(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110830333 A
(43)申请公布日 2020.02.21

(21)申请号 201810903670.2

(22)申请日 2018.08.09

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 邬立保 王玲 景思淋

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 王韬

(51)Int.Cl.
H04L 12/28(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)

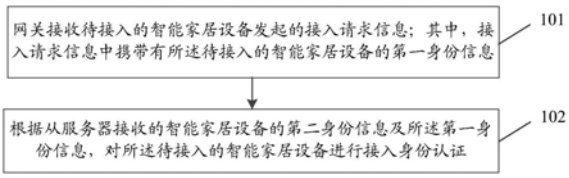
权利要求书2页 说明书21页 附图4页

(54)发明名称

智能家居设备接入认证方法、装置、网关及存储介质

(57)摘要

本发明实施例公开了一种智能家居设备接入认证方法，所述方法包括：网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。本发明实施例还公开了一种智能家居设备接入认证装置、网关及计算机存储介质。



CN 110830333 A

1.一种智能家居设备接入认证方法,其特征在于,所述方法包括:

网关接收待接入的智能家居设备发起的接入请求信息;其中,所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息;

根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息,对所述待接入的智能家居设备进行接入身份认证。

2.根据权利要求1所述的方法,其特征在于,所述根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息,对所述待接入的智能家居设备进行接入身份认证之前,所述方法还包括:

从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息;

根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息,对所述待接入的智能家居设备进行类型匹配认证。

3.根据权利要求2所述的方法,其特征在于,所述方法还包括:

当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配,且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时,则从智能家居设备的地址池中分配网络协议IP地址给所述待接入的智能家居设备。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

根据接收到的所述待接入的智能家居设备发起的接入请求信息,确定出待接入的智能家居设备的第一业务类型信息;

根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息,为所述网关分配相应的业务类型控制信息。

5.根据权利要求4所述的方法,其特征在于,所述第一业务类型信息包括:网络访问业务信息;

所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息,为所述网关分配相应的业务类型控制信息,包括:

比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息,若所述第二业务类型信息中携带有网络访问业务信息,则为所述网关分配网络访问的路由控制信息。

6.根据权利要求4所述的方法,其特征在于,所述第一业务类型信息包括:网络访问业务信息;

所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息,为所述网关分配相应的业务类型控制信息,包括:

比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息,若所述第二业务信息中未携带有网络访问业务信息,则为所述网关分配默认的路由控制信息。

7.根据权利要求2所述方法,其特征在于,所述方法还包括:

当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配,且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时,接收所述待接入的智能家居设备发送的第一身

份信息；

将所述第一身份信息上报至服务器。

8.一种智能家居设备接入认证装置，其特征在于，所述装置包括：接收模块和认证模块；

所述接收模块，用于接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求消息中携带有所述待接入的智能家居设备的第一身份信息；

所述认证模块，用于根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

9.一种网关，其特征在于，包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，其中所述处理器用于运行所述计算机程序时，实现权利要求1至7任一项所述的智能家居设备接入认证方法。

10.一种计算机存储介质，其特征在于，存储有可执行程序，所述可执行程序被处理器执行时，实现如权利要求1至7中任一项所述的智能家居设备接入认证方法。

智能家居设备接入认证方法、装置、网关及存储介质

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种智能家居设备接入认证方法、装置、网关及计算机存储介质。

背景技术

[0002] 随着通信技术的日益发展，智能家居的概念已经深入人心，且智能家居设备也迅速得到普及，例如最常见的数字电视，现在几乎家家户户都在使用，而目前，智能家居设备可能需要与对应的服务器进行认证，通过认证之后才可以从服务器获得对应的服务。以数字电视为例，与数字电视连接的机顶盒需要通过与服务器的认证才能获得服务器提供的视频服务。但是目前发现，智能家居设备的认证效率低；若认证效率低则进一步会延迟智能家居设备接入到对应服务器获得服务。

发明内容

[0003] 本发明实施例提供了一种智能家居设备接入认证方法、装置、网关及计算机存储介质。

[0004] 本发明实施例的技术方案是这样实现的：

[0005] 本发明实施例提供了一种智能家居设备接入认证方法，所述方法包括：

[0006] 网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；

[0007] 根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

[0008] 上述方案中，所述根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证之前，所述方法还包括：

[0009] 从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息；

[0010] 根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证。

[0011] 上述方案中，所述方法还包括：

[0012] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时，则从智能家居设备的地址池中分配网络协议IP地址给所述待接入的智能家居设备。

[0013] 上述方案中，所述方法还包括：

[0014] 根据接收到的所述待接入的智能家居设备发起的接入请求信息，确定出待接入的智能家居设备的第一业务类型信息；

[0015] 根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息。

[0016] 上述方案中，所述第一业务类型信息包括：网络访问业务信息；

[0017] 所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，包括：

[0018] 比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中携带有网络访问业务信息，则为所述网关分配网络访问的路由控制信息。

[0019] 上述方案中，所述第一业务类型信息包括：网络访问业务信息；

[0020] 所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，包括：

[0021] 比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务信息中未携带有网络访问业务信息，则为所述网关分配默认的路由控制信息。

[0022] 上述方案中，所述方法还包括：

[0023] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，接收所述待接入的智能家居设备发送的第一身份信息；

[0024] 将所述第一身份信息上报至服务器。

[0025] 本发明实施例提供了一种智能家居设备接入认证装置，所述装置包括：接收模块和认证模块；

[0026] 所述接收模块，用于接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求消息中携带有所述待接入的智能家居设备的第一身份信息；

[0027] 所述认证模块，用于根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

[0028] 本发明实施例还提供一种网关，包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，其中所述处理器用于运行所述计算机程序时，实现如上述所述的智能家居设备接入认证方法。

[0029] 本发明实施例还提供一种计算机存储介质，存储有可执行程序，所述可执行程序被处理器执行时，实现如上述所述的智能家居设备接入认证方法。

[0030] 上述实施例所提供的智能家居设备接入认证方法、装置、网关及计算存储介质，网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。由此，本发明实施例中由智能家居设备接入到网络的网关将所述第一身份信息与所述第二身份信息进行比对验证，就能直接在本地完成身份验证，可以减少触发身份验证的接入请求信息需要转发到对应的服务器才能进行验证的转发次数，减少了该接入请求信息发送到服务器再启动验证的时间差，从而提前了验证，相对于用户而言相当于提升了验证效率。另一方面，由各家居智能设备所连接的网关进行验证，相比较于由对应的服务器集中进行验证，实现了身份验证的分布式处理，避免了集中服务器验证导致的验证量大，因为验证量大进一步导

致的验证效率低的问题，从而提升了身份验证的效率，并由于身份验证效率高，减少了接入服务器和获取服务器提供的服务的延时。

附图说明

[0031] 图1为本发明实施例一所提供的智能家居设备接入方法的流程示意图；

[0032] 图2为本发明实施例二所提供的智能家居设备接入认证方法的流程示意图；

[0033] 图3为本发明实施例三所提供的机顶盒参数配置的具体流程示意图；

[0034] 图4为本发明实施例三所提供的家庭网关实现机顶盒接入认证的具体流程示意图；

[0035] 图5为本发明实施例三所提供的网关IPTV路由方式下机顶盒业务路由转发控制的具体流程示意图；

[0036] 图6为本发明实施例三所提供的IPTV桥接方式下机顶盒接入认证的具体流程示意图；

[0037] 图7为本发明实施例一所提供的智能家居设备接入认证装置功能结构示意图；

[0038] 图8为本发明实施例所提供的网关的硬件结构示意图。

具体实施方式

[0039] 本发明实施例提供一种智能家居设备接入认证方法，通过利用网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；并根据网关事先从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。由此，本发明实施例中由智能家居设备接入到网络的网关将所述第一身份信息与所述第二身份信息进行比对验证，就能直接在本地完成身份验证，可以减少触发身份认证的接入请求需要转发到对应的服务器才能进行验证的转发次数，减少了该接入请求信息发送到服务器并启动验证的时间差，从而提前了验证，相对于用户而言相当于提升了验证效率。另一方面，由各智能家居设备所连接的网关进行验证，相比较于由对应的服务器集中进行验证，实现了身份验证的分布式处理，避免了集中服务器验证导致的验证量大，因为验证量大进一步导致的验证效率低的问题，从而提升了身份验证的效率，并由于身份验证效率高，减少了接入服务器和获取服务器提供的服务的延时。

[0040] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明，应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0041] 除非另有定义，本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在本发明的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本发明。本文所使用的术语“和/或”包括一个或多个相关的所列项目的任意的和所有的组合。

[0042] 以下结合说明书附图及具体实施例对本发明技术方案做进一步的详细阐述。

[0043] 实施例一：

[0044] 图1为本发明实施例一所提供的智能家居设备接入认证方法的流程示意图，如图1所示，所述智能家居设备接入认证方法包括以下步骤：

[0045] 步骤101:网关接收待接入的智能家居设备发起的接入请求信息;其中接入请求信息中携带有所述待接入的智能家居设备的第一身份信息。

[0046] 所述接入请求信息,可以是当智能家居设备与网关有线连接,并在智能家居设备上电时,由智能家居设备向所述网关发送的接入请求消息,也就是说智能家居设备上电即请求其加入当前连接的网关,且在网关上电时,网关接收所述智能家居设备发起的接入请求信息。当然,在一些实施例中,所述智能家居设备与所述网关的连接方式还可以是无线连接的方式,例如蓝牙、红外、NFC(Near Field Communication,近距离无线通信技术)或局域网(如WiFi)连接等方式。

[0047] 这里,所述第一身份信息包括待接入的智能家居设备的用户名、密码等身份信息,甚至还包括智能家居设备的加密方式信息等。

[0048] 需要说明的是,所述网关是指智能家居设备,也就是客户端一侧的网关,是将智能家居设备与服务器进行连接的连接器或协议转换器,所述网关内部各种终端通过其用户侧接口与智能家居设备进行通信,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服务器,例如业务平台、应用管理平台等进行交互,实现网关与外部网络的通信,提供各种可管理、可控制的应用。例如,网关可以是各种连接互联网或者移动网络的接入设备,例如,路由器。所述智能家居设备包括具有一定信息处理能力的电器设备,例如,可包括:智能冰箱、智能空调、智能电灯、智能电视等。

[0049] 步骤102:根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息,对所述待接入的智能家居设备进行接入身份认证。

[0050] 这里,所述从服务器接收的智能家居设备的第二身份信息,可以是服务器预先下发所述网关支持的智能家居设备的第二身份信息,这里,所述步骤101之前,所述网关在服务器上进行了注册并认证,具体地,网关预先向服务器上报所述网关支持的所述智能家居设备,服务器通过认证后,向网关发送所述智能家居设备的第二身份信息,网关接收到所述第二身份信息,并将所述第二身份信息存储在本地,用于后续接入智能家居设备的直接进行身份认证;还可以是,所述网关接收到所述接入请求信息后向服务器发出获取第二身份信息的请求,再由服务器向所述网关发送第二身份信息。

[0051] 这里,所述第二身份信息包括:网关存储的所述智能家居设备的用户名、密码和/或加密方式。具体地,网关从所述接入请求信息中确定出第一身份信息,所述网关接收到所述待接入的智能家居设备的接入请求后,根据从存储在网关本地的第二身份信息及所述第一身份信息,对所述带接入的智能家居设备进行接入身份认证,包括:将所述接入请求中确定出的所述待接入请求的智能家居设备的用户名、密码和/或加密方式分别与存储在网关本地的智能家居设备的用户名、密码和/或加密方式进行匹配,若匹配一致,则所述待接入的智能家居设备身份认证成功。

[0052] 需要补充的是,网关从服务器中获取的第二身份信息,也就是从服务器中获取的智能家居设备的用户名、密码等信息,可以是由用户通过移动终端的应用对其绑定的所述待接入的智能家居设备的用户名、密码进行配置后上传到服务器的;还可以是用户通过在待接入的智能家居设备上对其用户名、密码进行配置后上传至服务器的。

[0053] 另外,所述的加密方式是指由网关与智能家居设备预先协商好的,或网关已知的可支持的加密算法,并在网关接收到所述待接入的智能家居设备的接入请求信息时,先进

行加密方式的解码后再与待接入的智能家居的加密方式的匹配。

[0054] 基于实施例一的方法，本发明还提供了另一实施例，在另一实施例中，所述接入请求信息还包括：待接入的智能家居设备的设备类型信息；所述步骤102，根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证之前，还包括：从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息；根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证。

[0055] 这里，所述第一设备类型信息，包括：待接入的智能家居设备的型号标识；所述第二设备类型信息，包括：所述网关存储的可支持的智能家居设备的型号标识。具体地，所述根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证，包括：将所述接入请求中确定出的所述待接入的智能家居设备的型号标识与存储在网关存储的智能家居设备的型号标识进行匹配，若匹配成功，则所述待接入的智能家居设备的类型匹配成功。需要说明的是，这里的型号标识可以是智能家居设备出厂时被标记的型号标识，也可以是由针对不同类型的智能家居设备设置的型号标识。所述第一设备类型信息，不仅包括型号标识，还可以是包括类别标识等其他用于区别每一个智能家居设备的标识信息。其中，型号标识可以用来标识设备型号，类别标识可以用来标识设备类别。

[0056] 进一步地，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时，则从智能家居设备的地址池中分配IP(Internet Protocol，网络协议)地址给所述待接入的智能家居设备。

[0057] 需要说明的是，在本实施例中，所述网关在接收所述待接入的智能家居设备的接入请求信息时，会先对所述待接入的智能家居设备的设备类型信息进行验证，只有在设备类型是属于所述网关所支持的设备类型时才会对所述待接入的智能家居设备进行身份验证。这里，所述网关先确定出所述接入请求信息的第一类型信息，并对第一类型信息进行匹配认证，认证成功后再确定出所述接入请求信息的第一身份信息，并对第一身份信息进行身份匹配认证。这样，可以直接过滤掉对不支持的家居智能设备进行身份认证的过程，减轻后续不必要的身份信息匹配，从而减少网关的负荷。当然，在另一实施例中，所述第一类型信息和第一身份信息可以同时确定出来，但在进行认证匹配时，先进行第一类型信息的匹配认证，所述第一类型信息匹配认证成功后，再进行第一身份信息的匹配认证。这样，也可以过滤掉对不支持的家居智能设备进行身份认证的过程，减轻后续不必要的身份信息匹配，从而减少网关的负荷。

[0058] 进一步地，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息不匹配时，所述网关可以忽视或直接丢弃所述接入请求信息，和/或给所述待接入的智能家居设备反馈类型认证失败的消息。

[0059] 进一步地，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，所述网关也可以忽视或直接丢弃所述接入请求信息，和/或给所述待接入的智能家居设备反馈身份认证失败消息。

[0060] 进一步地，在一可选的实施例中，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，所述网关接收所述待接入的智能家居设备发送的第一身份信息；并将所述第一身份信息上报至服务器。如此，便于服务器对新的身份信息进行开通和维护。如果需要将该智能家居设备接入所述网关中，所述网关可以将该智能家居设备的身份信息发给服务器进行认证，服务器认证成功，还可以将该智能家居的第一身份信息下发给所述网关，所述网关对该智能家居设备的第一身份信息进行存储，这样，该智能家居设备第二次接入时即可直接由网关调用该智能家居设备的第一身份信息，并对该智能家居设备进行本地的身份认证。

[0061] 例如，所述智能家居设备为智能冰箱，所述网关在接收到所述智能冰箱的接入请求信息后，先确定出接入请求信息中第一类型信息，也就是待接入的智能冰箱的类型信息，其中，类型信息包括：智能家居设备的类别标识、型号标识等信息，若网关中未存储有该智能冰箱这一类别、或该智能冰箱的型号，则该智能冰箱类型匹配失败。相应地，若网关中存储有该智能冰箱这一类别、或该智能冰箱的型号，则该智能冰箱类型匹配成功。进一步地，在智能冰箱类型匹配成功后，再按照所述步骤102对智能冰箱进行身份认证，也就是对从服务器接收的智能家居设备的第二身份信息及所述智能冰箱的第一身份信息进行匹配，若匹配成功，则允许所述智能冰箱接入所述网关。

[0062] 本发明实施例提供一种智能家居设备接入认证方法，通过利用网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；并根据网关事先从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。由此，本发明实施例中由智能家居设备接入到网关的网关将所述第一身份信息与所述第二身份信息进行比对验证，就能直接在本地完成身份验证，可以减少触发验证身份认证的接入请求需要转到对应的服务器才能进行验证的转发次数，减少了该接入请求信息发送到服务器并启动验证的时间差，从而提前量验证，相对于用户而言相当于提升了验证效率。另一方面，由各智能家居设备所连接的网关进行验证，相比较于由对应的服务器集中进行验证，实现了身份验证的分布式处理，避免了集中服务器验证导致的验证量大，因为验证量大进一步导致的验证效率第的问题，从而提升了身份验证的效率，并由于身份验证效率高，减少了接入服务器和获取服务器提供的服务的延时。另外，本实施例还提出了在对待接入的智能家居设备进行身份认证之前先对待接入的智能家居设备进行设备类型认证，只有在设备类型认证成功的情况下才进行身份认证，如此，可以过滤掉对不支持的家居智能设备进行身份认证的过程，减轻后续不必要的身份信息匹配，从而减少网关的负荷。

[0063] 实施例二：

[0064] 图2为本发明实施例二所提供的智能家居设备接入认证方法的流程示意图，如图2所示，所述智能家居设备接入认证方法包括以下步骤：

[0065] 步骤201：智能家居设备发起接入请求信息至网关。

[0066] 这里，需要说明的是，在网关接收所述待接入智能家居设备发起的接入请求信息之前，服务器预先下发网关支持的智能家居设备的第二设备类型信息、第二身份信息及第二业务类型信息。所述网关对所述智能家居设备的第二设备类型信息、第二身份信息及第

二业务类型信息进行保存。

[0067] 步骤202:网关从所述接入请求信息中确定出第一设备类型信息,并根据第一设备类型信息及第二设备类型信息,对智能家居设备进行类型匹配认证。

[0068] 这里,所述第一设备类型信息,包括:待接入的智能家居设备的型号标识;所述第二设备类型信息,包括:所述网关存储的可支持的智能家居设备的型号标识。具体地,所述根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息,对所述待接入的智能家居设备进行类型匹配认证,包括:将所述接入请求中确定出的所述待接入请求的智能家居设备的型号标识与存储在网关本地的智能家居设备的型号标识进行匹配,若匹配成功,则所述待接入的智能家居设备的类型匹配认证成功。需要说明的是,这里的型号标识可以是由智能家居设备出厂时所标记的型号标识,也可以是由针对不同类型的智能家居设备设置的型号标识。所述第一设备类型信息,不仅包括型号标识,还可以是包括类别标识等其他用于区别每一个智能家居设备的标识信息,例如设备厂商名称、MAC地址等。

[0069] 需要补充的是,若类型匹配认证失败,网关允许经过一定次数的重试,如果重试仍失败,则网关记录为未认证通过的智能家居设备,限制其接入并通过网关接口(如:网关的中间件DBUS接口)通知服务器(如:家庭网关云平台),上报当前待接入的智能家居设备的类型为未认证通过的智能家居设备的类型,以便后续通过服务器对新接入的智能家居设备的开通和维护。若类型匹配成功,则执行步骤203。

[0070] 所述步骤203:网关从所述接入请求信息中确定出所述第一身份信息,并根据所述第一身份信息及第二身份信息,对智能家居设备进行接入身份认证。

[0071] 这里,所述第一身份信息包括待接入的智能家居设备的用户名、密码等身份信息,甚至还包括智能家居设备的加密方式信息或加密算法信息等。所述第二身份信息包括:网关存储的所述智能家居设备的用户名、密码和/或加密方式。具体地,网关从所述接入请求信息中确定出第一身份信息,所述网关接收到所述待接入的智能家居设备的接入请求后,根据从存储在网关本地的第二身份信息及所述第一身份信息,对所述带接入的智能家居设备进行接入身份认证,包括:将所述接入请求中确定出的所述待接入请求的智能家居设备的用户名、密码和/或加密方式分别与存储在网关本地的智能家居设备的用户名、密码和/或加密方式进行匹配,若匹配成功,则所述待接入的智能家居设备身份认证成功。

[0072] 步骤204:若设备类型信息与身份信息均认证成功,网关则下发智能家居设备的IP地址至智能家居设备。

[0073] 需要说明的是,所述网关在接收所述待接入的智能家居设备的接入请求信息时,会先对所述待接入的智能家居设备的设备类型信息进行验证,只有在设备类型是属于所述网关所支持的设备类型时才会对所述待接入的智能家居设备进行身份验证。这里,所述若设备类型信息与身份信息均认证成功,可以理解为所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型匹配,且待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配。这里,所述网关先确定出所述接入请求信息的第一类型信息,并对第一类型信息进行匹配认证,认证成功后再确定出所述接入请求信息的第一身份信息,并对第一身份信息进行身份匹配认证。当然,在另一实施例中,所述第一类型信息和第一身份信息可以同时确定出来,但在进行认证匹配时,先进行第一类型信息的匹配认证,所述第一类型信息匹配认证成功后,再进行第一身

份信息的匹配认证。这样，可以过滤掉对不支持的家居智能设备进行身份认证的过程，减轻网关的负荷。

[0074] 进一步地，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息不匹配时，所述网关可以忽视或直接丢弃所述接入请求信息，和/或给所述待接入的智能家居设备反馈一类型认证失败的消息。

[0075] 进一步地，当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，所述网关也可以忽视或直接丢弃所述接入请求信息，和/或给所述待接入的智能家居设备反馈一身份认证失败消息。

[0076] 需要补充的是，若设备类型与身份信息均认证成功，则执行步骤2041；若设备类型匹配但身份信息认证失败，则执行步骤2042。

[0077] 步骤2041：若设备类型与身份信息均认证成功，则下发智能家居设备需要的其他信息。

[0078] 这里，所述若设备类型信息与身份信息均认证成功，可以理解为所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型匹配，且待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配。这里，所述智能家居设备需要的其他信息，例如可以是，所述智能家居设备需要对网关进行认证的认证信息。需要说明的是，所述网关对智能家居设备的接入需要进行认证，相反，所述智能家居设备也需要对网关进行认证。若网关对智能家居设备的设备类型与身份信息均认证成功，则下发一个智能家居设备对所述网关认证的相关消息至智能家居设备，以供智能家居设备对所述网关进行认证。

[0079] 步骤2042：若设备类型匹配但身份信息认证失败，网关则上报所述第一身份信息至服务器。

[0080] 这里，所述设备类型匹配但身份信息认证失败，可以理解为所述待接入的智能家居设备的第一设备类型信息与从该服务器接收的智能家居设备的第二设备类型匹配，但待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配。这时，由网关向服务器上报新接入的智能家居设备身份信息，以便后续进行开通和维护。当然，在一些实施例中，所述设备类型不匹配时，网关也会将新接入的智能家居设备的类型信息上报至服务器，以便后续对该类型的智能家居设备的开通和维护。另外，所述智能家居设备在新接入网关时主动上报，免去了家庭网关的认证匹配过程，提高了效率。这里，主动上报的形式，主要是通过家庭网关提前配置的形式，或者是用户通过在移动终端应用或在智能家居设备中输入配置的类型信息发送至服务器的形式。

[0081] 步骤205：智能家居设备反馈认证结果。

[0082] 这里，所述智能家居设备对网关认证成功，则反馈一接入成功消息至所述网关；所述智能家居设备对网关认证失败，则反馈一接入失败消息至所述网关。

[0083] 需要补充的是，步骤205：在网关对所述智能家居设备进行认证过程中，若设备类型匹配但身份信息认证失败，则网关上报所述第一身份信息至服务器。

[0084] 这里，当网关对所述智能家居设备进行认证过程中，若设备类型匹配但身份信息认证失败，可以理解为，当所述待接入的智能家居设备的第一设备类型信息与从服务器接

收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时。相应地，这时，网关接收所述待接入的智能家居设备发送的第一身份信息；将所述第一身份信息上报至服务器。如此，便于服务器对新的身份信息进行开通和维护。后续如果需要将该智能家居设备接入所述网关中，所述服务器可以将该智能家居的第一身份信息重新下发给所述网关，所述网关对该智能家居设备的第一身份信息进行存储，第二次接入时即可调用该智能家居设备的第一身份信息，并对该智能家居设备进行本地的身份认证。

[0085] 步骤206：若设备类型匹配且身份信息均认证成功，从所述接入请求中确定出第一业务类型信息，并根据第一业务类型信息及第二业务类型信息，对网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。

[0086] 这里，所述接入请求信息还包括：待接入智能家居设备的第一业务类型信息，网关根据接收到的所述待接入的智能家居设备发起的接入请求信息，确定出所述待接入的智能家居设备的第一业务类型信息。

[0087] 这里，所述第二业务类型信息是与所述待接入智能家居设备相关的业务类型信息，可以理解的是，所述第二业务类型信息是网关能支持的所述待接入智能家居设备的业务类型，例如某一网关具备两个接口，一个接口用于连接上网路由，另一个接口用于连接Other路由，例如：连接智能家居局域网路由。那么该网关可以有两种方式确定其所支持的业务类型，一种是默认的方式，该网关默认可以支持两种业务类型；另一种是由服务器对网关进行配置，配置所述网关仅能支持其中一种业务类型。进一步地，若是服务器对网关的，业务类型进行配置，配置好的业务类型，也就是第二业务类型信息也可以预先存储在网关中，可以理解为，服务器预先下发的第二业务类型信息，例如，机顶盒设备访问的DNS域名或目的IP只能走IPTV路由通道。如此，所述智能家居设备接入时，关于业务类型的请求也不需要再次与服务器进行交互，减轻了服务器的负荷，简化了交互流程。

[0088] 进一步地，当所述第一业务类型信息与第二业务类型信息匹配时，表示所述网关支持智能家居设备关于第一业务类型的请求，这时，网关自身根据匹配结果对网关分配相应的业务控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。可以理解的是，所述网关为智能家居设备执行第一业务类型相应的业务，需要先验证网关是否支持第一业务类型信息，若支持，则控制网关分配执行第一业务类型信息所需要的业务控制信息。

[0089] 这里，所述第一业务类型包括：网络访问业务信息；所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应的业务，包括：比对所述网络访问业务信息及所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中携带有网络访问业务信息，则为所述网关分配网络访问的路由控制信息，以控制所述网关为所述智能家居设备提供网络访问的业务。这里，路由控制信息可以是控制网关选择路由路径的信息或控制网关选择路由的目的地址或下一跳地址的信息。

[0090] 在另一实施例中，所述第一业务类型包括：网络访问业务信息；所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应的业务，包括：比对

所述网络访问业务信息及所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中未携带有网络访问业务信息，则为所述网关分配默认的路由控制信息，以控制所述网关为所述智能家居设备提供默认类型的业务。例如，所述智能家居设备为智能数字电视，则默认的路由控制信息可以是控制网关选择路由路径为广播电视的路由路径的信息；默认类型的业务则可以是广播电视业务。例如智能家居设备为智能冰箱，则默认的路由控制信息可以是控制网关的路由地址选择为家庭局域网路由地址的控制信息，默认类型的业务则可以是冰箱存储的食物相关的业务，例如，提醒业务等，与所述智能冰箱连接的移动终端记录所述智能冰箱中存储的食物即将过期，则通过家庭局域网，将提醒信息发送至智能冰箱，再通过文字的形式显示在所述智能冰箱的显示面板上或通过语音播报的形式由智能冰箱的扬声器定时播放。

[0091] 本发明实施例提供一种智能家居设备接入认证方法，在所述智能家居设备的设备类型和身份认证均成功后，还可以对所述智能家居设备的业务类型进行匹配，并能根据业务类型的匹配结果，对网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。这里，业务类型信息也可以预先存储于网关本地，这样，在所述智能家居设备进行业务类型请求后，也不需要上报至服务器，减轻了服务器的负荷，节省了网络资源，同时也不受服务器当前状态的影响，有利于业务类型请求后的业务正常执行，且由于在本地可以进行业务类型的控制，使得网关本身的业务控制更加灵活。

[0092] 基于上述实施例的方法，本发明实施例还提供了一具体实施例。

[0093] 实施例三：

[0094] 对本实施例进行进一步详细说明之前，对本实施例中涉及的名词和术语进行说明，本实施例中涉及的名词和术语适用于如下的解释。

[0095] 1、IP(Internet Protocol，网络协议)，IP是为计算机网络相互连接进行通信而设计的协议。

[0096] 2、IPTABLES是与最新的3.5版本Linux内核集成的IP信息包过滤系统。如果Linux系统连接到因特网或LAN(Local Area Network，局域网)、服务器或连接LAN和因特网的代理服务器，则该系统有利于在Linux系统上更好地控制IP信息包过滤和防火墙配置。

[0097] 3、ITV(interactive television，交互式电视)，ITV可以通过交互式电视，看电视、浏览信息、收发E—MAIL、发表评论、网上聊天可以同时进行，互不干扰。

[0098] 4、STB(Set Top Box，数字视频变换盒)，STB通常称作机顶盒或机上盒，是一个连接电视机与外部信号源的设备。它可以将压缩的数字信号转成电视内容，并在电视机上显示出来。信号可以来自有线电缆、卫星天线、宽带网络以及地面广播。机顶盒接收的内容除了模拟电视可以提供的图像、声音之外，更在于能够接收数字内容，包括电子节目指南、因特网网页、字幕等等。使用户能在现有电视机上观看数字电视节目，并可通过网络进行交互式数字化娱乐、教育和商业化活动。

[0099] 5、MAC(Media Access Control或者Medium Access Control，媒体访问控制或物理地址、硬件地址)，MAC地址用来定义网络设备的位置。

[0100] 6、IPTV(Internet Protocol Television，网络协定电视)，IPTV是宽频网络(宽带)作为介质传送电视信息的一种系统，将广播节目透过宽频上的网际协议向订户传递数码电视服务。

[0101] 7、DHCP(Dynamic Host Configuration Protocol,动态主机配置协议),DHCP是一个局域网的网络协议,使用UDP(User Datagram Protocol,用户数据报协议)协议工作,主要有两个用途:给内部网络或网络服务供应商自动分配IP地址,给用户或者内部网络管理员作为对所有计算机作中央管理的手段。DHCP协议采用客户端/服务器模型,主机地址的动态分配任务由网络主机驱动。当DHCP服务器接收到来自网络主机申请地址的信息时,才会向网络主机发送相关的地址配置等信息,以实现网络主机地址信息的动态配置。

[0102] 使用DHCP正常获取地址的过程中使用的是以下4种报文:

[0103] (1)客户端广播DHCP发现(DHCP Discovery)

[0104] (2)服务器回应DHCP响应(DHCP Offer)

[0105] (3)客户端广播DHCP请求(DHCP Request)

[0106] (4)服务器回应DHCP确认(DHCP ACK)

[0107] 具体地,DHCP的工作流程的四个步骤:

[0108] 第一步:客户端发送DHCP Discovery包,请求DHCP服务器,就是查找网络上的DHCP服务器;

[0109] 第二步:服务器向客户端回应DHCP Offer包,目的告诉客户端,服务器能为客户端提供IP地址;

[0110] 第三步:DHCP Request包,客户端向服务器请求IP地址;

[0111] 第四步:DHCP ACK包,确认报,服务器向客户端分配IP地址。

[0112] 其实还有其他类型的报文,客户端发现分配的IP地址已经被占用时,发送DHCP Decline,通知服务器IP地址已被占用,要求重新分配。

[0113] 客户端可以主动释放IP地址,DHCP Release。例如,客户端同时发给两台DHCP服务器,DHCP服务器会根据Request中的相应字段,来判断是和哪一个DHCP服务器请求IP地址,然后做出ACK的回应,而另一台服务器也可以把之前提供出去但没有被客户端使用的IP地址重新放回可分配IP的范围。当DHCP客户端不再需要使用分配IP地址时,就会主动向DHCP服务器发送RELEASE请求报文,告知服务器用户不再需要分配IP地址,请求DHCP服务器释放对应的IP地址。

[0114] 8、DHCP Option60,在DHCP协议中,定义了一个选项(Option)字段,该字段主要是用来扩展DHCP协议的,Option60(Vendor class indentifier)是DHCP报文中的一个选项字段,代码(code)为60,可以标识终端类型,根据不同的终端类型来选择接口下的网关。这个,各个厂家就可以在该字段中添加自身的标识,用于区别不同的终端。

[0115] 9、DHCP Option125,Option125功能是对标准DHCP协议一个补充标准。DHCP服务器在完成验证将客户端的IP地址等信息封装成DHCP OFFER包的时候,将Option 125信息封装DHCP OFFER包中再发送给客户端。客户端收到OFFER包以后,首先查看该OFFER包所带的OPTION 125的“Option-data 1”字段中所填写的特征值,并与预先存储的信息进行比对。比对结果为相同则使用此OFFER,如果比对结果不同或OFFER包中不带OPTION 125,则将此OFFER丢弃。可以理解的是,DHCP服务器需要在回给客户端的DHCP OFFER包中插入认证信息(option125)以便客户端能够对此信息进行鉴权,以辨别该OFFER包是否来自合法的DHCP服务器。

[0116] 10、管理媒介WEB,媒介管理是指研究媒介管理者协调、组织、领导和控制媒介员工

的工作和充分利用媒介资源来达到既定的媒介发展目标的过程;web(World Wide Web,全球广域网),web也称为万维网,它是一种基于超文本和HTTP的、全球性的、动态交互的、跨平台的分布式图形信息系统。是建立在Internet上的一种网络服务,为浏览者在Internet上查找和浏览信息提供了图形化的、易于访问的直观界面,其中的文档及超级链接将Internet上的信息节点组织成一个互为关联的网状结构。

[0117] 11、ITMS(Integrated Terminal Management System,终端综合管理系统),ITMS是我的E家终端管理系统,主要用于家庭网关的设备注册,初始化自动配置,远程故障诊断修复和设备监控等。它通过北向接口与BOSS系统,通过南向接口实现对我的E家终端的统一管理。

[0118] 12、TR-069是由DSL论坛(www.dslforum.org)所开发的技术规范之一,其全称为“CPE广域网管理协议”。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议,用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

[0119] 13、HTTP(HyperText Transfer Protocol,超文本传输协议),HTTP是互联网上应用最为广泛的一种网络协议。

[0120] 14、DBUS,数据总线,是一个低延迟,低开销,高可用性的ipc机制。

[0121] 15、BRAS(Broadband Remote Access Server,宽带远程接入服务器),BRAS是面向宽带网络应用的新型接入网关,它主要完成两方面功能,一是网络承载功能:负责终结用户的PPPoE(Point-to-Point Protocol Over Ethernet,是一种以太网上传送PPP会话的方式)连接、汇聚用户的流量功能;二是控制实现功能:与认证系统、计费系统和客户管理系统及服务策略控制系统相配合实现用户接入的认证、计费和管理功能。

[0122] 16、WAN(Wide Area Network,广域网),WAN是由许多交换机组成的,交换机之间采用点到点线路连接,几乎所有的点到点通信方式都可以用来建立广域网,包括租用线路、光纤、微波、卫星信道。而广域网交换机实际上就是一台计算机,有处理器和输入/输出设备进行数据包的收发处理。

[0123] 17、IGMP Snooping(Internet Group Management Protocol Snooping,互联网组管理协议窥探),它是运行在二层设备上的组播约束的机制,用于管理和控制组播组。

[0124] 本实施例中,待接入的智能家居设备作为客户端,所述待接入的智能家居设备以待认证机顶盒为例,所述网关以家庭网关为例。

[0125] 本实施例旨在解决:由于传统机顶盒的接入认证一般由机顶盒直接与IPTV认证平台服务器交互或通过家庭网关DHCP中继的方式与鉴权服务器交互,其机顶盒本身的设置及认证流程相对复杂,且对鉴权服务器的处理性能有一定依赖。

[0126] 请参阅图3,图3为本发明实施例三所提供的机顶盒参数配置的具体流程示意图。如图3所示,所述机顶盒参数配置的方法步骤为:

[0127] 步骤301:ITMS/WEB云平台客户端通过TR-069/HTTP/DBUS等网关对外提供的能力集接口向家庭网关下发待认证机顶盒的参数信息(包括该网关支持的机顶盒MAC地址、设备型号、待认证用户名密码、Option125认证信息配置等)和第二业务类型信息等。

[0128] 需要说明的是,上述的服务器以ITMS/WEB云平台客户端为例;上述的第二身份信息及第二设备类型信息以参数信息为例。这里,所述ITMS/WEB云平台客户端通过TR-069/HTTP/DBUS等网关的对外接口向家庭网关下发机顶盒的身份参数信息,这里,身份参数信息

包括:该家庭网关支持的机顶盒MAC地址、设备型号、机顶盒的用户名密码、Option125认证信息等。同时,还下发机顶盒的业务类型信息等。

[0129] 这里,机顶盒MAC地址可以用来识别机顶盒的网络位置;机顶盒的设备型号可以用来区分机顶盒,机顶盒MAC地址及机顶盒型号可以作为机顶盒的第二类型信息;机顶盒的用户名密码可以作为机顶盒的第二身份信息;Option125认证信息可以作为网关下发给机顶盒需要的认证信息。

[0130] 步骤302:家庭网关对应能力集接口解析管理媒介下发的机顶盒的参数信息和第二业务类型信息,并通知家庭网关内部机顶盒认证服务模块。

[0131] 需要说明的是,管理媒介可以理解为服务器中用于对其所述的家庭网关进行管理协调、组织、领导和控制的模块。家庭网关内部的机顶盒认证服务模块,可以理解为家庭网关内部用于对接入的机顶盒进行认证的模块。

[0132] 步骤303:家庭网关内部机顶盒认证服务模块保存上述机顶盒参数信息和第二业务类型信息。

[0133] 步骤304:家庭网关本地接收下挂机顶盒设备的DHCP Discovery和Request请求报文,并依此判断是否为待认证的机顶盒,如果是机顶盒且身份认证通过,则可以通过家庭网关对其进行相关的业务控制。

[0134] 需要补充的是,在一些实施例中,服务器下发的参数信息还包括家庭网关支持的机顶盒的设备类型标识符、加密方式。上述的所有的参数信息及第二业务类型信息均保存在家庭网关本地数据库中,以便机顶盒接入认证时判断使用。

[0135] 另外,本实施例中,待认证机顶盒接入家庭网关时,家庭网关上的DHCP服务器模块首先根据DHCP Option60进行设备类型判断,支持明文或密文传递Option选项内容的方式,以识别待认证机顶盒设备,确定是否允许该机顶盒接入,即根据DCHP Option60(明文或DES加密等算法生成的密文)识别出机顶盒的设备的生产厂商名称,设备种类,设备型号,设备的序列号,软/硬件版本号等信息,以防止非法类型的机顶盒设备接入。其中所述机顶盒需事先将上述信息封装到DHCP Discovery或Request报文中的Option60字段,对于家庭网关支持的设备型号的机顶盒,则记录对应的机顶盒MAC和厂商等信息至本地数据库中。

[0136] 进一步地,家庭网关在收到机顶盒发出的DHCP Discovery请求报文时,网关本地DHCP Server服务模块则首先解析后DHCP Option60信息中包含的机顶盒的厂商和MAC等信息内容,并通知家庭网关本地机顶盒认证服务模块对DHCP Option选项参数进行

[0137] 并校验判断,具体与通过ITMS、WEB或DBUS云平台管理媒介配置下发的机顶盒用户名密码等信息进行验证,以确认当前接入的设备是否为合法的机顶盒设备。

[0138] 具体地,请参阅图4,图4为本发明实施例三所提供的家庭网关实现机顶盒接入认证的具体流程示意图;如图4所示,家庭网关实现机顶盒接入认证的具体流程如下:

[0139] 步骤401:家庭网关管理媒介下发待认证机顶盒的参数信息和业务控制信息至家庭网关。

[0140] 这里,上述的第二身份信息和第二类型信息以参数信息为例;上述的第二业务类型信息以业务控制信息为例。这里,参数信息和业务控制信息由家庭网关的机顶盒认证服务模块接收并保存。

[0141] 步骤402:机顶盒发送DHCP Discovery(Option60)至家庭网关。

[0142] 需要说明的是,DHCP Option60携带有机顶盒的设备型号、身份信息、业务类型信息等,例如通过明文或密文携带“ITV”或“STB”等字样的设备标识,对这些标识进行类别识别。可以理解的是,这里DHCP Option60携带有机顶盒的第一身份信息、第一设备类型信息及第一业务类型信息。

[0143] 步骤403:家庭网关的DHCP Server接收DHCP Discovery,并从DHCP Option60确定出机顶盒的第一身份信息、第一设备类型信息及第一业务类型信息,从而获取机顶盒的设备型号、用户名密码等信息,发起本地认证请求。

[0144] 这里,家庭网关DHCP Server模块通过双方协商的加密算法(DES等)解Option60选项字段,或直接读取Option60明文信息,判断是否为家庭网关支持的认证类型的机顶盒设备。如果设备类型不支持,则默认为PC终端,分配PC地址池对应的网段IP地址,后续不允许其访问IPTV平面业务;如果为设备类型支持且已认证的机顶盒,则DHCP Server直接分配对应STB地址池段内的IP地址给该机顶盒。如果设备类型已支持,但未认证,即首次接入家庭网关等情况,则家庭网关本地DHCP Server模块将该机顶盒的MAC和用户身份帐号信息发送至本地机顶盒认证服务模块。

[0145] 步骤404:查询ITMS/WEB/云平台下发的机顶盒设备型号、MAC地址、用户名密码等信息,确认是否为机顶盒设备及是否通过身份认证。

[0146] 这里,家庭网关本地机顶盒认证服务模块,根据ITMS/WEB/云平台等媒介预先下发的机顶盒设备型号、MAC地址、用户名密码信息与当前接入的机顶盒DHCP Option60选项确定出的参数(包括机顶盒的用户名、密码,MAC地址,机顶盒的型号,软硬件版本号和序列号等信息)进行判断比较,以确定是否为机顶盒设备及是否允许该机顶盒接入家庭网关。

[0147] 如果认证未通过则执行步骤405,如果认证通过则执行步骤406。

[0148] 步骤405:向家庭网关管理媒介上报当前待认证机顶盒的匹配认证结果,或上报已识别的待认证机顶盒信息,便于开通和维护。

[0149] 这里,如果机顶盒未认证通过,则通过家庭网关中间件DBUS接口通知家庭网关云平台等管理媒介,上报当前家庭网关未认证通过的机顶盒信息,以便于后续通过云平台等管理媒介对新接入机顶盒的开通和维护。

[0150] 步骤406:保存机顶盒认证通过结果、机顶盒MAC地址等信息,并下发组播或网络访问的路由控制信息至家庭网关内部的相关业务模块。

[0151] 这里,如果机顶盒认证通过,则通知网关内部DHCP Server模块认证成功标志,允许其获取分配的地址,并下发允许其观看组播和网络访问的路由等控制信息,这里,网络访问的路由控制信息,用于控制DHCP Sever对路由路径或路由地址进行选择。该认证结果标志和业务类型信息同时保存本地数据库中,以便于家庭网关内部各个业务模块进行具体的业务控制时进行查询。

[0152] 步骤407:家庭网关向所述机顶盒下发DHCP Offer(Option125)。

[0153] 这里,机顶盒获取家庭网关分配的IP地址,及根据Option60自适应下发的机顶盒需要的Option125。

[0154] 具体地,家庭网关判断认证通过,则允许给机顶盒分配对应STB地址池段内的IP地址,并根据DHCP Option60自适应下发插入携带Option125编码内容信息的DHCP Offer响应给机顶盒,以便客户端能够对此信息进行鉴权。DHCP Request和DHCP ACK的交互同正常协

议流程,DHCP ACK报文中也携带有相应的Option125信息。

[0155] 需要补充的是,为了支持机顶盒认证家庭网关,家庭网关下可同时下挂有多个机顶盒的应用场景,在一些实施例中,家庭网关还提供兼容不同类型机顶盒Option125编码格式。家庭网关预先从BRAS或ITMS网管节点获取机顶盒认证需要的Option125信息,并保留至本地数据库中,在机顶盒获取分配的IP地址时由家庭网关根据需要通过DHCP Offer或ACK报文携相应的Option125参数给机顶盒进行认证。其中,所述的DHCP Option125信息内容,一般在家庭网关的WAN侧DHCP路由WAN连接获取大网地址时,由BRAS下发。如果WAN侧DHCP Server没有下发,则也可以由ITMS网管根据对应Option60设备型号的机顶盒直接下发其所需的Option125认证配置信息。本方法中的家庭网关可以根据DHCP Discovery请求的Option60信息内容自动下发其认证所需要的Option125编码格式内容信息,以兼容不同机顶盒的接入,提高了相互认证成功效率。

[0156] 由此,本实施例中由机顶盒接入到网络中的家庭网关,将其设备型号、身份信息、业务类型信息等与家庭网关中的参数信息(包含可支持的设备型号、身份信息、业务类型信息)进行比对验证,就能直接在家庭网关本地完成身份验证,可以减少触发身份认证的接入请求需要转发到对应的家庭网关管理媒介(服务器)才能进行验证的转发次数,减少了该接入请求信息发送到家庭网关管理媒介(服务器)并启动验证的时间差,从而提前了验证,相对于用户而言相当于提升了验证效率。另一方面,由各机顶盒所连接的各自的家庭网关对其进行验证,相比较于由总的家庭网关管理媒介(服务器)集中进行验证,实现了身份验证的分布式处理,避免了集中家庭网关管理媒介(服务器)验证导致验证量答,因为验证量大进而导致的验证效率低的问题,从而提升了身份验证的效率,并由于身份验证效率高,减少了接入家庭网关管理媒介(服务器)和获取家庭网关管理媒介(服务器)提供的服务的延时。

[0157] 进一步地,如果机顶盒认证成功,家庭网关根据接收到的待认证机顶盒的接入请求信息,确定出待认证机顶盒的第一业务类型信息。这里,以网络访问业务信息为例。

[0158] 家庭网关内部机顶盒认证服务模块通知用户态其他业务模块下发允许机顶盒开通接入及是否允许其接入网络访问业务等相关业务类型,给机顶盒分配相应特殊STB地址池网段内的IP地址。机顶盒通过家庭网关本地认证后,其认证结果和网络访问业务保存在家庭网关的本地数据库中,并将相关认证的设备MAC和认证结果等信息下发至内核桥模块。如果有多个机顶盒,则按照不同MAC分别记录对应的认证结果。

[0159] 具体地,为了控制IPTV机顶盒同时访问IPTV与互联网两种业务,在本实施例中,如在家庭网关全路由应用场景中为了实现下挂机顶盒对应网络访问业务和视频业务分离的目的,可通过家庭网关ITMS网管节点或WEB等管理媒介预配置对应家庭网关中WAN连接的全路由规则参数实现,如下发IPTV业务相关目的IP地址段或DNS域名参数范围和IPTV路由WAN连接接绑定,以使得不同目的IP数据流和DNS请求分别发送至指定的网络访问业务和IPTV业务平面,以实现家庭网关对机顶盒的业务类型的控制。其中,当家庭网关获知不允许该机顶盒上网时,则通过配置对应源IP地址段的Iptable规则,机顶盒所有业务包括DNS请求只能经过IPTV路由平面转发。当允许机顶盒进行网络访问业务时,按照上述全路由策略规则,只有符合特定IPTV平面“白名单”规则内的目的IP、DNS域名走IPTV路由平面转发,其他业务默认走Internet路由平面转发。当然在一些实施例中,当允许机顶盒进行网络访问业务时,则为家庭网关分配网络访问的路由控制信息,以控制所述家庭网关为所述机顶盒提供网络

访问的业务。

[0160] 具体地，请参阅图5，图5为本发明实施例三所提供的网关IPTV路由方式下机顶盒业务路由转发控制的具体流程示意图，如图5所示，网关IPTV路由方式下机顶盒业务路由转发控制的具体流程如下：

[0161] 步骤501：机顶盒发起数据业务请求。

[0162] 这里，机顶盒发起数据业务请求即为机顶盒向家庭网关发起上网访问请求。

[0163] 步骤502：家庭网关判断机顶盒是否开通网络访问业务。

[0164] 如果没有开通，则执行步骤503；如果有开通，则执行步骤504。

[0165] 步骤503：家庭网关将所有业务请求默认经IPTV路由转发。

[0166] 这里，如果没有开通网络访问业务，则在机顶盒获取到IP地址时，同步配置对应源IP地址段的Iptable规则，该机顶盒的所有业务包括DNS请求只能经过IPTV路由WAN连接转发，即只能访问IPTV业务平面的业务。

[0167] 步骤504：家庭网关判断目的IP、DNS域名是否在IPTV平面白名单规则内。

[0168] 这里，家庭网关判断该机顶盒已开通了网络访问业务，则进一步根据本地ITMS网管配置的IPTV路由平面的指定目的IP地址段规则和DNS域名规则，进行判断转发。

[0169] 步骤505：符合IPTV路由策略规则的请求经IPTV路由转发。

[0170] 这里，如果访问的数据业务请求符合特定IPTV平面“白名单”规则内的目的IP、DNS域名规则，则从走IPTV路由平面转发。其中配置的域名规则，可以由家庭网关中的DNS代理模块匹配该域名请求成功后动态确定出指定域名对应的目的IP地址，并同步配置相关规则至内核路由转发模块实现。

[0171] 步骤506：家庭网关控制其他默认经过Internet路由转发。

[0172] 这里，对于符合特定IPTV平面“白名单”规则外的目的IP、DNS域名规则，默认走Internet路由平面转发。

[0173] 需要补充的是，如果机顶盒有允许接入互联网的权限，则后续机顶盒可以访问A平面Internet域内的业务；否则仅放开其默认允许访问的B平面IPTV业务的权限。如果认证失败，则允许经过一定次数的重试，如果重试仍失败，则在家庭网关中记录为未认证通过的机顶盒，限制其接入并通过网关中间件DBUS接口通知家庭网关云平台，上报当前网关未认证通过的机顶盒信息，以便于后续通过云平台对家庭网关新接入机顶盒的开通和维护。由此，对于网络访问业务的路由控制也不需要经过服务器，减少了服务器认证机顶盒网络访问业务的时间，也减少了服务器对家庭网关分配网络访问相关路由路径的时间，提高了机顶盒网络访问效率。

[0174] 本实施例通过家庭网关实现机顶盒接入认证，其认证工作可由家庭网关本地认证完成。本实施例所提供的机顶盒接人认证方法，在机顶盒接入时不需要机顶盒和IPTV认证平台鉴权服务器进行直接交互认证，方便了机顶盒的接入使用，机顶盒直接设置成DHCP路由模式就可以上网。如此，避免了因机顶盒认证鉴权服务的性能的影响，简化了机顶盒本身的设置和认证流程。

[0175] 进一步地，本实施例中，对于IPTV桥WAN连接组播业务的转发，家庭网关通过DHCP Option60实现桥端口下挂机顶盒的内核组播业务控制如下：对于DHCP桥方式接入的机顶盒，可以由家庭网关用户态管理模块，预先下发DHCP Option60选项的匹配验证参数至内核

桥协议栈模块，后续内核桥模块在内核态收到机顶盒对应LAN侧端口发出的DHCP Discovery请求报文时，在内核确定出DHCP Option60选项参数并与下发的机顶盒认证参数进行比较，或者经过3DES解密后再进行比较。如果识别出该接入设备为机顶盒，则标记该下挂设备的源MAC为STB机顶盒MAC，后续在内核二层组播协议模块可根据该学习的源MAC标记信息对收到的“组播加入报文”进行转发控制，只有机顶盒的MAC才可以正常观看组播节目，其加入报文正常转发到WAN侧IPTV桥WAN连接，否则，默认丢弃该组播加入报文。该策略控制信息，也可以对具体的某个组播组进行转发控制。同样，对于PPPoE接入方式的机顶盒，可以解析PPPoE Option选项部分参数内容。

[0176] 具体地，请参阅图6，图6为本发明实施例三所提供的IPTV桥接方式下机顶盒接入认证的具体流程示意图；如图6所示，IPTV桥接方式下机顶盒接入认证方法，主要是在内核协议栈桥模块通过截获DHCP Discovery请求报文中的Option60选项参数，以实现桥端口下挂机顶盒的内核组播业务控制，其方法流程步骤如下：

[0177] 步骤601：机顶盒向家庭网关发起DHCP Discovery请求报文。

[0178] 这里，机顶盒通过DCHP桥接方式接入家庭网关，其DHCP服务由WAN侧BRAS服务器提供，网关本身不再为其分配IP地址。

[0179] 步骤602：转发并解析DHCP Option60，并与用户态下发的用户名、密码等认证参数进行比较，确认是否为机顶盒STB的MAC，并学习记录。

[0180] 这里，内核协议栈桥模块截获该DHCP Discovery请求报文，解析DHCP Option60选项参数，并与用户态机顶盒认证服务模块下发的待认证用户名、密码等认证参数进行比较，以确认是否为合法的机顶盒，并学习记录其源MAC为STB的MAC标记。

[0181] 步骤603：有IPTV桥WAN连接转发DHCP Discovery请求报文至家庭网关的DHCP Server。

[0182] 这里，IPTV桥WAN连接转发DHCP Discovery请求报文至WAN侧DHCP Server。

[0183] 步骤604-606：接收DHCP Server的DHCP Offer响应报文。

[0184] 步骤607：机顶盒发起发起组播业务请求。

[0185] 这里，机顶盒切换直播频道发送上行组播加入报文，网关二层组播协议IGMP Snooping模块接收到该上行组播加入报文时判断该报文的源MAC是否为机顶盒的MAC。

[0186] 步骤608：判断机顶盒MAC是否为认证通过的STB MAC。

[0187] 这里，对于桥端口的入向组播加入报文，内核二层组播协议模块查询该加入报文的源MAC是否已成功学习。

[0188] 这里，判断机顶盒MACC是否为认证通过的STB MAC也是通过解析机顶盒发起的DHCP Option60中的第一类型信息和第一身份信息，分别与家庭网关中预存的第二类型信息和第二身份信息是否匹配的方式来判断。

[0189] 如果通过认证，则执行步骤409；如果未通过认证，则执行步骤410。

[0190] 步骤609：允许组播协议报文转发。

[0191] 这里，家庭网关判断如果为机顶盒STB的MAC，则允许转发组播加入报文至IPTV桥。

[0192] 步骤610：丢弃组播协议报文。

[0193] 这里，家庭网关判断如果为非机顶盒STB的MAC，不允许转发至IPTV桥，即不允许组播业务接入。

[0194] 需要说明的是，机顶盒是否通过DCHP桥接方式接入家庭网关也是由家庭网关的组网是否配置有第二业务类型信息决定的，若机顶盒接入请求信息中携带有按照DCHP桥接方式接入的信息，IPTV桥WAN连接相当于二层透传(不需要路由寻址)，而IPTV路由WAN连接，则需要经过路由寻址转发。上述步骤601-610则为以桥接方式接入家庭网关的方法步骤。由此，对于接入方式的业务类型请求，也不需要经过服务器，减少了服务器对机顶盒接入方式的业务类型的判断的时间，节约了接入流程，提高了接入效率。

[0195] 进一步地，本发明实施例还提供了一种智能家居设备接入认证装置，图7为本发明实施例一所提供的智能家居设备接入认证装置功能结构示意图，如图7所示，所述装置包括：接收模块71和认证模块72；

[0196] 所述接收模块71，用于接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求消息中携带有所述待接入的智能家居设备的第一身份信息；

[0197] 所述认证模块72，用于据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

[0198] 所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；

[0199] 可选地，所述装置还包括：设备类型确定模块和设备类型匹配认证模块；

[0200] 所述设备类型确定模块，用于根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证之前，从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息；

[0201] 所述设备类型匹配认证模块，根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证。

[0202] 可选地，所述装置还包括：地址分配模块；

[0203] 所述地址分配模块，用于当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时，则从智能家居设备的地址池中分配网络之间互联协议IP地址给所述待接入的智能家居设备。

[0204] 可选地，所述装置还包括：业务类型确定模块及业务类型控制模块；

[0205] 所述业务类型确定模块，用于根据接收到的所述待接入的智能家居设备发起的接入请求信息，确定出待接入的智能家居设备的第一业务类型信息；

[0206] 所述业务类型控制模块，用于根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。

[0207] 可选地，所述第一业务类型信息包括：网络访问权限信息；

[0208] 所述业务类型控制模块，具体用于比对所述网络访问权限信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中携带有网络访问权限信息，则为所述网关分配网络访问的路由控制信息，以控制所述网关为所述智能家居设备提供网络访问的业务。

[0209] 可选地，所述业务类型控制模块，具体还用于比对所述网络访问权限信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务信息中未携带有网络访问权限信息，则为所述网关分配分配默认的路由控制信息，以控制所述网关为所述智能家

居设备提供默认类型的业务。

[0210] 可选地，所述装置还包括：上报模块；

[0211] 所述接收模块，还用于当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，接收所述待接入的智能家居设备发送的第一身份信息；

[0212] 所述上报模块，用于将所述第一身份信息上报至服务器。

[0213] 进一步地，为实现本发明实施例的方法，本发明实施例还提供了一种网关，用于实现本发明智能家居设备接入认证的方法的具体细节，达到相同的效果。

[0214] 图8为本发明实施例所提供的网关的硬件结构示意图，如图8所示，所述网关，包括：处理器81，以及用于存储能够在处理器81上运行的计算机程序的存储器82；其中，

[0215] 所述处理器81，用于运行所述计算程序时，执行：

[0216] 接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；

[0217] 根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

[0218] 可选地，所述接入请求信息还包括：待接入的智能家居设备的设备类型信息；

[0219] 所述处理器81，用于运行所述根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证之前的程序，执行：

[0220] 从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息；

[0221] 根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证。

[0222] 可选地，所述处理器81用于运行所述计算机程序，执行：

[0223] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时，则从智能家居设备的地址池中分配网络之间互联协议IP地址给所述待接入的智能家居设备。

[0224] 可选地，所述处理器81用于运行所述计算机程序，执行：

[0225] 根据接收到的所述待接入的智能家居设备发起的接入请求信息，确定出待接入的智能家居设备的第一业务类型信息；

[0226] 根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。

[0227] 可选地，所述第一业务类型信息包括：网络访问权限信息；

[0228] 所述处理器81，用于运行所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务的程序，执行：

[0229] 比对所述网络访问权限信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中携带有网络访问权限信息，则为所述网关分配网络访问

的路由控制信息，以控制所述网关为所述智能家居设备提供网络访问的业务。

[0230] 可选地，所述处理器81，用于运行所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务的程序，执行：

[0231] 比对所述网络访问权限信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务信息中未携带有网络访问权限信息，则为所述网关分配分配默认的路由控制信息，以控制所述网关为所述智能家居设备提供默认类型的业务。

[0232] 可选地，所述处理器81，用于运行所述计算机程序，执行：

[0233] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，接收所述待接入的智能家居设备发送的第一身份信息；

[0234] 将所述第一身份信息上报至服务器。

[0235] 进一步地，本发明还提供一种计算机存储介质，所述计算机存储介质中存储有计算机可执行程序，所述可执行程序被处理器执行时实现以下步骤：

[0236] 网关接收待接入的智能家居设备发起的接入请求信息；其中，所述接入请求信息中携带有所述待接入的智能家居设备的第一身份信息；

[0237] 根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证。

[0238] 可选地，所述接入请求信息还包括：待接入的智能家居设备的设备类型信息；所述可执行程序被处理器执行时，以具体实现所述根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证之前的步骤：

[0239] 从所述接入请求信息中确定出所述待接入的智能家居设备的第一设备类型信息；

[0240] 根据从服务器接收的智能家居设备的第二设备类型信息及第一设备类型信息，对所述待接入的智能家居设备进行类型匹配认证。

[0241] 可选地，所述可执行程序被处理器执行时，以具体实现以下步骤：

[0242] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息匹配时，则从智能家居设备的地址池中分配网络之间互联协议IP地址给所述待接入的智能家居设备。

[0243] 可选地，所述可执行程序被处理器执行时，以具体实现以下步骤：

[0244] 根据接收到的所述待接入的智能家居设备发起的接入请求信息，确定出待接入的智能家居设备的第一业务类型信息；

[0245] 根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务。

[0246] 可选地，所述第一业务类型信息包括：网络访问业务信息；所述可执行程序被处理器执行时，以具体实现所述根据所述第一业务类型信息及与所述待接入智能家居设备相关

的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务的步骤：

[0247] 比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务类型信息中携带有网络访问业务信息，则为所述网关分配网络访问的路由地址，以控制所述网关为所述智能家居设备提供网络访问的业务。

[0248] 可选地，所述可执行程序被处理器执行时，以具体实现所述根据所述第一业务类型信息及与所述待接入智能家居设备相关的第二业务类型信息，为所述网关分配相应的业务类型控制信息，以控制所述网关为所述智能家居设备执行相应类型的业务的步骤：

[0249] 比对所述网络访问业务信息及与所述待接入智能家居设备相关的第二业务类型信息，若所述第二业务信息中未携带有网络访问业务信息，则为所述网关分配分配默认的路由地址，以控制所述网关为所述智能家居设备提供默认类型的业务。

[0250] 可选地，所述可执行程序被处理器执行时，以具体实现以下步骤：

[0251] 当所述待接入的智能家居设备的第一设备类型信息与从服务器接收的智能家居设备的第二设备类型信息匹配，且所述待接入的智能家居设备的第一身份信息与从服务器接收的智能家居设备的第二身份信息不匹配时，接收所述待接入的智能家居设备发送的第一身份信息；

[0252] 将所述第一身份信息上报至服务器。

[0253] 除非另有定义，本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在本发明的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本发明。

[0254] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。本发明的保护范围应以所述权利要求的保护范围以准。

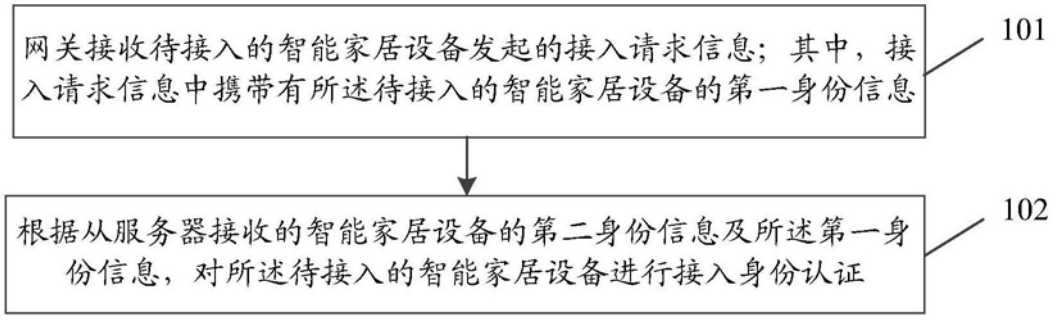

网关接收待接入的智能家居设备发起的接入请求信息；其中，接入请求信息中携带有所述待接入的智能家居设备的第一身份信息
101
根据从服务器接收的智能家居设备的第二身份信息及所述第一身份信息，对所述待接入的智能家居设备进行接入身份认证
102

图1

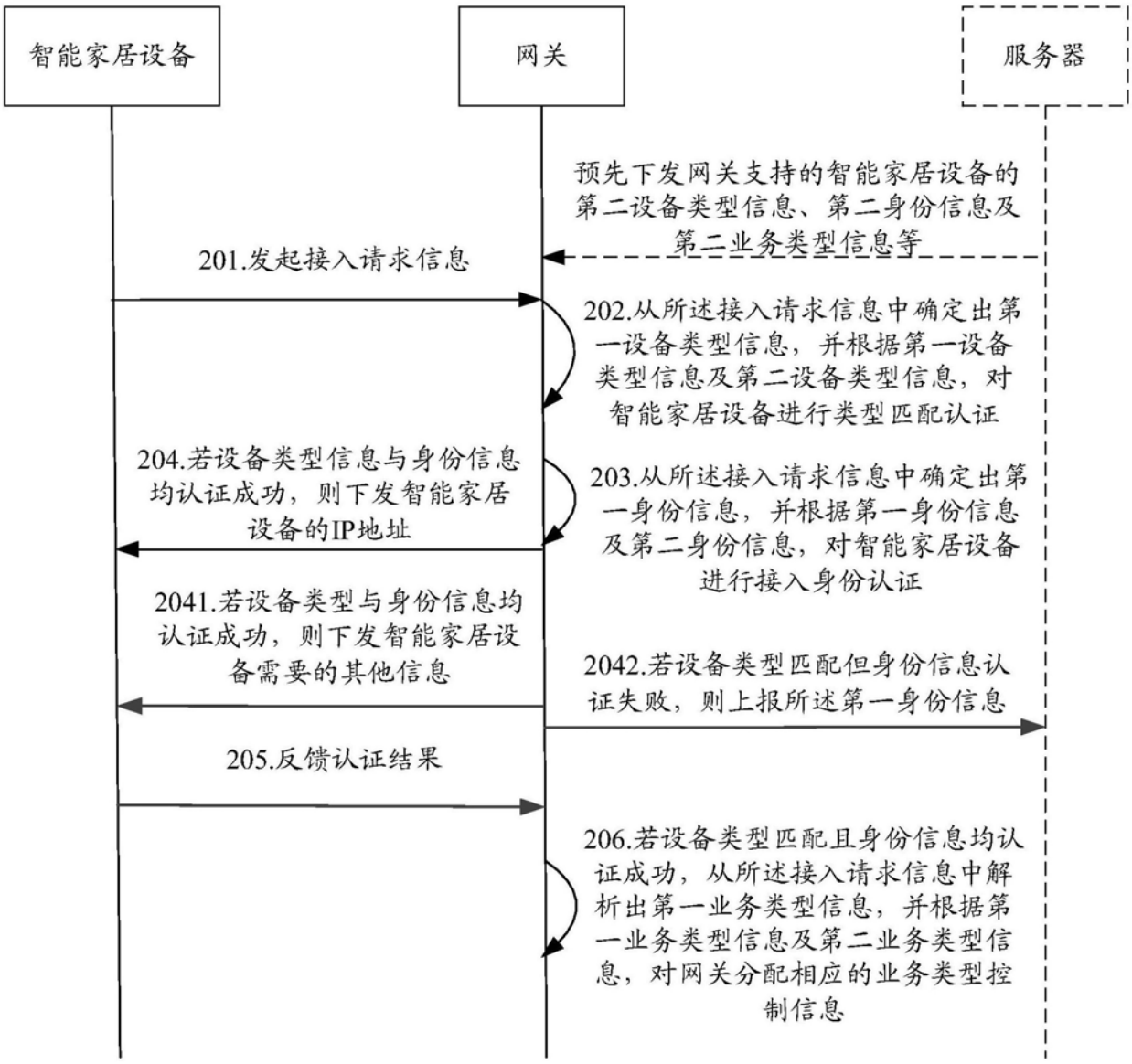

智能家居设备
网关
服务器
预先下发网关支持的智能家居设备的第二设备类型信息、第二身份信息及第二业务类型信息等
201.发起接入请求信息
202.从所述接入请求信息中确定出第一设备类型信息，并根据第一设备类型信息及第二设备类型信息，对智能家居设备进行类型匹配认证
204.若设备类型信息与身份信息均认证成功，则下发智能家居设备的IP地址
203.从所述接入请求信息中确定出第一身份信息，并根据第一身份信息及第二身份信息，对智能家居设备进行接入身份认证
2041.若设备类型与身份信息均认证成功，则下发智能家居设备需要的其他信息
2042.若设备类型匹配但身份信息认证失败，则上报所述第一身份信息
205.反馈认证结果
206.若设备类型匹配且身份信息均认证成功，从所述接入请求信息中解析出第一业务类型信息，并根据第一业务类型信息及第二业务类型信息，对网关分配相应的业务类型控制信息

图2

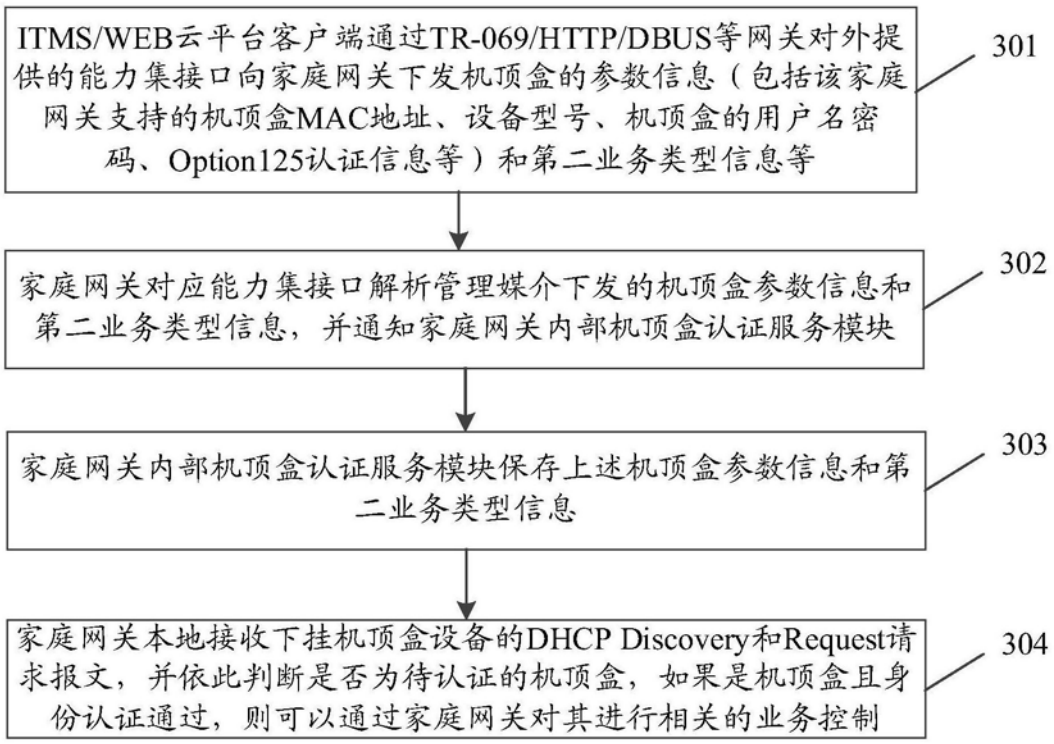

ITMS/WEB云平台客户端通过TR-069/HTTP/DBUS等网关对外提供的能力集接口向家庭网关下发机顶盒的参数信息（包括该家庭网关支持的机顶盒MAC地址、设备型号、机顶盒的用户名密码、Option125认证信息等）和第二业务类型信息等
301
家庭网关对应能力集接口解析管理媒介下发的机顶盒参数信息和第二业务类型信息，并通知家庭网关内部机顶盒认证服务模块
302
家庭网关内部机顶盒认证服务模块保存上述机顶盒参数信息和第二业务类型信息
303
家庭网关本地接收下挂机顶盒设备的DHCP Discovery和Request请求报文，并依此判断是否为待认证的机顶盒，如果是机顶盒且身份认证通过，则可以通过家庭网关对其进行相关的业务控制
304

图3

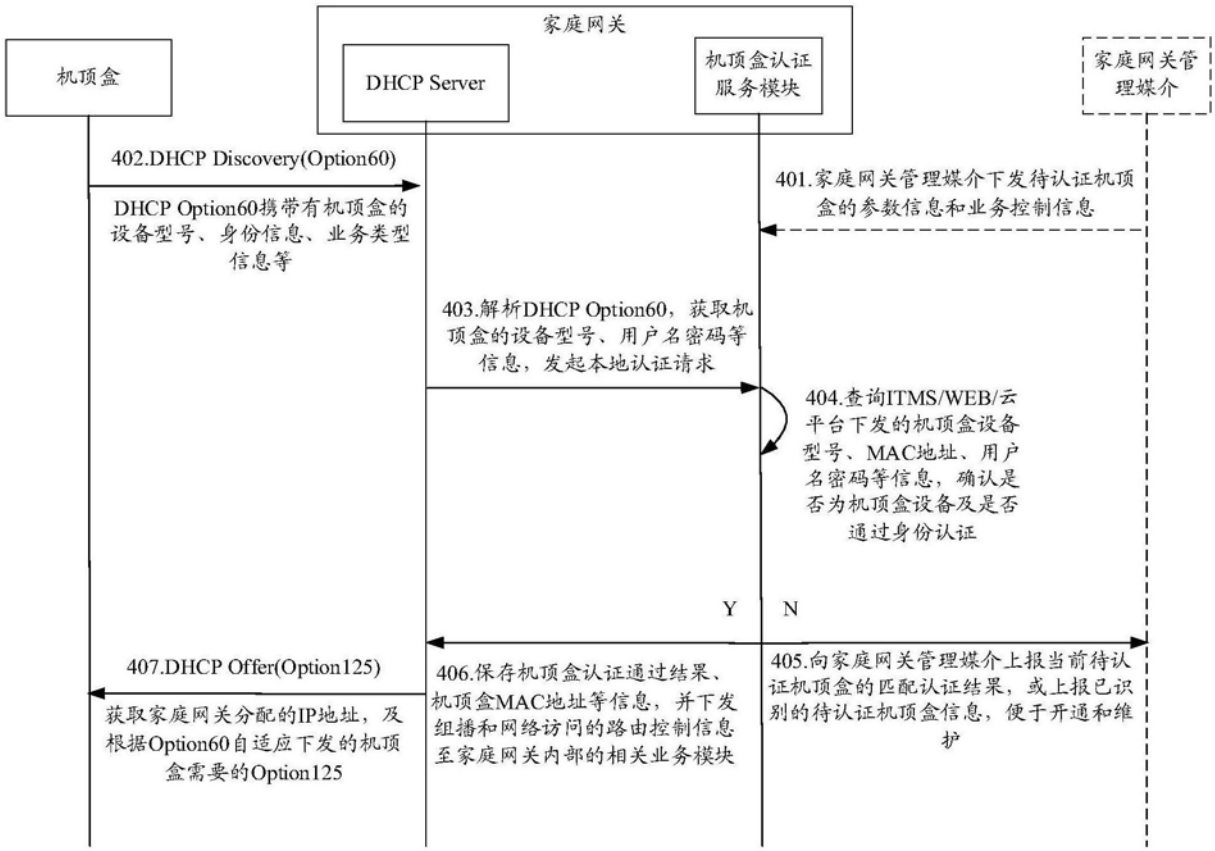

家庭网关
机顶盒
DHCP Server
机顶盒认证服务模块
家庭网关管理媒介
402.DHCP Discovery(Option60)
DHCP Option60携带有机顶盒的设备型号、身份信息、业务类型信息等
401.家庭网关管理媒介下发待认证机顶盒的参数信息和业务控制信息
403.解析DHCP Option60，获取机顶盒的设备型号、用户名密码等信息，发起本地认证请求
404.查询ITMS/WEB/云平台下发的机顶盒设备型号、MAC地址、用户名密码等信息，确认是否为机顶盒设备及是否通过身份认证
Y
N
407.DHCP Offer(Option125)
获取家庭网关分配的IP地址，及根据Option60自适应下发的机顶盒需要的Option125
406.保存机顶盒认证通过结果、机顶盒MAC地址等信息，并下发组播和网络访问的路由控制信息至家庭网关内部的相关业务模块
405.向家庭网关管理媒介上报当前待认证机顶盒的匹配认证结果，或上报已识别的待认证机顶盒信息，便于开通和维护

图4

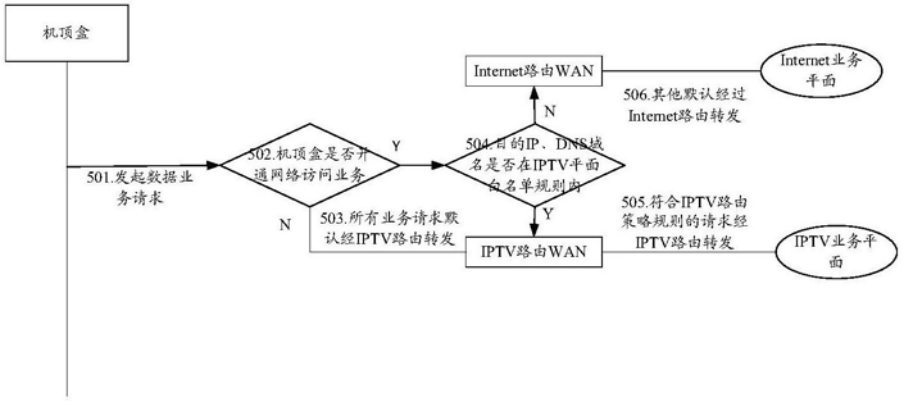

机顶盒
501.发起数据业务请求
502.机顶盒是否开通网络访问业务
Y
N
503.所有业务请求默认经IPTV路由转发
504.目的IP、DNS域名是否在IPTV平面白名单规则内
N
Y
Internet路由WAN
506.其他默认经过Internet路由转发
Internet业务平面
IPTV路由WAN
505.符合IPTV路由策略规则的请求经IPTV路由转发
IPTV业务平面

图5

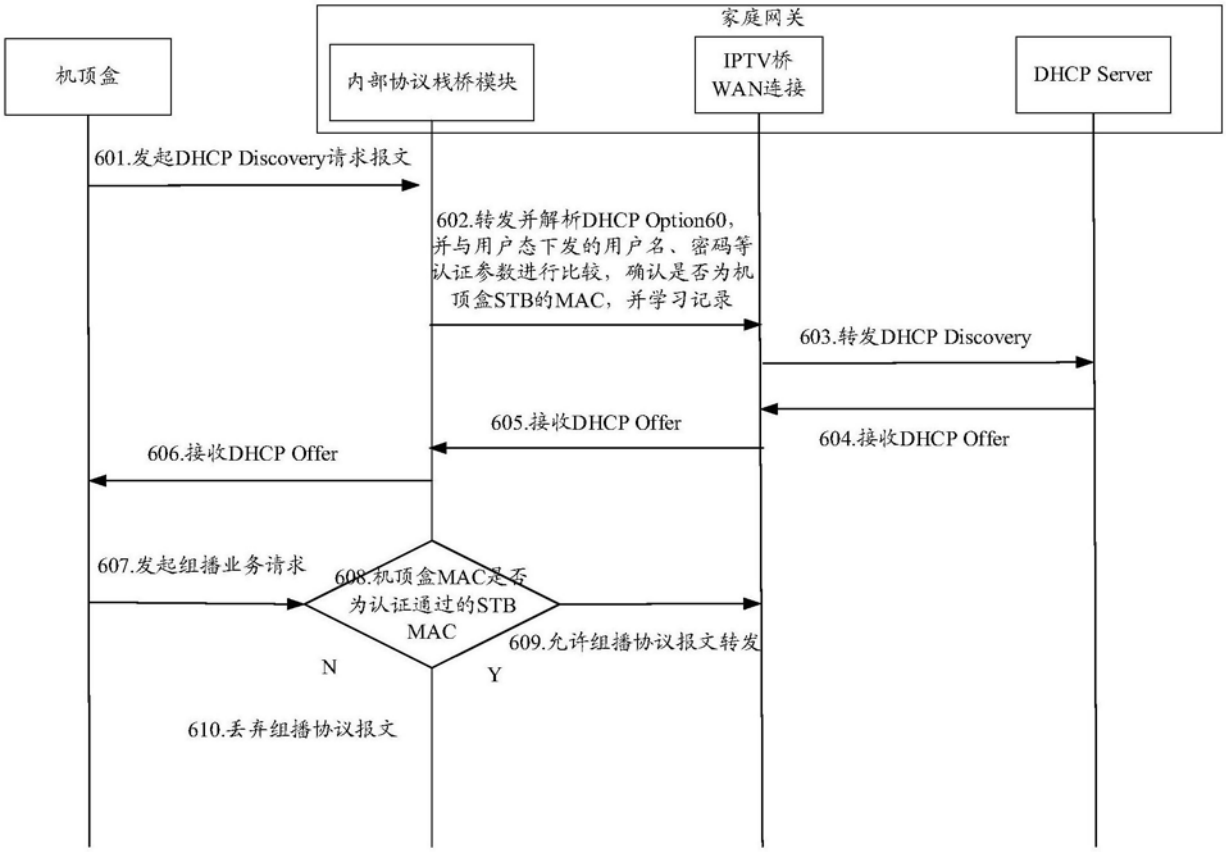

家庭网关
机顶盒
内部协议栈桥模块
IPTV桥WAN连接
DHCP Server
601.发起DHCP Discovery请求报文
602.转发并解析DHCP Option60，并与用户态下发的用户名、密码等认证参数进行比较，确认是否为机顶盒STB的MAC，并学习记录
603.转发DHCP Discovery
604.接收DHCP Offer
605.接收DHCP Offer
606.接收DHCP Offer
607.发起组播业务请求
608.机顶盒MAC是否为认证通过的STB MAC
609.允许组播协议报文转发
N
Y
610.丢弃组播协议报文

图6

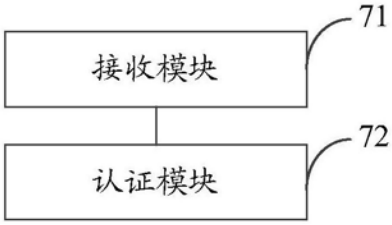


图7

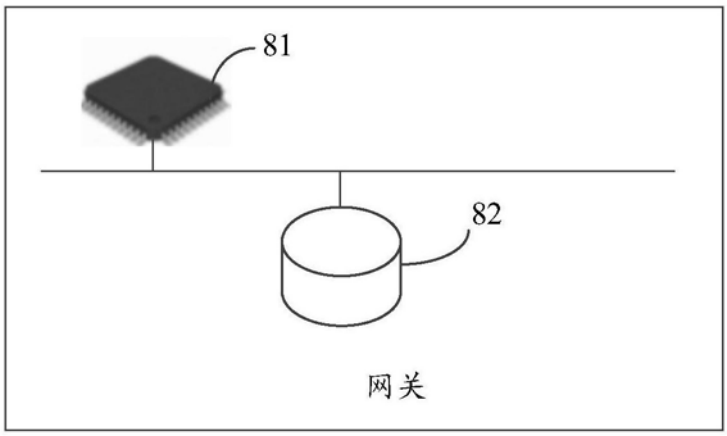


图8