAC,IN UNIT32 APNumber,IN DICT<STRING, UINT32>BSSIDandChannel,OUT UINT32 result，OUT STRING errdesc）

11k测量请求

参数说明:

MAC: STA的MAC地址

APNumber: 扫描的AP个数；

BSSIDandChannel: DICT数组，包含BSSID跟Channel，需要测量扫描的AP设备

* StartSTABSSTransitionRequest(IN STRING MAC, IN UINT32 Channel,IN STRING BSSID，OUT UINT32 result，OUT STRING errdesc)

BSS 切换请求，并返回BSS切换结果。

* GetSTARSSIQuery（IN DICT<STRING,UINT32>MACandChannel，OUT UINT32 result，OUT STRING errdesc）

获取非关联STA（指定MAC和channel）的RSSI值

**信号**

* APRSSIQueryResult (UINT32 Result,STRING MAC, DICT<STRING, INT32>BSSIDandRSSI，STRING errdesc)

说明：

表示StartAPRSSIQuery方法完成，信号告知扫描结果。

MAC: STA的MAC地址。

BSSIDandRSSI：表示扫描的结果。

Result: 表示执行结果，0表示成功，1表示失败。

errdesc: 如果出错，表示错误描述。

* STABSSTransitionResult (UINT32 Result,STRING MAC, UNIT32 StatusCode, STRING errdesc)

说明：

表示StartSTABSSTransitionRequest方法完成，信号告知STA响应11v BTM的切换结果。

Result：表示执行结果，0表示成功，1表示失败。

MAC: STA的MAC地址。

StatusCode：表示STA的BSS切换结果（如0表示Accept，具体见IEEE Std 802.11v-2011Table7-57v16 Status code definitionss）。

errdesc: 如果出错，表示错误描述。

* STARSSIQueryResult(UINT32 Result, DICT<STRING, INT32>MACandRSSI，STRING errdesc)

说明：

表示GetSTARSSIQuery方法完成，信号告知扫描非关联STA的RSSI结果。GetSTARSSIQuery方法的超时时间设为6秒。如果在6秒内一直未扫描到指定STA的RSSI值，可返回-100作为该STA的RSSI值。如果已获取到所有指定STA的RSSI值，应立即返回结果。

MACandRSSI：表示扫描的结果。

Result: 表示执行结果，0表示成功，1表示失败。

errdesc: 如果出错，表示错误描述。

* + - * 1. com.ctc.igd1.STAInfo

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| MAC\_STA | STRING(12) | read | 无 | 上线STA MAC地址 | 1.1 |
| Channel | UINT32 | read | 无 | STA接入的信道 | 1.1 |
| BSSID | STRING | read | 无 | STA接入的BSSID | 1.1 |
| BSS\_Transition | BOOLEAN | read | 无 | STA是否支持BSS Transition | 1.1 |
| Beacon\_Report\_Support | BOOLEAN | read | 无 | STA是否支持802.11K定义的Beacon report; | 1.1 |
| RSSI | INT32 | read | 无 | STA到AP的RSSI值 | 1.1 |

**信号**

* STARSSILowAlarm(STRING MAC\_STA,IN BOOLEAN TYPE,IN INT32RSSI,UINT RFBand), 表示STA RSSI低于门限值告警信号及告警清除。（备注：在STA RSSI的一次变化过程中（RSSI由高于Threshold1\_RSSI变为低于Threshold1\_RSSI，或者由低于Threshold2\_RSSI变为高于Threshold2\_RSSI），只需要产生一次告警/告警消除信号）

参数: MAC\_STA, STA的的MAC地址

TYPE: False表示RSSI低于门限值

True表示RSSI 高于门限值，解除警报。

RSSI: 计算的STA到AP的RSSI值。

RFBand: 对应无线模块的无线频段，0：表示2.4GHz，1：表示5GHz。

**方法：**

* SetSTADeassociationRequest（IN STRING MAC\_STA，OUT UINT32 result，OUT STRING errdesc）

发起一次针对指定MAC终端的去关联请求（备注：AP应通过Deassociation帧和STA解除连接）。去关联之后，该实例同时应该被删除。

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Config/WLAN/2G/Roaming | com.ctc.igd1.Roaming | Roaming的策略配置，只适用于2.4G第一个SSID |
| /com/ctc/igd1/Config/WLAN/5G/Roaming | com.ctc.igd1.Roaming | Roaming的策略配置，只适用于5G第一个SSID |
| /com/ctc/igd1/Config/WLAN/STA/{i} | com.ctc.igd1.Info.STAInfo  com.ctc.igd1.ObjectManager | STA配置2.4G及5G第一个SSID关联的STA列表，不要求支持AddObject、DeleteObject方法，需要支持interfacesAdded 及interfacesRemoved信号) |
| /com/ctc/igd1/Config/WLAN/STA | com.ctc.igd1.ObjectManager | STA配置 |
| /com/ctc/igd1/Config/WLAN/STA/{i} | com.ctc.igd1.Info.STAInfo | 2.4G及5G第一个SSID关联的STA列表，不要求支持AddObject、DeleteObject方法，需要支持interfacesAdded 及interfacesRemoved信号) |

* + 1. 网关质量诊断服务
       1. DBus接口
          1. com.ctc.igd1.OMDiag

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| CPUTemperature | UINT32 | read | 无 | CPU温度（对不支持实时测量的产品，缺省值为0） | 1.1 |
| CPUTempThreshold | UINT32 | readwrite | 无 | CPU温度报警阈值。  如果当前系统CPU温度5分钟采样平均值大于等于CPUTempThreshold, 发送SysCPUTempAlarm信号, 信号内容请参考下面本接口SysCPUTempAlarm信号规范。 | 1.1 |
| PONTempThreshold | UINT32 | readwrite | 无 | PON温度报警阈值。  如果当前系统PON温度5分钟采样平均值大于等于PON  TempThreshold, 发送SysPONTempAlarm信号, 信号内容请参考下面本接口SysPONTempAlarm信号规范。 | 1.1 |
| SystemFlashThreshold | UINT32 | readwrite | 无 | 系统可读写分区占用率阈值取值范围0-100。  如果当前系统可读写分区的占用率大于等于SystemFlashThreshold, 发送SysWritableFlashAlarm信号, 信号内容请参考下面本接口SysWritableFlashAlarm信号规范。 | 1.1 |
| ConntrackNumber | UINT32 | read | 无 |  | 1.1 |
| ConnNumThreshold | UINT32 | readwrite | 无 | 网络连接数告警阈值。  如果当前系统Connection Conntrack数量大于等于ConnNumThreshold, 发送SysConnNumAlarm信号, 信号内容请参考下面本接口SysConnNumAlarm信号规范。 | 1.1 |
| LAN1NegoRate | UINT32 | read | 无 | LAN1协商速率，单位kbps  1Mbps=1000kbps  1Gbps=1000Mbps | 1.11 |
| LAN2NegoRate | UINT32 | read | 无 | LAN2协商速率，单位kbps  1Mbps=1000kbps  1Gbps=1000Mbps | 1.11 |
| LAN3NegoRate | UINT32 | read | 无 | LAN3协商速率，单位kbps  1Mbps=1000kbps  1Gbps=1000Mbps | 1.11 |
| LAN4NegoRate | UINT32 | read | 无 | LAN4协商速率，单位kbps  1Mbps=1000kbps  1Gbps=1000Mbps | 1.11 |

**方法**

* CollectWiFiInfo (OUT UINT32 result, OUT STRING errdesc);

开始收集WiFi信息，成功后网关将组装的json内容放到/tmp/diaginfo/wifi\_info文件中去(参见附录H)。调用成功则创建LOG文件，调用失败不创建文件.

result: 方法调用结果，成功时为0，失败为1

errdesc: 错误信息，成功时为空（””），失败时填失败原因

说明：此方法为异步调用,如果调用完成，发送CollectWiFiInfoStatus信号。

**信号**

* SysCPUTempAlarm (UINT32 cputemp), 系统CPU温度超阈值报警信号。

用于质量插件报告网关CPU占用率超阈值事件.

参数: cputemp，类型为UINT32(u)，表示超过阈值的时候的CPU实时温度

* SysPONTempAlarm (UINT32 pontemp), 系统PON模块温度超阈值报警信号。

用于质量插件报告网关PON模块温度超阈值事件.

参数: pontemp，类型为UINT32(u)，表示超过阈值的时候的PON模块的实时温度

* SysWritableFlashAlarm (UINT32 flashoccupy), 系统可读写分区占用率超阈值报警信号。

用于质量插件报告网关可读写分区占用率超阈值事件.

参数: flashoccupy，类型为UINT32(u)，表示超过阈值的时候的系统可读写分区占用率，如80%时为80

* SysConnNumAlarm (UINT32 connum), 系统网络连接数超阈值报警信号。

用于质量插件报告网关连接数超阈值事件.

参数: flashoccupy，类型为UINT32(u)，表示超过阈值的时候的网关实时连接数

* CollectWiFiInfoStatus (UINT32 Result,, STRING errdesc), 无线信息搜集状态信号。

用于告知CollectWiFiInfo方法调用完成。

参数: Result, 类型为STRING(s), 表示方法调用结果。0表示成功，1表示失败。

STRING errdesc：当返回成功时，这个参数应为空，失败时，表示失败原因描述。

* WiFiConnFailure (STRING ssid, STRING bssid, STRING reason), 无线客户端连接失败告警。

用于质量插件报告无线客户端连接网关SSID失败.

参数: ssid，类型为STRING(s)，表示无线客户端连接的网关SSID

bssid，类型为STRING(s)，表示无线客户端的bssid

reason，类型为STRING(s)，表示连接失败的原因

* SysVoiceEvents (STRING event, STRING description), 语音模块事件

用于质量插件报告语音模块事件

参数: event，类型为STRING(s)，表示事件类型，可取值为ONHOOK, OFFHOOK, REGISTER

description，类型为STRING(s)，表示事件的描述.

当event为ONHOOK，OFFHOOK（用户摘挂机操作）时，description为空（""）；当没有帐号注册成功的情况 下，可以不记录ONHOOK，OFFHOOK操作；当event为REGISTER时，description可为注册成功（区分Line1/Line2）， 认证失败，SIP Registrar域名无法解析，VoIP获取IP失败，服务器地址不可达，注册超时，以及厂家自定义的 其它失败。

* + - * 1. com.ctc.igd1.OMDiagResource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ServiceName | STRING(32) | readwrite | 无 | 资源受控进程名 | 1.1 |
| CPUPercentage | UINT32 | readwrite | 无 | 该进程CPU占用率报警阈值，0表示不监控取值范围0-100 | 1.1 |
| MEMPercentage | UINT32 | readwrit | 无 | 该进程内存占用率报警阈值，0表示不监控取值范围0-100 | 1.1 |

* + - * 1. com.ctc.igd1.OMDiagProcess

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| ServiceName | STRING(32) | readwrite | 无 | 受控进程名 | 1.1 |

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Telecom/OMDiag | com.ctc.igd1.OMDiag | 质量诊断类服务 |
| /com/ctc/igd1/Telecom/OMDiag/Resource | com.ctc.igd1.ObjectManager | 进程占用资源阈值配置 |
| /com/ctc/igd1/Telecom/OMDiag/Resource/{i} | com.ctc.igd1.OMDiagResource | 进程占用资源阈值配置 |
| /com/ctc/igd1/Telecom/OMDiag/Process | com.ctc.igd1.ObjectManager | 进程运行异常监控配置 |
| /com/ctc/igd1/Telecom/OMDiag/Process/{i} | com.ctc.igd1.OMDiagProcess | 进程运行异常监控配置 |

* + 1. 桥接模式平台上报服务

网关桥接模式时，能够通过探测的mac/pppoe/ip 等信息，通过dbus接口提供给中间件。

网关对于远端回复的报文，可以通过添加流量特征规则，将远端回复的指定报文复制上报到桥接口，并且不影响该报文向LAN口转发。

对于下面的InterfaceName, 指的是网关的桥接WAN的设备接口名，中间件可以创建raw socket通过这个网络接口，发送报文并接受符合com.ctc.igd1.bridgedata.acl接口流量规则的下行流量。

* + - 1. DBus接口
         1. com.ctc.igd1.bridgedata

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| InterfaceName | STRING(31) | read | 无 | 桥接wan的dev name. | 1.2 |
| SMAC | STRING(12) | read | 无 |  | 1.2 |
| DMAC | STRING(12) | read | 无 |  | 1.2 |
| SessionID | UINT32 | read | 无 | PPPoE Session ID | 1.2 |
| IP | STRING(15) | read | 无 |  | 1.2 |
| DNS | STRING(15) | read | 无 | DNS服务器地址 | 1.2 |

说明: InterfaceName指的是网关的桥接WAN的设备接口名，中间件可以创建raw socket通过这个网络接口，发送报文并接受符合com.ctc.igd1.bridgedata.acl接口流量规则的下行流量。

* + - * 1. com.ctc.igd1.bridgedata.acl

**属性**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 变更通知 | 备注 | 版本 |
| IP | STRING(15) | readwrite | 无 | 从WAN口进来流量的源IP地址，可以为空。 | 1.2 |
| Port | STRING(12) | readwrite | 无 | 从WAN口进来流量的源端口，可以为空。 | 1.2 |
| Protocol | STRING(12) | readwrite | 无 | 从WAN口进来流量的协议，取值为“TCP”, “UDP”, “ICMP”, “ALL” | 1.2 |

说明: IP跟协议端口信息，可以只设置IP（Port字段为空，Protocl字段为“ALL”）,也可以只设置端口信息（IP字段设置为空及Protocol不设置为“ALL”）此配置设备重启后清除

* + - 1. DBus对象

|  |  |  |
| --- | --- | --- |
| Object Path | 接口 | 权限 |
| /com/ctc/igd1/Telecom/BridgeData | com.ctc.igd1.bridgedata | 桥接数据服务 |
| /com/ctc/igd1/Telecom/BridgeData/ACL | com.ctc.igd1.ObjectManager | 桥接流量特征配置 |
| /com/ctc/igd1/Telecom/BridgeData/ACL/{i} | com.ctc.igd1.bridgedata.acl | 桥接流量特征配置 |

* 1. DPI对网关接口要求
     1. 会话信息

用于网关向插件提供流信息。具体定义如下：

typedef struct CtSgwTupleInfo\_ {

unsigned char direct;

unsigned char proto;

unsigned char new\_conntrack; /\* 是否为新建会话 \*/

unsigned int sipv4;

unsigned int dipv4;

unsigned int sipv6[4];

unsigned int dipv6[4];

unsigned short sport;

unsigned short dport;

unsigned int in\_iif; /\* 报文进接口index \*/

unsigned int out\_iif; /\* 报文出接口index \*/

} CtSgwTupleInfo;

* + 1. 插件识别信息

用于插件向网关提供相关信息，具体定义如下：

typedef struct CtSgwGwInfo\_

{

/\* 用于返回识别的协议ID \*/

unsigned int layer7\_id;

/\* 用于返回DNAT的目的 \*/

#if LINUX\_VERSION\_CODE > KERNEL\_VERSION(3, 7, 0)

struct nf\_nat\_range nat\_range;

#elif LINUX\_VERSION\_CODE > KERNEL\_VERSION(3, 3, 0)

struct nf\_nat\_ipv4\_range nat\_range;

#elif LINUX\_VERSION\_CODE > KERNEL\_VERSION(2, 6, 21)

struct nf\_nat\_range nat\_range;

#else

struct ip\_nat\_range nat\_range;

#endif

} CtSgwGwInfo;

* + 1. 流程处理接口
       1. 注册接口

插件使用以下函数向网关注册流处理相关回调函数：

int ctSgw\_appRegisterFunc(ctSgw\_dpiFuncs \*funcs);

传递的结构具体定义如下：

typedef struct ctSgw\_dpiFuncs\_ {

ctSgw\_appCtxCreate ctSgw\_appCtxCreateHook;

ctSgw\_appCtxDestroy ctSgw\_appCtxDestroyHook;

ctSgw\_appProcAppId ctSgw\_appProcAppIdHook; // 2+1版本中不再使用

} ctSgw\_dpiFuncs;

typedef int (\*ctSgw\_appCtxCreate)(void\*\* p\_app\_ctx, unsigned char flag);

该函数用于在会话创建时创建插件相关的上下文到conntrack结构上。

参数说明：

1、p\_app\_ctx（IN）：指向挂载在conntrack结构中上下文信息的指针地址；

2、flag（IN）：保留，目前只需要传入0。

typedef void (\*ctSgw\_appCtxDestroy)(void\*\* p\_app\_ctx);

该函数用于在会话销毁时释放conntrack结构上插件相关的上下文信息。

参数说明：p\_app\_ctx（IN）：指向挂载在conntrack结构中上下文信息的指针地址；

返回值：无

typedef int (\*ctSgw\_appProcAppId)(unsigned char \*layer2data, CtSgwTupleInfo \*tupleinfo, void \*p\_app\_ctx, unsigned int \*layer7\_id);

该函数用于在报文处理流程（FORWARD）节点上执行插件主流程。该函数在2+1以后网关中被其它接口代替，不再使用。

* + - 1. 注销接口

插件使用以下函数向网关注销流处理相关回调函数：

void ctSgw\_appUnRegisterFunc(void);

* + 1. 报文处理接口

用于向NETFILTER的PREROUTING或者FORWARD节点上注册回调函数。

* + - 1. PREROUTING节点注册接口

插件使用以下函数向网关报文处理流程的PREROUTING节点注册回调函数。

int ctSgw\_appRegisterPreProc(CtSgwPreProcInfo \*info);

传递的结构具体定义如下：

typedef struct CtSgwPreProcInfo\_

{

ctSgw\_appPreProc hook; /\* 回调函数 \*/

int priority; /\* 优先级 \*/

void \*priv\_data; /\*用于存储相应的NF结构，外部不需要关注\*/

} CtSgwPreProcInfo;

回调函数具体定义如下：

typedef int (\*ctSgw\_appPreProc)(unsigned char \*layer2data, CtSgwTupleInfo \*tupleinfo,

void \*p\_app\_ctx, CtSgwGwInfo \*gwinfo, void \*data);

参数说明：

1、layer2data（IN）：报文的layer2以上的payload；

2、tupleinfo（IN）：报文对应的会话信息，具体见结构体定义；

3、p\_app\_ctx（IN）：挂载在conntrack结构中上下文信息的指针；

4、gwinfo(OUT)：插件返回给网关的信息，具体见结构体定义；

5、data（IN）：暂时不使用，方便后继扩展。

返回值：

0，表示未完成，对应会话的后继报文需要继续调用本接口；

1，表示完成，对应会话的后继报文不需要继续调用本接口。

3，表示需要转发，网关需要根据插件返回的信息对相应会话进行DNAT操作。

* + - 1. PREROUTING节点注销接口

插件使用以下函数向网关报文处理流程的PREROUTING节点注销回调函数。

void ctSgw\_appUnRegisterPreProc(CtSgwPreProcInfo \*info);

* + - 1. FORWARD节点注册接口

插件使用以下函数向网关报文处理流程的FORWARD节点注册回调函数。

int ctSgw\_appRegisterForwardProc(CtSgwForwardProcInfo \*info);

传递的结构具体定义如下：

typedef struct CtSgwForwardProcInfo\_

{

ctSgw\_appForwardProc hook; /\* 回调函数 \*/

int priority; /\* 优先级 \*/

void \*priv\_data; /\*用于存储相应的NF结构，外部不需要关注\*/

} CtSgwForwardProcInfo;

回调函数具体定义如下：

typedef int (\*ctSgw\_appForwardProc)(unsigned char \*layer2data, CtSgwTupleInfo \*tupleinfo,

void \*p\_app\_ctx, CtSgwGwInfo \*gwinfoi, void \*data);

参数说明：

1、layer2data（IN）：报文的layer2以上的payload；

2、tupleinfo（IN）：报文对应的会话信息，具体见结构体定义；

3、p\_app\_ctx（IN）：挂载在conntrack结构中上下文信息的指针；

4、gwinfo(OUT)：插件返回给网关的信息，具体见结构体定义；

5、data（IN）：暂时不使用，方便后继扩展。

返回值：

0：表示DPI未完成，对应会话有新报文到达时，需要继续调用本接口；

1：表示数据检测完成，对应会话后续报文无需调用本接口；

2：表示该报文所属会话需要被阻止，内核接收到该返回信息后，需要阻止此会话的后续报文；

3：表示该报文所属会话需要被转发，网关需要根据插件返回的信息对相应会话进行DNAT操作。（该返回值只存在PER\_ROUTING链上）。

4(0x04)：表示该报文所属会话需要进入QOS默认优先级的转发队列，默认优先级是哪个由网关决定。

0x104:表示该报文所属会话需要进入QoS为最高优先级的转发队列；

0x204：表示该报文所属会话需要进入QoS为次高优先级的转发队列；

0x304：表示该报文所属会话需要进入QoS为第3优先级的转发队列；

0x404：表示该报文所属会话需要进入QoS为第4优先级的转发队列；

0x504：表示该报文所属会话需要进入QoS为第5优先级的转发队列；

0x604:表示该报文所属会话需要进入QoS为第6优先级的转发队列；

0x704:表示该报文所属会话需要进入QoS为第7优先级的转发队列；

0x804:表示该报文所属会话需要进入QoS为第8优先级的转发队列；

0x904：表示该报文所属会话需要进入QoS为第9优先级的转发队列；

备注：目前只列出9个优先级。

    如果网关支持的优先级少于9个，则将插件返回低于网关最低优先级的会话均放入最低优先级队列中。即如果网关只支持5个优先级，则将插件返回的优先级>=5的会话均放入第5优先级的队列中。如果网关支持的优先级需要高于9个，插件按低8位为4，高24位表示优先级的规则对返回值进行扩展。

* + - 1. FORWARD节点注销接口

插件使用以下函数向网关报文处理流程的FORWARD节点注销回调函数。

void ctSgw\_appUnRegisterForwardProc(CtSgwForwardProcInfo \*info);

* + 1. 插件信息获取接口

用于网关中其它插件获取DPI插件信息，目前仅用于流量分发插件获取DPI插件信息。

* + - 1. 注册获取接口

该函数用于DPI插件向网关注册获取信息接口函数。

int ctSgw\_appRegisterGetInfo(ctSgw\_appGetInfoProc funcs);

获取信息接口函数定义如下：

typedef int (\*ctSgw\_appGetInfoProc)(void \*app\_ctx, void \*app\_info);

参数说明：

1、app\_ctx（IN）：挂载在conntrack结构中上下文信息的指针；

2、app\_info（OUT）：DPI插件的信息。

* + - 1. 注销获取接口

该函数用于DPI插件向网关注销获取信息接口函数。

void ctSgw\_appUnRegisterGetInfo(void);

* + - 1. 获取接口

该函数用于第三方插件获取DPI插件信息。

int ctSgw\_appGetInfo(void \*app\_ctx, void \*app\_info)。

1. （规范性附录）  
   告警信息
   1. 告警编号规则
2. 告警编号采用6位数字：

第1位：告警所属主分类；

第2、3位：告警所属次分类；

第4、5、6位：序列号，序列号从000~999，500后可由厂商自定义。

1. 前三位定义见表D.1。

**表D.1 告警编号前三位定义**

|  |  |
| --- | --- |
| 第1位含义 | 第2、3位含义 |
| 1：设备告警 | 00 与主机、板卡有关的硬件故障  01与网络有关的硬件故障  02 与存储有关的硬件故障  03与外设有关的硬件故障  04 终端设备告警 |
| 2：服务质量告警 | 01越门限告警  02信号源引起的服务质量下降 |
| 3：处理出错告警 | 01软件错误引起的故障  02 配置错误引起的故障  03 安全相关的故障 |
| 4：通讯告警 | 01连接中断 |
| 5：环境告警 |  |

* 1. 设备告警信息列表

设备告警信息见表D.2。

**表D.2 设备告警信息**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 告警类别 | 告警名称 | 告警编号 | 附加信息 | 告警级别 | 触发条件 | 应用范围 |
| 设备功能类 | 设备重启 | 104001 |  | 次要告警 | 设备重启 | 日志、向ITMS上传告警 |
| 端口不可用 | 104006 | 端口号 | 严重告警 | 端口不可用 | 日志、向ITMS上传告警 |
| WLAN相关 | WLAN硬件故障 | 104012 |  | 严重告警 | 硬件故障导致WLAN不可用，例如无线芯片检测不到、无线芯片异常（包括无中断，停止收发包等） | 日志、向ITMS上传告警 |
| WLAN应用故障 | 104013 |  | 严重告警 | 无线固件加载失败等情况导致WLAN不可用 | 日志、向ITMS上传告警 |
| 设备状态、统计参数类 | CPU使用率过高 | 104030 |  | 主要告警 | 连续5分钟在95%以上 | 日志、向ITMS上传告警 |
| 保留 | 104031~104035 |  | 次要告警 |  |  |
| RAM使用率过高 | 104036 |  | 主要告警 | 连续5分钟在95%以上 | 日志、向ITMS上传告警 |
| 文件相关 | 文件服务器不可达 | 104050 |  | 严重告警 | 文件服务器不可达 | 日志 |
| 文件服务器用户名/密码错误 | 104051 |  | 严重告警 | 文件服务器用户名/密码错误 | 日志 |
| 下载文件超时 | 104052 |  | 严重告警 | 超过5分钟 | 日志 |
| 服务器上无指定文件 | 104053 |  | 严重告警 | 找不到文件 | 日志 |
| 更新配置文件失败 | 104054 |  | 严重告警 | 更新未正确完成 | 日志 |
| 备份配置文件失败 | 104055 |  | 严重告警 | 备份未正确完成 | 日志 |
| 恢复配置文件失败 | 104056 |  | 严重告警 | 恢复未正确完成 | 日志 |
| 配置文件不可用 | 104057 |  | 严重告警 | 文件校验出错 | 日志 |
| 软件升级失败 | 104058 |  | 严重告警 | 升级未正确完成 | 日志 |
| Flash空间不足 | 104059 |  | 严重告警 | 不够存放文件 | 日志 |
| 用户自助软件升级上报故障 | 104060 |  | 严重告警 | 软件自动上报 | 日志 |
| 日志文件无法上传 | 104061 |  | 严重告警 | 无法上传 | 日志 |
| 业务类－语音 | 软交换服务器不可达 | 104102 |  | 严重告警 | 服务器不可达 | 日志、向ITMS上传告警 |
| 注册失败－鉴权失败 | 104104 |  | 严重告警 | 鉴权失败 | 日志、向ITMS上传告警 |
| 注册失败－其它 | 104105 |  | 严重告警 | 其它原因导致注册失败 | 日志、向ITMS上传告警 |
| 注册无响应 | 104106 |  | 严重告警 | 注册无响应 | 日志、向ITMS上传告警 |
| 业务类－上网 | 上网WAN连接连续拨号失败 | 104111 |  | 主要告警 | 路由上网模式下，持续上电期间路由上网WAN连接PPPoE拨号连续失败10次以上 | 日志、向ITMS上传告警 |
| 上网WAN连接重新拨号 | 104112 |  | 次要告警 | 路由上网模式下，持续上电期间路由上网WAN连接重新拨号获取了IP地址 | 日志、向ITMS上传告警 |
| 业务类－IPTV | EPG Server无法访问 | 104122 |  | 严重告警 | 服务器不可访问（仅当IPTV为路由模式） | 日志、向ITMS上传告警 |

1. （规范性附录）  
   日志文件格式
   1. 文件格式

|  |
| --- |
| Manufacturer:XXXX;  ProductClass:XXXX;  SerialNumber:XXXX;  IP:X.X.X.X;  HWVer:001.001.001;  SWVer:001.001.001;  （换行）  YYYY-MM-DD HH:MM:SS [Severities] Message |

文件中的分隔符均为半角字符。

* 1. Syslog Message Severities

Syslog Message Severities如表E.1所示。

**表E.1 Syslog Message Severities**

|  |  |  |
| --- | --- | --- |
| Numerical Code | Severity | Explain |
| 0 | Emergency | system is unusable |
| 1 | Alert | action must be taken immediately |
| 2 | Critical | critical conditions |
| 3 | Error | error conditions |
| 4 | Warning | warning conditions |
| 5 | Notice | normal but significant condition |
| 6 | Informational | informational messages |
| 7 | Debug | debug-level messages |

1. （规范性附录）  
   基于宽带识别码的设备首次认证用户提示信息
   1. 基于宽带识别码的设备首次认证用户提示信息

基于宽带识别码的设备首次认证过程中，家庭网关注册界面应根据ITMS+远程下发的参数内容（Internet­Gateway­Device.X\_CT-COM\_UserInfo.Status和Internet­Gateway­Device.X\_CT-COM\_UserInfo.Result）和认证次数限制情况提供明确的用户提示信息，具体要求参见表F.1。

**表F.1 基于宽带识别码的设备首次认证用户提示信息**

|  |  |  |  |
| --- | --- | --- | --- |
| Internet­Gateway­Device.X\_CT-COM\_UserInfo.Status | Internet­Gateway­Device.X\_CT-COM\_UserInfo.Result | 认证次数限制情况 | 用户提示信息 |
| 0 | 99 |  | 注册ITMS成功，等待ITMS平台下发业务数据 |
| 0 |  | * 正在下发业务数据，请勿断电或拨*光纤（或网线）*（InternetGatewayDevice.X\_CT-COM\_UserInfo. ServiceName不可识别时） * ITMS平台正在下发\*\*业务数据，请勿断电或拨\*\*（InternetGatewayDevice.X\_CT-COM\_UserInfo. ServiceName可识别时） |
| 1 |  | * ITMS平台业务数据下发成功，共下发了\*\*、\*\*、\*\*#个业务，欢迎使用悦me（当家庭网关不需要重启时） * ITMS平台业务数据下发成功，共下发了\*\*、\*\*、\*\*#个业务，天翼网关需要重启，请等待…（当家庭网关需要重启时） |
| 2 |  | ITMS下发业务异常！请联系客户经理或拨打10000 |
| 1~3 |  | 未超过最大限制次数 | 在ITMS上注册失败！请检查宽带识别码和密码是否正确，如无法解决请联系客户经理或拨打10000 |
|  | 超过最大限制次数 | 在ITMS上注册失败！请3分钟后重试，如无法解决请联系客户经理或拨打10000 |
| 4 |  |  | 注册超时！请检查线路后重试，如无法解决请联系客户经理或拨打10000 （说明：不增加失败次数Internet­Gateway­Device.X\_CT-COM\_UserInfo.Times的数值） |
| 5 |  |  | 已经在ITMS注册成功，无需再注册 |

说明：InternetGatewayDevice.X\_CT-COM\_UserInfo.Result和InternetGatewayDevice.X\_CT-COM\_UserInfo.Status的数值掉电不可丢失

* 1. 注册初始界面提示要求

在注册初始界面中对用户进行操作提示，具体内容如下：

* + - * *在注册及业务下发过程中不要断电、不要拨光纤（或网线）*
      * *本注册功能仅用于新设备的认证及业务下发，已正常在用设备请勿重新注册*

图形风格可参见图F.1。



**图F.1 宽带识别码注册初始界面示例**

* 1. 注册和业务下发过程中的提示规范要求

1. 终端正常注册和下发业务时使用动态进度条显示进度，关键提示要求如下：
2. 20%（仅针对PON上行设备）：在向OLT发起注册时提示 “正在注册OLT”
3. 30%（仅针对PON上行设备）：在OLT授权成功时提示 “注册OLT成功，正在获取管理IP”
4. 40%：TR069的WAN连接获得IP地址时提示 “已获得管理IP，正在连接ITMS”
5. 50%：在ITMS平台注册成功时（Status=0且Result不等于0、1或2）提示“注册ITMS成功，等待ITMS平台下发业务数据”
6. 60%~99%：在Status=0且Result=0，根据ITMS下发的将要配置的业务类型（InternetGatewayDevice.X\_CT-COM\_UserInfo. ServiceName），提示“ITMS平台正在下发\*\*业务数据，请勿断电或拨光纤”（界面显示的业务类型包括“上网”、“iTV”、“语音”、“其它”或前三者的组合；根据ITMS下发的用户业务数量（InternetGatewayDevice.X\_CT-COM\_UserInfo.SeviceNum）均衡确定每个业务配置需显示的百分比进度）
7. 100%：在Status=0且Result=1时提示下发成功，如“ITMS平台业务数据下发成功，共下发了宽带、语音、ITV三个业务，欢迎使用”或“ITMS平台业务数据下发成功，共下发了宽带、语音、ITV三个业务，天翼网关需要重启，请等待…”（注：根据家庭网关是否需要重启选择两者之一，且下发几个业务就提示几个业务）
8. 终端注册和下发业务时主要出错情形的提示要求如下：
9. 在OLT上注册失败：提示“在OLT上注册失败，请检查光纤是否已正常连接、宽带识别码和密码是否正确，如无法解决请联系客户经理或拨打10000”
10. 不能连接ITMS：提示“到ITMS的通道不通，请联系客户经理或拨打10000”
11. 在ITMS上注册失败（Status=1或Status=2或Status=3，未超过最大限制次数）：提示“在ITMS上注册失败！请检查宽带识别码和密码是否正确，如无法解决请联系客户经理或拨打10000”
12. 在ITMS上注册失败（Status=1或Status=2或Status=3，超过最大限制次数）：提示“在ITMS上注册失败！请3分钟后重试，如无法解决请联系客户经理或拨打10000”
13. 在ITMS上注册超时（Status=4，或家庭网关向ITMS的注册报文发出120秒后仍未收到ITMS下发的Status或Result值）：提示“在ITMS上注册超时！请检查线路后重试，如无法解决请联系客户经理或拨打10000”
14. ITMS未下发业务或业务下发异常（Status =0且Result=2）：提示“ITMS下发业务异常！请联系客户经理或拨打10000”
15. （规范性附录）  
    提供的服务及协议端口汇总
    1. 网络侧协议及端口的开关要求

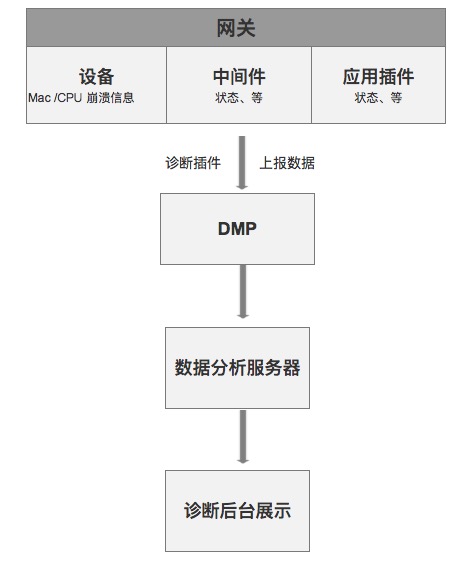
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务** | | **默认端口号** | **默认开关状态** | **是否允许修改** |
| FTP | | 21（TCP） | 关闭 | 只可通过ITMS+、智家平台远程进行“开启/关闭”控制（ITMS+可修改端口号） |
| Telnet | | 23（TCP） | 关闭 | 只可通过ITMS+、智家平台远程进行“开启/关闭”控制（ITMS+可修改端口号） |
| SAMBA | | 137（UDP），138（UDP），445（TCP） | 关闭 | 只可通过智家平台远程进行“开启/关闭”控制 |
| ITMS主动连接家庭网关的端口（用于反向触发家庭网关上报inform消息） | | 端口号（TCP）由家庭网关设置，并通过Inform消息上报给ITMS+平台（端口号范围在1000以上）。 | 开启 |  |
| DHCPv4 | Client端（用于从网络侧获取IP地址） | 68（UDP） | 仅在配有DHCP认证WAN连接时开启 | 不可修改 |
| DHCPv6 | Client端（用于从网络侧获取IP地址） | 546（UDP） | 仅在配有DHCP认证WAN连接时开启 | 不可修改 |
| 手机APP管理 | 网关管理平台与网关通信的指定端口 | 端口号（UDP、TCP）由厂家和智能OS自行设置 | 开启 |  |
| VoIP | 控制报文端口 | 端口号（UDP/TCP）由厂家自行设置，网关自动和平台协商（端口号范围在1000以上）。  SIP协议默认是5060。 | 仅在配有语音业务时开启 |  |
| 数据报文端口 | 端口号（UDP）由厂家自行设置，网关自动和对方协商（端口号范围在1000以上）。 | 仅在配有语音业务时开启 |  |
| IPTV业务 | IGMP查询报文 |  | 开启 | 不可修改 |
| 组播数据流报文 |  | 开启 | 不可修改 |
|  | | 其它TCP或UDP端口号 | 关闭 | 不可修改 |

* 1. 用户侧协议及端口的开关要求

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **服务** | | **默认端口号** | | **默认开关状态** | | **是否允许修改** | | **说明** | |
| FTP | | 21（TCP） | | 开启 | | 只可通过ITMS+、智家平台远程进行“开启/关闭”控制及端口号修改 | | 该服务只能访问家庭网关所插U盘或内置硬盘的内容。该服务不允许匿名访问，缺省帐号为网关标签上的useradmin帐号，帐号可通过ITMS+、智家平台远程修改 | |
| Telnet | | 23（TCP） | | 关闭 | | 只可通过ITMS+、智家平台远程进行“开启/关闭”控制及端口号修改 | |  | |
| DNS | | 53（TCP/UDP） | | 开启 | | 不可修改 | |  | |
| HTTP | | 80（TCP） | | 开启 | | 不可修改 | | 网关本地管理GUI | |
| 8080 | | 开启 | | 不可修改 | | 智能插件本地WEB服务 | |
| DNS重定向 | | 84（TCP/UDP） | | 允许开启（该端口非强制使用） | | 不可修改 | | 网关可将dns报文重定向到该端口进行查错或匹配处理。该端口的服务终结于家庭网关，不能转发到公网及私网 | |
| SAMBA | | 137（UDP），138（UDP），445（TCP） | | 开启 | | 只可通过智家平台远程进行“开启/关闭”控制 | | 该服务只能访问家庭网关所插U盘或硬盘的内容。该服务默认关闭匿名访问，缺省帐号为网关标签上的useradmin帐号（每台设备的密码随机），帐号可通过ITMS+、智家平台远程修改 | |
| DLNA | | 2468（TCP），4361（TCP） | | 开启 | | 不可修改 | | 该类报文不能转发到公网 | |
| 手机APP管理 | 手机APP本地连接家庭网关 | 17998（TCP） | | 开启 | | 可以通过手机APP管理平台对端口进行配置 | | 该端口的服务终结于家庭网关，不能转发到公网及私网 | |
| DHCPv4 | Server端（用于给PC等终端分配IP地址） | 67（UDP） | | 开启 | | 不可修改 | | 该端口的服务终结于家庭网关，不能转发到公网及私网 | |
| DHCPv6 | Server端（用于给PC等终端分配IP地址） | 547（UDP） | | 开启 | | 不可修改 | | 该端口的服务终结于家庭网关，不能转发到公网及私网 | |
| UPNP | 协议交互报文 | 1900（UDP） | 开启 | | 不可修改 | | 该类报文不能转发到公网 | |
| 协议交互报文 | 5431（TCP） | 开启 | | 不可修改 | | 该类报文不能转发到公网 | |
| 数据传输报文 | 52869（TCP/UDP） | 开启 | | 不可修改 | | 该类报文不能转发到公网 | |
| 自动组网 | 配置信息同步 | 32768端口（TCP） | 关闭 | | 自动组网插件启动后开启 | | 该类报文不能转发到公网 | |
| IPTV业务 | IGMP加入请求报文、离开报文、查询响应报文 |  | 开启 | | 不可修改 | |  | |
| 其它 | | 其它TCP或UDP端口号 | | 建议关闭 | | 不可修改 | | 该类报文不能转发到公网 | |

1. （规范性附录）  
   网关质量诊断信息收集要求
   1. 方案架构

网关设备应按要求上报自身运行相关的质量诊断信息，具体分为设备监控类、插件监控类和中间件（即Framework）监控类三种。上报时机分为系统启动时上报、周期性间隔上报两种。网关应支持通过装网关质量诊断插件，用以读取网关收集的质量诊断信息并上报到网络侧的DMP平台。总体架构如图H.1所示。



**图H.1 运行诊断状态收集总体架构**

为了便于上报及内容处理，采集后的数据统一采用JSON格式保存在指定的文件中。

JSON 协议定义如下:

{

“Event\_Type”: “”,

“Version”: 1.0,

“OSVer” :3,

“ID”:“”,

"MAC":"",

"Manufacture":"",

"ProductClass":""，

“Event\_Data”: “String”

}

说明:

* Event\_Type表示信息类型，具体取值见表H.1。

**表H.1  Event\_Type取值信息**

|  |  |
| --- | --- |
| “REBOOT” | 网关重启信息（E8C） |
| “VOICE\_INFO” | 语音模块信息（E8C） |
| “KERN\_CRASH” | 内核崩溃信息（E8C） |
| “BASIC\_INFO” | 网关基础信息上报（插件） |
| “DEVICE\_INFO” | 网关运行信息上报（插件） |
| “WIFI\_INFO” | 无线模块运行信息（E8C） |
| “LANPORTRATE” | LAN口信息（插件） |
| “INTERNET\_WANINFO” | PPPoE连接状态变化信息（插件） |
| “CPUMEM\_INFO” | 网关进程监控信息（E8C） |
| “PROCESS\_INFO” | 进程异常监控信息（E8C） |
|  |  |
| “PLUGIN\_EXCEPTION” | 插件异常监控信息（中间件） |
| “NETSTAT” | 网关端口开放信息（E8C） |
| “PLUGIN\_ALARM” | 插件紧急问题告警（插件） |
| “CLOUDCLI\_INFO” | 云客户端工作信息（中间件） |
| “CLOUDCLI\_ALARM” | 云客户端失连告警信息 |

* Version: 版本管理，表示上报协议版本管理。部署上线之后，如果有新的接口功能需要实现，版本需要递增。
* OSVer: 智能网关平台系统版本，1:OSGI；2:CTWRT；3:CTWRT(3.0)
* ID: 表示唯一的消息ID。
* MAC:表示当前网关的mac信息。
* Manufacture：表示设备厂商。
* ProductClass：表示该网关的型号。
* Event\_Data: JSON格式，用于封装详细的消息内容。
  1. 网关质量诊断相关DBUS接口定义

网关应支持如下DBUS接口，满足网关质量诊断插件获取信息的需求：

#define CTC\_DIAG\_DBUS\_SERVICE\_NAME “com.ctc.igd1”

#define CTC\_DIAG\_DBUS\_OBJECT\_PATH “/com/ctc/igd1/OMDiag”

#define CTC\_DIAG\_DBUS\_OBJECT\_INTERFACE “com.ctc.igd1.OMDiag”

* 1. 信息文件互斥

网关在创建LOG文件的时候，文件的owner的读写权限(rw)需打开，路径上的目录有都有x权限。

网关和网关质量诊断插件对网关质量诊断信息文件存取时应进行加锁处理，有任何读写操作之前，都要用 flock (fd, LOCK\_EX | LOCK\_NB)做锁文件操作，以防访问冲突。

* 1. 服务器获取
     1. 内核崩溃信息

当内核因为非法地址访问、死锁、OOM等原因导致系统崩溃时，内核应自动把相关的堆栈以及寄存器信息等以文件方式保存到FLASH上（一个定义好的分区），待系统重启后上报。(不考虑因为系统崩溃造成文件不可写的情况)。

文件名为：crash\_info。

文件路径: /opt/upt/apps/info/。

文件内容为具体的崩溃堆栈信息，网关不需要将其包装为json格式。

实现方式可参考中国电信提供的参考代码。

* + 1. 设备重启信息

通过日志方式来记录网关设备重启信息（是否正常、时间、次数等），并判断是硬重启还是软重启（进一步细分是用户侧触发还是平台侧触发）。正常重启的时候写一个值，非正常重启不写值就为异常。然后通过平台侧大数据分析来判断网关用户的断电情况。

文件名为：reboot\_info

文件路径: /opt/upt/apps/info/

文件格式如下JSON格式:

格式如下:

｛

"Time":"2016-12-06 08:01:57"，

"Source":""，用于表示产生Reboot信号的来源，取值: “ITMS”, “Telecomadmin”, “DBus”, “Terminal”,“Power”, “Exception”.

}

上报平台之后，会删除该文件。

说明：”Terminal”是指从串口（包括telnet/ssh）上执行reboot/restore命令导致网关重启的情况

“Exception”是各种软件运行错误导致的系统异常重启，包括但不限于内核错误导致的重启，关键进程异常导致的重启;

“Power”是系统断电造成的重启。当网关发生软件错误后已经挂起（hang）无法响应了，但是没有重启，后经手动断电重启，这种情况Source应该是”Exception”，而不是”Power”。

* + 1. WIFI信息收集

WIFI信息收集，包括WiFi的速率、频宽、模式、加密、信道、干扰等，通过大数据分析来判断WIFI模块是否出现问题，或者WIFI模块的健康度判断。网关质量插件每隔一段时间（周期平台可配置）调用网关的DBUS方法来获取相关WIFI信息并上报。

文件名: wifi\_info

文件路径: /tmp/diaginfo/

DBUS方法定义如下：

CollectWiFiInfo (OUT UINT32 result, OUT STRING errdesc);

result：0为成功，1为失败

errdesc：错误信息，成功时没有

开始收集WiFi信息，成功后网关将组装的json内容放到/tmp/diaginfo/wifi\_info文件中去。

调用成功则创建LOG文件，调用失败不创建文件。

此方法可异步实现，WiFi信息搜集的结果，通过信号CollectWiFiInfoStatus告诉插件搜集结果完成。

文件内容包含:

{

"Time":"2017-04-05 10:18:43",

"Enable":%d, // WiFi总开关是否Enable

"24GWiFiEnable":%d, // 2.4GWIFI模块是否Enable，取值0/1

"5GWiFiEnable":%d, // 5GWIFI模块是否Enable，取值0/1，单频网关取0

"dualband":%d, // 是否支持双频，取值0/1（由插件加这个字段）

"Info": [{

"SSID":"%s"，

“SSIDIndex”:”%s”,

“SSIDAlias”:”%s”, // 如2.4G-1、2.4G-2、5G-1

“Enable”:”%s”, // SSID是否enable,取值0/1

“Band”:”%s”, // 取值2.4G/5G(从com.ctc.igd1.WLANConfiguration.RFBand来)

“Rate”:”%s”, // 当前信道的速率，单位Kbps

“Bandwidth”:”%s”, // 20MHz, 40MHz，80MHz等

“Mode”:”%s”, // com.ctc.igd1.WLANConfiguration.Standard

“Security”:”%s”, // com.ctc.igd1.WLANConfiguration.BeaconType

“Channel”:”%s”,

“ClientCount”:%d, // 连接到本SSID上的无线客户端个数

“RSSI”:”%s”, // 信号强度，单位dBm

“BER”:”%s” //无线误码率（Bit Error Rate），取数字，如10%则取10

}]

"Interference\_2G":[{

"SSID”:”%s", // 周边AP的SSID名称

"Channel":"%s", // 该AP所用的信道

“RSSI”:”%s” // 信号强度，单位dBm

}],

“Interference\_5G”:[{

“SSID”:”%s”, // 周边AP的SSID名称

“Channel”:”%s”, // 该AP所用的信道

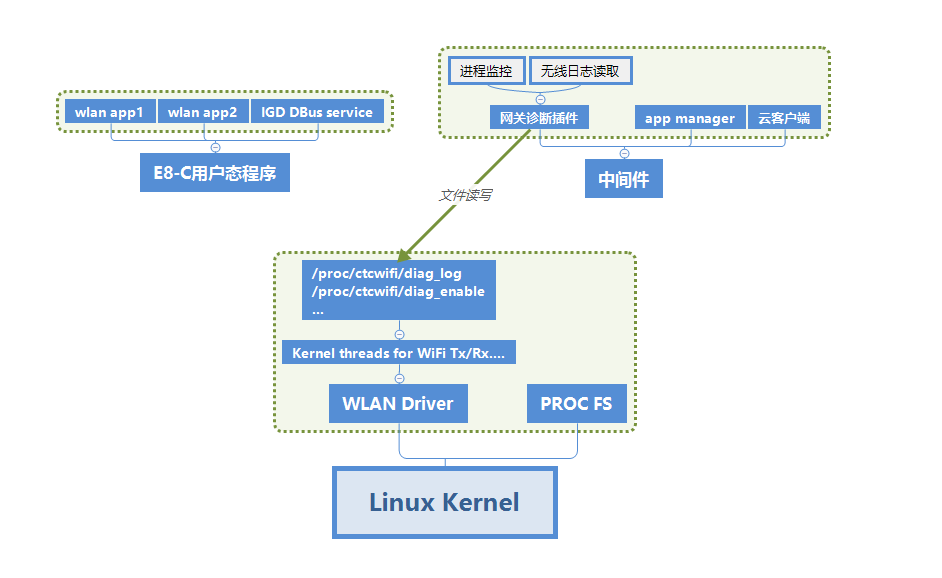
“RSSI”:”%s” // 信号强度，单位dBm

}]}

网关还需记录WiFi客户端尝试连接网关无线网络失败的信息。失败后发送信号WiFiConnFailure，其具体定义见WiFiConnFailure信号定义

* + 1. WIFI诊断

**WIFI诊断方案：**



**监控方案:**

1. **对WiFi的核心线程及进程状态进行监控.**
2. **对WiFi的异常事件, 采用读取/proc文件的方式获取无线的异常状态及日志.**

**采用proc文件系统作为读取WiFi驱动状态的接口, 有以下优点:**

1. **状态及日志都保存在内核内存中, 因为读取性能及对系统影响小.**
2. **插件通过标准的文件IO接口, 获取状态及日志, 兼容性好.**

WIFI诊断DEBUS接口：

在诊断接口下面, 增加一个方法, 用于查询WiFi 内核及进程.

接口com.ctc.igd1.OMDiag

方法: GetWiFiProcess(OUT ARRAY<STRUCT<STRING Name, INT32Pid, BOOLEAN isProcess>>wifiProcessList, OUT UINT32 result, OUT STRING errdesc)

说明:

返回所有WiFi的内核线程及进程.

Name: 进程或线程名

Pid: 进程号

isProcess: 是否是进程, true为进程, false表示是内核线程。

result：0（成功）/1（失败）。

errdesc：如果方法返回成功，则为NULL, 反之则在方法失败的时候填充上失败原因描述。

**Proc及日志文件定义：**

整体要求: 对于下面日志型文件, 例如/var/ctcwifi/association\_errors\_2G, /var/ctcwifi/diag\_log\_2G等,

存在tmpfs中, 文件最大大小是1M.,如果文件已经满了, 新记录覆盖时间最早的记录

无线模块统计

/proc/ctcwifi/Stat2G

/proc/ctcwifi/Stat5G

包含内容:

tx\_packets:

rx\_packets:

tx\_fails:

连接失败日志

/var/ctcwifi/association\_errors\_2G

/var/ctcwifi/association\_errors\_5G

格式：一条记录为一行

YYYY-MM-DD HH:MM:SS STA-MAC SSID: 错误[详细描述]

错误须包含下面定义的错误:

WiFi frames losing.

Capability checking failed.

Authentication failed.

Rejected by blacklist.

Rejected by STA limitation.

De-authed. 需描述de-auth的原因.

Association ignored by band steering.

参考例子:

2018-05-23 09:49:06 789682A39ABC ChinaNet-METH: Rejected by blacklist.

/proc/ctcwifi/diag\_enable\_2G

/proc/ctcwifi/diag\_enable\_5G

取值0、1和2：是否开启诊断模式，默认值是0，没有开启诊断模式。

0: 表示关闭诊断模式, 如果已经在诊断中, 设置为0表示停止diag过程。

1: 表示开启诊断模式1, 需要记录管理帧及控制帧到诊断日志文件（/var/ctcwifi/diag\_log\_2G或者/var/ctcwifi/diag\_log\_5G）。

2: 表示开启诊断模式2, 只需要记录管理帧到诊断日志文件。

如果已经在诊断中, 设置为1或者2表示清空诊断日志, 重新开始诊断。

/proc/ctcwifi/diag\_duration\_2G

/proc/ctcwifi/diag\_duration\_5G

单位秒，诊断模式持续时间，默认60秒, 最大值不得超过300秒.

STA/AP连接过程(诊断模式开启后记录)

/var/ctcwifi/diag\_log\_2G

/var/ctcwifi/diag\_log\_5G

格式：

YYYY-MM-DD HH:MM:SS SSID sends/receives 帧类型 from/to STA MAC[data/frame body].

要包含以下帧类型.

管理帧: Beacon, Probe Request, Probe Response, ATIM, Disassociation, Deauthentication, Association Request, Reassociation Request, Authentication

控制帧: RTS, CTS, ACK。(只诊断模式1要求记录控制帧)。

对于管理帧, framebody(data)用16进制文本格式保存.

例子:

2018-06-01 12:11:12 China-Net-home sends Beacon to FFFFFFFFFFFF[16进制表示的帧data]

统计信息 (有小数的，精确到小数点后2位)

信道占用率(百分比)

/proc/ctcwifi/channel\_occupancy\_2G

/proc/ctcwifi/channel\_occupancy\_5G

格式：

Channel occupancy

1. 50

基于STA的统计信息

/proc/ctcwifi/stats\_2G

/proc/ctcwifi/stats\_5G

格式：

STA SNR RSSI TXSUCC

STA-MAC1 XX XX XX.XX

STA-MAC2 XX XX XX.XX

RXCRCERR XX

其中TXSUCC为百分比， RXCRCERR为总的RXCRC错误次数

* + 1. 断网检测

当检测到PPPOE拨号断开时上报断网信息。

质量插件监听com.ctc.igd1.NetworkInfo.WANConnectionStatus及com.ctc.igd1.NetworkInfo.IPV6\_WANConnectionStatus的DBUS变更信号。若收到Internet IPv4/IPv6 WAN连接断开信号，运维插件会去取com.ctc.igd1.NetworkInfo.PPPoEDialReason/com.ctc.igd1.NetworkInfo.IPv6\_PPPoEDialReason作为断线的Reason/Reason6的值，并在下次Internet WAN连接建立后上报该信息。

另外，质量插件也会通过探针的方式来检测Internet WAN的连接性。例如，网关没有上报PPPoE断线的事件，但如果探测网络不通，也会上报检测结果。

网关需要在WAN连接状态发生变化的时候在com.ctc.igd1.NetworkInfo.PPPoEDialReason、com.ctc.igd1.NetworkInfo.IPv6\_PPPoEDialReason、com.ctc.igd1.NetworkInfo.WANConnectionStatus、com.ctc.igd1.NetworkInfo.IPv6\_WANConnectionStatus、com.ctc.igd1.NetworkInfo.WANIPAddr、com.ctc.igd1.NetworkInfo.WANIPv6Addr填入断线的详细信息，然后通过DBus发送INTERNET WAN连接的变更信号。

Json格式:

{

"Time":"2016-12-06 08:01:57"，

“Source”:”%s”, //用于表示PPPoE断线的事件来源，取值: “E8C”, “DiagApp”

“IPv6Support”:%d, //是否支持IPv6

“Event”:”%s”, //表示IPv4事件类型，取值：”WAN4DOWN”, ”IPCHANGE”, 若无该事件则 //可不带

“IPAddr”:”%s”, // IPv4地址，在WANDOWN的时候没有

“Event6”:”%s”, //表示IPv6事件类型，取值“WAN6DOWN”, “IP6CHANGE”，若无该事件 //则可不带

“IPAddr6”:”%s”, // IPv6地址, 在WAN6DOWN时没有

“Reason”:””, //表示IPv4断线的详细原因，在WAN4DOWN的时候从

// PPPoEDialReason中读取

“Reason6”:””, //表示IPv6断线的详细原因，在WAN6DOWN的时候从

// IPv6\_PPPoEDialReason中读取

}

说明：在网络掉线的情况下，网关需要将DBUS信息填充后再发送DBUS属性变更信号，尤其是PPPoEDialReason/IPv6\_PPPoEDialReason，当插件收到网络连接断开的dbus信号后，会根据需要去查询这两个值，若事先不填充这两个属性，插件就获取不了断网原因

其中，PPPoEDialReason的可取值范围为：

“ERROR\_NONE”

“ERROR\_ISP\_TIME\_OUT”

“ERROR\_NOT\_ENABLED\_FOR\_INTERNET”

“ERROR\_USER\_DISCONNECT”

“ERROR\_ISP\_DISCONNECT” (注：局方主动断网)

“ERROR\_IDLE\_DISCONNECT”

“ERROR\_FORCED\_DISCONNECT”

“ERROR\_SERVER\_OUT\_OF\_RESOURCES”

“ERROR\_ACCOUNT\_DISABLED”

“ERROR\_PASSWORD\_EXPIRED”

“ERROR\_AUTHENTICATION\_FAILURE”

“ERROR\_NO\_CARRIER” （注：无光信号）

“ERROR\_NO\_ANSWER”

“ERROR\_IP\_CONFIGURATION”

“ERROR\_UNKNOWN”

* + 1. 网关进程资源监控

网关系统监控E8C关键进程CPU/内存占用信息。平台可设置受控的进程及其CPU/内存阈值。应用进程占用的CPU/内存百分比超过该阈值时网关将进程名占用的CPU/内存信息保存到文件中，多个进程的告警信息用追加的方式记录。待质量插件上报DMP后插件会删除该文件。

文件名: e8c\_cpumem\_info

路径:/tmp/diaginfo/

JSON格式:

{

"Info": [{

“Time”:“2016-12-06 08:01:57”

“AppName”: “”,

“Description”:“%s”

}]

}

其中：

1. 当AppName为”SYSTEM”的时候，表示当前系统的CPU和memory告警，对于其他具体进程的情况，AppName填具体的进程名。

进程的名字定义如下，网关在收到相应的进程名后自己去对应网关的进程：

#define CTC\_GW\_SERVICE\_NAME\_HTTP “http”

#define CTC\_GW\_SERVICE\_NAME\_VOICE “voice”

#define CTC\_GW\_SERVICE\_NAME\_WIFI “wifi”

#define CTC\_GW\_SERVICE\_NAME\_DBUS “igddbus”

#define CTC\_GW\_SERVICE\_NAME\_SAMBA “samba”

#define CTC\_GW\_SERVICE\_NAME\_APPMGR “appmgr”

#define CTC\_GW\_SERVICE\_NAME\_CLOUDCLI “cloudcli”

#define CTC\_GW\_SERVICE\_NAME\_SAF “saf”

#define CTC\_GW\_SERVICE\_NAME\_OTHER “tr069c”

以及各个厂商自身关键应用。

默认的资源监控进程列表为：

#define CTC\_GW\_SERVICE\_NAME\_VOICE “voice”

#define CTC\_GW\_SERVICE\_NAME\_WIFI “wifi”

#define CTC\_GW\_SERVICE\_NAME\_DBUS “igddbus”

#define CTC\_GW\_SERVICE\_NAME\_APPMGR “appmgr”

#define CTC\_GW\_SERVICE\_NAME\_CLOUDCLI “cloudclient”

#define CTC\_GW\_SERVICE\_NAME\_SAF “saf”

#define CTC\_GW\_SERVICE\_NAME\_TR069C “tr069c”

2.Description格式为“ current A occupancy factor is B%, while threshold is C%”。

A=cpu或memory

B为当前进程实际使用的百分比，取值1-100

C为当前监控进程设置的阈值，取值1-100

**网关资源监控在实现时需注意一下问题：**

1. **CPU和**memory**占用率的计算需要考虑5分钟内的平均CPU和**memory**占用率，通过2次或2次以上读取/proc/<pid>/stat文件来计算。**
2. 当整个系统或者单个进程的CPU或memory占用量超过阈值的时候都要写LOG。
3. 当同一监控进程的CPU占用率和memory使用率都超过阈值时，需要分别产生2条告警，一条是cpu的告警，一条是memory的告警。
4. SYSTEM的CPU和memory默认阈值为85，其他默认监控进程的CPU和memory默认阈值为40。
   * 1. 插件异常监控信息（中间件实现）

中间件会用PING-PONG的方式对插件进行监测，当发送PING后插件连续三次没有回复，则认为该插件发生异常，并将相应的信息写到log文件中

文件名：/tmp/diaginfo/plugin\_info（中间件中）

JSON格式定义：

{

"Info":[

{

"AppName": "%s",

"Time": "2017-02-02 12:12:12",

"Reason": "xxxx"，

“Logs”:”%s”

}

]

}

* + 1. 网关受控进程异常信息

记录进程异常信息，包括进程本身逻辑错误造成的运行异常，SIGSEG，SIGBUS导致的进程崩溃，各种外因造成的进程异常（如异常收包）等等。网关根据应用的逻辑来决定怎样监控具体的进程，比如可以通过检测nf\_conntrack的收发包字节数来判断网关网络连接模块是否正常等。

当进程运行异常时网关应尽可能清楚详细地将错误描述写入文件。尤其是出现如SIGSEG，SIGBUS等信号造成异常时，要将信号值写入错误描述里面。多个异常时追加到文件

受控进程可以通过平台来进行设置

文件名：process\_info

路径: /tmp/diaginfo/

JSON格式

{

“Info”: [

{

”AppName”: “%s”,

“Time”: “2016-12-06 08:01:57”,

“Reason”: “%s”, 表示异常的原因

“Logs”:”%s” // 错误日志（若有）

}

]

}

默认的进程列表包括：

CTC\_GW\_SERVICE\_NAME\_VOICE，

CTC\_GW\_SERVICE\_NAME\_WIFI，

CTC\_GW\_SERVICE\_NAME\_DBUS，

CTC\_GW\_SERVICE\_NAME\_SAF

CTC\_GW\_SERVICE\_NAME\_TR069C

当AppName为GW\_SERVICE\_NAME\_TR069C时，除发生异常时网关要记录（原因填具体异常的描述）外，还需要在TR069的WAN连接状态变化的时候（包括网关重启后TR069的WAN连接获取不了地址的情况），或者每半个小时，网关需要将WAN状态变化及TR69c最后一次向ACS（ITMS）发送Inform的时间也记录到文件里面去，这种情况下Reason的内容为:

“Reason”:{”TR069WANStatus”:”%s”,”TR069WANIP”:”%s”,“LastInformTime”:”%s”}

另考虑到厂家可能需要对自己特有的重要进程进行监控，各厂家可将其认为比较重要的进程放到默认列表里面去（毕竟厂家自己也可能需要用到这些异常信息）

* + 1. 网关端口监测（网关质量插件实现）

网关质量插件将当前系统开放的端口进行采集上报，网关只需提供netstat工具供网关质量插件使用即可，文件则由网关质量插件按需生成

。

文件名：plug\_port\_info

路径：/tmp/diaginfo/

网关只需提供netstat工具供网关质量诊断插件使用，文件则由网关质量诊断插件按需生成。

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 192.168.1.1:17998 0.0.0.0:\* LISTEN 4772/cloudclient

tcp 0 0 0.0.0.0:www 0.0.0.0:\* LISTEN 27659/uhttpd

tcp 0 0 127.0.0.1:5916 0.0.0.0:\* LISTEN 3418/acsd

tcp 0 0 0.0.0.0:32768 0.0.0.0:\* LISTEN 2889/inter\_connd

tcp 0 0 192.168.1.1:1990 0.0.0.0:\* LISTEN 3420/wps\_monitor

tcp 0 0 :::netbios-ssn :::\* LISTEN 889/smbd

tcp 0 0 :::www :::\* LISTEN 27659/uhttpd

tcp 0 0 :::webcache :::\* LISTEN 647/smd

tcp 0 0 :::38514 :::\* LISTEN 647/smd

tcp 0 0 :::ftp :::\* LISTEN 647/smd

tcp 0 0 :::30010 :::\* LISTEN 647/smd

tcp 0 0 :::445 :::\* LISTEN 889/smbd

* + 1. 语音模块信息采集

厂商监控语音模块的重要事件，包括摘挂机、号码注册状态变化等，在状态发生变化的时候，根据C.9.12节定义的SysVoiceEvents信号，发送相应的DBUS信号，质量插件会监听com.ctc.igd1.OMDiag.SysVoiceEvents信号，并生成以下格式的日志上报DMP。

具体事件定义请参见C.9.12节相关信号定义。JSON格式:

{

“Info”:[

{

“Time”: “”,

“Event”:“%s”,

“Description”:“”

}

]

}

网关只需发送com.ctc.igd1.OMDiag.SysVoiceEvents信号 ,无需生成VOICE\_INFO文件。

* + 1. 其它需要实现的接口

诊断插件通过预订信号来监控com.ctc.igd1.NetworkInfo**.**WANConnectionStatus，com.ctc.igd1.NetworkInfo.WANIPAddr，com.ctc.igd1.NetworkInfo.IPv6\_WANConnectionStatus，com.ctc.igd1.NetworkInfo.WANIPv6Addr这四个属性值，网关需保证当这四个属性值变化的时候会发出相应的信号。

* + 1. 补充要求

**关于超阈值后日志记录的说明**

对于设有阈值的监控对象，网关需将该采样参数在5分钟之内的平均值作为是否上报的依据。若5分钟内的平均值超过阈值就上报一次，否则不上报，并继续监控。

3.0网关当CPU温度、PON模块温度、FLASH占用、最大连接数超过设置阈值的时候，网关只需发送相应的接口信号，无需生成告警文件。

**需要定期采集用于大数据分析的数据项**

以下信息需要每天定期采集上报大数据分析平台，用于获取网关运行状态的常态数据：

CPU使用率、内存使用率、目录大小、SLAB信息、网络链接数、无线信号（信道，强度，无线连接设备量，无线误码率）、语音状态（语音状态监控（注册，异常，摘机等）、光模块温度

上述信息上报周期频次必须可以配置。

1. （资料性附录）  
   网关快联配网
   1. 快联配网基础

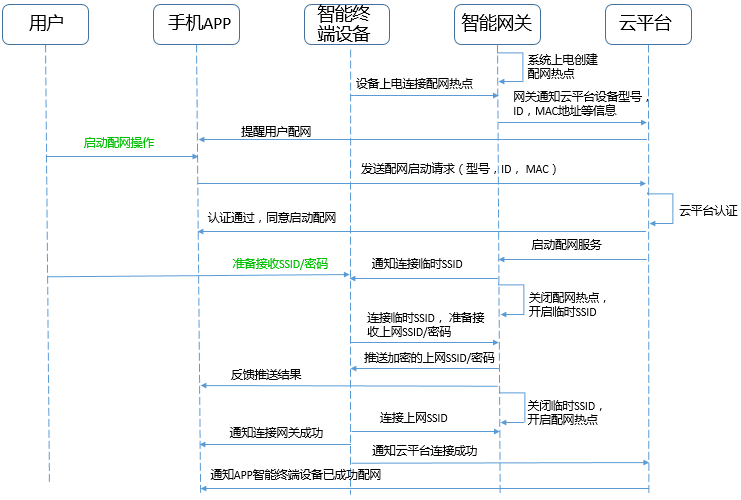
智能终端设备：指无线AP，repeater，无线摄像头以及智能插座、智能灯泡、智能等等支持802.11 WiFi技术的家庭终端设备。

网关快联配网，是指智能网关能够识别和认证家庭网络中的智能终端设备，并且将自身WiFi的security信息（主要是SSID和密码）自动推送到合法智能终端设备，使之能够在免用户配置的情况下快速接入家庭网络的能力。

网关的快联配网能力，是智能家庭网络能力的一部分，可能需要手机APP，智能终端设备，智能网关，智能云平台等多种实体的相互配合，才能实现无屏无键盘的智能终端设备在免配置情况下快速接入家庭网络。

对于具备WPS协商能力的智能终端设备，应采用WPS机制与智能网关进行配网。对于不具备WPS能力的智能终端设备，宜采用以下快联配网方案快速接入家庭网络。

* 1. 基于云平台认证的快联配网



**图I.1 基于云平台认证的快联配网流程**

网关需具备能力：

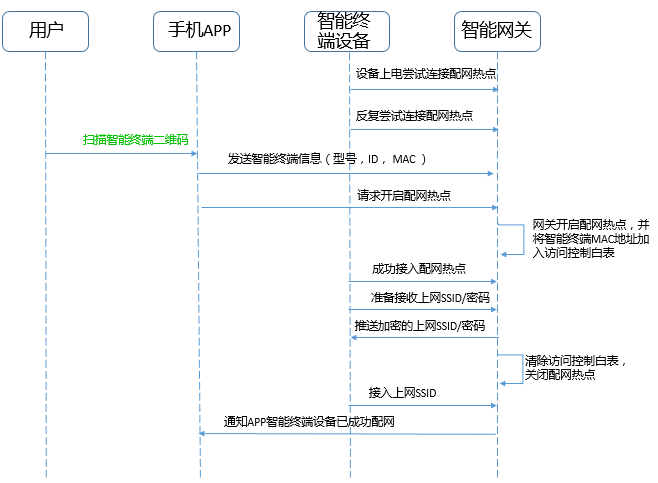
1. 创建配网SSID
2. 指定SSID的有效时间
3. 指定SSID流量能够访问的IP地址和端口
4. 接收智能终端请求（插件实现）
5. 推送上网SSID/密码（插件实现）
6. 通知云平台智能终端信息（插件实现）
7. 接收云平台启动配网指令（插件实现）

网关在系统启动以后，应在空闲的SSID中创建一个配网SSID，用于接收智能终端设备的连接，配网插件通过配网SSID接收智能终端设备上报的设备信息（设备ID，MAC地址）。当云平台完成鉴权通知插件启动配网后，插件应关闭配网SSID同时创建一个临时SSID（可通过修改原有配网SSID名称为新的临时SSID名称来实现），并将临时SSID信息推送给终端设备。

智能终端接收到临时SSID信息以后，应重新连接临时SSID。配网插件通过临时SSID，将加密以后的上网SSID名称和密码推送到智能终端设备。终端重新连接上网SSID，获取Internet访问服务，完成配网过程。

配网SSID和临时SSID是没有物理层鉴权机制的SSID，为了避免对网关设备的安全性造成危害，配网SSID和临时SSID应支持：

1. 配网SSID和临时SSID均应关闭SSID广播
2. 配网SSID和临时SSID均应禁止提供Internet网络访问服务
3. 配网SSID和临时SSID均应与用户家庭内网隔离
4. 配网SSID和临时SSID均应只允许用户侧流量访问网关LAN侧管理IP地址+指定端口
5. 临时SSID应仅在短时间内存在（1-5分钟，由配网插件创建时确定），终端设备配网完成以后，临时SSID应关闭。如果配网不成功，存续时间到期以后，临时SSID也应关闭。临时SSID关闭以后，应同时重新开启配网SSID
6. 当配网插件卸载以后，配网SSID可以由中间件回收，重新设置为空闲状态
   1. 基于动态配网热点的快联配网



**图I.2 基于动态配网热点的快联配网流程**

网关需具备能力：

1. 创建配网SSID
2. 将指定MAC地址加入配网SSID白表
3. 接收手机请求：智能终端信息，开启配网热点请求（插件实现）
4. 推送上网SSID/密码（插件实现）

当网关接收到手机APP发送的配网请求以后，应在空闲的SSID中创建一个配网SSID，用于接收智能终端设备的连接，配网插件通过配网SSID接收智能终端设备上报的设备信息（设备ID，MAC地址），并将终端设备的MAC地址加入配网SSID的访问白表当中。

网关创建配网SSID后，智能终端成功连接配网SSID。配网插件通过配网SSID将加密后的上网SSID和密码推送至智能终端。终端重新连接上网SSID，获取Internet访问服务，完成配网过程。

配网SSID是没有物理层鉴权机制的SSID，为了避免对网关设备的安全性造成危害，配网SSID应支持：

1. 配网SSID应关闭SSID广播
2. 配网SSID应禁止提供Internet网络访问服务
3. 配网SSID应与用户家庭内网隔离
4. 智能终端设备MAC地址应加入配网SSID的访问控制白表中，仅有智能终端设备自身可以和配网SSID连接
5. 配网SSID应仅在短时间内存在（1-5分钟，由配网插件创建时确定），终端设备配网完成以后，配网SSID应关闭。如果配网不成功，存续时间到期以后，配网SSID也应关闭。
   1. 智家易联无感配网流程
6. **无感配网总体流程**



**图I.3 智家易联无感配网流程**

待配网设备在配网模式下周期性在Wi-Fi的全信道（在所有的合法Wi-Fi信道）上进行Probe Request做AP列表扫描，在Probe Request中携带智家易联无感配网扩展IE1；

天翼网关作为配网设备收到Probe Request，根据Probe Request携带的扩展IE1识别是否是支持e-Link开放的配网能力(即智家易联无感配网能力)的设备；如支持，则向平台发送通知消息，平台向小翼管家APP发送发现待配网设备的提示；

用户通过APP或者按键申请配网后，天翼网关开启临时SSID,等待待配网设备发送ProbeRequest（扩展IE1），这个等待过程大约10秒，如果10秒内有待配网设备发送ProbeRequest，进入配网过程。

当天翼网关接收到待配网设备发送带扩展IE1的Probe Request，回复一个Probe Response（携带一个扩展IE2），这个扩展IE2中带有临时SSID，用来给待配网设备接入。

*注：这个临时的SSID使用隔离的网络，这个网络无法和天翼网关下挂的其他Wi-Fi客户端互通，也无法和外网连接访问。这个临时的局域网是给配网过程使用。图I.3中的用户授权操作这一步骤可以根据取舍。*

待配网设备接收到Probe Response中携带有扩展IE2，则根据携带的临时SSID和信道号，切换到Station模式，并连接到指定的临时SSID上。获取到IP地址后，进行IP层安全协商和配网过程。获得入网SSID、加密模式及其他信息，配网设备通过该入网SSID接入天翼网关，天翼网关关闭临时SSID，完成配网。

如果安全协商和配网过程有错误，待配网设备应该重新切换到SoftAP模式，并进行周期AP列表扫描，即回到配网模式。

1. **扩展IE1和IE2的定义**
2. IE1各字段含义

|  |  |  |
| --- | --- | --- |
| 字段名 | 取值 | 含义 |
| Tag number | 0xDD | 十进制221，Wi-Fi联盟规定的厂商自定义标识 |
| OUI | 00-E0-XX | 中国电信OUI，需要申请 |
| Vendor specific type | 0xXX | 固定 |
| Data | TLV8格式 | 此字段定义Vendor自定义的数据内容，见下方表格 |

扩展IE1中的TLV8字段定义：

1. IE1中Data字段含义

|  |  |  |  |
| --- | --- | --- | --- |
| T  1byte | L  1byte | V | 说明 |
| 1 | 2 | 2字节开放生态ID | 用来识别设备属于哪个开放生态下的设备。  00 01-电信e-Link生态 |
| 2 | 4 | 4字节产品ID | （电信e-Link生态编码格式） |
| 3 | 1 | bit0：PN数字伪随机验证码  bit1：QR Code  bit2：NFC Tag  bit3：路由器配对  bit4：默认S码格式  bit5-bit6  （高2位保留未来使用） | 是否需要配网S码，用于路由器、手机App提示。  该字段支持“或”方式，可以将数字序列、QR Code、NFC Tag同时支持。  bit0~bit2---表示通过非中国电信路由器配网是否需要配对码以及配对形式；  bit3---表示是否允许通过中国电信路由器配网一键配网；  bit4---默认S码格式，仅非中国电信路由器配网不需要配对码或运行中国电信路由器配网下有效，0---全局S码 1---生态S码  bit5-bit6: 加密方式，由各生态自行定义 |
| 4 | 1 | SoftAP的信道号 | 待配网设备当前SoftAP所在信道编号。 |
| 5 | 2 | 距离下次全信道扫描时间 | 待配网设备告知距离下次全信道扫描时间（s），避免全信道扫描时候无法进行SOFTAP配网 |
| 6 | X | 临时SoftAP的SSID | 待配网设备当前SoftAP的SSID |
| 7 | Y | 非电信e-Link生态下的产品标识。长度、数据格式由不同生态定义。  在天翼网关，则按一个Y长度的byte数组进行处理（如果是字符串则就等效大小写敏感） | 待配网设备在自身生态中的唯一标识。用于在手机OS、App等场景下用来检索设备信息。 |

扩展IE2中的Data字段定义：

1. IE2中各字段含义

|  |  |  |
| --- | --- | --- |
| 字段名 | 取值 | 含义 |
| Tag number | 0xDD | 十进制221，Wi-Fi联盟规定的厂商自定义标识 |
| OUI | 00-E0-XX? | 中国电信OUI |
| Vendor specific type | 0xXX | 固定 |
| Data | TLV8格式 | 此字段定义Vendor自定义的数据内容，见下方表格 |

扩展IE2中的TLV8字段定义：

1. IE2中Data字段含义

|  |  |  |  |
| --- | --- | --- | --- |
| T  1byte | L  1byte | V | 说明 |
| 0x80 | X | 临时AP的SSID | e-Link临时AP的SSID，开放的、随机的，且隐藏的 |
| 0x81 | 1 | 临时SSID信道编号 | 临时AP所在信道编号。通常和路由器主信道一致，也有可能和主信道不一样 |

1. **IP层安全协商**

IP层协商都是基于CoAP over UDP方式， CoAP over UDP收发都用同一个端口，默认为5683。

如果模组端侧资源受限，可以不用使用完整的CoAP协议栈，而直接针对配网过程的几个请求响应消息按CoAP的格式进行编码。

1. **主流程**



**图I.4　安全协商业务流程图**

1. 配网设备与待配网设备间Wi-Fi连接建立后，配网设备向待配网设备发起配网请求启动消息，启动SPEKE协商，携带协商版本号。

*注：协商版本号是双方分别携带当前使用版本号、支持的最小版本号、支持的所有版本号，双方基于这几个字段决定最终使用的版本号。*

1. 待配网设备收到配网请求启动消息，生成随机盐值salt1，待配网设备根据salt1与S码生成待配网设备侧SPEKE公私钥对pk1、sk1；生成随机挑战值challenge1。

公式：

secret = HKDF(S, salt1, "hichain\_speke\_base\_info", 32B)；

base = secret^2 mod P；

sk1 = rand；

pk1 = base ^ sk1 mod P;

1. 待配网设备回送配网请求启动响应，携带salt1、协商版本号、pk1、challenge1。
2. 配网设备收到回送配网请求启动响应，根据salt1与S码生成配网设备侧SPEKE公私钥对pk2、sk2；再根据pk1、sk2生成共享秘钥SharedSecret，再加上salt派生出会话秘钥SessionKey1（用于配对数据加密）、SessionKey2（用于挑战值HMAC计算），生成随机挑战值challenge2；再根据SessionKey2和两个挑战值生成配网设备侧凭证hmac2；最后在根据SessionKey1根据salt1派生出数据加密秘钥DataEncKey。

公式：

secret = HKDF(S, salt1, "hichain\_speke\_base\_info", 32B)；

base = secret^2 mod P；

sk2 = rand；

pk2 = base ^ sk2 mod P;

SharedSescret = pk1 ^ sk2 mod P;

SessionKey1 || SessionKey2 = HKDF(SharedSecret, salt1, "hichain\_speke\_sessionkey\_info", 32B);

（派生出的32个字节，前16个字节为会话秘钥1、后16个字节为会话秘钥2）

Hmac2 = HMAC（SessionKey2, challenge1 || challenge2）;

DataEncKey = HKDF(SessionKey1, salt1, "hichain\_return\_key", 16B)

1. 配网设备发生配网请求验证消息，携带pk2、challenge2、hmac2，hmac2使用sessionkey1加密。
2. 待配网设备收到配网请求验证消息，根据pk2、sk1生成共享秘钥SharedSecret。使用SharedSecret及salt1派生会话秘钥SessionKey1、SessionKey2验证hmac2，验证通过后派生数据加密秘钥DataEncKey。在根据SessionKey2和两个挑战值生成待配网设备侧凭证hmac1；最后在根据SessionKey1根据salt1派生出数据加密秘钥DataEncKey。

公式：

SharedSescret = pk2 ^ sk1 mod P;

SessionKey1 || SessionKey2 = HKDF(SharedSecret, salt1, "hichain\_speke\_sessionkey\_info", 32B);

（派生出的32个字节，前16个字节为会话秘钥1、后16个字节为会话秘钥2）

Hmac1 = HMAC（SessionKey2, challenge2 || challenge1）;

DataEncKey = HKDF(SessionKey1, salt1, "hichain\_return\_key", 16B)

1. 待配网设备回送配网请求验证响应，携带sessionkey1加密后的hmac1。
2. 配网设备收到配网请求验证响应，验证hmac1。
3. 配网设备发送配网信息：SSID、密码、扩展数据，配网数据使用DataEncKey加密。
4. 待配网设备使用DataEncKey解密配网数据，临时保存到本地。

待配网设备根据配网信息连接到家庭路由器Wi-Fi网络，监听本地控制UDP端口。

1. **报文发送和重试时序**

待配网设备连接到天翼网关的临时AP，获得IP地址后；配网设备对对端地址（手机的IP，或者网关IP）进行第一条协商报文的发送，配网设备将以100ms间隔发送第一条报文，直到收到待配网设备发送的第二条协商报文。

对于中间协商报文，每个1秒重发一次，一共发送5次。配网设备和待配网设备需要对报文的重发做出冗余处理。

待配网设备在发送最后一条协商报文时，为确保配网设备接收成功率，这条报文会发送5次，每次间隔100ms。也就是说在500ms后，才会开始切换模式，连接指定的AP。

1. **默认S码**

默认S码用于配网流程中不需要输入S码的情况，默认S码可能无法解决近端确认问题，因此可能存在设备被其他用户截取配网问题，但是可以通过设备在获取到配网注册信息后，要求一定时间内用户在设备按键或进行一次开关以激活配网注册信息以进行近端确认。

默认S码为全局默认S码，后续会增加支持生态默认S码：

全局默认S码为中国电信统一分配，固定为：78965425

* 1. Beacon/Probe帧中扩展Vendor-specific Information Element信息的快联配网

应支持插件接收Probe Request帧中Vendor-specific Information Element字段和在发送Beacon帧中添加Vendor-specific Information Element字段的能力，具体要求如下：

* 1. 插件注册需要接收的，在Probe Request帧中Vendor-specific Information Element字段内的OUI值。当网关WiFi接口收到Probe Request帧中，包含插件注册的OUI值的Vendor-specific Information Element字段时，将该字段返回插件；
  2. 插件有能力在指定的无线接口发送的beacon、Probe Response帧中，添加自定义的Vendor-specific Information Element字段。

1. （资料性附录）  
   无STB的IPTV技术方案
   1. 总体系统概述
2. 系统总体目标

在家庭网络环境下，开发手机客户端功能作为用户使用IPTV的界面，用户通过该客户端选取节目，然后在支持DLNA的智能电视机上观看节目内容，并在手机客户端上进行节目播放控制，实现IPTV的业务功能。

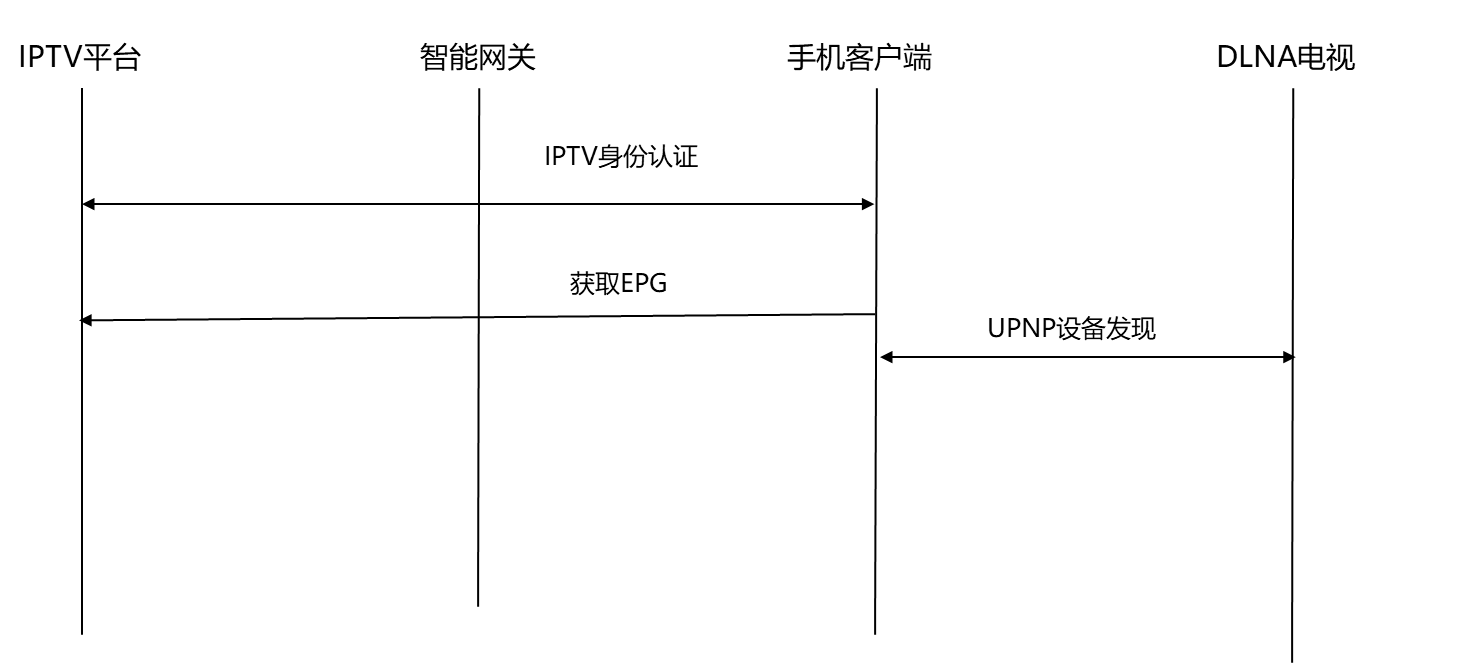
1. 系统基本流程

网关通过导入网络侧媒体资源支持承担DMS角色，手机承担DMC角色，与DMR角色（电视机）配合，基于DLNA协议实现设备发现、播放控制等功能。

手机支持将DLNA投屏控制报文推送到电视机；电视机获取投屏控制报文中媒体URL地址，并向网关发起媒体流请求。

网关支持依据电视机的媒体流请求，向IPTV平台获取媒体流；并支持媒体流的协议类型转换，将组播及媒体承载协议转换为DLNA数据流所用的HTTP协议。

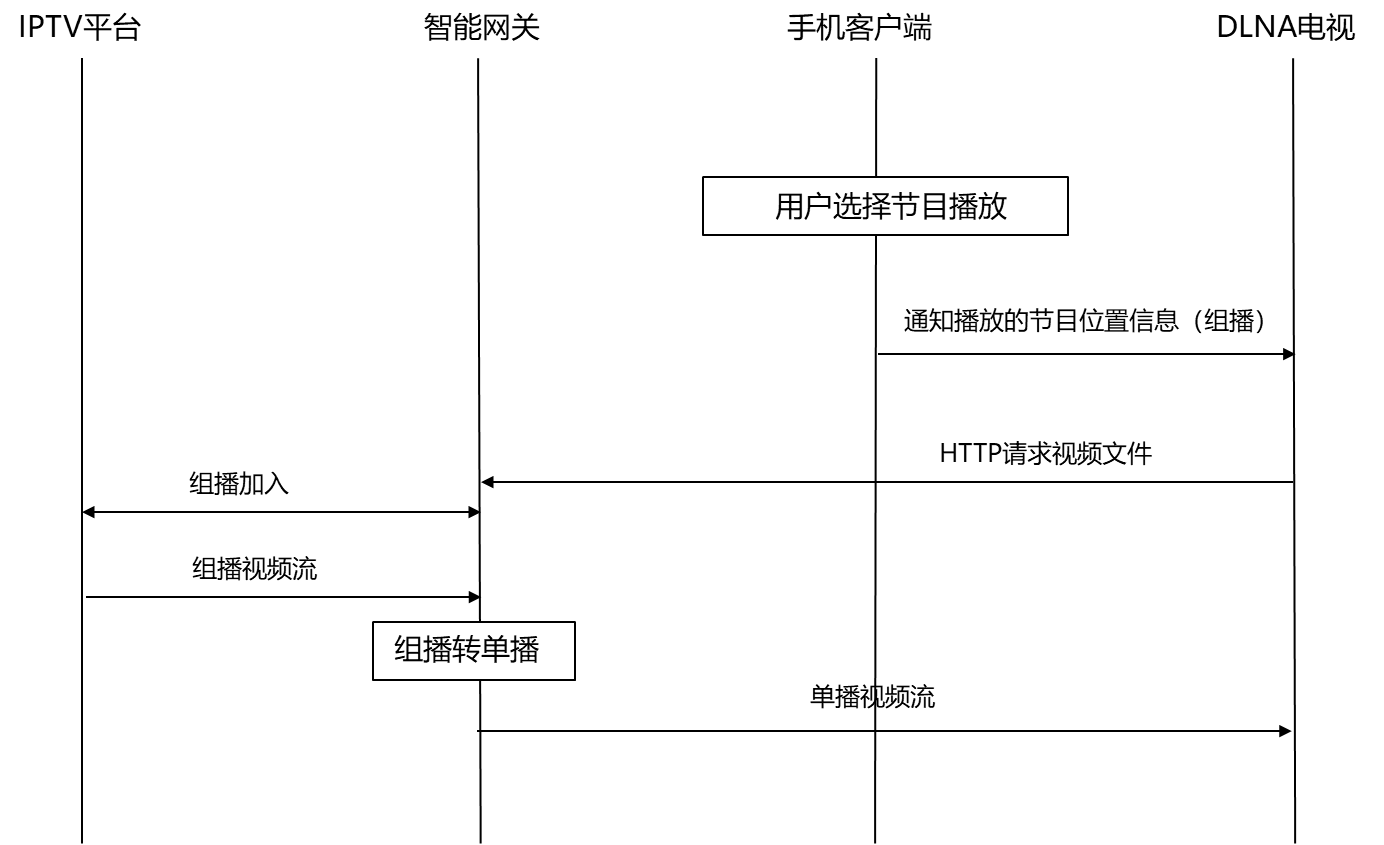
1. 系统初始化：



说明：

* + 手机APP与IPTV server 进行注册认证，获取EPG及媒体地址

1. IPTV组播：



* + 手机APP将用户选择频道信息以DLNA格式发送到DMR（DLNA电视）
  + DMR向DMS(网关)请求媒体流
  + DMS发送Jion报文到对应组播组，同时将组播媒体流转为单播媒体流，推送到DMR

1. DLNA 控制命令（DMC投屏：DMC->DMR）中媒体地址的设置规则：
   * 组播投屏命令：

http://192.168.1.1:9090/IGMP:224.1.1.2:2024/urn:schemas-upnp-org:service:AVTransport\_control

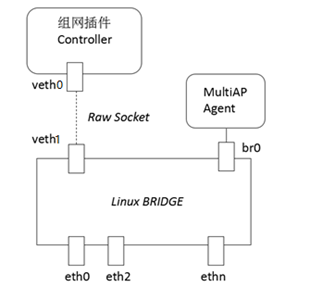
* 1. 智能网关IPTV手机客户端功能要求

1. 支持DLNA的DMC功能，发现家庭网络的DMR。
2. 支持IPTV开机认证关联流程，详见电信《IPTV 业务系统终端与业务运营平台接口技术要求V3.0》6.1.2 终端开机认证关联流程。
3. 获取IPTV EPG，并提取节目内容地址与相关信息。
4. 完成用户操作（支持播放、停止、快进、快退）。
5. （资料性附录）  
   网关Mesh Controller和Agent接口参考设计

智能网关中，Controller和Agent由不同开放者实现，设计中应尽量保证二者之间低耦合，降低相互之间的依赖。

* 1. Controller和Agent的接口设计

在内置AP的网关中，MultiAP Controller和MultiAP Agent之间需符合如下架构：



创建一对虚接口veth1，veth0；其中veth1挂载到Linux Bridge上，Controller通过绑定RAW套接字绑定到veth0上。

通过技术手段保证veth0上的MAC在UNI侧具有唯一性。

MultiAP Controller和MultiAP Agent之间采用标准的WFA MultiAP协议进行通信。

组网插件（Controller）通过DBUS接口获取网关WiFi配置信息。

* 1. 参考**调用接口**

利用如下命令，网关预置创建veth0、veth1接口。

dev@debian:~$ sudo ip link add veth1 type veth peer name veth0

dev@debian:~$ sudo ip link set veth1 up

dev@debian:~$ sudo ip link set veth0 up

* 1. 创建**RAW Socket**

struct ifreq ifr;

struct sockaddr\_ll ll;

//创建raw套接字

int fd = socket(PF\_PACKET, SOCK\_RAW, htons(0x893A));

//ioctl获取veth0接口index

memset(&ifr, 0, sizeof(ifr));

strcpy(ifr.ifr\_name, "veth0");

ioctl(fd, SIOCGIFINDEX, &ifr)

//bind将raw套接字fd绑定到veth0上

memset(&ll, 0, sizeof(ll));

ll.sll\_family = AF\_PACKET;

ll.sll\_protocol = htons(0x893A);

ll.sll\_ifindex = ifr.ifr\_ifindex;

bind(fd, (struct sockaddr \*) &ll, sizeof(ll)

* 1. 获取**veth0的MAC地址**

BYTE mac[6] = {0};

struct ifreq ifReq = {{0}};

//ioctl取veth0上的mac地址

strncpy(ifReq.ifr\_name, “veth0”, sizeof (ifReq.ifr\_name) - 1);

ioctl(fd, SIOCGIFHWADDR, &ifReq)

memcpy(mac, ifReq.ifr\_hwaddr.sa\_data, 6)

* 1. **Controller DBUS**接口
     1. com.ctc.map1.Management

**属性**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 | 版本 |
| Enable | boolean | readwrite | 是否开启Multi-AP Controller自动配置功能，true开启，false禁用，不处理CMDU包 |  |
| ssid2G | STRING(32) | readwrite | Controller配置Agent 2.4G WiFi的SSID |  |
| authMode2G | STRING(16) | readwrite | 配置Agent 2.4G认证模式，仅支持wpa2psk和open两种 |  |
| key2G | STRING(32) | readwrite | 配置2.4G密码，ascii码!与~之间字符 |  |
| backhaul2G | boolean | readwrite | true表示既支持backhaul又支持fronthaul，false表示仅支持fronthaul |  |
| backhaulOnly2G | boolean | Readwrit  e | true表示仅支持backhaul（不管backhaul2G值是false还是true），如果是false再根据backhaul2G的值判断 |  |
| tearDown2G | boolean | readwrite | true表示改Radio即2.4G设置的ssid不能连接任何client，不发送beacon帧，类似禁用，agent忽略ssid、key等配置内容  false为默认值，controller正常配置agent |  |
| ssid5G | STRING(32) | readwrite | Controller配置Agent 5G WiFi的SSID |  |
| authMode5G | STRING(16) | readwrite | 配置Agent 5G认证模式，仅支持wpa2psk和open两种 |  |
| key5G | STRING(32) | readwrite | 配置5G密码 |  |
| backhaul5G | boolean | readwrite | true表示既支持backhaul又支持fronthaul，false表示仅支持fronthaul |  |
| backhaulOnly5G | boolean | readwrite | true表示仅支持backhaul（不管backhaul5G值是false还是true），如果是false再根据backhaul5G的值判断 |  |
| tearDown5G | boolean | readwrite | true表示改Radio即5G设置的ssid不能连接任何client，不发送beacon帧，类似禁用，agent忽略ssid、key等配置内容  false为默认值，controller正常配置agent |  |
| enablebh | BYTE | readwrite | 0表示M2中不下发backhaul配置，1表示2.4G和5G均下发backhaul配置，2表示仅下发2.4G backhaul配置，3表示仅下发5G backhaul配置，如果controller收到的M1中”AP radio basic capabilities” TLV中”Maximum BSS Support”值为1，则根据协议不管该值为多少都不下发backhaul配置 |  |
| ssidbh | STRING(32) | readwrite | Controller配置Agent Backhaul BSS的SSID，默认值为随机生成的16个字符，字符范围0~9a~zA~Z |  |
| keybh | STRING(32) | readwrite | Controller配置Agent Backhaul BSS的密码，默认密码为8个随机字符，字符范围0~9a~zA~Z |  |
| authModebh | STRING(16) | readwrite | 配置Agent Backhaul ssid认证模式，仅支持wpa2psk和open两种，默认为wpa2psk |  |
| tearDownbh | boolean | readwrite | true表示backhaul连接断开  false为默认值，backhaul连接正常 |  |

**方法**

* **ChannelSet**(IN STRING alMac, IN STRING alModel, IN UINT channel, IN UINT transmitpower, OUT UINT32 result, OUT STRING errdesc);

向指定Agent发送Channel Selection Request消息。 [[17.2.13 17.2.15]](#_[2]Multi-AP_Specification_v1.0.pdf)

输入参数说明如下：

alMac: 指定Agent的AL Mac地址，string类型，取值为字符串类型的MAC地址，命令行传参，例如：string:"00:0c:43:28:80:15"

alModel：指定agent上的radio频段，string类型 “2.4g” 或“ 5g”.

channel ：指定agent和radio上期待配置的信道， uint32类型，0：自动配置。>0 期望的信道。其中中国2.4G为1~13，5G为36、40、44、48、52、56、60、64、149、153、157、161、165

Radiotransmitpower： 指定agent和radio上期待配置的radio发射功率，单位dBm。Uint32类型：期望radiotrasmitpower。1mW=0dBm，小于1mW，则为负数，我国标准是小于50mW，即17dBm，增强模式2.4G到200mW即23dBm，5G到400mW即26dBm，所以该值2.4G最大为23，5G最大为26

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Managemen com.ctc.map1.Management.ChannelSet string:"00:0c:43:28:80:A3" string:"2.4g" uint32:7 uint32:0

* **ClientSteeringRequest**(IN BYTE requestMode, IN ARRAY<STRING> STAMacList, IN ARRAY<STRING> TargetBSSIDList, OUT UINT32 result, OUT STRING errdesc);

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Management com.ctc.map1.Management.ClientSteeringRequest byte:1 array:string:"14:5f:94:db:c6:57" array:string:"00:0c:43:26:60:40"

输入参数说明如下：

requestMode: Request模式，是强制模式还是By Opportunity模式，byte类型，取值为0或1，0表示Opportunity Steering[MAP文档11.2]，1表示Mandate Steering[MAP文档11.1]，例如：byte:1

staMacList: STA Mac地址列表，array:string类型，即字符串数组类型，命令行传参，例如：array:string:"14:5f:94:db:c6:57","00:9d:6b:07:a9:b4"，不能为空

targetBSSIDList: 目标BSSID列表，array:string类型，即字符串数组类型，命令行传参，例如：array:string:"00:0c:43:26:60:40"，该值为一个或者多个，如果为多个则要与staMacList个数保持一致且顺序一致，当为一个时，可以为全F通配MAC（FF:FF:FF:FF:FF:FF）,该情况由Agent自己决策选择最合适目标BSSID

* **SetClientSteeringPolicy**(IN BYTE ChannelUtilizationThreshold2G, IN BYTE ChannelUtilizationThreshold5G, IN BYTE RCPISteeringThreshold, OUT UINT32 result, OUT STRING errdesc);

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Management com.ctc.map1.Management.SetClientSteeringPolicy byte:70 byte:80 byte:112

输入参数说明如下：

ChannelUtilizationThreshold2G: 2.4G信道使用率阈值，取值范围为0 ~ 255，byte类型，命令行传参，例如：byte:70

ChannelUtilizationThreshold5G: 5G信道使用率阈值，取值范围为0 ~ 255，byte类型，命令行传参，例如：byte:80

RCPISteeringThreshold: RCPI阈值，取值范围为0 ~ 220，byte类型，命令行传参，例如：byte:112

* **ClientAssociationControlRequest**(IN STRING bssid, IN BYTE associationControl, IN ARRAY<STRING> STAMacList, OUT UINT32 result, OUT STRING errdesc);

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Management com.ctc.map1.Management.ClientAssociationControlRequest string:"00:0c:43:26:60:40" byte:0 array:string:"68:3e:34:3f:b3:06","14:5f:94:db:c6:57"

输入参数说明如下：

bssid: BSSID，string类型，取值为字符串类型的MAC地址，例如：string:"00:0c:43:87:82:6A"

associationControl: 关联控制标志，取值为0或1，0表示Block，阻止staMacList中客户端连接到指定BSSID，1表示Unblock， byte类型，例如：byte:0

staMacList: STA Mac地址列表，array:string类型，即字符串数组类型，例如：array:string:"14:5f:94:db:c6:57","00:9d:6b:07:a9:b4"

* **APMetricQuery**(IN STRING alMac, IN ARRAY<STRING> BSSIDList, OUT UINT32 result, OUT STRING errdesc);

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Management com.ctc.map1.Management.APMetricQuery string:"00:0C:43:28:80:B3" array:string:"00:0c:43:87:82:6A"

输入参数说明如下：

alMac: 指定Agent的AL Mac地址，string类型，取值为字符串类型的MAC地址，命令行传参，例如：string:"00:0c:43:28:80:15"

BSSIDList: BSSID列表，array:string类型，即字符串数组类型，命令行传参，例如：array:string:"00:0c:43:87:82:6A"，不能为空

* **SetMetricReportingPolicy**(IN BYTE ReportingRCPIThreshold, IN BYTE ReportingRCPIHysteresis, IN BYTE ChannelUtilizationThreshold, OUT UINT32 result, OUT STRING errdesc);

DBus命令示例：

dbus-send --system --print-reply --dest=com.upointech.easymesh1 /com/ctc/map1/Management com.ctc.map1.Management.SetMetricReportingPolicy byte:120 byte:5 byte:76

输入参数说明如下：

ReportingRCPIThreshold: RCPI上报阈值，取值范围为1 ~ 220，byte类型，命令行传参，例如：byte:120

ReportingRCPIHysteresis: RCPI上报阈值余量，即ReportingRCPIThreshold可以上下波动的范围，范围1~220， 0表示使用Agent默认余量值，此值>0表示使用该值作为RCPI阈值余量，byte类型，命令行传参，例如：byte:5

ChannelUtilizationThreshold: 信道使用率上报阈值，取值0 ~ 255，0表示Metrics不根据信道利用率上报，byte类型，命令行传参，例如：byte:80

**信号**

* StationOnOffSignal(BYTE onOff, STRING(16) staMac, STRING(16) BSSID)

终端上下线信号通知.

参数:

onOff，0表示下线，1表示上线

staMac，终端MAC

BSSID，终端所属AP MAC

* SteeringDoneSignal()

client steering完成通知.

参数: 无

* easymeshOnOffSignal(BYTE onOff)

Easymesh controller enable/disable（使能/禁用）通知信号

参数:

onOff，0表示disable，1表示enable

* + 1. com.ctc.map1.APNeighbors

**属性**

|  |  |  |  |
| --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 |
| mac | STRING(16) | read | 邻居设备MAC，邻居设备为MAP设备，格式001122AABBCC |
| connectType | BYTE | read | Backhaul连接类型，0表示有线，1表示无线，2表示其它 |
| owner | STRING(16) | read | 邻居设备Backhaul Link AP MAC |

* + 1. com.ctc.map1.Stations

**属性**

|  |  |  |  |
| --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 |
| mac | STRING(16) | read | 下挂终端设备MAC |
| bssid | STRING(16) | read | 下挂终端设备其AP BSSID，即AP MAC，仅连接类型为1有值 |
| ssid | STRING(32) | read | 所挂AP的SSID，仅连接类型为1有值 |
| connectType | BYTE | read | 终端连接类型，0表示有线，1表示无线，2表示其它 |
| owner | STRING(16) | read | 下挂设备所在ssid MAC |

* + 1. com.ctc.map1.ApCapability

**属性**

|  |  |  |  |
| --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 |
| radioUID | STRING(16) | read | BSSID of Agent’s Radio |
| maxBSS | BYTE | read | 该Radio最多支持BSS个数 |
| operatingClassesNum | UINT16 | read | 该Radio支持的Operating Classes个数 |
| operatingClasses | Array (BYTE) | read | 每个Operating Class对应具体值，数组 |
| mode | BYTE | read | 0表示未知，1表示HT(High Throughput)，2表示VHT(Very High Throughput)，3表示HE(High Effiency) |
| shortGI20 | BYTE | read | 如果是HT，是否支持short GI 20MHz |
| shortGI40 | BYTE | read | 如果是HT，是否支持short GI 40MHz |
| shortGI80 | BYTE | read | 如果是VHT，是否支持short GI 80MHz |
| shortGI160 | BYTE | read | 如果是VHT，是否支持short GI 160MHz和80+80MHz |

* + 1. com.ctc.map1.BackhaulLinkMetric

**属性**

|  |  |  |  |
| --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 |
| packetErrorsTx | INT32 | read | 测量期间当前link发送端丢包个数预估值 |
| packetErrorsRx | INT32 | read | 测量期间当前link接收端丢包个数预估值 |
| transmittedPackets | INT32 | read | 同一测量期间当前link发送的包个数的预估值，用于预估packetErrors |
| macThroughputCapacity | INT16 | read | 发送端最大MAC吞吐率，以Mb/s表示 |
| linkAvailability | INT16 | read | 当前link可用于数据传输的时间平均百分比预估值 |
| phyRate | INT16 | read | 当前link发送端物理传输速率预估值，以Mb/s表示  当当前接口的媒体类型为1905 Table 6-12中的0, 2, 3时，该值时物理传输速率，其他情况下，设置为0xFFFF |
| packetsReceived | INT32 | read | 在同一测量期间，接口接收到的包个数，用于计算packetErrors |
| rssi | BYTE | read | 当媒体类型为IEEE802.11时，该值是接收方接收信号强度标识，以dB表示，其他媒体类型该值设置为0xFF |

* + 1. com.ctc.map1.ApLinkMetric

**属性**

|  |  |  |  |
| --- | --- | --- | --- |
| 属性名 | 类型 | 权限 | 备注 |
| bssid | STRING(16) | read | 被测量的BSSID |
| channelUtilization | BYTE | read | 信道使用率 |
| totalSTANumber | UINT16 | read | 关联到当前BSS的所有STA个数 |
| accessCategory | BYTE | read | 访问类别，bit7表示AC=BE,该bit为必须置1；bit6表示AC=BK；bit5表示AC=VO；bit4表示AC=VI；bit3~0保留 |
| EstimatedServiceParameters | ARRAY<BYTE>(12) | read | 依据上面的accessCategory决定是否存在对应的Estimated Server Parameters，该数组长度为12个BYTE |
| associatedStaTrafficStats | ARRAY(STRING,ARRAY(STRING,VARIANT)) | read | 当前AP下关联的STA流量统计结果 |
| associatedStaLinkMetrics | ARRAY(STRING,ARRAY(ARRAY(STRING,VARIANT))) | read | 当前AP下关联的STA Link测量结果 |

* 1. Controller DBUS对象

|  |  |
| --- | --- |
| Object Path | 接口 |
| /com/ctc/map1/Management | com.ctc.map1.Management |
| /com/ctc/map1/ApNeighbors | com.ctc.igd1.ObjectManager |
| /com/ctc/map1/ApNeighbors/{i} | com.ctc.map1.ApNeighbors |
| /com/ctc/map1/Stations | com.ctc.igd1.ObjectManager |
| /com/ctc/map1/Stations/{i} | com.ctc.map1.Stations |
| /com/ctc/map1/ApCapability | com.ctc.igd1.ObjectManager |
| /com/ctc/map1/ApCapability/{i} | com.ctc.map1.ApCapability |
| /com/ctc/map1/BackhaulLinkMetric | com.ctc.igd1.ObjectManager |
| /com/ctc/map1/BackhaulLinkMetric/{i} | com.ctc.map1.BackhaulLinkMetric |
| /com/ctc/map1/ApLinkMetric | com.ctc.igd1.ObjectManager |
| /com/ctc/map1/ApLinkMetric/{i} | com.ctc.map1.ApLinkMetric |

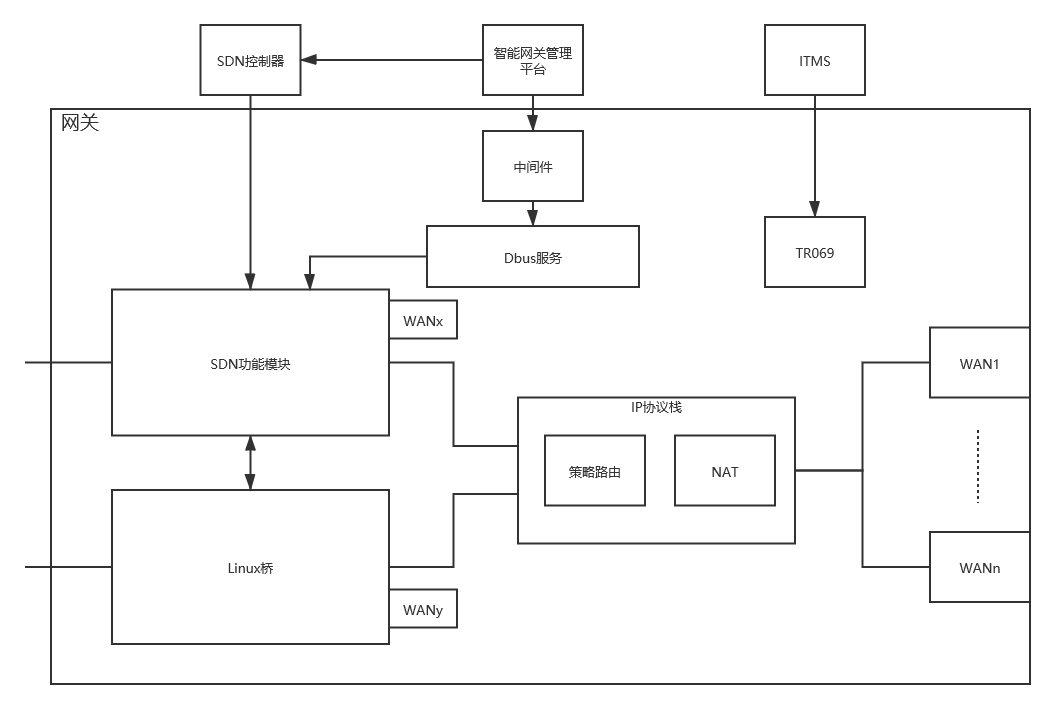
1. (规范性附录)SDN特性技术要求
   1. 总体架构

天翼网关添加SDN特性，结合SDN控制器为电信光宽带用户提供SDN化控制的业务。要实现网关对接SDN控制器，需要网关支持：

* 向SDN控制器建立OpenFlow连接以及进行OpenFlow交互的能力。
* 支持连接智能网关管理平台以及根据智能网关管理平台的控制来开启、关闭和配置SDN特性的能力。

从而实现业务的SDN化控制。

方案的建议整体架构图如下



天翼网关同时具备Linux网桥和SDN网桥（SDN功能模块），这两种网桥可以使天翼网关工作在不同模式下（即：纯Linux网桥模式和Linux+SDN的双网桥模式），模式之间可以根据管理Dbus接口下发的配置进行切换。在双网桥模式下，SDN网桥和Linux网桥间会建立回传链路。当业务流在SDN网桥中没有匹配到回传Linux网桥之外的转发流表项时，天翼网关应支持将该业务流通过SDN网桥和Linux网桥间的回传链路，转发至Linux网桥进行处理。

SDN网桥和Linux网桥作用类似，仅做桥方式的转发。SDN网桥的特殊之处是根据SDN功能模块中保存的OpenFlow流表进行转发。

网关的LAN、WAN接口按照L.7.3节的Dbus接口配置来挂载或移出SDN网桥。挂载到SDN网桥的WAN连接如果是路由WAN连接，SDN网桥上会为每个挂载在SDN网桥上的WAN连接建立一个对应的桥接口，即一个SDN网桥侧的路由WAN连接需要对应一个SDN网桥上的桥接口。挂载到SDN网桥的WAN连接如果是桥接WAN连接，该WAN连接的网络接口会直接添加到SDN网桥中。WAN连接如果挂载到SDN网桥，Linux网桥侧的流不可再从此WAN连接通过。

在没有控制器下发流表对网关ip和mac地址获取报文做特殊控制的情况下，挂载到SDN网桥的LAN接口的下挂终端获取的网关地址和Linux网桥下LAN接口的下挂终端相同。

* 1. 数据转发功能要求
     1. 路由业务

对于LAN侧，SDN网桥的LAN口上行报文，如果匹配到转发至SDN网桥上某个WAN口的流表，则由SDN网桥将报文转发往相应WAN口，否则SDN网桥将报文通过回传链路转发至Linux网桥，由Linux网桥转发往应去的WAN口；Linux网桥的LAN口上行报文，仅可转发往未挂载到SDN网桥的WAN口。

对于WAN侧，SDN网桥上WAN口的下行报文，如果是到SDN网桥的LAN口下挂终端，则由SDN网桥转发；Linux网桥上WAN口的下行报文，如果是到Linux网桥的LAN口下挂终端，则由Linux网桥转发，否则Linux网桥将报文通过回传链路转发至SDN网桥，由SDN网桥转发至应去的LAN口。由于Linux网桥的LAN口上行报文，仅可转发往未挂载到SDN网桥的WAN口，因此不存在SDN网桥上WAN口的下行报文到Linux网桥的LAN口下挂终端的情况。

* + 1. 桥接业务

对于LAN侧，SDN网桥的LAN口上行报文，如果匹配到转发至SDN网桥上某个WAN口的流表，则由SDN网桥将报文转发至相应WAN口，否则SDN网桥将报文通过回传链路转发至Linux网桥，由Linux网桥转发至应去的WAN口；Linux网桥的LAN口上行报文，仅可转发至未挂载到SDN网桥的WAN口。

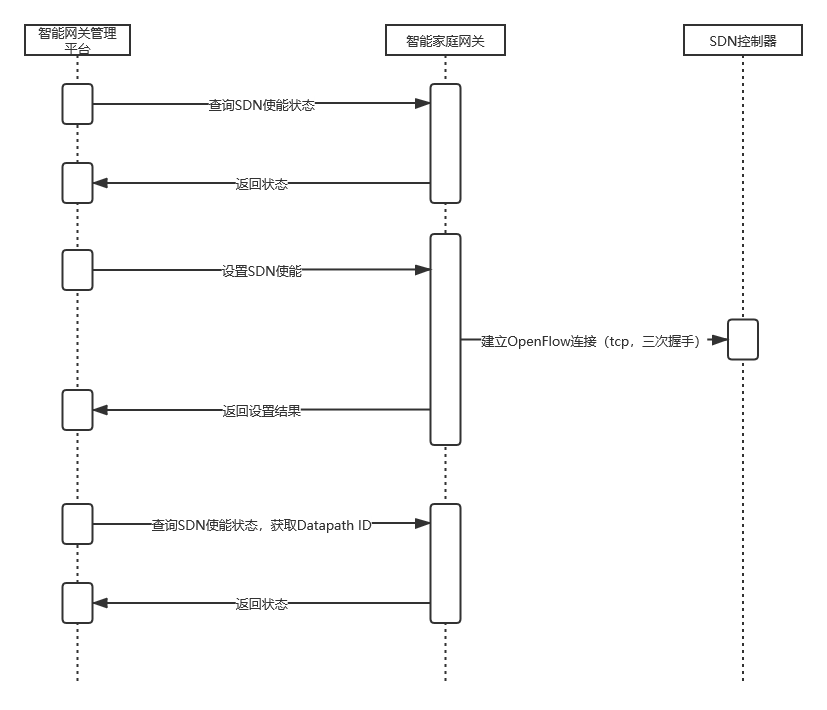
对于WAN侧，SDN网桥仅可在挂载到它的WAN口上收发，Linux网桥仅可在挂载到它的WAN口上收发。SDN网桥上WAN口的下行报文，如果是到SDN网桥的LAN口下挂终端，则由SDN网桥转发。Linux网桥上WAN口的下行报文，如果是到Linux网桥的LAN口下挂终端，则由Linux网桥转发，否则通过回传链路发送到SDN网桥，由SDN网桥转发。由于Linux网桥的LAN口上行报文，仅可转发至未挂载到SDN网桥的WAN口，因此不存在SDN网桥上WAN口的下行报文到Linux网桥的LAN口下挂终端的情况。

* 1. 网关与控制器的连接

网关由SDN功能模块来建立网关到SDN控制器的OpenFlow1.3连接。连接基于TCP协议，网关连接SDN控制器的目的端口为6633或6653，OpenFlow版本为OpenFlow1.3。

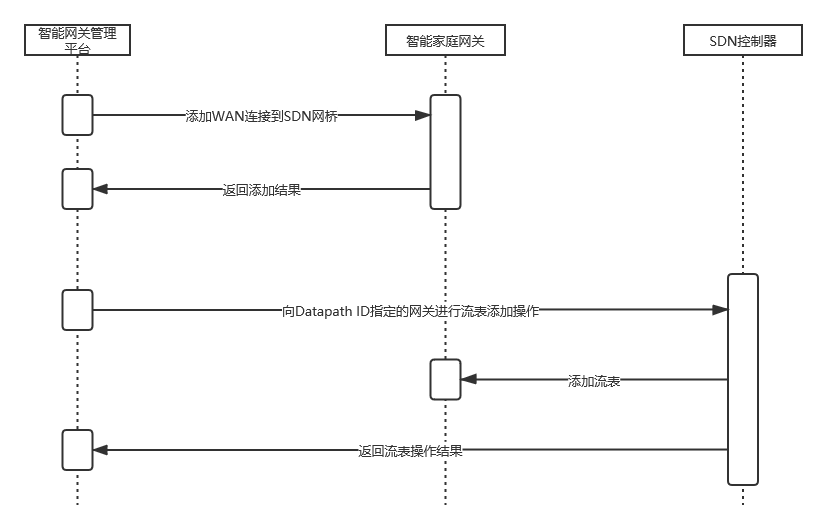
* 1. SDN特性使能及获取网关在SDN控制器上的标识

使能网关SDN特性并获取网关在SDN控制器上标识的流程如下

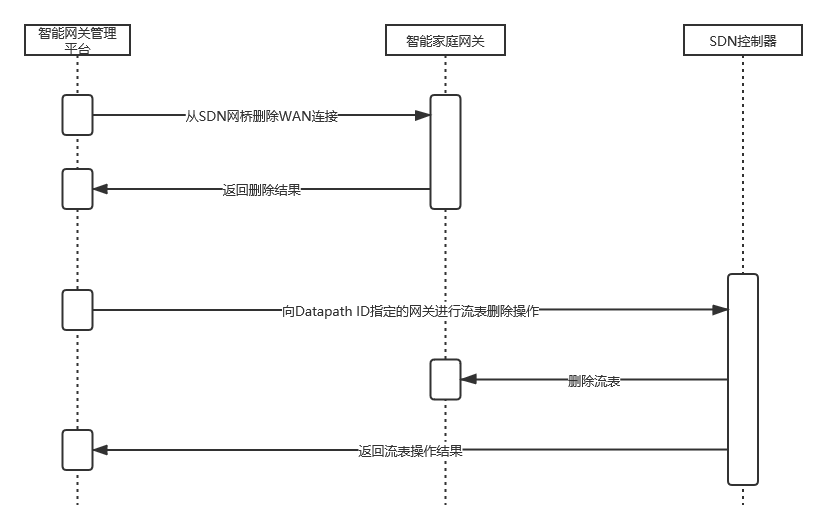


1. 智能网关管理平台向智能家庭网关查询SDN特性是否使能。
2. 智能家庭网关返回使能状态。如果已使能，会在返回信息里包含网关的Datapath ID，且本流程下述步骤可省略。
3. 如果未使能，智能网关管理平台向智能家庭网关下发设置使能SDN特性。
4. 智能家庭网关启动SDN网桥并建立到SDN控制器的OpenFlow连接。
5. 智能家庭网关返回SDN特性使能结果给智能网关管理平台。
6. 智能网关管理平台向智能家庭网关查询SDN特性使能状态，以获取Datapath ID来控制流表下发等操作。
7. 智能家庭网关返回使能状态。如果已使能，会在返回信息里包含网关的Datapath ID。
   1. 业务流表管理

业务流表的下发和删除跟随WAN连接在SDN网桥上的添加和删除进行。流程如下



1. 智能网关管理平台添加WAN连接到智能家庭网关的SDN网桥。
2. 智能家庭网关返回添加WAN连接到SDN网桥的结果。
3. 智能网关管理平台通过Datapath ID来指定网关，操作SDN控制器向该指定网关添加流表。
4. SDN控制器向Datapath ID指定的网关添加流表。
5. SDN控制器向智能网关管理平台返回流表添加结果。



1. 智能网关管理平台从智能家庭网关的SDN网桥删除WAN连接。
2. 智能家庭网关返回从SDN网桥删除WAN连接的结果。
3. 智能网关管理平台通过Datapath ID来指定网关，操作SDN控制器从该指定网关删除流表。
4. SDN控制器从Datapath ID指定的网关删除流表。
5. SDN控制器向智能网关管理平台返回流表删除结果。
   1. 策略路由

SDN网桥上会为每个挂载在SDN网桥上的WAN连接建立一个对应的桥接口，即一个SDN网桥侧的WAN连接需要对应一个SDN网桥上的桥接口。对于所有没挂载在SDN网桥上的WAN连接，对应SDN网桥上的回传链路接口。

对于SDN网桥的上行报文，SDN网桥会根据OpenFlow流表将要去往某个WAN连接的上行报文发送到对应的桥接口。如果该桥接口对应的WAN连接在SDN网桥侧，策略路由需要将该桥接口来的上行报文送到其对应的WAN接口。如果该桥接口对应的WAN连接不在SDN网桥侧，报文会通过回传链路被发送到Linux网桥，然后智能家庭网关将按照本文档“6.1 网络协议及数据转发功能要求”对报文进行转发。

对于Linux网桥的上行报文，仍按照本文档“6.1 网络协议及数据转发功能要求”进行转发。

对于SDN网桥侧WAN接口来的下行报文，经过DNAT后如果其目的是到SDN网桥上LAN口的下挂终端，则策略路由需要将该下行报文送到SDN网桥上此WAN接口对应的网桥接口。SDN网桥会根据OpenFlow流表将该报文发送到目的终端所在的LAN口。

* 1. Dbus接口
     1. com.ctc.igd1.sdnfunc1.ONUInfo

本接口用来获取配置当前网关的SDN功能是否开启，获取网关Datapath ID等信息。

当接收到关闭SDN功能命令（EnableSDN=0）时，应清空以前所有的SDN相关配置，比如端口挂载记录。

* + - 1. DBus对象和方法

|  |  |  |
| --- | --- | --- |
| Object Path | 方法名 | 备注 |
| /com/ctc/igd1/Network/sdnfunc1/ONUInfo | com.ctc.igd1.sdnfunc1.ONUInfo.GetONUInfo | 获取onu信息，包括SDN使能状态、Datapath ID、连接SDN控制器的wan连接、SDN控制器的IP地址 |
| /com/ctc/igd1/Network/sdnfunc1/ONUInfo | com.ctc.igd1.sdnfunc1.ONUInfo.SetONUInfo | 设置SDN使能状态、连接SDN控制器的wan连接，SDN控制器模式 |

EnableSDN取值0/1/-1，-1表示忽略此参数，0关闭，1开启。

Ofpusewan取值为internet/tr069/"空值",空值表示清空此参数，使网关断开与控制器的连接。

* GetONUInfo(OUT INT32 EnableSDN,OUT STRING(63) DatapathID,OUT STRING(63) Ofpusewan,OUT STRING(63) ControlAddr,OUT INT32 result,OUT STRING(63) errdesc)

获取ONU的SDN控制器连接相关信息。

EnableSDN：-1（表示忽略此参数）/0（关闭）/1（开启）。

DatapathID：智能家庭网关中SDN网桥的Datapath ID。

Ofpusewan：internet（INTERNET上网WAN）/tr069（tr069管理WAN）/"空值"（ONU不与控制器连接）。

ControlAddr：控制器的IP地址。

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* SetONUInfo(IN INT32 EnableSDN, IN STRING(63) Ofpusewan,IN STRING(63) ControlAddr, OUT INT32 result,OUT STRING(63) errdesc)

设置ONU的SDN功能模块的启停、SDN控制器连接相关信息。

EnableSDN：-1（表示忽略此参数）/0（关闭）/1（开启）。开启时，启动SDN功能模块，建立OVS桥到Linux桥的回传链路，导入默认回传流表。关闭时，停止SDN功能模块，删除OVS桥到Linux桥的回传链路。启动并建立OVS桥时，需指定OVS桥的datapath ID为com.ctc.igd1.DeviceInfo返回的MAC，从而每个设备的datapath ID为固定值，以便OVS桥重启时SDN控制器能自动下发之前配置的流表。datapath ID要求长度为16个字符，不足时请在前部补零。

Ofpusewan：internet（INTERNET上网WAN）/tr069（tr069管理WAN）/"空值"（ONU不与控制器连接）。

ControlAddr：控制器的IP地址。

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + 1. com.ctc.igd1.sdnfunc1.SDNInfo

本接口用来获取网关SDN功能信息。其中输出信息中的portlist格式为a{su},s代表ifname，u代表portid。

* + - 1. DBus对象和方法

|  |  |  |
| --- | --- | --- |
| Object Path | 方法名 | 备注 |
| /com/ctc/igd1/Network/sdnfunc1/SDNInfo | com.ctc.igd1.sdnfunc1.SDNInfo.GetSDNInfo | 获取SDN信息 |

* GetSDNInfo(OUT ARRAY<DICT<STRING(63), UINT32>> portlist, OUT INT32 result,OUT STRING(63) errdesc)

Portlist：ifname – STRING,portid – UINT32

获取OVS桥上的端口信息。所有设备上存在且挂载了的port，无论物理接口状态是up还是down。

Portlist:端口信息数组。每个端口信息包含两个元素，ifname（端口名称）和portid（端口ID）。WAN接口的ifname为com.ctc.igd1.WANConnectionInfo中的WANName，或com.ctc.igd1.VPNConnection中的tunnel\_name。LAN口的ifname为LAN1~LAN4，分别对应InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.1~InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.4。2.4GHz频段WLAN口的ifname为2.4G-1~2.4G-8，分别对应com.ctc.igd1.WLANConfiguration的SSIDAlias的2.4G-1~2.4G-8。5GHz频段WLAN口的ifname为5G-1~5G-8，分别对应com.ctc.igd1.WLANConfiguration的SSIDAlias的5G-1~5G-8。 portid定义如下，WAN连接和VPN隧道的portid由网关根据查询到的顺序依次分配。

LAN1~4：1~4

2.4G-1~2.4G-8：5~12

5G-1~5G-8：13~20

WAN1~8：21~28（由于可以建多个WAN，因此需要智能网关管理平台在通知SDN控制器下流表时告知控制器相关的WAN是什么业务，告知控制器时WAN也须按这里的WAN编号表示）

VPN隧道1~8：29~36（需要智能网关管理平台在通知SDN控制器下流表时告知控制器对应VPN的加速域名或IP或MAC是什么，告知控制器时VPN也须按这里的VPN编号表示）

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + 1. com.ctc.igd1.sdnfunc1.Ports

获取网关上所有可以挂载到SDN桥上的端口列表，包含端口名称和端口ID。

* + - 1. DBus对象和方法

Object Path：/com/ctc/igd1/Network/sdnfunc1/Ports

其中GetPortList方法的输出信息中的portlist格式为a{su},s代表ifname，u代表portid。

|  |  |  |
| --- | --- | --- |
| Object Path | 方法名 | 备注 |
| /com/ctc/igd1/Network/sdnfunc1/Ports | com.ctc.igd1.sdnfunc1.Ports.GetPortList | 获取设备上可新添加到SDN桥上的网络接口信息（不含已添加的） |
| /com/ctc/igd1/Network/sdnfunc1/Ports | com.ctc.igd1.sdnfunc1.Ports.AddPorttoSDN | 启用指定端口的SDN特性 |
| /com/ctc/igd1/Network/sdnfunc1/Ports | com.ctc.igd1.sdnfunc1.Ports.RemovePortFromSDN | 禁用指定端口的SDN特性 |

当AddPorttoSDN方法中的参数ifname=all时，应将所有ofp端口启用SDN特性，同时保留启用单独某个端口的SDN特性的能力。

当RemovePortFromSDN方法中的参数ifname=all时，应禁用所有ofp端口的SDN特性，同时保留禁用单独某个端口的SDN特性的能力。

* GetPortList(OUT ARRAY<DICT<STRING(63), UINT32>> portlist, OUT INT32 result,OUT STRING(63) errdesc)

Portlist：ifname – STRING,portid – UINT32

获取设备上可新添加到SDN桥上的网络接口信息（不含已添加过的）。对于LAN侧，如WiFi接口，若SSID未使能对应的WiFi接口未up，则不可用于转发，认为不可添加。对于WAN侧，已配置的WAN均应可添加。

Portlist:端口信息数组，定义同GetSDNInfo方法的portlist。

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* AddPorttoSDN(IN ARRAY<DICT<STRING(63), UINT32>> portlist, OUT INT32 result,OUT STRING(63) errdesc)

Portlist：ifname – STRING,portid – UINT32

启用指定端口的SDN特性。

Portlist:端口信息数组，定义同GetSDNInfo方法的portlist。

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* RemovePortFromSDN(IN ARRAY<DICT<STRING(63), UINT32>> portlist, OUT INT32 result,OUT STRING(63) errdesc)

Portlist：ifname – STRING,portid – UINT32

禁用指定端口的SDN特性。

Portlist:端口信息数组，定义同GetSDNInfo方法的portlist。

result：0（成功）/1（失败）/L.7.4中定义的错误码。

errdesc：若为NULL或者函数成功，则不用管；若传入的值不为NULL，则在方法失败的时候填充上失败原因。

* + - 1. 信号
* PortStatusChanged(STRING(63) ifname, UINT32 portid, STRING(63) status)，WAN连接状态变更信号

当网关上任意WAN连接（包含VPN）状态发生改变时应发出信号报告连接状态变化。

参数：ifname，类型为STRING(s)，表示连接名称。ifname为com.ctc.igd1.WANConnectionInfo中的WANName，或com.ctc.igd1.VPNConnection中的tunnel\_name。

Portid，类型为UINT32(u)，表示连接的SDN端口编号。和com.ctc.igd1.sdnfunc1.Ports.GetPortList中的portid相同。

Status，类型为STRING(s)，表示连接状态。取值：down/up/del。del表示VPN故障断开，此时三次重拨均失败后将VPN业务从SDN去使能，去使能会删除相关流表和VPN配置信息，不再重试。

* + 1. 错误码信息及注意事项
       1. 错误码信息

如下表格为所有方法或接口中result和errdesc提供参考，当调用接口或方法错误时，请根据如下信息返回相关错误码及错误描述。

对于1（未知错误），errdesc可以自定义。

为便于未来问题定位查找，厂商可增加错误码来细化自己的错误信息，所增加的错误码请从-1000开始。

|  |  |  |
| --- | --- | --- |
| 0 | SUCCESS | 正确 |
| 1 | ERR\_UNKOWN | 未知错误 |
| -2 | ERR\_INPUT\_ARGS | 输入参数错误 |
| -101 | ERR\_SDN\_FUNC\_CLOSED | SDN功能已关闭 |
| -201 | ERR\_NO\_SDNFUNC | 没有发现SDN功能 |
| -301 | ERR\_NO\_THIS\_PORT | 没有发现此端口 |
| -302 | ERR\_EXIST\_PORT | 此端口已存在 |
|  |  |  |

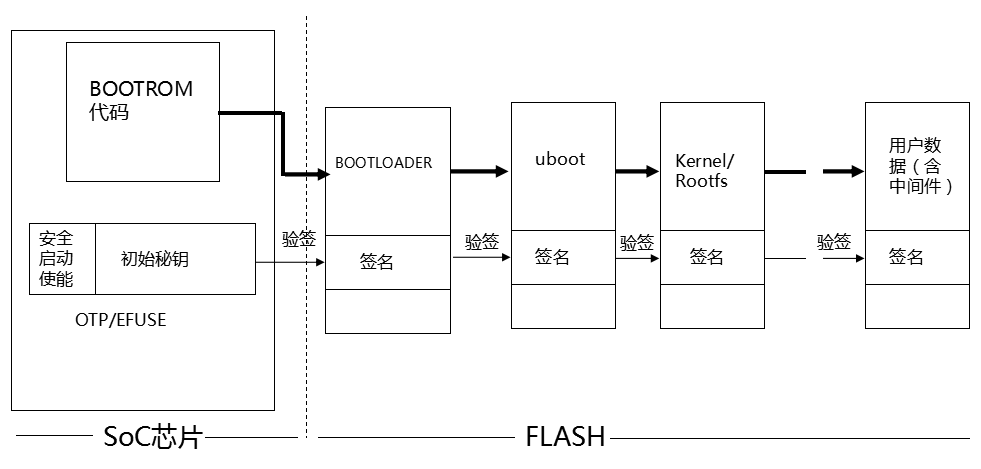
1. （资料性附录）  
   安全启动参考方案
   1. 需求背景

家庭网关中的固件存在着被非授权访问篡改和替换的风险，损害运营商和设备商的利益，要求只有经过认证的、可信任的软件才可以在家庭网关中运行。

* 1. 方案说明

安全启动是在网关的固件系统中，自下而上建立起信任链，这个信任链的最底层是SoC芯片内部的BOOTROM及OTP/EFUSE，后续依次为FLASH中的BOOTLOADER、uboot、系统软件、最后是用户数据。信任链中的每一个环节都对下一个环节进行验证和确认，从而保证整个系统是可靠的。

信任链开始于BOOTROM和OTP/EFUSE，在OTP/EFUSE中一次性写入“安全启动使能”标志及用于后续校验的初始秘钥（例如初始BOOT的签名公钥或HASH值）；芯片上电以后，BOOTROM代码读取“安全启动使能”标志的状态及初始秘钥，利用此初始秘钥校验FLASH中BOOTLOADER代码的可靠性和完整性，如果校验通过，则BOOTLOADER正常启动；BOOTLOADER再校验下一级代码的可靠性和完整性，依次类推，在启动的过程中，每一个环节都对下一个环节进行校验，确保信任链的完整性。



注：芯片中OTP/EFUSE区域，由设备厂商在生产时一次性烧录，后续无法再被更改，这是信任链的源头。

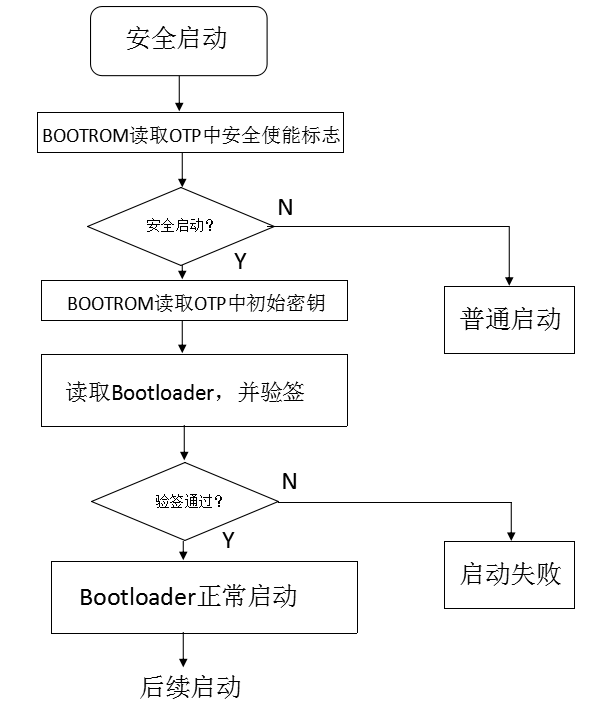
* + 1. 校验算法

采用标准的签名算法，如RSA、ECDSA或HASH等，可以根据需要使用多组签名私钥/公钥，私钥用于固件版本的签名，要妥善保管，公钥可以公开，用于对固件版本签名的验签，这些签名秘钥可以属于芯片厂商、运营商和设备商，用于不同启动阶段的的固件版本校验，形成层次化的秘钥体系。宜支持加密。

天翼网关的签名秘钥全部由设备厂商提供。

* + 1. 安全启动流程

安全启动的启动流程，如下图所示：



* 1. 操作说明

1）设备商根据需要提供和保管若干签名私钥/公钥；

2）设备商利用Linux版本签名工具及签名私钥，完成对固件版本的签名；

3）设备商提供系统编译阶段打开安全选项的配置，编译出签名的安全版本镜像，把安全选项关闭编译出的是普通的版本镜像；

4）设备商在生产时，一次性将“安全启动使能”标志及初始秘钥烧录到芯片内部的OTP/EFUSE区域，同时禁止通过JTAG接口访问SoC芯片。

* 1. 安全升级

由厂商或运营商使用私钥对升级包进行签名，升级时，升级程序对升级包进行验签，通过后才能升级，否则拒绝升级。

安全升级与安全启动没有必然的关联，仅是一种安全增强措施。