GY

中华人民共和国广播电视和网络视听行业标准

GY/T XXX—XXXX

有线电视单向网关与 4K 超高清晰度插入式微型机顶盒的交互协议规范

Specification of interaction protocol between the unidirectional gateway of cable television and the 4K ultra high definition pluggable mini set-top box

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家广播电视总局　　发 布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　通则 2
6　功能要求 3
6.1　概述 3
6.2　设备发现 3
6.3　节目搜索 3
6.4　清流节目播放 3
6.5　加扰节目播放 4
6.6　网关设备管理 4
6.7　网关信息查询 4
6.8　事件信息发送 4
6.9　安全功能 4
7　接口要求 4
7.1　通则 4
7.2　设备发现 5
7.3　资源申请 9
7.4　锁频设置 11
7.5　PID 过滤设置 12
7.6　信号质量查询 13
7.7　卡状态查询 14
7.8　卡复位 14
7.9　机卡通信 15
7.10　故障信息查询 15
7.11　设备管理 16
7.12　网关信息查询 19
7.13　通信密钥协商 20
7.14　设备身份认证 21
7.15　消息报文 22
7.16　基于以太网口的数据传输格式 24
7.17　基于 USB 口的数据传输格式 24
8　流程要求 25
8.1　设备发现 25
8.2　节目搜索 29
8.3　清流节目播放 30
8.4　加扰节目播放 31
8.5　网关升级 32

附录A（资料性） 条件接收 36
A.1 有卡CA 36
A.2 无卡CA 38
附录B（规范性） 安全机制 39
B.1 概述 39
B.2 设备认证 39
B.3 安全通信模式 40
B.4 TS再加密 42
参考文献 44

前　言

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

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国广播电影电视标准化技术委员会（SAC/TC 239）归口。

本文件起草单位：国家广播电视总局广播电视科学研究院、中国广电网络股份有限公司、江苏省广电有线信息网络股份有限公司、东方有线网络有限公司、北京歌华有线电视网络股份有限公司、深圳市茁壮网络股份有限公司、国微集团（深圳）有限公司、苏州龙擎视芯集成电路有限公司、北京数码视讯科技股份有限公司、北京永新视博数字技术有限公司、北京数字太和科技有限责任公司。

本文件主要起草人：赵翠、刘建国、解伟、万涛、王野秋、安亚超、姚辉军、王明敏、董原、朱里越、陈宝霞、朱允斌、张辰、徐佳宏、刘若鋆、彭美意、谢天、梁涛、祁娟、刘荣军、吴英栋、廖凌、田江明、田雪冰、李金库、郑力铮、廖凌。

有线电视单向网关与4K超高清晰度插入式微型机顶盒的交互协议规范

1 范围

本文件规定了有线电视单向网关与4K超高清晰度插入式微型机顶盒应用软件之间的交互协议。

本文件适用于有线电视单向网关及其连接的客户端的应用软件的开发、联调与测试。

2 规范性引用文件

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

GY/Z 175—2001 数字电视广播条件接收系统规范

GY/T XXX—XXXX 4K超高清晰度插入式微型机顶盒技术要求和测量方法

GY/T XXX—XXXX 有线电视单向网关技术要求和测量方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全通信模式 secure communication mode

在HTTP基础上通过传输加密和身份认证过程实现对有线电视单向网关部分接口进行安全访问的通信机制。

3.2

SM3算法 SM3 algorithm

一种密码杂凑算法，其输出为256bit。

3.3

SM4算法 SM4 algorithm

一种分组密码算法，分组长度为128bit，密钥长度为128bit。

3.4

AES128算法 AES128 algorithm

一种分组密码算法，分组长度为128bit，密钥长度为128bit。

3.5

BASE64编码 BASE64 encoding

一种将二进制数据转换为ASCII字符的编码方法。

3.6

消息摘要 message digest

一种通过对消息进行哈希运算而生成的固定长度的数据摘要。

3.7

ECDH密钥交换算法 ECDH key exchange algorithm

一种基于椭圆曲线的密钥交换协议。

4 缩略语

AES 高级加密标准（Advanced Encryption Standard）
APDU 应用协议数据单元（Application Protocol Data Unit）
APP 应用程序（Application）
ATR 复位应答（Answer To Reset）
CA 条件接收（Conditional Access）
CBC 密码分组链接（Cipher Block Chaining）
CW 控制字（Control Word）
DCAS 可下载条件接收系统（Downloadable Conditional Access System）
DHCP 动态主机配置协议（Dynamic Host Configuration Protocol）
ECDH 椭圆曲线笛福-赫尔曼（Elliptic Curve Diffie-Hellman）
ECM 授权控制信息（Entitlement Control Message）
EMM 授权管理信息（Entitlement Management Message）
HFC 光纤-同轴电缆混合网（Hybrid Fiber Coaxial）
HKDF 基于HMAC的提取和扩展密钥派生函数（HMAC-based Extract-and-Expand Key Derivation Function）
HTTP 超文本传输协议（Hyper Text Transfer Protocol）
ID 标识符（Identifier）
IP 互联网协议（Internet Protocol）
MAC 媒体访问控制（Media Access Control）
MD5 消息摘要5（Message Digest 5）
MEF 最大以太网帧个数（Maximum Ethernet Frames）
MTU 最大传输单元（Maximum Transmission Unit）
PID 包识别码（Packet Identifier）
PSI 节目特定信息（Program Specific Information）
QAM 正交幅度调制（Quadrature Amplitude Modulation）
RMACT 随机数-MAC地址-口令（Random-MAC-Token）
SECP 椭圆曲线密码学（Standards for Efficient Cryptography）
SHA 安全散列算法（Secure Hash Algorithm）
SI 业务信息（Service Information）
SSDP 简单服务发现协议（Simple Service Discovery Protocol）
TCP 传输控制协议（Transmission Control Protocol）
TS 传送流(Transport Stream)
UDP 用户数据报协议（User Datagram Protocol）
UPnP 通用即插即用（Universal Plug and Play）
URL 统一资源定位符（Uniform Resource Locator）
USB 通用串行总线（Universal Serial Bus）
UTC 协调世界时（Coordinated Universal Time）
UUID 通用唯一识别码（Universally Unique Identifier）
WAN 广域网（Wide Area Network）

5 通则

在采用HFC网络以数字电视广播方式传输直播业务的有线电视网络中，插入式微型机顶盒（以下简称“机顶盒”）和有线电视单向网关（以下简称“网关”）配合使用，可以替代传统机顶盒，接收以广播方式传输的有线电视直播节目。机顶盒应符合GY/T XXX—XXXX《4K超高清晰度插入式微型机顶盒技术要求和测量方法》的规定，网关应符合GY/T XXX—XXXX《有线电视单向网关技术要求和测量方法》的规定。

网关接收以数字电视广播方式传输的有线电视节目，将这些节目以IP方式传送给机顶盒。机顶盒接收来自网关以IP方式传输的节目内容，进行解码播放。

在功能上，网关实现对广播信号的接收、解调、解复用和解扰（可选）功能，机顶盒实现有线电视PSI/SI的解析及频道节目信息的显示与处理，并实现节目信号的解码与显示等功能。机顶盒与网关配合实现CA。

本文件规定机顶盒等终端设备的应用软件与网关之间的交互协议，分为协议交互和数据传输两部分，见图1。协议交互主要通过网关提供的服务接口以及网关和机顶盒之间的消息报文来实现。数据传输指网关根据机顶盒的设置将相应的媒体数据传送给机顶盒。通过与网关的协议交互和数据传输，机顶盒从网关中获取到所需的节目报文，送到电视机上进行显示，满足用户的观看需求。

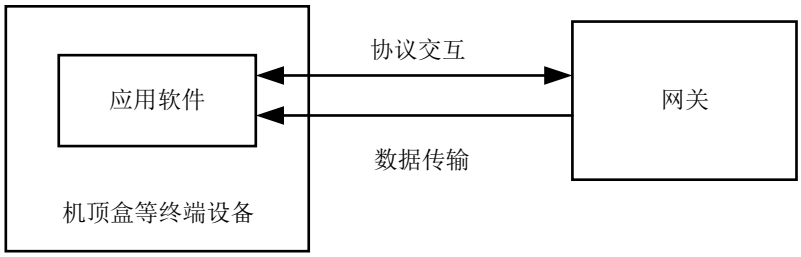


图1　交互协议框架

机顶盒与网关的物理接口包括以太网接口和USB接口两种，应至少支持其中一种。物理接口决定了网关和机顶盒之间的设备发现机制，同时决定了协议和数据报文的传输格式。网关和机顶盒之间的USB口应采用USB2.0协议中规定的High-speed模式或USB2.0以上协议。

6　功能要求

6.1　概述

机顶盒与网关之间通过协议交互，实现的功能主要包括设备发现、节目搜索、清流节目播放、加扰节目播放、网关设备管理、网关信息查询、事件信息发送和安全机制八类。

6.2　设备发现

设备发现指在同一局域网内机顶盒与网关之间建立连接的过程。机顶盒和网关都应支持设备发现功能。设备发现协议取决于两者之间的物理接口。

对于以太网口的设备发现，应利用SSDP协议实现。机顶盒启动后应以5s为间隔发送搜索请求报文，同时接收存续报文，与网关建立连接后，机顶盒停止发送搜索请求报文并停止接收存续报文；网关启动后应以5s为间隔发送存续报文，并接收搜索请求报文，当与机顶盒建立连接后，网关应继续接收搜索请求报文，并持续以5s为间隔发送存续报文。此外，本文件基于SSDP报文格式扩展定义广播存续报文，网关启动后应以5s为间隔发送广播存续报文，机顶盒接收到广播存续报文应与网关建立连接。

对于USB口的设备发现，应包含基于USB协议枚举机制的设备识别和USB设备通信协商两个步骤。机顶盒检测USB网关设备描述符，识别网关设备后与网关进行设备通信协商，双方获取对方的MAC地址且机顶盒为网关设置IP地址，为后续通信做好准备。

6.3　节目搜索

节目搜索功能指通过频道节目的搜索，获取完整的频道列表数据。节目搜索为可选功能。在进行节目搜索时，机顶盒调用网关提供的服务接口，实现资源申请、频点锁定、PSI/SI表数据过滤的PID设置。网关根据机顶盒设置的PID过滤出PSI/SI表数据并发送给机顶盒，机顶盒接收并解析后生成频道列表数据。机顶盒通过节目搜索获取频道列表数据并进行保存，为后续的直播频道播放做好准备。

6.4　清流节目播放

机顶盒通过与网关交互实现清流频道节目的播放。机顶盒通过读取节目搜索保存的频道列表数据获得相应的频道节目信息，之后调用网关提供的服务接口，实现资源申请、频点的锁频、音视频数据过

滤的PID设置。网关根据机顶盒设置的PID过滤出清流频道节目的音视频TS数据并发送给机顶盒进行播放。

6.5 加扰节目播放

机顶盒通过与网关交互实现加扰频道节目的播放，两者之间的交互流程取决于CA实现方式。

机顶盒和网关可根据业务需要集成CA模块和解扰模块，包括以下组合模式：

——机顶盒解扰：机顶盒集成 CA 模块和解扰模块，实现完整 CA 功能，宜支持无卡 CA；

——网关解扰：网关集成 CA 模块和解扰模块，实现完整 CA 功能，宜支持无卡 CA；

——基于拆分库的网关解扰：机顶盒集成 CA 主模块、网关集成 CA 子模块和解扰模块，具体规定见附录 A；宜支持有卡 CA，符合 GY/Z 175—2001。

6.6 网关设备管理

机顶盒与网关交互实现对网关的管理和控制。网关应对外提供可管理配置的能力，具体功能包括系统重启、恢复出厂设置、网关升级、加载CA程序、启用/停用无卡CA以及与安全通信模式有关的参数设置等。

6.7 网关信息查询

机顶盒与网关交互实现对网关进行信息查询。网关应对外提供信息查询能力，包括网关的IP地址和MAC地址、设备简要信息（如设备ID等）、资源信息（如调谐器数量等）、CA相关信息、故障信息以及安全通信模式相关信息等。机顶盒基于查询到的网关信息，确定对调用网关接口时的请求参数以及是否采用安全通信模式。

6.8 事件信息发送

网关设备对外主动发送消息，用于向机顶盒报告网关的状态信息，包括锁频状态、智能卡状态、故障信息和系统升级等信息。

6.9 安全功能

分为用于控制终端接入的设备认证功能、用于接口访问的安全通信模式和用于视频流数据传输安全的TS再加密功能，均为必选功能。机顶盒为安全功能的发起方。

设备认证功能用来实现机顶盒与网关两端设备的身份互相认证，保证通信两端的身份合法性。

安全通信模式是指，在HTTP基础上通过传输加密和身份认证过程实现对网关部分接口进行安全访问的通信机制。在安全通信模式下，机顶盒应采用HTTP安全通信方式访问资源申请接口、机卡通信接口和设备管理接口。

当网关具备CA解扰能力时，为保证解扰后的TS包在网关和机顶盒之间的传输安全，网关和机顶盒可选支持TS再加密功能，即网关对解扰的TS包进行再加密，机顶盒接收到加密数据后进行解密。若要实现TS再加密，网关和机顶盒应同时支持该功能。TS再加密功能仅作用于TS流中原本加扰并在网关上解扰的视频数据包，并非TS流中的所有数据包。

安全机制应符合附录B的规定。安全通信模式和TS再加密功能均要求网关和机顶盒要先进行密钥协商。在本文件中，密钥协商和设备认证只是功能目标描述不同，实现过程完全一致，都是先利用通信密钥协商进行密钥协商，再利用设备身份认证进行认证，只有认证通过后协商的密钥才有效，双方才可进行后续正常通信。若网关和机顶盒支持任一安全功能，则应在设备发现后立即进行设备认证（亦完成密钥协商）。

7 接口要求

7.1 通则

机顶盒和网关之间定义1类接口协议、12个服务接口和1种消息格式，见表1。其中1类接口协议为设备发现协议，分为基于SSDP协议的设备发现和基于USB接口的设备发现，机顶盒和网关都应支持设备发

现；12个服务接口为网关提供的服务接口，供机顶盒调用；1种消息格式为机顶盒与网关之间约定的消息报文格式，用于网关主动推送消息及机顶盒实现消息接收。

表1　接口和消息定义

序号	名称	接口提供方
1	设备发现	—
2	资源申请接口	有线电视单向网关
3	锁频设置接口	有线电视单向网关
4	PID 过滤设置接口	有线电视单向网关
5	信号质量查询接口	有线电视单向网关
6	卡状态查询接口	有线电视单向网关
7	卡复位接口	有线电视单向网关
8	机卡通信接口	有线电视单向网关
9	故障信息查询接口	有线电视单向网关
10	设备管理接口	有线电视单向网关
11	网关信息查询接口	有线电视单向网关
12	通信密钥协商接口	有线电视单向网关
13	设备身份认证接口	有线电视单向网关
14	消息报文	—

网关的服务接口通过 HTTP 协议进行调用，其中资源申请接口、机卡通信接口和设备管理接口还支持通过 HTTP 安全通信方式进行调用。当开启安全通信模式时，机顶盒应采用 HTTP 安全通信方式对资源申请接口、机卡通信接口和设备管理接口进行调用，报文格式和交互流程应符合 B.2 的规定。

机顶盒调用接口时，若网关发现不支持该接口，网关应返回 HTTP 状态码 404，表示不支持该接口。

7.2　设备发现

7.2.1　基于以太网口

网关和机顶盒之间通过以太网口连接时，双方采用SSDP协议中规定的搜索请求报文和存续报文或基于SSDP协议扩展定义的广播存续报文实现设备的发现。网关和机顶盒应根据所获取的IP地址类型发送对应的设备发现报文。

SSDP组播地址应符合表2的定义。

表2　组播地址定义

序号	组播地址	端口号	描述
1	239.255.255.250	1900	IPv4
2	FF0x::C	1900	IPv6

搜索请求报文格式应符合表3的定义。

表3　搜索请求报文

序号	报文	内容	描述
1	M-SEARCH * HTTP/1.1		搜索请求报文
2	HOST	组播地址和端口号	指定了请求的目标主机和端口，取值固定，见表 2
3	ST	urn:schemas-upnp-org:device:device-Type: version	指定搜索的目标，其中： device-Type 字段的取值默认为 CableGatewayDevice，表明指定搜索的设备类型为网关设备； version 字段的默认取值为 1，表明设备的版本
4	MAN	"ssdp:discover"	搜索请求的标识符
5	MX	N	N 为设备等待响应时长，单位为秒（s）

搜索应答报文格式应符合表4的定义。

表4　搜索应答报文

序号	报文	内容	描述
1	HTTP/1.1 200 OK		请求成功
2	HOST	组播地址和端口号	指定组播地址和端口，取值固定，见表 2
3	Cache-Control	max-age=N	N 为指定通知消息存活时间，单位为秒（s）
4	Location	http://ip:port/get_info	指定网关设备的地址和端口，其中 ip 为网关设备的 IP 地址；port 为网关设备的端口号；get_info 表示可以从该接口获取网关信息
5	NT	upnp:rootdevice	UPnP 标识符，指示设备类型为根设备
6	USN	uuid:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx::upnp:rootdevice	网关设备的唯一标识符，其中 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx 为网关设备的 UUID

存续报文格式应符合表5的定义。

表5　存续报文

序号	报文	内容	描述
1	NOTIFY * HTTP/1.1		设备通知报文
2	HOST	组播地址和端口号	指定组播地址和端口，取值固定，见表 2
3	Cache-Control	max-age=N	N 为指定通知消息存活时间，单位为秒（s）
4	Location	http://ip:port/get_info	指定网关设备的地址和端口，其中 ip 为网关设备的默认 IP 地址；port 为网关设备的端口号；get_info 表示可以从该接口获取网关信息
5	NT	upnp:rootdevice	UPnP 标识符，指示设备类型为根设备
6	NTS	ssdp:alive	网关设备存在信息
7	USN	uuid:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx::upnp:rootdevice	网关设备的唯一标识符，其中 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx 为网关设备的 UUID

广播方式发送存续报文格式应符合表6的定义，该报文仅用于IPv4网络。

表6　广播存续报文

序号	报文	内容	描述
1	NOTIFY * HTTP/1.1		设备通知报文
2	HOST	xxx.xxx.xxx.255:19000	指定设备所在局域网的广播地址和端口，取值固定
3	Location	http://ip:port/get_info	指定网关设备的地址和端口，其中ip为网关设备的默认IP地址；port为网关设备的端口号；get_info表示可以从该接口获取网关信息
4	ST	urn:schemas-upnp-org:device:deviceType:version	指定网关设备的标识，其中： device-Type字段的取值默认为CableGatewayDevice，表明指定搜索的设备类型为网关设备； version字段的默认取值为1，表明设备的版本
5	MX	N	N为设备等待响应时长，单位为秒（s）

下线报文格式应符合表7的定义。

表7　下线报文

序号	报文	内容	描述
1	NOTIFY * HTTP/1.1		设备通知报文
2	HOST	组播地址和端口号	指定组播地址和端口，取值固定，见表2
3	NTS	ssdp:byebye	网关设备下线信息
4	USN	uuid:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx::upnp:rootdevice	网关设备的唯一标识符，其中xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx为网关设备的UUID

7.2.2　基于 USB 口

7.2.2.1　概述

当网关与机顶盒通过USB口连接时，设备发现过程包含两个步骤，首先机顶盒与网关之间应完成USB设备识别，然后机顶盒还应完成与网关设备的通信协商。只有成功完成通信协商，机顶盒和网关之间才可以开始后续业务流程。

7.2.2.2　基于 USB 的设备识别

网关和机顶盒之间通过USB协议的枚举机制完成设备识别过程。机顶盒为主设备，网关为从设备。应采用USB2.0协议第9.6.5规定的接口描述符描述网关设备，接口描述符中部分参数的取值应符合表8的定义，同时该接口的字符串描述符应设为“Cable TV unidirectional gateway interface”。

表8　接口描述符参数取值

字段名称	长度/字节	取值	取值说明
bInterfaceClass	1	0xFFH	根据USB协议，取值为0xFFH，表示本接口为厂商定义
bInterfaceSubClass	1	0xC0	表示为有线电视单向网关
bInterfaceProtocol	1	0x01	

机顶盒应根据接口子类码、协议码和接口字符串三个参数，识别出插入的USB设备为有线电视单向网关设备。若机顶盒不支持字符串描述符，则根据接口子类码和协议码来进行识别。

网关和机顶盒之间的 USB 接口应包含两个端点，用于协议交互和数据传输。应采用 USB2.0 协议第 9.6.6 规定的端点描述符对端点进行描述。两个端点中，一个为批量传输入端点，端点描述符中部分参数的取值应符合表 9 的定义；一个为批量传输出端点，端点描述符中部分参数的取值应符合表 10 的定义。为保证传输效率，端点容量应至少为 512Byte。

表9　入端点的端点描述符参数取值

字段名称	长度/字节	取值	取值说明
bEndpointAddress	1	Bit7 = 1	Bit7：表示端点的数据传输方向，取值0b1代表入端点
bmAttributes	1	Bit1-0 = 10	Bit1-0：表示端点的传输类型，取值0b10代表批量传输

表10　出端点的端点描述符参数取值

字段名称	长度/字节	取值	取值说明
bEndpointAddress	1	Bit7 = 0	Bit7：表示端点的数据传输方向，取值0b0代表出端点
bmAttributes	1	Bit1-0 = 10	Bit1-0：表示端点的传输类型，取值0b10代表批量传输

7.2.2.3　基于 USB 的设备通信协商

在完成 USB 设备识别后，网关和机顶盒应先进行设备通信协商，即网关和机顶盒之间按序进行 MAC 地址查询和 IP 地址设置。协商完成后，双方均应具备有效的 MAC 地址和 IP 地址，并得到对方的 MAC/IP 地址信息。只有完成设备通信协商，才可以开始业务流程。

设备通信协商报文包括 MAC 地址信息查询报文、MAC 地址信息查询回复报文、IP 地址设置报文、IP 地址设置回复报文，报文格式为以太网帧，应分别符合表 11～表 14 的定义。

在设备通信协商时，首先进行 MAC 地址信息查询，机顶盒应向网关发送 MAC 地址信息查询报文，网关接收到报文后应返回 MAC 地址信息查询回复报文，其中应包含网关的实际 MAC 地址和网关支持的业务通信协议；然后机顶盒为网关设置 IP 地址，机顶盒应发送 IP 地址设置报文，为网关设置通信的 IP 地址，网关接收到报文后应发送对应的回复报文，一旦机顶盒接收到回复报文，表明通信协商过程完成。

表11　MAC 地址信息查询报文

字段名称	长度	取值/参数	描述
目的 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
源 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
数据类型	2Byte	EA 86	固定值
数据负载	＜1500Byte	/query_macaddr_info	固定值，查询网关的 MAC 地址信息

表12　MAC 地址信息查询回复报文

字段名称	长度	取值/参数	描述
目的 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
源 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
数据类型	2Byte	EA 86	固定值
数据负载	＜1500Byte	Reply	查询成功与否的标志，取值为： ok：成功； failed：失败
		MAC	网关的 MAC 地址，十六进制表示并用“-”隔开
		Data-Protocol	网关支持的通信协议类型，多个协议项之间用逗号’,’隔开；网关应支持 IPv4、IPv6，可选支持 ARP、802.1Q 等
		IP	网关的 IP 地址，没有时为空白
		Reason	失败原因，只有请求失败时才返回
		MEF	网关支持的一次 USB Bulk Transfer 中可封装的以太网帧最大个数，不设置时默认为 1

表13　IP 地址设置报文

字段名称	长度	取值/参数	描述
目的 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
源 MAC 地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
数据类型	2Byte	EA 86	固定值
数据负载	＜1500Byte	/set_ip?ip=aaa.aaa.aaa.aaa(或 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)&mac=**-**-**-**-**-**&subnet=a&mef=b&vlan=c	参数说明如下： ip：对网关设置的 IP 地址； mac：上述网关的 MAC 地址，十六进制表示并用“-”隔开； subnet：子网掩码的位宽，可选参数。对于 IPv4 地址，该参数不指定时默认为 24(即高 24bit)，对于 IPv6 地址默认为 64； mef[a]：对网关设置一个 USB transfer 中最多可负载的以太网帧数量；

字段名称	长度	取值/参数	描述
			vlan:对所设置的IP地址指定以太网帧的VLAN TAG值，使用802.1Q以太帧格式，为可选参数
[a] 客户端根据自身和网关的支持能力，确定一个USB transfer中最多可负载的以太网帧数量后设置给网关。			

表14　IP地址设置回复报文

字段名称	长度	取值/参数	描述
目的MAC地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
源MAC地址	6Byte	FF:FF:FF:FF:FF:FF	固定值
数据类型	2Byte	EA 86	固定值
数据负载	＜1500Byte	Reply	设置成功与否的标志，取值为： ok：成功； failed：失败
		IP	网关的IP地址
		MAC	网关的MAC地址，十六进制表示并用“-”隔开
		Location	资源快速访问路径，格式为：http://ip:port/get_info,其中ip为网关的IP地址；port为网关设备的端口号；get_info表示可以访问网关信息查询接口
		Reason	失败原因，请求失败的时候才返回

表12和表14中，数据负载的格式定义为Key: value\r\n，其中“:”为英文半角，与value之间应有一个空格，结束行为\r\n。

表12的数据负载示例：

```
Reply: ok\r\nMAC: 74-84-E1-07-7D-D0\r\nData-Protocol: IP,ARP,802.1Q\r\nIP: 10.168.22.1\r\n\r\n
```

7.3　资源申请

机顶盒在使用网关资源之前，应先调用资源申请接口与网关协商资源操作口令并申请所需资源的使用权，并在资源使用过程中，以5s为时间间隔调用此接口对使用权进行续期。网关应根据接口请求参数中的clientuuid为调用该接口的机顶盒分配或保留相应资源，当超过10s未接收到资源续期时，网关应将相应的资源回收，并停止数据的转发。若启用了安全通信模式，则本接口纳入管控。

接口URL：http://ip:port/reserve_resource。

接口协议：HTTP GET。

接口请求参数应符合表15的定义。

表15　资源申请接口请求参数

参数名称	类型	是否必选	描述
clientuuid	字符串	是	客户端APP的UUID，为客户端APP的标识
clientip	字符串	是	客户端设备的IP地址
rtoken	字符串	是	资源操作口令，为随机字符串(a-zA-Z0-9)，长度不小于8Byte
tuner	字符串	否	申请占用/保留的调谐器的数量，取值为： m：代表m个调谐器，m为整数，取值应不超出从网关信息查询接口的调谐器参数获取的可用调谐器的总数； all：代表全部调谐器

参数名称	类型	是否必选	描述
descrambler	字符串	否	申请占用/保留的解扰器数量，取值为： n：代表 n 个解扰器，n 为整数，取值应不超出从网关信息查询接口的 Descrambler 参数获取的可用解扰器的总数； all：代表全部解扰器
smartcard	字符串	否	申请占用/保留智能卡资源，应先从网关信息查询接口的 Smartcard-Status 参数获取智能卡状态 all：代表申请占用/保留智能卡资源
submsg	字符串	否	指定要订阅的消息 default：订阅除故障信息外的消息； all：订阅所有消息； lock：订阅锁频状态消息； card：订阅卡插拔消息； malfunction：订阅故障信息
subport	字符串	是	指定接收订阅消息的 UDP 端口

调用者生成随机数作为令牌，申请占用所有资源，指定消息接收端口以及客户端的IP地址，资源申请接口请求参数示例：

```
http://ip:port/reserve_resource?clientuuid=aff1dc1e7f3c43a0b14bd13f2c5026ac&
rtoken=a3cbda7162&descrambler=all&smartcard=all&tuner=all&submsg=all&subport=50067&clientip=192.168.1
.101
```

调用者申请保留一个调谐器，不占有智能卡、解扰器等资源，监听锁频消息，指定消息接收端口和客户端的IP地址，资源申请接口请求参数示例：

```
http://ip:port/reserve_resource?clientuuid=aff1dc1e7f3c43a0b14bd13f2c5026ac&rtoken=a3cbda7162&tuner=1
&submsg=lock&subport=50067&clientip=192.168.1.101
```

接口返回参数应符合表16的定义。

表16　资源申请接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	申请成功与否的标志，取值为： ok：成功； failed：失败
Tuner-Size	数值	是	分配的调谐器数量，取值为： x：代表已分配 x 个调谐器，x 为整数
Descrambler-Size	数值	是	分配的解扰器数量，取值为： y：代表已分配 y 个解扰器，y 为整数
Smartcard-Size	数值	是	分配智能卡资源（卡/卡槽）的结果，取值为： 0：代表未分配智能卡资源； 1：代表已分配智能卡资源
MSGNAT[a]	字符串	否	指示接收网络穿透报文的 IP 地址和端口号
Reason	字符串	否	失败原因，只在失败的时候返回，取值定义为： Bad parameter：请求参数错误； Res already reserved：资源被占用； 其他可自定义
[a] 参数取值不为空时，客户端设备应按照 7.16 的规定定期向网关发送穿透报文			

请求成功时，资源申请接口返回参数示例：

```
Reply: ok
Tuner-Size: 1
Descrambler-Size: 2
Smartcard-Size: 1
MSGNAT: 192.168.88.1:34621
```

请求失败时，资源申请接口返回参数示例：

```
Reply: failed
Reason: Bad parameter
```

7.4 锁频设置

网关对外提供锁频设置接口，用于根据接口调用方设置的参数锁定对应频点。网关应根据接口参数中的Userhandle对相应的调谐器进行频点设置。若启用了安全通信模式，则本接口纳入管控。

接口URL：http://ip:port/lock_delivery。

接口协议：HTTP GET。

接口请求参数应符合表17的定义。

表17 锁频设置接口请求参数

参数名称	类型	是否必选	描述
userhandle	数值	是	客户端的上下文句柄，取值为客户端当前操作所对应的调谐器资源的序号。客户端对申请保留的每个调谐器资源分配序号，序号的取值从1开始，最大值为保留调谐器的数量。网关利用该参数区分客户端的操作所对应的调谐器。
rtoken	字符串	是	资源操作口令，与调用资源申请接口时协商的口令一致
usertick	数值	是	计时时间戳，每次锁频时的客户端系统时间，毫秒值，整数，取值为基于UTC 1970年01月01日00时00分00秒至当前时间的总毫秒数
delivery	字符串	是	传输方式，取值定义为： DVB-C：有线； DTMB：地面无线
freq	字符串	是	频点的物理参数，格式为：频点.符号率.调制方式，其中频点单位为Hz、符号率单位为baud、调制方式取值为QAM调制的阶数
pids	字符串	是	PID 列表，多个 PID 以','隔开，例如 Pids=0,1,20,45，取值定义为： -1：全通过滤； -2：无空包全通过滤； 0～8191：TS 中的 PID； PID列表为空：不接收任何TS流
target	字符串	是	TS 报文的接收方的 IP 地址和 UDP 端口
gwse	字符串	否	启用 TS 再加密，并设置 TS 再加密的算法和密钥 KT，设置格式为（算法名称，Key-ID，“密钥 KT+初始向量 IV”的密文）

在表17中，参数gwse的设置格式分为三段，描述如下。

——算法名称：指 TS 再加密要采用的算法，取值见网关信息查询接口的返回参数 GWSE-Alg。

——Key-ID：指通信密钥协商和设备身份认证确定的对称密钥的 Key-ID。

——“密钥 KT+初始向量 IV”的密文：共 32Byte。其中密钥 KT 指用于 TS 再加密算法。“密钥 KT+初始向量 IV”的明文为随机生成的 32Byte 二进制数，其中前 16Byte 为密钥 KT，后 16Byte 为初始向量 IV；通过密钥协商的对称密钥算法及 Key-ID 所对应的对称密钥对密钥 KT 和初始向量 IV 进行加密后，再进行 BASE64 编码得到“密钥 KT+初始向量 IV”的密文。

锁频设置接口请求参数示例：

```
http://ip:port/lock_delivery?delivery=DVB-C&freq=411000000.6875.64QAM&pids=0,1&
userhandle=1&rtoken=a3cbda7162&usertick=2312321&target=192.168.88.103:43221&gwse=AES128-
CBC,Adfk1e3ia5Po,Igkfie1239Gaskdjfielasdkfje12894eboa34e6nw6==
```

接口返回参数应符合表18的定义。

表18　锁频设置接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	设置成功与否的标志，取值为： ok：成功； failed：失败； nat：子网穿透，需要客户端发送穿透报文
Target	字符串	否	目标客户端的 IP 地址与 UDP 端口，不穿透时应返回
NAT	字符串	否	穿透报文的目标地址和端口，需要子网穿透时返回
MX	数值	否	穿透报文的时间间隔，单位为秒（s），不设置时默认取值为 10，需要子网穿透时返回
Reason	字符串	否	失败原因，只在失败时返回，取值定义为： Request parameter exception：请求参数错误； res reserved by other client：资源被占用； have not reserving resources：还没有申请占用资源； resource has expired：申请的资源已过期； Frequency locking failure：调用锁频接口返回失败； 其他可自定义

请求成功时，锁频设置接口返回参数示例：

```
Reply: ok
Target: 192.168.88.103:43221
```

需要发送穿透报文的场景中，客户端锁频时，网关返回穿透报文的信息，锁频设置接口返回参数示例：

```
Reply: nat
NAT: 192.168.88.1:34621
MX: 10
```

7.5　PID 过滤设置

网关对外提供PID过滤设置接口，用于根据接口调用方设置的PID过滤对应的数据。
接口URL：http://ip:port/set_pids。
接口协议：HTTP GET。
接口请求参数应符合表19的定义。

表19　PID 过滤设置接口请求参数

参数名称	类型	是否必选	描述
userhandle	数值	是	客户端的上下文句柄，与表 18 中的描述相符合
rtoken	字符串	是	资源操作口令，与调用资源申请接口时协商的口令一致
usertick[a]	数值	是	客户端锁频时所发送的计时时间戳，毫秒值，整数，取值为基于 UTC 1970 年 01 月 01 日 00 时 00 分 00 秒至当前时间的总毫秒数
count	数值	是	客户端锁频后调用 PID 过滤设置接口进行计数，count 参数值从 0 开始，每次递增 1

参数名称	类型	是否必选	描述
pids	字符串	是	PID 列表，多个 PID 以','隔开，例如 Pids=0,1,20,45，取值定义为： -1：全通过滤； -2：无空包全通过滤； 0～8191：TS 中的 PID； PID 列表为空：不接收任何 TS 流
noca[b]	字符串	否	取值为： 1：当前调谐器下的数据不启用解扰； 0：默认值，允许常规解扰
[a] 操作者锁频后调用本接口时，该参数的取值为锁频时的时间戳，与锁频设置接口中 usertick 参数取值相同。 [b] 当客户端需要获取 TS 原始流时，可设置此参数。			

接口返回参数应符合表20的定义。

表20　PID 过滤设置接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	设置成功与否的标志，取值为： ok：成功； failed：失败
Reason	字符串	否	失败原因，只在失败时返回，取值定义为： Bad Arguments：请求参数错误； Request usertick parameter exception：usertick 参数和 lock_delivery 不匹配； 其他可自定义

7.6　信号质量查询

网关对外提供的用于查询信号质量的接口。机顶盒调用此接口可获取网关的调谐器和信号的状态等相关信息。

接口URL：http://ip:port/get_tuner_status。

接口协议：HTTP GET。

接口请求参数：无。

接口请求返回参数应符合表21的定义。

表21　信号质量查询接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	查询成与否的标志，取值为： ok：成功； failed：失败
Tuner-Size	数值	是	网关的调谐器资源数量
for(i=0;i＜Tuner-Size;i++){			
Tuner-i-User-Handle	数值	是	调谐器当前的客户端的上下文句柄
Tuner-i-User-IP	字符串	是	调谐器当前的客户端的 IP 地址
Tuner-i-Status	数值	是	调谐器的状态，取值为： 0：无信号； 1：已锁定； 2：锁频中
Tuner-i-Freq	数值	是	当前锁定的频点信息，单位为 Hz
Tuner-i-Signal	字符串	是	信号状态，依次为： 误码率，采用科学计数法； 信号电平，单位为 dBuV；

参数名称	类型	是否必选	描述
			信号强度，取值范围为0～100； 信号质量，取值范围为0～100； 信噪比，单位为dB
}			
Reason	字符串	否	失败原因，只在失败的时候返回，取值定义为： no resource：没有调谐器资源； 其他可自定义

信号质量查询接口返回参数示例：

```
Reply: ok
Tuner-Size: 2
Tuner-0-User-Handle: 1
Tuner-0-User-IP: 192.168.88.102
Tuner-0-Status: 0
Tuner-0-Freq: 514000000.6875.QAM64
Tuner-0-Signal: 1.345E-7,90,80,75,36
Tuner-1-User-Handle: 2
Tuner-1-User-IP: 192.168.88.102
Tuner-1-Status: 0
Tuner-1-Freq: 514000000.6875.QAM64
Tuner-1-Signal: 1.345E-7,90,80,75,36
```

7.7 卡状态查询

网关对外提供的用于查询智能卡状态的接口。机顶盒调用此接口可查询网关侧智能卡的插入状态。
接口URL：http://ip:port/get_card_status。
接口协议：HTTP GET。
接口请求参数：无。
接口请求返回参数应符合表22的定义。

表22 卡状态查询接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	查询成功与否的标志，取值为： ok：成功； failed：失败
CardStatus	数值	是	智能卡状态，取值定义为： 0：未插卡； 1：卡插入（无电气信号）； 2：卡插入
Reason	字符串	否	失败原因，只在失败的时候返回，取值定义为： errorno=-1：调用底层接口获取卡状态失败，打印返回值错误码； 其他可自定义

7.8 卡复位

网关对外提供智能卡复位接口，用于智能卡的复位操作和识别智能卡类型。
接口URL：http://ip:port/card_reset。
接口协议：HTTP GET。
接口请求参数应符合表23的定义。

表23 卡复位接口请求参数

参数名称	类型	是否必选	描述
rtoken	字符串	是	资源操作口令，与调用资源申请接口时协商的口令一致
raw	字符串	否	指示 ATR 数据的来源，取值为： true：获取智能卡的 ATR； false：网关 CA 子模块代理获取 ATR； 若未包含该字段，则默认该字段取值为 false

接口返回参数应符合表24的定义。

表24　卡复位接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	请求成功与否的标志，取值为： ok：成功； failed：失败
ATR	字符串	是	智能卡特征值，取决于 CA 厂商定义
Reason	字符串	否	失败原因，只在失败的时候返回，取值定义为： Request parameter exception：请求参数错误； smartcard reset fail：调用底层接口返回值失败； 其他可自定义

7.9　机卡通信

网关对外提供的用于机顶盒与网关智能卡进行通信的接口。当机顶盒要与网关智能卡通信时，应调用此接口，将发送给智能卡的数据通过接口请求参数进行传送。若启用了安全通信模式，则本接口纳入管控。

接口URL：http://ip:port/card_transfer。

接口协议：HTTP GET。

接口请求参数应符合表25的定义。

表25　机卡通信接口请求参数

参数名称	类型	必选	描述
rtoken	字符串	是	资源操作口令，与调用资源申请接口时协商的口令一致
send	字符串	是	CA主模块要发送给智能卡的数据，采用BASE64编码

接口返回参数应符合表26的定义。

表26　机卡通信接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	请求成功与否的标志，取值为： ok：成功； failed：失败
Recv	字符串	是	智能卡返回给CA主模块的数据，采用BASE64编码
Reason	字符串	否	失败原因，只在机卡通信失败的时候返回，取值定义为： Request parameter exception：请求参数错误； smartcard transfer fail：调用接口返回值失败； error：调用平台接口回调失败； 其他可自定义

7.10　故障信息查询

网关对外提供的用于查询网关的故障信息的接口。当机顶盒需要主动查询网关的故障信息时，应调用此接口，以及时得到故障的细节数据。

接口URL：http://ip:port/get_malfunction_info。
接口协议：HTTP GET。
接口请求参数：无。
接口返回参数应符合表27的定义。

表27　故障信息查询接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	查询成功与否的标志，取值为： ok：成功； failed：失败
Status	字符串	是	网关工作状态，取值为： normal：正常； malfunction：异常
State-Size	数值	是	故障码数量
for(i=0;i＜State-Size;i++){			
State-i-ID	数值	是	故障码 ID，取值为： 701，702，703，其他可自定义
State-i-Info	字符串	是	故障信息，取值与 ID 对应，取值定义为： 当 ID=701 时，为“升级失败”； 当 ID=702 时，为“CA 模块启动失败”； 当 ID=703 时，为“读卡器失败”； 其他可自定义
}			

7.11　设备管理

该接口用于机顶盒对网关进行配置管理。
接口URL：http://ip:port/device_ctrl。
接口协议：HTTP GET。
接口请求参数说明如下。
——action：操作类型，取值应符合表 28 的定义。
——表 28 中的设置网关升级软件地址接口参数应符合表 29 的定义。
——表 28 中的加载网关侧 CA 程序模块接口的参数应符合表 30 的定义。
——表 28 中的启用/停用无卡 CA 接口参数应符合表 31 的定义。
——表 28 中的设置 Key-ID 并启用安全通信模式参数应符合表 32 的定义。
——表 28 中的检查 Key-ID 对应的对称密钥是否有效接口的参数应符合表 33 的定义。
——表 28 中的登记已开通业务包接口的参数应符合表 34 的定义。

表28　action 取值

参数名称	类型	是否必选	描述
reboot	字符串	否	重启系统，若启用了安全通信模式，则本接口纳入管控
factory_reset	字符串	否	恢复出厂设置，若启用了安全通信模式，则本接口纳入管控
get_sysinfo	字符串	否	查系统信息
launch_upgrade	字符串	否	指定升级软件的 URL 地址，发起软件升级，参数说明见表 29； 若启用了安全通信模式，则本接口纳入管控
load_ca	字符串	否	加载网关侧 CA 程序，参数说明见表 30； 若启用了安全通信模式，则本接口纳入管控
set_nocardca	字符串	否	启用/停用无卡 CA[a]，参数说明见表 31； 若启用了安全通信模式，则本接口纳入管控
set_ssmode	字符串	否	设置对称密钥的 Key-ID，启用安全通信模式，参数说明见表 32；

			设置仅在当前网关系统开机阶段生效，如果重启系统，则恢复到默认状态
check_sskeyid	字符串	否	检查 Key-ID 对应的对称密钥是否有效，参数说明见表 33
set_servicepack	字符串	否	登记已开通的业务包，参数说明见表 34
[a] 优先级高于有卡 CA			

表29　设置网关升级软件地址参数

参数名称	类型	是否必选	描述
url	字符串	是	UrlEncode后的URL字符串，升级文件在盒端的下载地址
md5	字符串	是	请求的HTTP负载内容的MD5校验值

表30　加载网关侧 CA 程序参数

参数名称	类型	是否必选	描述
caname	字符串	是	CA模块的名字

表31　启用/停用无卡 CA 参数

参数名称	类型	是否必选	描述
caname[a]	字符串	是	启用或停用无卡CA，取值定义为： 无卡CA模块的名字：启用该无卡CA模块； 空：停用当前无卡CA模块
[a] 网关接收到本接口参数后，应主动向机顶盒发送智能卡状态消息			

表32　设置 Key-ID 并启用安全通信模式参数

参数名称	类型	是否必选	描述
key_id	字符串	是	对称密钥的 Key-ID
client_uuid	字符串	是	客户端的 UUID

表33　检查 Key-ID 对应的对称密钥是否有效参数

参数名称	类型	是否必选	描述
key_id	字符串	是	对称密钥的 Key-ID

表34　登记已开通业务包参数

参数名称	类型	是否必选	描述
mode	字符串	是	不为空表示开通的业务套餐名称，为空表示取消登记

除查系统信息外，所有设备管理接口返回参数应符合表35的定义。查系统信息接口返回参数应符合表36的定义。

表35　设备管理接口（除查系统信息外）返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	请求成功与否的标志，取值为： ok：成功（或有效）； failed：失败（或无效）
Duration	数值	否	预计操作消耗时长，单位为秒（s）
Reason	字符串	否	失败原因，只在失败的时候返回，取值定义为： forbidden：禁止；

参数名称	类型	是否必选	描述
			load CA fail：CA 加载失败； Invalid Name：无对应 CA； 其他可自定义

表36　查系统信息接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	查询成功与否的标志，取值为： ok：成功； failed：失败
System-Version	字符串	是	系统版本
OS-Name	字符串	是	操作系统名称
SN	字符串	是	产品序列号
CPU	数字	是	芯片主频，单位为兆赫（MHz）
RAM	数字	是	内存大小，单位为千字节（KB）
FLASH	数字	是	FLASH 大小，单位为千字节（KB）
QAM	字符串	是	支持的 QAM 调制方式，多种调制方式之间用逗号隔开，如：64-QAM,128-QAM
HSIC	字符串	是	网关芯片是否支持高安，取值为： yes：支持； no：不支持
Operator-Name	字符串	是	运营商名称，一般是域名
Operator-UUID	字符串	是	运营商的 UUID
GWCA-Size	数字	是	预置 CA 模块数量
GWCA-Current	数字或 nil	是	当前使用的 CA 模块的索引，取值范围为[0,GWCA-Size)；若无预置 CA 模块或 CA 模块未使用时，该参数取值为 nil
for(i=0;i＜GWCA-Size;i++){			
GWCA-i-Name	字符串	否	索引为 i 的 CA 模块的名字
GWCA-i-Vendor	字符串	否	索引为 i 的 CA 模块的提供商
GWCA-i-Version	字符串	否	索引为 i 的 CA 模块的版本
GWCA-i-Type	字符串	否	索引为 i 的 CA 模块的类型
}			

查系统信息接口返回参数示例：

```
Reply: ok
System-Version: 1.0.6
OS-Name: tvos-lite
SN: 187263517727363721
CPU: 200
RAM: 200
FLASH: 512
QAM: 32-QAM, 64-QAM, 128-QAM, 256-QAM
HSIC: yes
Operator-Name: catv
```

```
Operator-UUID: dd4da04a62414b55a735fed753ccc208
GWCA-Size: 2
GWCA-Current: 0
GWCA-0-Name: foo1
GWCA-0-Vendor: abc
GWCA-0-Version: 1.0.4
GWCA-0-Type: gwnocardca
GWCA-1-Name: foo2
GWCA-1-Vendor: xyz
GWCA-1-Version: 2.0.3
GWCA-1-Type: gwnormal
```

7.12 网关信息查询

网关对外提供的用于进行信息查询的接口。机顶盒调用此接口，可以查询网关的基本信息，包括网关的MAC地址、WAN口的信息、网关的IP地址、正在使用网关的客户端的ID、网关的设备ID及基本信息、网关的解扰器、调谐器等资源信息、网关的CA相关基本信息以及是否开启安全通信模式等。

接口URL：http://ip:port/get_info。

接口协议：HTTP GET。

接口请求参数：无。

接口返回参数应符合表37的定义。

表37 网关信息查询接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	查询成功与否的标志，取值为： ok：成功； failed：失败
MAC	字符串	是	网关的 MAC 地址，十六进制表示并用“-”分隔
WAN-MAC	字符串	否	WAN 口的 MAC 地址，十六进制表示并用“-”隔开 如果网关没有 WAN 口，则不返回此字段
WAN-Mode	字符串	否	WAN 口的工作模式，取值为： none：不支持 WAN，无双向网络接入； wan：普通 WAN
IP	字符串	是	网关的 IP 地址（局域网地址，由 DHCP 分配或者静态指定）
ClientUUID	字符串	是	当前在使用网关的客户端 APP 的 UUID，若没有则为 none
Device-ID	字符串	是	网关的设备 ID，格式见 GY/T XXX—XXXX《有线电视单向网关技术要求和测量方法》附录 A
Device-Info	字符串	是	网关的其他简要设备信息
Tuner	字符串	是	设备支持的调谐器的 ID 列表。对于单调谐器设备，取值为 1；对于多调谐器设备，返回的多个取值以逗号分隔，取值为： 1：代表调谐器 1； 2：代表调谐器 2； 以此类推对应 ID
Descrambler	字符串	是	设备支持的解扰器的 ID 列表。对于单解扰器设备，取值为 1；对于多解扰器设备，返回的多个取值以逗号分隔，取值为： 1：代表解扰器 1； 2：代表解扰器 2； 以此类推对应 ID
Gateway-Version	字符串	是	网关的软件版本
Gateway-Vendor	字符串	是	网关的制造商名称
Smartcard-Status	数值	是	当前卡状态，取值为： 0：未插卡； 1：卡插入（无电气信号）； 2：卡插入
Smartcard-Type	数值	是	智能卡的类型，取值为：

			0：不支持智能卡； 1：普通智能卡 CA； 2：无卡 CA； 3：安全智能卡 CA； 4：安全无卡 CA
Smartcard-ATR	字符串	是	智能卡的 ATR，采用 BASE64 编码格式，若没有时为 0
StrictSecurity	数值	否	是否启用安全通信模式，取值为： 0：不启用； 1：启用
ServicePackage	字符串	否	空表示未登记，否则为业务套餐名称，不超过 15Byte
Tick	数值	否	网关计时滴答基准，单位：毫秒
GWSS-Alg	字符串	否	网关支持的对称密钥算法列表，取决于网关的实现，取值可为： AES128-CBC：AES128 算法，CBC 模式 SM4-CBC：SM4 算法，CBC 模式
GWSE-Alg	字符串	否	网关支持的 TS 再加密算法列表，取决于网关的实现，取值可为： AES128-CBC：AES128 算法，CBC 模式 SM4-CBC：SM4 算法,CBC 模式
GWKN-Alg	字符串	否	网关支持的密钥协商算法列表，取决于网关的实现，取值为： ECDH-SECP256R1：采用椭圆曲线为 SECP256R1 的 ECDH 密钥交换算法 ECDH-SM2：采用椭圆曲线为 ECDH-SM2 的 ECDH 密钥交换算法

网关信息查询接口返回参数示例：

```
Reply: ok
MAC: 74-84-E1-07-7D-D0
WAN-MAC: 74-84-E1-07-7D-D3
WAN-Mode: wan
IP: 10.168.22.1
ClientUUID: none
Device-ID: 11012420000010000000009
Device-Info: ETH,0,0,VGRVDR01W
Descrambler: 1,2,3,4,5,6
Tuner: 1,2
Gateway-Version: v2.0.1
Gateway-Vendor: Gateway-Server
Smartcard-Status: 1
Smartcard-Type: 1
Smartcard-ATR: 0
StrictSecurity: 0
ServicePackage:
GWSS-Alg: AES128-CBC
GWSE-Alg: AES128-CBC
GWKN-Alg: ECDH-SECP256R1
```

7.13 通信密钥协商

机顶盒调用此接口与网关进行通信密钥协商，双方得到共享密钥。之后机顶盒和网关应各自基于共享密钥，通过HKDF算法派生出对称密钥算法所需的对称密钥KS。HKDF算法取决于协商的对称秘钥算法，协商的对称密钥算法使用AES128-CBC时，HKDF应采用SHA256摘要算法；协商的对称密钥算法为SM4-CBC时，HKDF应采用SM3摘要算法。HKDF算法的输入密钥为协商获取的共享密钥，派生出32Byte密钥，其中前16Byte作为协商的对称密钥算法的对称密钥KS，后16Byte在安全通信模式下用作对称密钥算法的初始向量IV。机顶盒和网关应将对称密钥KS和初始向量IV与接口请求参数中的Key-ID进行关联，用于后续操作。

接口URL：http://ip:port/key_negotiation。

接口协议：HTTP GET。

接口请求参数应符合表38的定义。

参数名称	类型	是否必选	描述
alg_neg[a]	字符串	是	密钥协商采用的算法，从网关信息查询接口的算法列表中获取，取值为“ECDH-SECP256R1”或“ECDH-SM2”
alg_key[a]	字符串	是	协商的对称密钥算法，从网关信息查询接口的算法列表中获取，取值可为“AES128-CBC”或“SM4-CBC”
px	字符串	是	公钥点X坐标
py	字符串	是	公钥点Y坐标
key_id	字符串	是	密钥标识Key-ID，取值为随机字符串，长度不少于12Byte
expired	数字	否	未指定用途的密钥的过期时间，单位为秒（s），默认取值为30s，取值应不超过180s
[a] 参数 alg_neg 和 alg_key 的取值对应关系为：当 alg_neg 取值为 ECDH-SECP256R1 时，alg_key 的取值应为 AES128-CBC；当 alg_neg 取值为 ECDH-SM2 时，alg_key 的取值应为 SM4-CBC。			

表38　通信密钥协商接口请求参数

密钥协商接口请求参数示例：

```
http://ip:port/key_negotiation?alg_neg=ECDH-SECP256R1&alg_key=AES128-
CBC&px=1233723126253172&py=8126387162351762573 6&key_id=abcbdda1232&expired=10
```

接口返回参数应符合表39的定义。

表39　通信密钥协商接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	请求成功与否的标志，取值为： ok：成功； failed：失败
Px	字符串	是	网关返回的公钥点X坐标
Py	字符串	是	网关返回的公钥点Y坐标

7.14　设备身份认证

机顶盒与网关完成通信密钥协商后，还应进行身份认证。网关对外提供设备身份认证接口。机顶盒调用此接口，用来实现机顶盒与网关两端设备的身份互相认证，保证通信两端的身份合法性。一旦设备身份经过认证，机顶盒和网关应保存对称密钥KS、初始向量IV及对应的Key-ID，用于安全通信模式或TS再加密过程。

设备身份认证要求接口的调用方（客户端）和被调用方（网关）应预置统一的验证口令，该口令可以采用网关设备外包装上的序列号或验证码。在进行设备身份认证时，机顶盒和网关应分别基于RMACT生成认证信息的明文，并计算得到认证信息的密文，再通过调用本接口实现认证信息密文的交换，双方相互进行数据核对实现身份认证。

RMACT是一种认证信息明文的组成方法的名称，指通过JOIN(Random,MAC,Token)计算认证信息明文，其中，JOIN函数表示按字节序列依次串接各参数内容，各参数的含义依次为：Random为随机字符串、MAC为网关的MAC地址（格式为十六进制表示并用“-”隔开，即**-**-**-**-**-**）、Token为验证口令。

生成认证信息明文后，通过计算对应消息摘要及利用协商的对称密钥算法进行加密的方式来计算得到认证信息的密文，计算方法如下。

——采用 AES128-CBC 时，为 BASE64(AES128-CBC(SHA256(KN), SHA256(JOIN(Random, MAC, Token))))，使用 SHA256 计算得到摘要值，仅使用其前 128bit 作为密钥。

——采用 SM4-CBC 时，为 BASE64(SM4-CBC(SM3(KN), SHA256(JOIN(Random, MAC, Token))))，使用 SM3 算法计算得到摘要值，仅使用其前 128bit 作为密钥。

其中KN密钥计算方法为JOIN(KS,Token)，参数说明如下。

——通过参数 key_id 获取到指定的基于密钥协商接口协商的对称密钥 KS。
——Token 口令数据应通过其他安全渠道获取，如通过设置界面填写或者从网络获取等。
接口URL：http://ip:port/key_authentication。
接口协议：HTTP GET。
接口请求参数应符合表40的定义。

表40　设备身份认证接口请求参数

参数名称	类型	是否必选	描述
step	数字	是	身份认证的步骤，取值为： 1：步骤1； 2：步骤2
alg	字符串	是	认证信息明文组成方法，取值为“RMACT”
auth	字符串	步骤2必选	认证信息的密文
random	字符串	步骤1必选	随机字符串（a-zA-ZO-9），长度为32个字符
key_id	字符串	是	密钥标识Key-ID，取值为通信密钥协商接口协商好的Key_ID

设备身份认证步骤1，接口请求参数示例：

```
http://ip:port/key_authentication?step=1&alg=RMACT&random=1238bfdafdefdefdeadfe81324ldegnr&key_id=Jfaie8123hfasd
```

设备身份认证步骤2，接口请求参数示例：

```
http://ip:port/key_authentication?step=2&alg=RMACT&auth=Mfjeiud121j23k12JJHHJasdf12j3dwg&key_id=Jfaie8123hfasd
```

接口返回参数应符合表41的定义。

表41　设备身份认证接口返回参数

参数名称	类型	是否必选	描述
Reply	字符串	是	请求成功与否的标志，取值为： ok：成功； failed：失败
Auth	字符串	步骤1必选	认证信息的密文
Random	字符串	步骤1必选	随机字符串(a-zA-ZO-9)，长度为32个字符
Reason	字符串	否	失败原因，认证失败时返回，取值定义为： Invalid：无效参数； 其他可自定义

7.15　消息报文

消息报文用于网关主动向机顶盒报告信息，包括锁频消息、智能卡状态消息、故障消息、系统升级消息、时间基准消息和用户自定义消息。消息报文以'MSG:'为起始内容，其报文的长度小于256Byte。消息报文发送到机顶盒的消息数据接收端口。

锁频消息参数应符合表42的定义。

表42　锁频消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为 lock-status
TunerID	字符串	是	本消息所报告的调谐器的 ID
UserHandle	数值	是	该调谐器当前的客户端的上下文句柄
LockStatus	数值	是	指示锁频状态，取值为： 0：无信号； 1：已锁定；

			2：锁频中

智能卡状态消息参数应符合表43的定义。

表43 智能卡状态消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为 card-status
CardSlot	数值	是	指示智能卡的状态，取值为： 0：未插卡； 1：卡插入（无电气信号）； 2：卡插入

故障消息参数应符合表44的定义。

表44 故障消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为 malfunction
State-Size	数值	是	故障码状态数量
for(i=0;i < State-Size;i++){			
State-i-ID	数值	是	故障码 ID，取值为： 701，702，703，其他可自定义
State-i-Info	字符串	是	故障信息，取值与 ID 对应，取值定义为： 当 ID=701 时，为“升级失败”； 当 ID=702 时，为“CA 模块启动失败”； 当 ID=703 时，为“读卡失败” 其他可自定义
}			

系统升级消息参数应符合表45的定义。在网关升级过程中，应通过系统升级消息将升级开始、升级进度及升级结束等相关信息传递给机顶盒，用于用户界面展示。

表45 系统升级消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为 sys-upgrade
Subtype	字符串	是	升级消息子类型
Content	字符串	是	根据子类型不同

时间基准消息参数应符合表46的定义。根据需要，网关应定期向机顶盒发送该消息，发送间隔不超过5min。

表46 时间基准消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为tick-base
Tick	字符串	是	网关计时滴答基准，单位为毫秒（ms）

用户自定义消息参数应符合表47的定义。

表47 用户自定义消息参数

参数名称	类型	是否必选	描述
MSG	字符串	是	取值固定，为 userdefine
Subtype	字符串	是	消息子类型，用户自定义

Content	字符串	是	用户自定义

7.16 基于以太网口的数据传输格式

机顶盒与网关之间为以太网连接时，消息报文和TS数据均封装为UDP单播报文进行传输。在进行消息报文接收或TS数据接收之前，机顶盒应先创建UDP套接字、绑定端口，并将端口信息通知网关，之后两个设备之间再进行消息和数据的传输。

对于TS数据接收，机顶盒在每次准备接收数据即进行锁频操作前，应先创建UDP套接字、绑定端口。机顶盒每次锁频都应切换接收端口以避免接收脏数据。当机顶盒需要从网关的多个调谐器接收数据时，机顶盒应对应开启多个接收端口，每个端口接收来自一个调谐器的数据。

对于TS数据传输，UDP单播数据报文格式为：每个UDP报文承载7个连续TS包，共1316Byte。机顶盒根据接收的TS包的顺序，将TS包封装到UDP报文，并将UDP报文依次顺序发送。

对于消息报文传输，一个UDP单播报文中承载一个消息报文，内容为多行文本。

在IPv4网络中，当网关与机顶盒不在同一子网内时需要机顶盒定期向上（向网关）发送穿透报文，方可接收到网关的数据以及消息的UDP报文,定期发送的时间间隔由锁频设置接口返回,默认取值为10s。子网穿透报文应符合表48的定义，仅用于IPv4网络。

表48 子网穿透报文

参数名称	类型	是否必选	描述
NAT	字符串	是	取值固定，为 TS
Client-IP	字符串	是	客户端 IP 地址
User-Tick[a]	数值	是	客户端锁频时所发送的计时时间戳，毫秒值，取值为基于 UTC 1970 年 01 月 01 日 00 时 00 分 00 秒至当前时间的总毫秒数
User-Handle	数值	是	客户端的上下文句柄
[a] 操作者锁频后发送子网穿透报文时，该参数取值为锁频时的时间戳，与锁频设置接口 usertick 参数取值相同。			

7.17 基于 USB 口的数据传输格式

网关和机顶盒之间通过USB口连接时，机顶盒调用接口应符合7.3～7.14所规定的接口访问方式，机顶盒与网关之间的消息格式和消息/数据传输应符合7.15和7.16的规定，网关和机顶盒应支持TCP/IP通信过程，应支持IEEE 802.3规定的以太网帧格式，若支持VLAN则应支持IEEE 802.1Q规定的以太网帧格式。

通过USB口连接时，机顶盒与网关应将USB作为协议报文的物理层传输通道，规定如下。

——在设备通信协商、接口访问、消息发送和 TS 数据发送时，以太网帧均应封装到 USB Transfer 中进行传输。

——一个 USB Transfer 中可承载的 MEF 应由机顶盒和网关通过设备通信协商过程确定，机顶盒根据从网关获得的 MEF 信息和自身的支持能力，确定一个 USB transfer 中最多可负载的以太网帧数量后并设置给网关。

——USB Transfer 应符合 USB2.0 或 USB3.2 协议的规定。

——以太网帧的 MTU 为 1500Byte。在文件中，当上层协议报文未超过 MTU 长度时，应将上层协议报文封装到同一以太网帧中，不做分包处理。

——机顶盒与网关之间应采用图 2 所规定的方式将以太网帧按序封装到 USB Transfer 中，其中填充字段用于指示紧跟其后的以太网帧信息，应符合表 49 的定义。

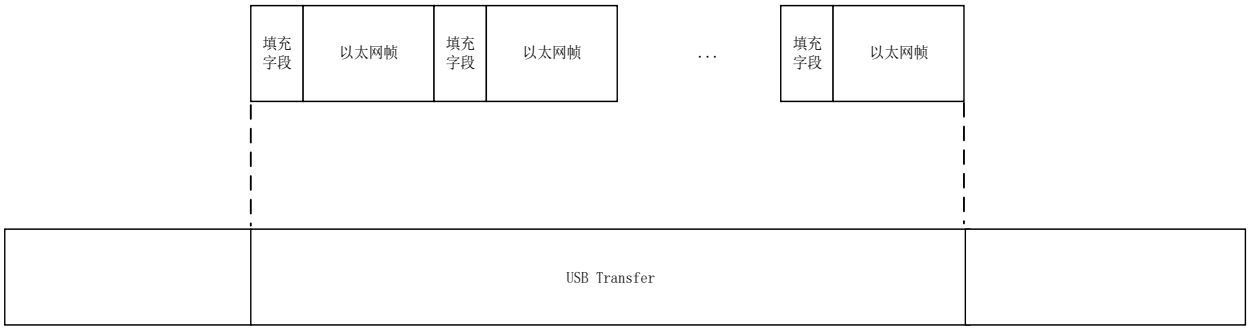


图2　以太网帧到 USB Transfer 的封装

表49　填充字段

参数名称	长度	描述
last_indicator	1Byte: bit7	是否最后一个以太帧的标识，取值为： 1：最后一个以太网帧； 0：不是最后一个以太网帧
reserved	1Byte: bit6 - bit4	保留使用，默认值为0
padding_len	1Byte: bit3 - bit0	以太网帧后面的填充字节数
reserved	1Byte	保留使用，默认值为0
ef_len	2Byte	以太网帧的字节数，格式为网络字节序

8　流程要求

8.1　设备发现

8.1.1　基于以太网口

机顶盒/网关启动后，均应先加入SSDP的组播，接收SSDP组播报文，同时，机顶盒应发送搜索请求报文，网关应发送存续报文和广播存续报文，以发现当前局域网内的对端设备。设备发现可具体分为以下三种场景。

——通过存续报文建立设备连接：

机顶盒加入SSDP组播后，就立即接收到网关的存续报文，此时机顶盒将不再发送搜索请求报文。在此场景下，网关通常先于机顶盒启动，局域网中已存在网关的存续报文。

在此场景下的设备发现流程图见图3，流程如下。

1)　网关设备正常启动后，应先加入 SSDP 组播。
2)　在局域网络环境下，网关应间隔 5s 持续发送存续报文，让网络环境内的其他设备能够发现网关。
3)　机顶盒设备正常启动后，应先加入 SSDP 组播。
4)　在机顶盒发送搜索请求报文前，先接收到网关存续报文，获取到网关设备的相关信息。
5)　机顶盒记录网关信息，用于后续与网关设备的交互。

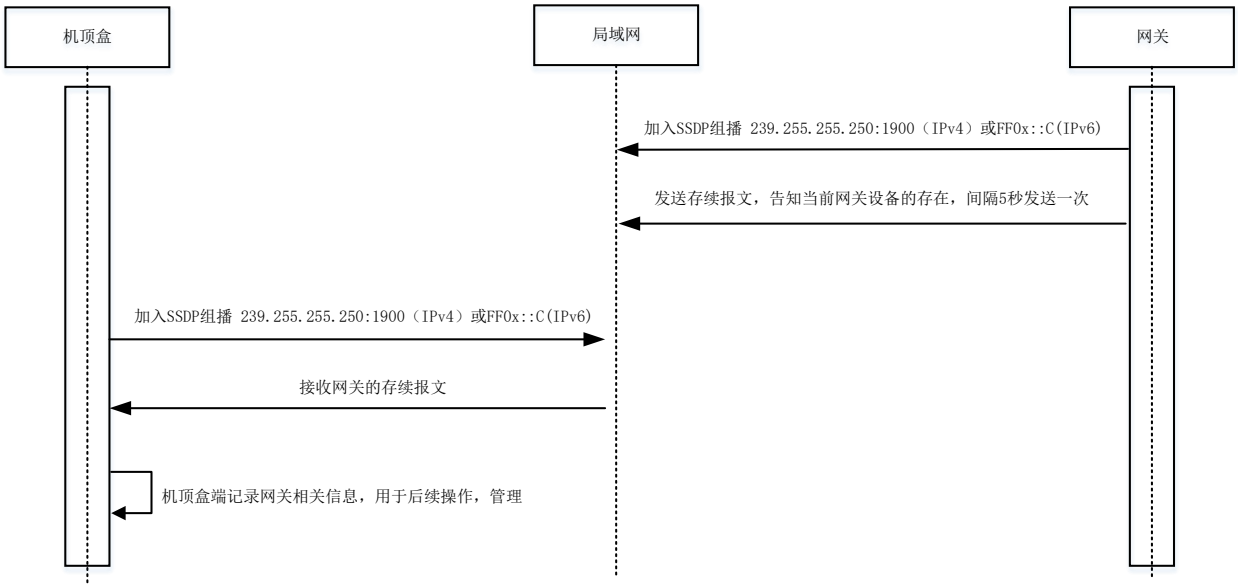


图3　基于存续报文完成设备发现流程图

——通过搜索请求报文建立设备连接：

机顶盒加入SSDP组播后，并未立刻接收到网关的存续报文，因此机顶盒会发送搜索请求报文，若网关接收到搜索请求报文，并向机顶盒发送搜索应答报文，双方将建立连接。在此场景下，通常是机顶盒先于网关启动，局域网中已存在搜索请求报文。

此场景下的设备发现流程图见图4，流程如下。

1）　机顶盒设备正常启动后，应先加入 SSDP 组播。
2）　在局域网络环境下，机顶盒应间隔 5s 发送搜索请求报文，用于寻找网络中的网关设备。
3）　网关设备正常启动后，应先加入 SSDP 组播。
4）　在局域网络环境下，网关应间隔 5s 持续发送存续报文，让网络环境内的其他设备能够发现网关。
5）　网关设备接收到机顶盒的探测报文，应立即向机顶盒发送搜索应答报文。
6）　机顶盒接收到网关的搜索应答报文，停止发送搜索请求报文。
7）　机顶盒记录网关信息，用于后续与网关设备的交互。

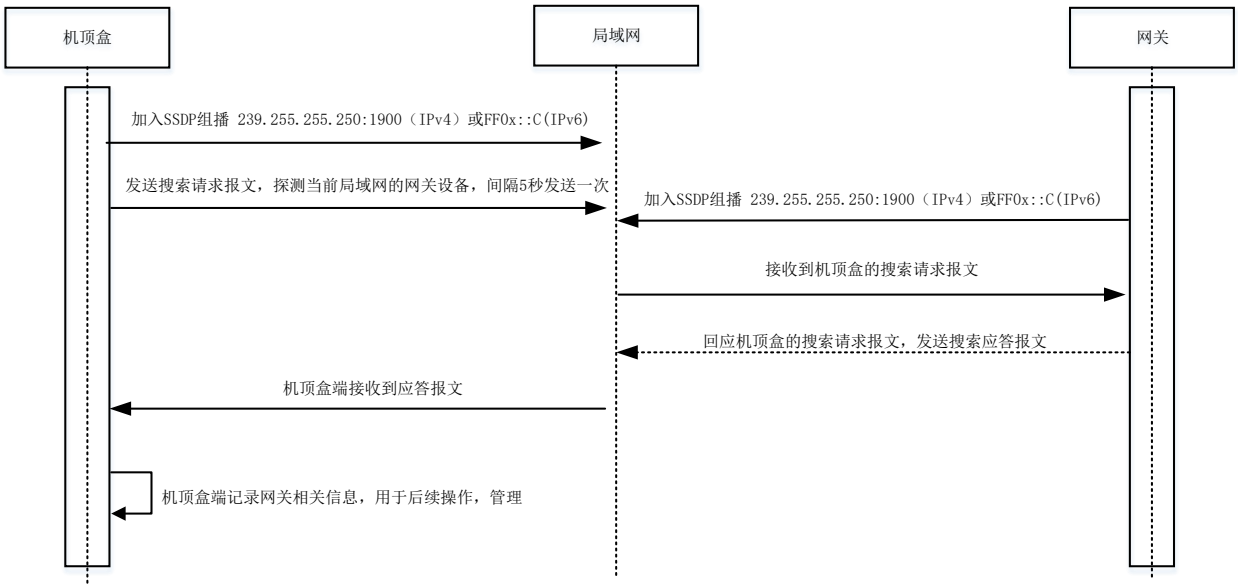


图4　基于搜索请求报文完成设备发现流程图

——通过广播存续报文建立设备连接：

机顶盒启动后立即接收到网关的广播存续报文，此时机顶盒将不再发送搜索请求报文。在此场景下，网关通常先于机顶盒启动，局域网中已存在网关的广播存续报文。

在此场景下的设备发现流程图见图5，流程如下。

1) 网关设备正常启动后，应间隔 5s 持续发送广播存续报文，让网络环境内的其他设备能够发现网关。
2) 机顶盒设备正常启动后，接收广播存续报文。
3) 若先接收到网关的广播存续报文，机顶盒记录网关信息，用于后续与网关设备的交互。

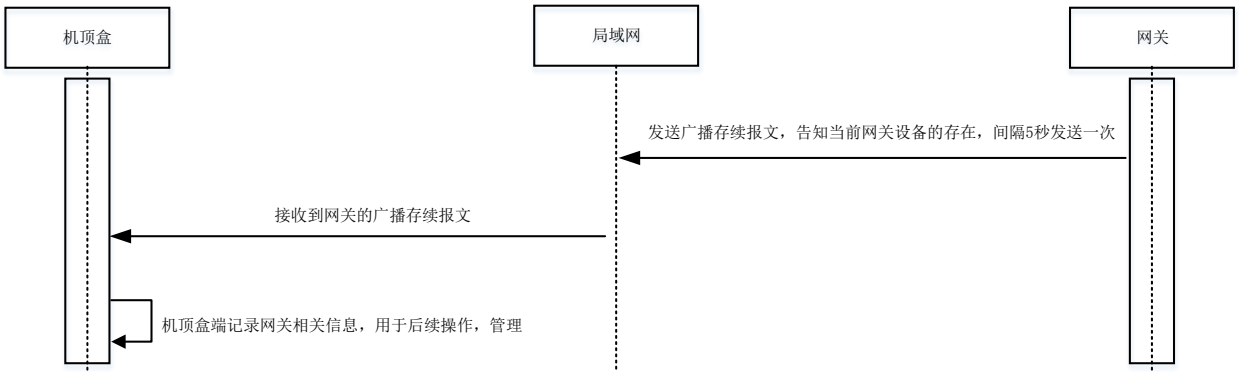


图5　基于广播存续报文完成设备发现流程图

8.1.2　基于 USB 口

8.1.2.1　概述

网关作为USB设备插入机顶盒，或者在已经插入的情况下机顶盒开机，都会触发基于USB口的设备发现流程。网关和机顶盒之间的USB设备发现流程包括两个步骤：基于USB的设备识别和设备通信协商。

8.1.2.2　基于 USB 的设备识别

网关作为USB设备插入机顶盒，或者在已经插入的情况下机顶盒开机，都会触发基于USB口的设备识别，此时机顶盒通过设备接口类型、设备接口子类型及协议字符串来识别插入的设备是否为网关设备。

基于USB的设备识别流程图见图6，流程如下。

a) 在 USB 网关已经插入机顶盒的情况下机顶盒正常启动，或者机顶盒启动后 USB 网关插入机顶盒，均触发机顶盒应用去扫描 USB 设备。
b) 机顶盒应用遍历 USB 设备信息，若获取到的 USB 信息当中的设备接口类型的值为 0xFFH、设备接口子类型的值为 0xC0、协议字符串为“Cable TV unidirectional gateway interface”的设备，则判定为网关设备）。
c) 基于机顶盒操作系统的安全通信规范，在首次插入设备时，机顶盒在用户界面弹出提示窗，提示用户对 USB 通信进行授权；若用户授权一次后，没有插拔设备则无需再次授权。
d) 用户授权后，机顶盒完成 USB 网关设备的识别，将进入设备通信协商流程。

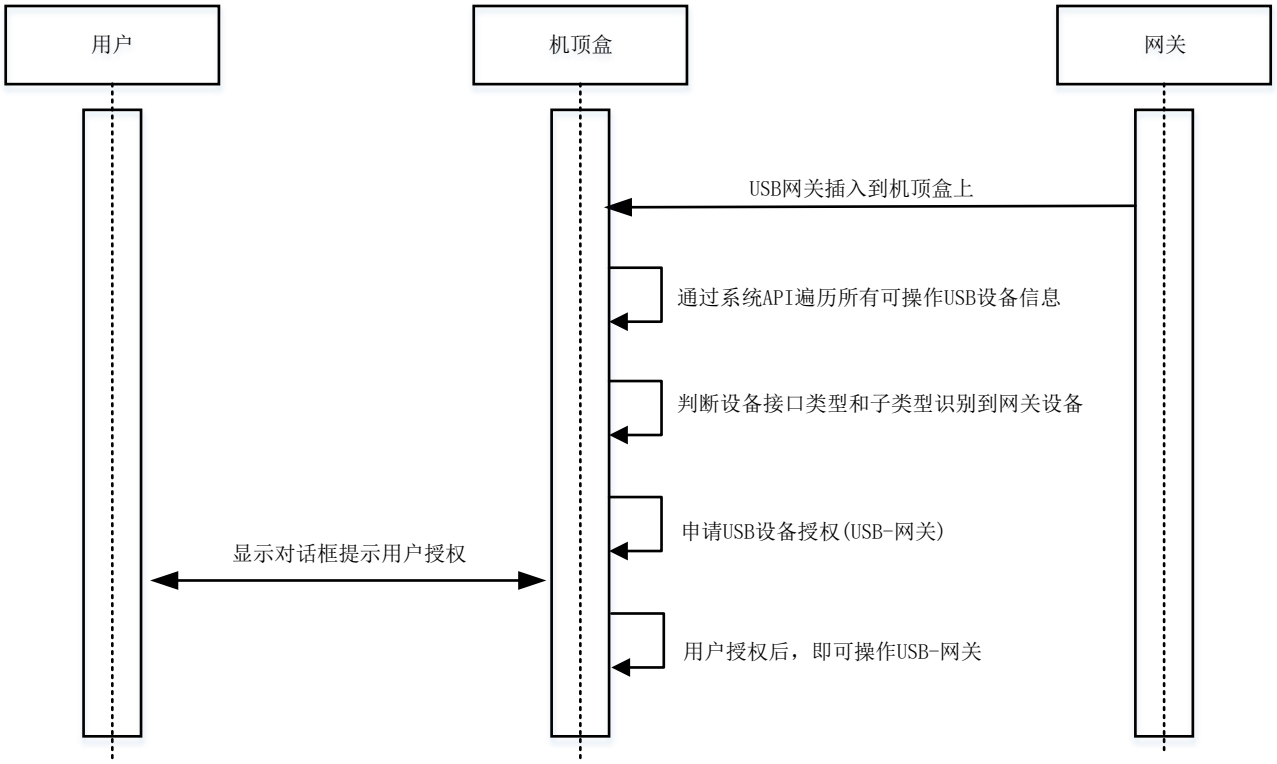


图6　基于 USB 的设备识别流程图

8.1.2.3　USB 设备通信协商流程

机顶盒识别USB网关设备后，基于USB协议规范，可通过USB出端点可以向网关设备写入数据，通过USB入端点可以从网关设备接收数据。在进行USB设备通信协商流程时，协商报文直接封装到USB数据包中传输。

基于USB的设备通信协商流程图见图7，流程如下。

a)　机顶盒基于出端点，向网关发送 MAC 地址查询报文，以获取网关的 MAC 地址和数据通信协议。
b)　网关基于入端点，向机顶盒回传网关 MAC 地址和支持的数据通信协议。
c)　机顶盒基于出端点，向网关发送 IP 地址设置报文，给网关设置 IP 地址。
d)　网关基于入端点，向机顶盒回传设置状态是否成功。
e)　协商结束后，机顶盒和网关都具有有效的 MAC 地址和 IP 地址，后续将基于此地址将上层报文封装成对应的业务报文进行协议交互和数据传输。

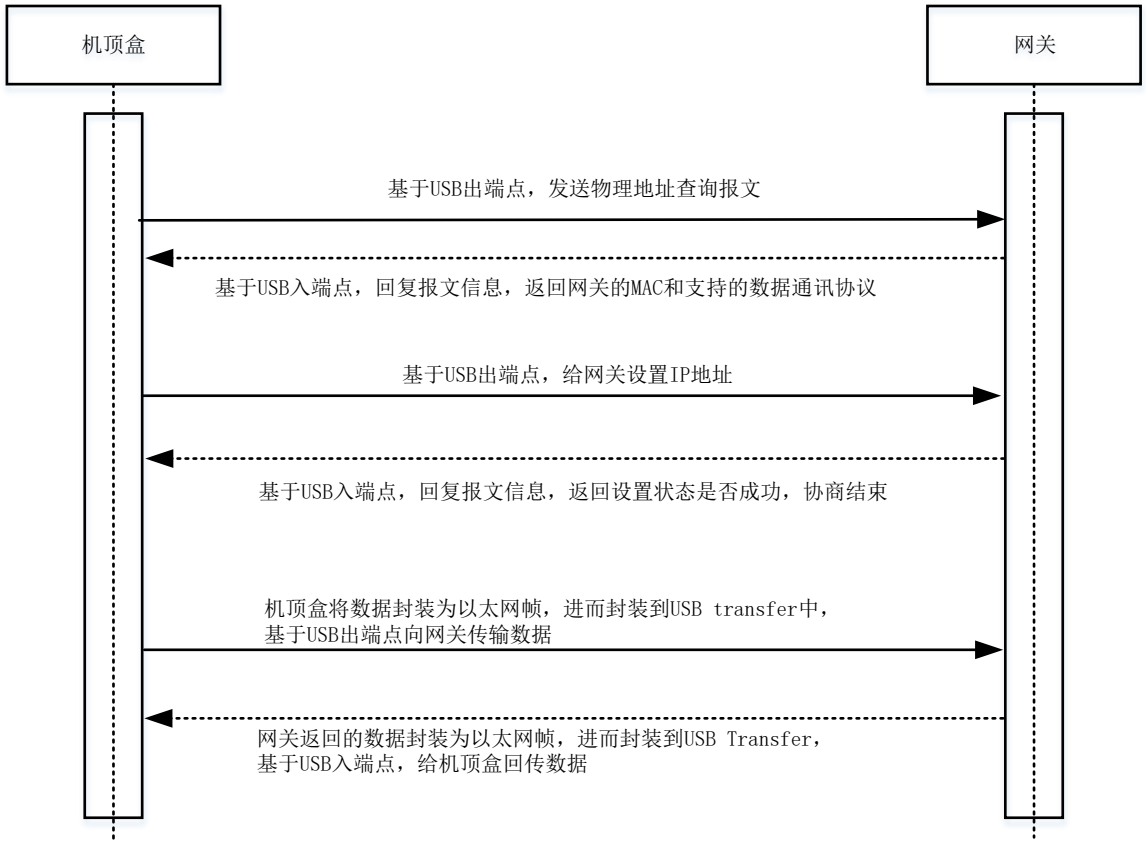


图7　基于 USB 的设备通信协商流程图

8.2　节目搜索

节目搜索流程图见图8，流程如下。

a) 机顶盒调用网关的资源申请接口（http://ip:port/reserve_resource），申请调谐器资源，并订阅需要收取的网关消息。
b) 机顶盒在资源申请成功后，创建 UDP 套接字，绑定端口，建立一个套接字接口通信通道，为后续数据接收做准备。
c) 机顶盒调用网关的锁频设置接口（http://ip:port/lock_delivery），指定要锁定的频点，并将 UDP 端口号通知到网关。
d) 机顶盒在频点锁定成功后，调用网关的 PID 过滤设置接口（http://ip:port/set_pids），设置过滤对应表的 PID。
e) 网关根据接口请求参数中的 PID 列表，从 TS 流中过滤出对应的数据包，并将其封装为 UDP 单播报文，发送到机顶盒提供的接收数据报文的 UDP 端口。
f) 机顶盒通过之前绑定的 UDP 接收数据端口，接收到对应表的 PID 报文数据。
g) 机顶盒将收取到的 PID 数据进行解析，生成频道列表相关数据保存到应用的存储目录下。
h) 机顶盒完成一个频点的节目搜索后，重新从头开始下一个频点的节目搜索过程，直到完成全部频点的节目搜索。

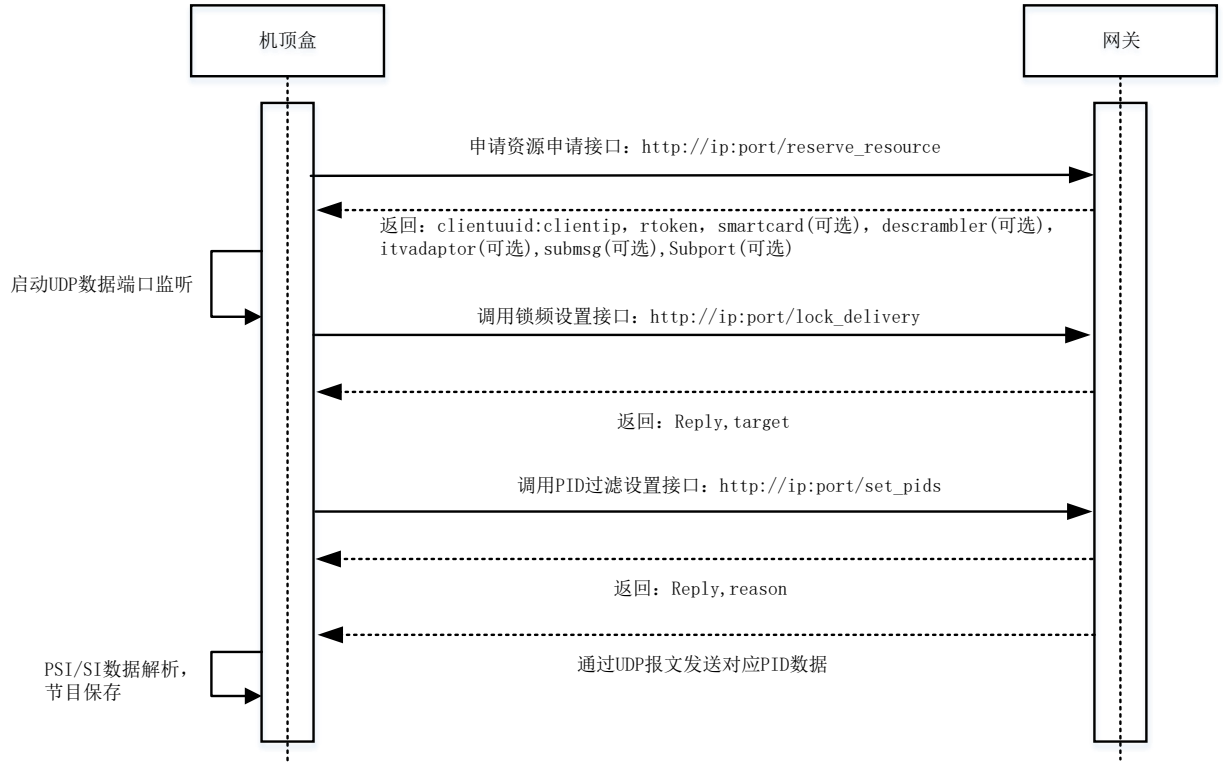


图8　节目搜索流程图

8.3　清流节目播放

清流节目播放流程图见图9，流程如下。

a) 机顶盒调用网关的资源申请接口（http://ip:port/reserve_resource），申请调谐器资源，并订阅需要收取的网关消息。
b) 机顶盒在资源申请成功后，创建 UDP 套接字，绑定端口，建立一个套接字接口通信通道，为后续数据接收做准备。
c) 机顶盒调用网关的锁频设置接口（http://ip:port/lock_delivery），指定要锁定的频点，并将 UDP 端口号通知到网关。
d) 机顶盒在频点锁定成功后，调用网关的 PID 过滤设置接口（http://ip:port/set_pids），设置过滤对应视频的音视频 PID。
e) 网关根据接口请求参数中的 PID 列表，从 TS 流中过滤出对应的数据包，并将其封装为 UDP 单播报文，发送到机顶盒提供的接收数据报文的 UDP 端口。
f) 机顶盒通过之前绑定的 UDP 接收数据端口，接收对应的视频流数据并进行播放。

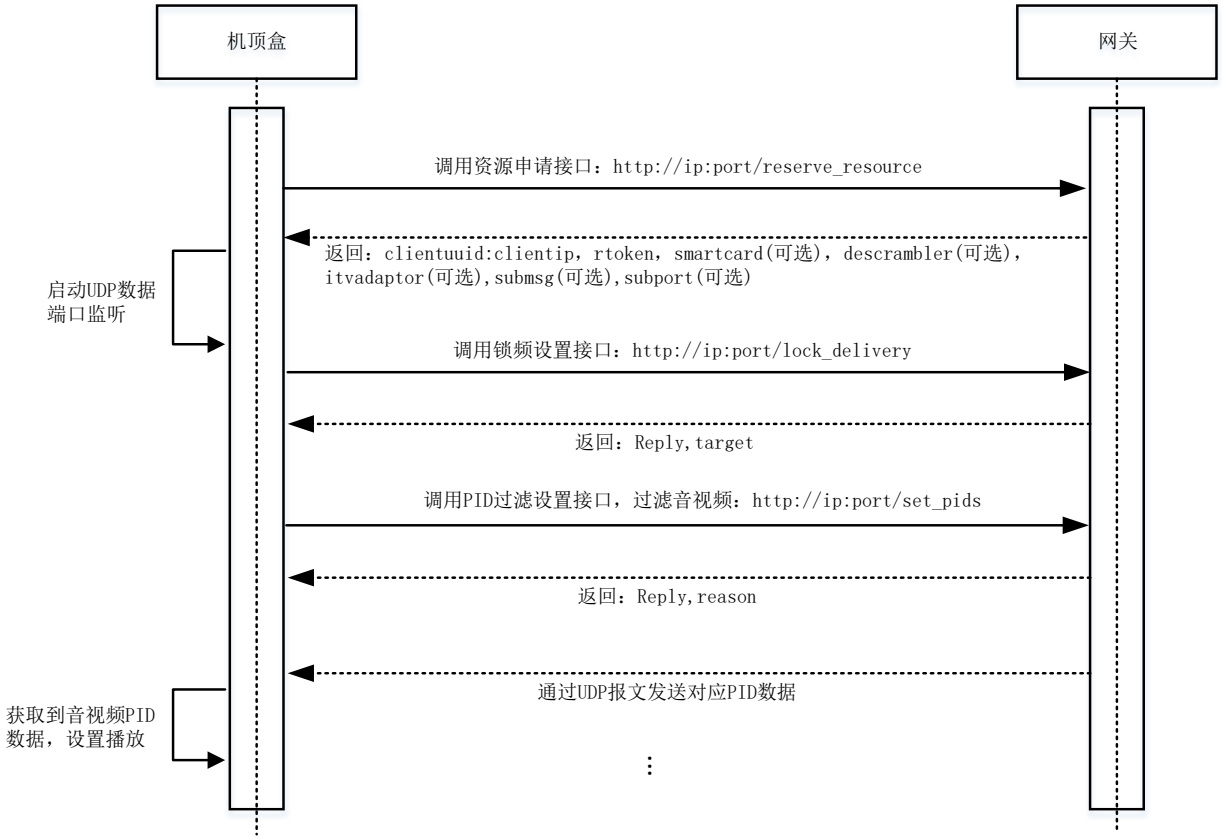


图9　清流节目播放流程图

8.4　加扰节目播放

加扰节目播放流程图见图10，流程如下。

a) 机顶盒调用网关的资源申请接口（http://ip:port/reserve_resource），申请调谐器、智能卡和解扰器资源，并订阅需要收取的网关消息。
b) 机顶盒在资源申请成功后，创建 UDP 套接字，绑定端口，建立一个套接字接口通信通道，为后续数据接收做准备。
c) 机顶盒调用网关的锁频设置接口（http://ip:port/lock_delivery），指定要锁定的频点，并将 UDP 端口号通知到网关。
d) 机顶盒在频点锁定成功后，调用网关的 PID 过滤设置接口（http://ip:port/set_pids），设置过滤对应视频的音视频 PID 和 ECM/EMM 表的 PID。
e) 网关根据接口请求参数中的 PID 列表，从 TS 流中过滤出对应的数据包，并将其封装为 UDP 单播报文，发送到机顶盒提供的接收数据报文的 UDP 端口。
f) 若采用机顶盒解扰模式，机顶盒接收到 UDP 报文后进行解扰、播放。若采用基于拆分库的网关解扰模式，应执行下述步骤：
    1) 机顶盒通过之前绑定的 UDP 接收数据端口，接收对应 PID 列表的 ECM/EMM 的报文数据；
    2) 机顶盒应用软件将收取到的 ECM/EMM 报文数据转发到机顶盒 CA 主模块。
    3) 机顶盒 CA 主模块通过网关提供的机卡通信接口，建立连接请求，通过 UDP 的通信通道，完成 EMM/ECM 数据交互。
    4) 网关 CA 子模块接收到 EMM/ECM 数据，基于 GB/T 16649.3 协议同智能卡进行交互，计算出 CW，设置到解扰器。
    5) 网关将解扰后的音视频流推送到机顶盒进行播放。

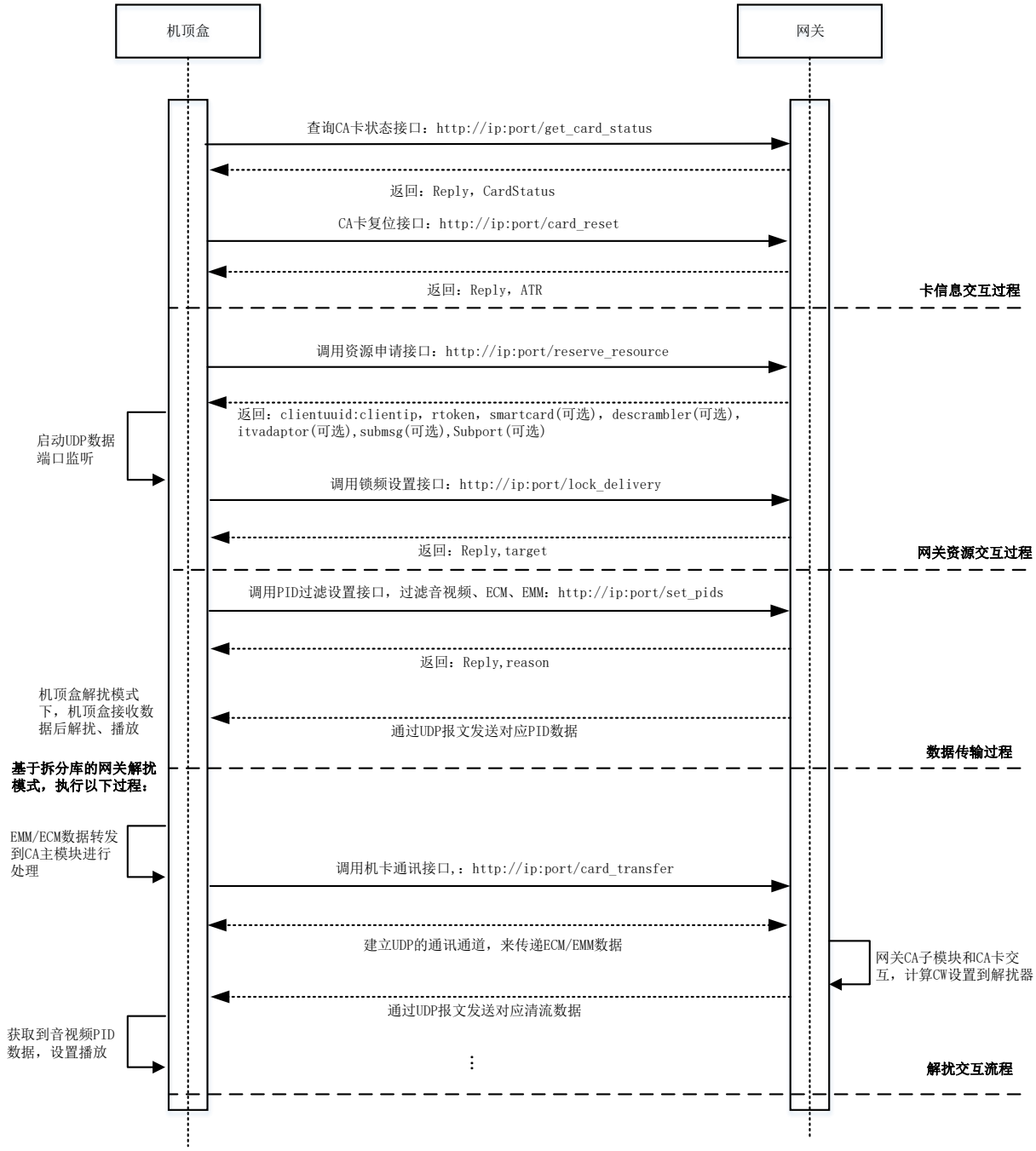


图10　加扰节目播放流程图

8.5　网关升级

机顶盒应负责获取网关的升级包并启动对网关的升级流程。根据网关升级包的获取来源，网关升级有两种方式，一种为在线升级，网关升级包由前端升级管理系统下发；一种为本地升级，网关升级包来自插入机顶盒USB接口的存储设备。对于在线升级，机顶盒可以通过单向广播通道或者双向网络通道获取到升级信息。

机顶盒通过单向广播通道对网关进行在线升级的流程图见图11，流程如下。

a)　机顶盒通过调用网关信息查询接口获取当前版本信息，并监听网关升级信息。

b)　机顶盒监听到网关升级信息后，调用 PID 过滤设置接口（http://ip:port/set_pids），获取与升级数据包相关的描述符数据。

c) 机顶盒根据升级描述符数据，解析升级数据包所在的频点和 PID。
d) 机顶盒根据解析出的频点信息，调用锁频接口（http://ip:port/lock_delivery），指定要锁定的频点，并将 UDP 端口号通知到网关。
e) 机顶盒在频点锁定成功后，调用 PID 过滤设置接口（http://ip:port/set_pids），设置过滤对应升级数据包的 PID。
f) 网关根据接口请求参数中的 PID 列表，从 TS 流中过滤出对应的数据包，并将其封装为 UDP 单播报文，发送到机顶盒提供的接收数据报文的 UDP 端口。
g) 机顶盒通过之前绑定的 UDP 接收数据端口，接收对应的升级数据文件，保存到盒端对应目录。
h) 机顶盒调用网关的设备管理接口（http://ip:port/device_ctrl），通知网关进行升级，并告知网关升级文件的目录地址。
i) 网关从机顶盒拉取升级文件，并进行升级。
j) 网关将升级状态通过消息发送给机顶盒。

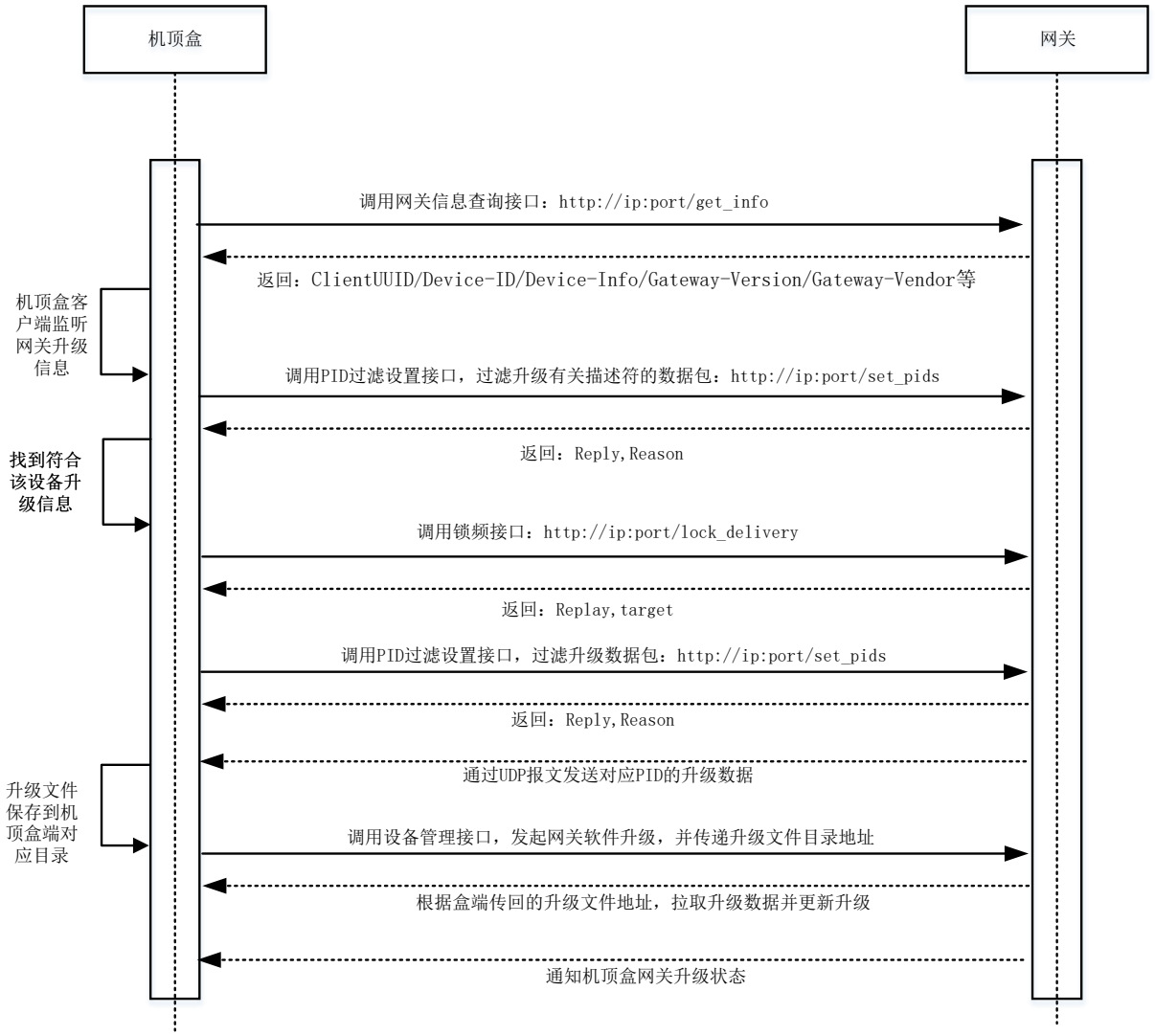


图11　通过单向广播通道对网关在线升级的流程图

机顶盒通过双向网络通道获取升级文件后，通过在线升级方式对网关升级的流程图见图12，流程如下。

a) 机顶盒通过双向网络通道从升级服务器下载了网关升级文件，并保存在机顶盒端对应目录。

b) 机顶盒调用网关的设备管理接口（http://ip:port/device_ctrl），通知网关进行升级，并告知升级文件目录地址。
c) 网关从机顶盒拉取升级文件，并进行升级。
d) 网关将升级状态通过消息发送到机顶盒。

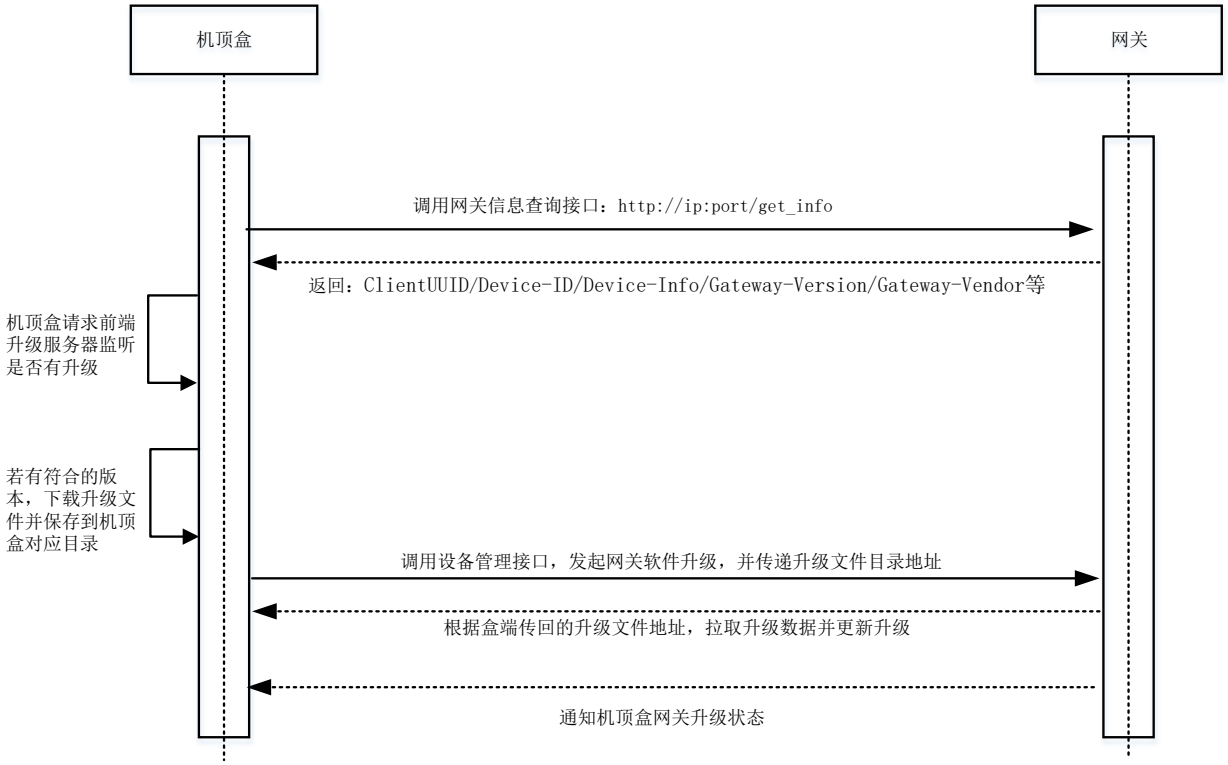


图12　机顶盒获取升级包后对网关在线升级的流程图

通过本地升级方式对网关升级的流程图见图 13，流程如下。

a) 机顶盒上插入 U 盘，U 盘根目录存放网关升级文件。
b) 机顶盒识别到升级文件后，调用网关信息查询接口查询当前网关设备信息，匹配上升级包，确认需要升级，则进入下一步。
c) 机顶盒调用网关的设备管理接口（http://ip:port/device_ctrl），通知网关进行升级，并告知升级文件目录地址。
d) 网关从机顶盒拉取升级文件，并进行升级。
e) 网关将升级状态通过消息发送到机顶盒。

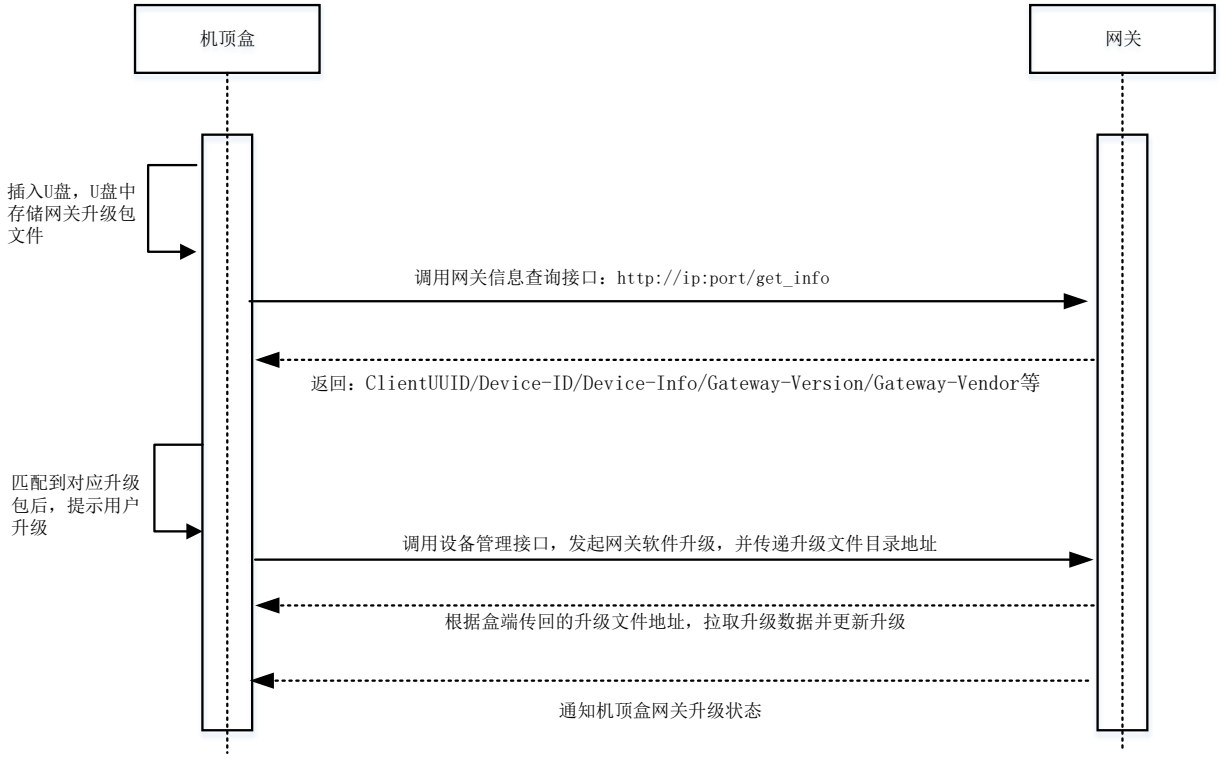


图13　网关本地升级流程图

附 录 A
（资料性）
条件接收

A.1 有卡 CA

A.1.1 概述

有卡CA指需要实体智能卡的条件接收系统，具体规定见GY/Z 175—2001。本附录给出了有卡CA的基于拆分库的网关解扰模式，主要特征如下。

——对 CA 模块进行了功能拆分，分为 CA 主模块和 CA 子模块。CA 主模块负责接收、解析和校验 ECM、EMM 数据，获取经过安全校验的 ECM/EMM APDU 指令；CA 子模块负责根据智能卡处理 ECM/EMM APDU 指令的输出进行解密得到 CW。

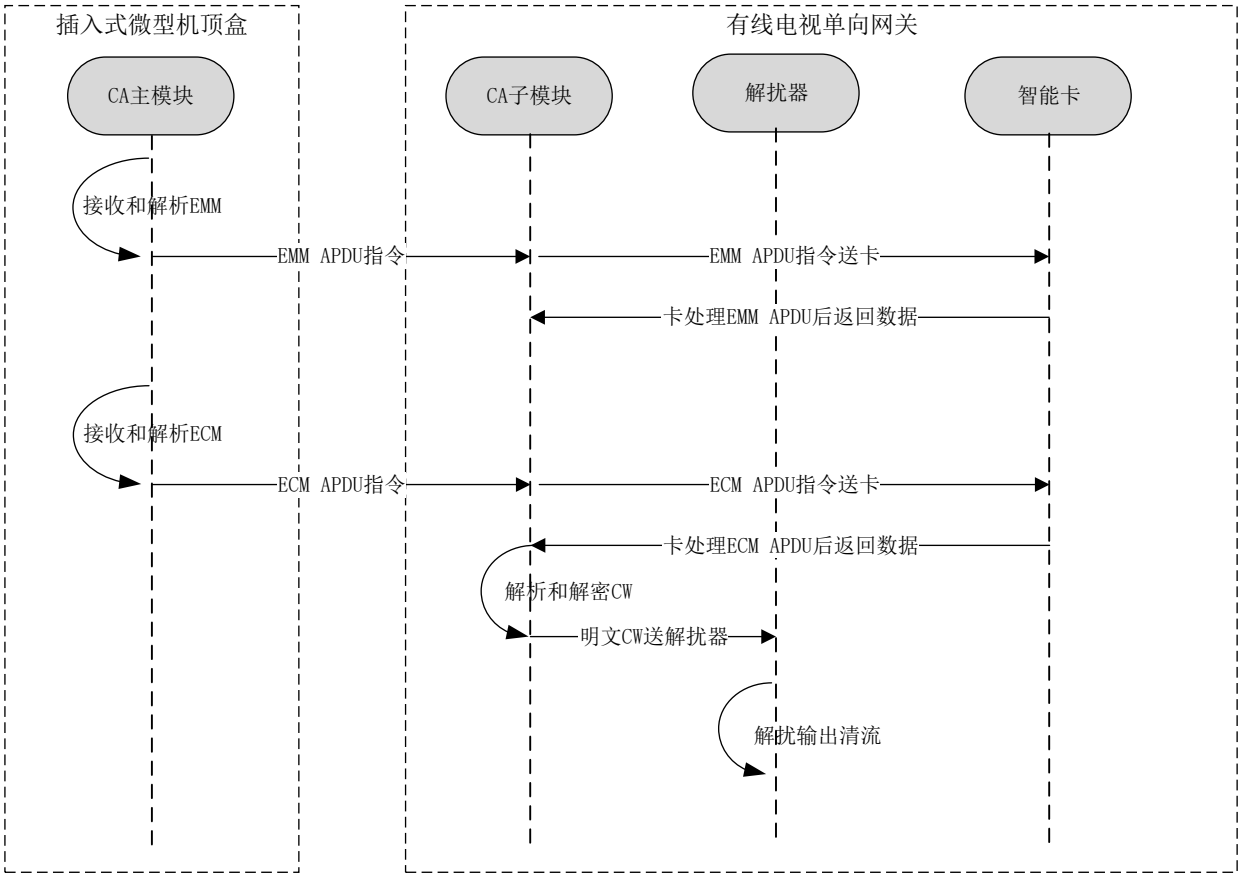
——条件接收与信号解扰功能的分离实现，即网关上插智能卡，集成 CA 子模块，实现广播信号的解调、解复用和解扰功能，同时，对 TS 数据的分析、SI 解释及与 CA 有关的 ECM/EMM 数据处理等由软件实现的功能则借助机顶盒的芯片能力实现。

在此方式下，机顶盒的CA主模块负责接收、解析和校验ECM、EMM数据，获取经过安全校验的ECM/EMM APDU指令；网关的CA智能卡处理ECM/EMM APDU指令并将输出提供给CA子模块，CA子模块解密得到CW，解扰模块根据控制字对加扰频道节目进行解扰。

A.1.2 交互流程

机顶盒和网关之间的 CA 交互流程见图 A.1，具体描述如下：

a) 机顶盒的 CA 主模块负责接收、校验和解析 EMM 数据，并以网络通信的方式（调用网关的服务接口）将解析出的 EMM APDU 指令送到网关 CA 子模块；
b) 网关 CA 子模块将 EMM APDU 指令送智能卡处理，并解析智能卡返回的数据；
c) 网关 CA 子模块将解析后的显示消息返回给 CA 主模块；
d) CA 主模块负责接收、校验和解析 ECM 数据，并以网络通信的方式将解析出的 ECM APDU 指令送到网关 CA 子模块；
e) 网关 CA 子模块解析 ECM APDU 指令并保存当前节目的频点和音视频传输的 PID，之后将 ECM APDU 指令送智能卡处理；
f) 网关 CA 子模块解析 ECM APDU 送卡后返回的数据，并解密 CW；
g) 网关 CA 子模块将明文 CW、当前节目的频点和音视频 PID 送解扰器接口；
h) 解扰器基于接收到的 CW 解扰输出清流。



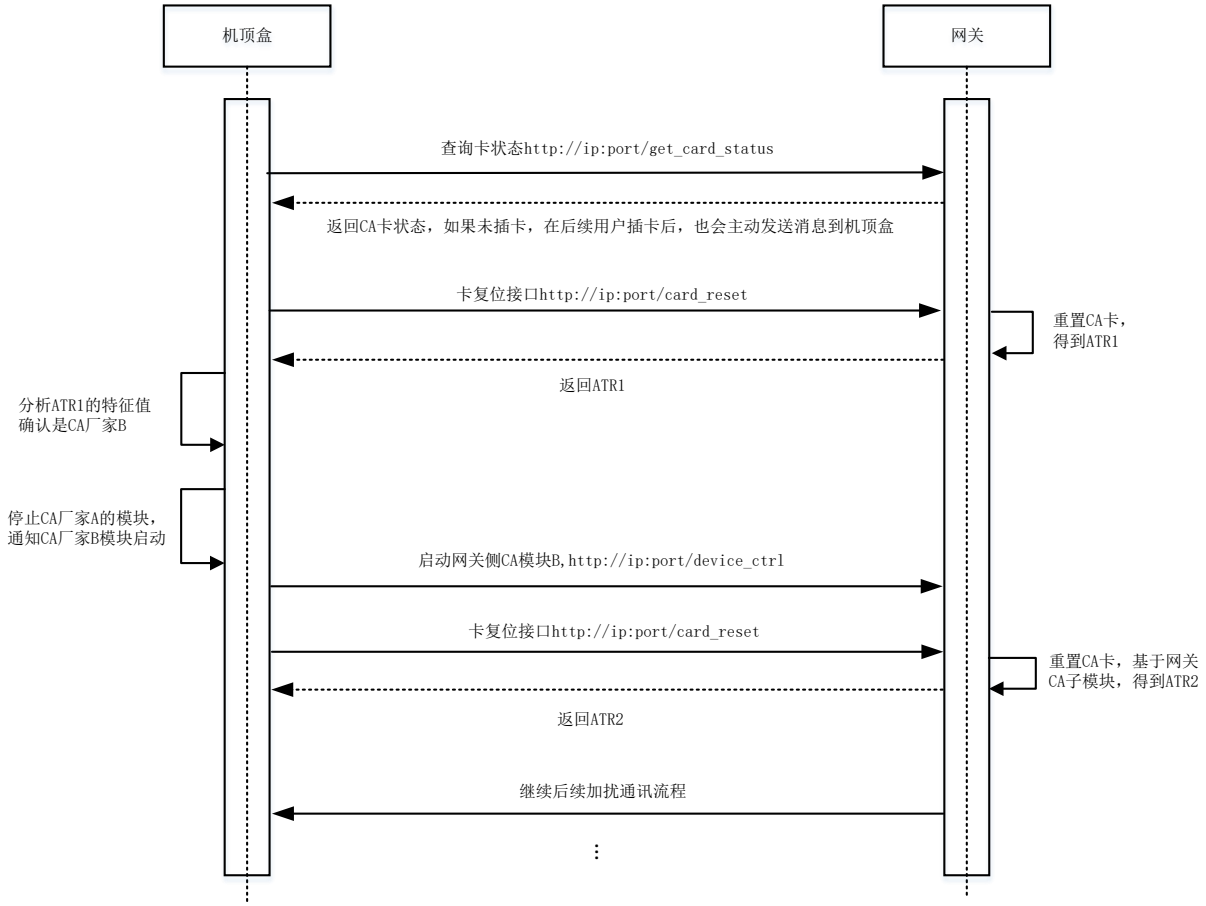
图A.1 机顶盒和网关之间的 CA 交互流程图

A.1.3 全国统一CA库

为了解决网关和机顶盒的通用化问题，本文件规定的有卡CA方案，应采用CA全国统一移植库的方式，终端只需集成一次即可全国通用。

A.1.4 CA启用流程

当机顶盒需要进行解扰节目播放时，或者网关存在智能卡插拔或者更换智能卡的情形时，均需要先启用CA，启用流程见图A.2。



图A.2 有卡 CA 启用流程图

A.2 无卡 CA

无卡CA指通过软件实现实体智能卡替代的条件接收系统，根据客户端软件的部署方式又可分为预先集成客户端软件的无卡CA系统和可下载客户端软件的DCAS系统。

预先集成客户端软件的无卡CA系统也可以采用与有卡CA类似的CA模块拆分方式，CA模块拆分为CA主模块和CA子模块。机顶盒集成CA主模块，负责接收、解析和校验ECM、EMM数据；网关集成CA子模块并具备解出CW能力，负责完成ECM、EMM数据处理、解密获取CW及数据解扰。机顶盒和网关双方通过调用本文件定义的相关接口实现CA有关指令数据的交互。

附 录 B
（规范性）
安全机制

B.1 概述

当机顶盒和网关之间支持任一安全功能时，两者在设备发现之后应立即执行设备认证功能。本文件中，设备认证功能的实现方式和密钥协商过程完全一致。设备认证完成后，机顶盒和网关双方获得的对称密钥，可用于安全通信模式和TS再加密。

若要启动安全通信模式，机顶盒根据协商的密钥，调用设备管理接口告知网关开启安全通信模式，之后可采用HTTP安全通信方式访问相关接口。

若要启动TS再加密，机顶盒根据协商的密钥，调用锁频接口告知网关启用TS再加密，之后网关应对解扰后的TS视频数据包进行TS再加密后再传送给机顶盒。

安全通信模式和TS再加密共用相同的对称密钥。当同时启动安全通信模式和TS再加密时，机顶盒和网关之间无需重复进行密钥协商。

B.2 设备认证

设备认证（密钥协商）的完整交互流程见图B.1。交互流程如下。

a) 机顶盒发起密钥协商，生成密钥对和对称密钥的 Key-ID。
b) 机顶盒调用通信密钥协商接口，传递密钥协商算法、公钥点坐标、对称密钥算法和对称密钥 Key-ID 等信息。
c) 网关生成密钥对，生成非对称共享密钥，并基于共享密钥通过 HDKF 算法派生出对称密钥算法的对称密钥 KS 和初始向量 IV，将他们与 Key-ID 进行关联；网关返回公钥点坐标。
d) 机顶盒生成非对称共享密钥，并基于共享密钥通过 HDKF 算法派生出对称密钥算法的对称密钥 KS 和初始向量 IV，将他们与 Key-ID 进行关联。
e) 机顶盒发起设备身份认证，生成随机数 R1，调用设备身份认证接口传递相关参数。
f) 网关根据 RMACT（“随机数 R1+网关 MAC 地址+验证口令 Token”）生成认证核对信息 D1，并生成随机数 R2，返回认证核对信息 D1 和随机数 R2。
g) 机顶盒核对认证信息 D1，根据 RMACT（“随机数 R2+网关 MAC 地址+验证口令 Token”）生成反向认证核对信息 D2，并调用设备身份认证接口将反向认证核对信息 D2 传送给网关。
h) 网关核对认证信息 D2，返回认证接口，完成双方身份认证。
i) 认证成功后，机顶盒和网关均保存对称密钥 KS、初始向量 IV 及对应的 Key-ID。

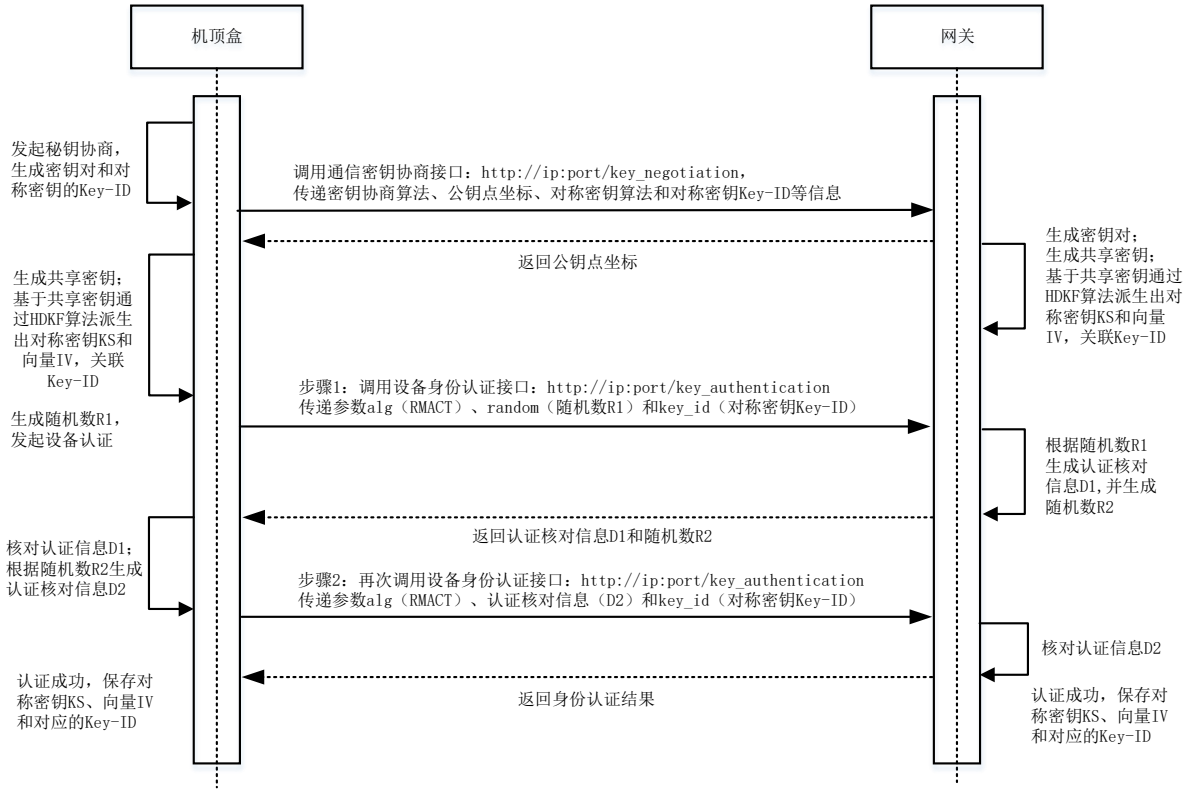


图 B.1　安全通信模式交互流程

B.3　安全通信模式

B.3.1　报文格式

在安全通信模式下，机顶盒应采用HTTP安全通信方式对资源申请接口、机卡通信接口和设备管理接口进行调用，此时应在HTTP的报文头部增加下列属性字段。

——GWSS-Tick：通过网关信息查询接口的 Tick 值同步给用户侧设备，一般为网关设备的开机计时滴答数基准加上当前系统时间偏移，用以防重放攻击，时间容差为正负 15s。

——GWSS-Key-ID：对称密钥的 Key-ID。

——GWSS-Random：发起 HTTP 安全通信请求时机顶盒生成的 32Byte 的随机字符串（a-zA-Z0-9），用于当次 HTTP 通信的签名。

——GWSS-SHA1：“HTTP 通信的 URL（HTTP Head)+负载数据”的 SHA1 消息摘要，再做 BASE64 编码得到。

——GWSS-Sign：本次通信的签名，计算过程如下：

1) 计算签名的明文 TX，通过 JOIN(GWSS-SHA1,GWSS-Random,GWSS-Tick)得到，其中 JOIN 函数表示按字节序列依次串接各参数内容。

2) 计算签名信息，通过协商的对称密钥算法对签名的明文 TX 进行加密得到，计算方法为 BASE64(AES128-CBC(KS,SHA256(TX))或者 BASE64(SM4-CBC(KS, SHA256(TX))。

采用HTTP安全通信方式调用资源申请接口的报文示例：

```
GET /lock_delivery?delivery=
DVB-C&freq=411000000.6875.64QAM&pids=0,1&userhandle=1&rtoken=a3cbda7162
&usertick=2312321&target=192.168.88.103:43221 HTTP/1.1\r\n
Host: 192.168.1.101\r\n
GWSS-Tick: 10998\r\n
GWSS-Key-ID: fd7a6d6e6af6e661723771\r\n
GWSS-Random: KFiehajfue123nasdfkj12ijfjakdfhe\r\n
GWSS-SHA1: UadfkeifaduyqYHBLFdkfwuefk243kjhf\r\n
```

```
GWSS-Sign: VWFkZmtlaWZhZHV5cVlIQkxGZGtmd3VlZmsyNDNramhm\r\n
Content-Length: 0\r\n
\r\n
```

在上述示例中，GWSS-SHA1是“/lock_delivery?delivery=DVB-C&freq=411000000.6875.64QAM&pids=0,1&userhandle=1&rtoken=a3cbda7162&usertick=2312321&target=192.168.88.103:43221”这一段的SHA1值(HTTP的负载为空)。

HTTP接口应答示例：

```
HTTP/1.1 200 OK\r\n
Host: 192.168.1.101\r\n
GWSS-Tick: 10998\r\n
GWSS-Random: BfefAEf8917384123Feade126eglgwdb\r\n
GWSS-SHA1: UadfkeifaduyqYHBLFdkfwuefk243kjhf\r\n
GWSS-Sign: Mkdfeiua98341luafo83ASDGAVASERAvdansjkerjha34123p8u56hs\r\n
Content-Length: 41\r\n
\r\n
Reply: ok
Target: 192.168.88.103:43221
```

应答中包括了回复时刻的时间滴答数GWSS-Tick、新生成的随机字符串GWSS-Random、负载的SHA1值GWSS-SHA1以及重新计算的签名数据GWSS-Sign，其算法保持与HTTP的请求一致，密钥也一致。

B.3.2 交互流程

安全通信模式的完整交互流程见图B.2，包括密钥协商过程和安全通信过程。交互流程如下。

a) 机顶盒与网关之间执行密钥协商过程，双方获取到对称密钥 KS，该过程与 B.2 设备认证流程相同；若机顶盒与网关已执行过密钥协商并保存了有效的对称密钥，则跳过此步骤。
b) 机顶盒调用设备管理接口，传递对称密钥 Key-ID，并启动安全通信模式。
c) 网关开启安全通信模式。
d) 机顶盒调用资源申请接口、机卡通信接口和设备管理接口时应采用 HTTP 安全通信方式。

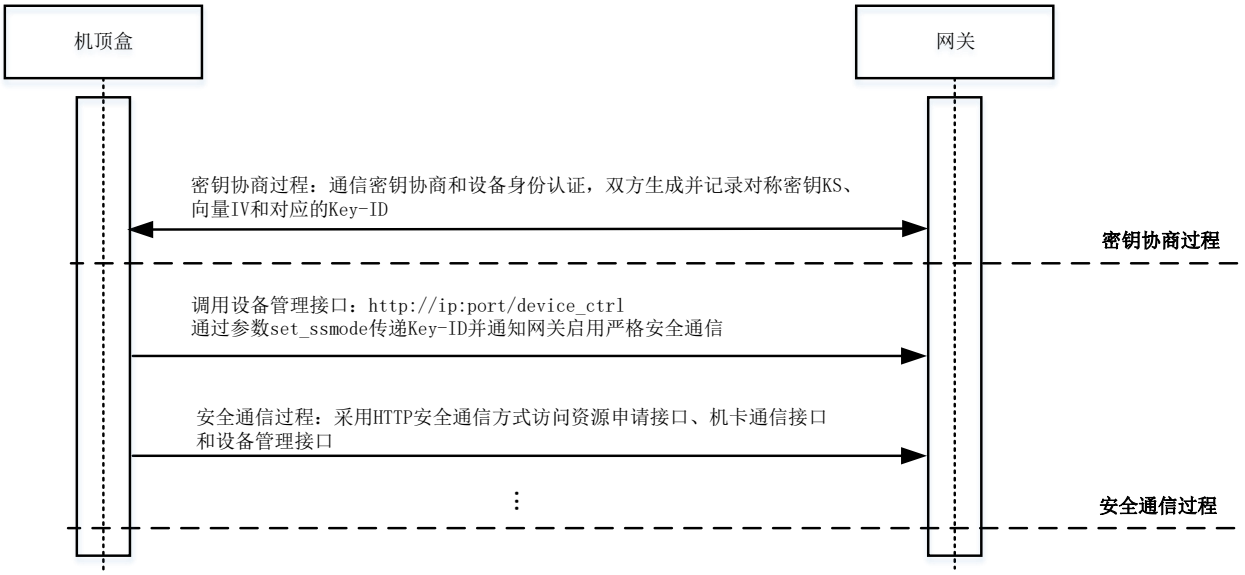


图 B.2 安全通信模式交互流程

在执行密钥协商过程前，机顶盒应调用设备管理接口，检查Key-ID是否有效：若Key-ID有效，则直接进入图B.1中的安全通信过程；若Key-ID无效，则需执行图B.2中的完整流程。

B.4 TS 再加密

B.4.1 加密算法

当网关具备对CA加扰流进行解扰的功能时，为避免网关向机顶盒发送清流数据，网关对解扰后的TS数据包进行再次加密，并将加密后的数据发送给机顶盒。TS再加密功能仅作用于TS包的净荷，即原本加扰并在网关上解扰的负载数据。机顶盒在每次锁频前更新TS再加密算法的密钥KT并在锁频时通过锁频接口传送给网关，至下一次锁频前密钥KT不做更换。

进行TS再加密时，TS包头的格式仍应符合GY/Z 175—2001中表I2的规定，其中TS包头中的transport_scrambling_control字段的意义，应符合表B.1的定义。

表 B.1 transport_scrambling_control 字段的意义

比特值	描述
00	TS包净荷不加密
01	预留将来使用
10	TS包用偶密钥加密，偶密钥为TS再加密算法的密钥KT
11	TS包用奇密钥加扰，奇密钥与偶密钥相同

对TS包的负载数据进行TS再加密应符合如下规定。

——根据 TS 包头信息计算得到负载内容的起始偏移量，确定负载内容的起始位置。

——从负载内容的起始位置开始，按照 TS 再加密算法的密钥算法的分组长度逐段截取负载数据进行加密。

——若最后剩余的负载数据长度小于密钥算法的分组长度，则保持明文不加密。

B.4.2 TS再加密流程

TS再加密的完整交互流程见图B.3，流程如下。

a) 机顶盒与网关之间执行密钥协商过程，双方获取到对称密钥 KS，该过程与 B.2 安全通信模式流程中的密钥协商过程相同；若机顶盒与网关已执行过密钥协商并保存了有效的对称密钥，则跳过此步骤。
b) 机顶盒生成用于 TS 再加密算法的密钥 KT，并通过协商的对称密钥 KS 对其进行加密。
c) 机顶盒调用锁频设置接口，将 TS 再加密的算法和加密后的密钥传递给网关，开启 TS 再加密。
d) 网关根据对称密钥 KS 解出密钥 KT，开启 TS 再加密。
e) 网关与机顶盒之间执行正常的 CA 解扰流程，与加扰节目播放中的 CA 解扰交互流程相同。
f) 网关解出清流节目数据后，利用 TS 再加密算法和密钥 KT 对清流节目数据进行 TS 再加密。
g) 网关将基于 KT 加密的 TS 再加密数据通过 UDP 报文发送给机顶盒。
h) 机顶盒基于 KT 密钥解密后进行播放。

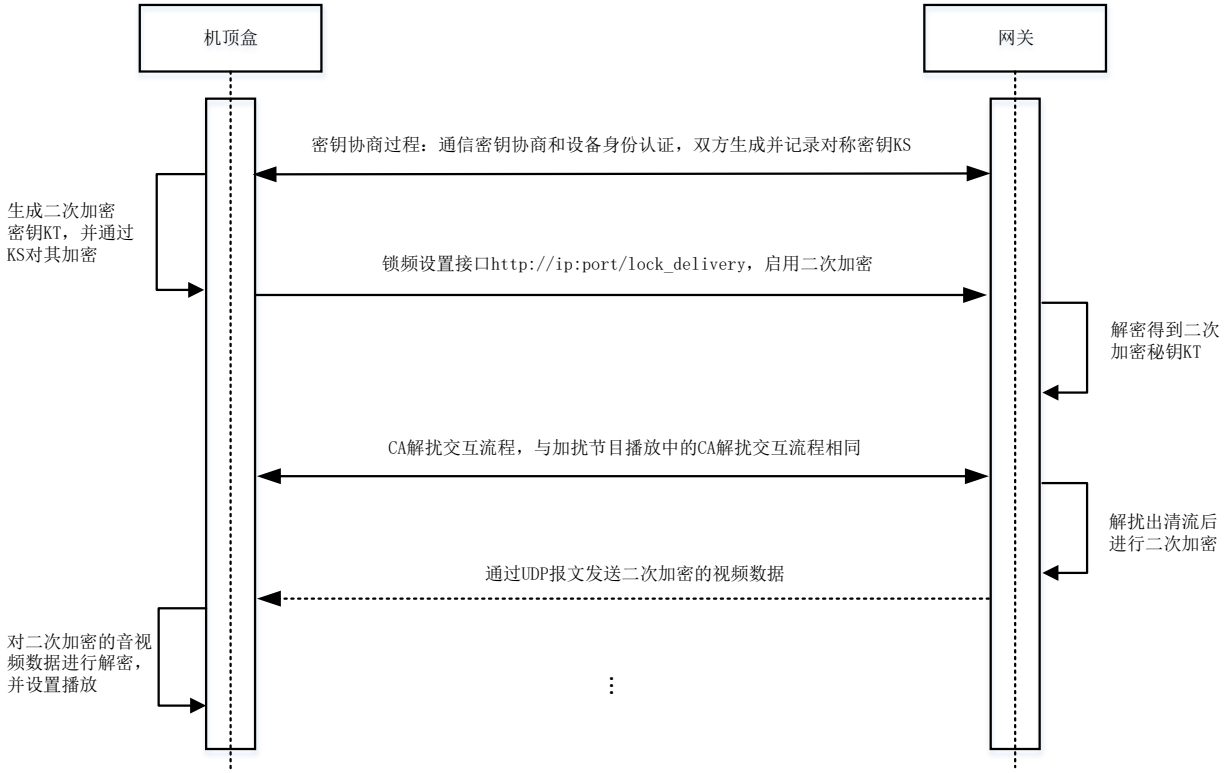


图 B.3　TS 再加密流程

在密钥协商之前，机顶盒应调用设备管理接口，检查Key-ID是否有效：若Key-ID有效，则直接在锁频时启用TS再加密过程；若Key-ID无效，则需执行图B.3中的完整流程。

参 考 文 献

[1] GB/T 16649.1—2006 识别卡 带触点的集成电路卡 第1部分：物理特性
[2] GB/T 16649.2—2006 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置
[3] GB/T 16649.3—2006 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议
[4] GB/T 17975.1—2010 信息技术 运动图像及其伴音信息的通用编码 第1部分：系统
[5] GB/T 28161—2011 数字电视广播业务信息规范
[6] GB/T 32907—2016 信息安全技术 SM4分组密码算法
[7] IEEE 802.1Q-2022 IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks
[8] IEEE 802.3-2022 IEEE Standard for Ethernet
[9] RFC 4648 The Base16, Base32, and Base64 Data Encodings
[10] RFC 5869 HMAC-based Extract-and-Expand Key Derivation Function (HKDF)
[11] RFC 6234 US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)
[12] RFC 7748 Elliptic Curves for Security
[13] NIST FIPS 197-upd1 Advanced Encryption Standard (AES)
[14] UPnP Device Architecture 2.0
[15] Universal Serial Bus Specification, Revision 2.0
[16] Universal Serial Bus 3.2 Specification, Revision 1.1