(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102695167 B
(45)授权公告日 2015.04.29

(21)申请号 201210157472.9
(22)申请日 2012.05.18
(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号
(72)发明人 买彦州 何华杰 杨成中 欧阳秀平 朱旭明 敖绮 朱振祺 李磊 罗宏兰 梁鹏
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 程爽
(51)Int.Cl.
H04W 12/00(2009.01)
H04W 8/26(2009.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102036227 A,2011.04.27,
CN 101500014 A,2009.08.05,
CN 101437229 A,2009.05.20,权利要求1-16,说明书第,4页第10行-第7页第6行.
CN 101399853 A,2009.04.01,
CN 101287162 A,2008.10.15,
US 2003072315 A1,2003.04.17,
CN 102036227 A,2011.04.27,

审查员 刘亚男

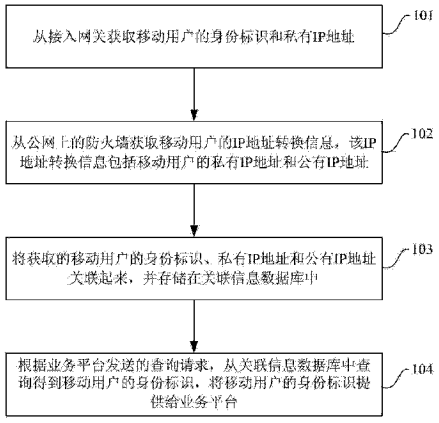
权利要求书2页 说明书8页 附图3页

(54)发明名称

移动用户身份标识管理方法和装置

(57)摘要

本发明公开了一种移动用户身份标识管理方法和装置。该方法包括:从接入网关获取移动用户的身份标识和私有IP地址;从公网上的防火墙获取移动用户的IP地址转换信息,所述IP地址转换信息包括移动用户的私有IP地址和公有IP地址;将获取的移动用户的身份标识、私有IP地址和公有IP地址关联起来,并存储在关联信息数据库中;根据业务平台发送的查询请求,从关联信息数据库中查询得到移动用户的身份标识,将移动用户的身份标识提供给业务平台。本发明技术方案可以有效对移动用户的身份标识进行管理,以便于访问HTTP业务或非HTTP业务。



CN 102695167 B

1. 一种移动用户身份标识管理方法，其特征在于，包括：

从接入网关获取移动用户的身份标识和私有 IP 地址；

从公网上的防火墙获取移动用户的 IP 地址转换信息，所述 IP 地址转换信息包括移动用户的私有 IP 地址和公有 IP 地址；

将获取的移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台；

获取移动用户访问的服务提供商提供的网页地址，并生成唯一的业务标识码，将所述业务标识码作为附加参数，重新定向移动用户到访问的服务商的页面地址；

将所述业务标识码与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

所述根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台具体为：

接收业务平台发送的业务标识码，从所述关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台；

根据业务平台发送的查询请求中移动用户的公有 IP 地址，确定移动用户归属的移动用户身份标识管理装置，将所述业务平台发送的查询请求定向到移动用户归属的移动用户身份标识管理装置。

2. 根据权利要求 1 所述的移动用户身份标识管理方法，其特征在于，所述根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台具体为：

接收业务平台发送的移动用户的公有 IP 地址，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

3. 根据权利要求 1 ～ 2 任一所述的移动用户身份标识管理方法，将移动用户的身份标识提供给业务平台之前还包括：

对发送查询请求的业务平台进行鉴权，以在业务平台鉴权后，将移动用户的身份标识提供给业务平台。

4. 一种移动用户身份标识管理装置，其特征在于，包括：

身份标识获取模块，用于从接入网关获取移动用户的身份标识和私有 IP 地址；

IP 地址获取模块，用于从公网上的防火墙获取移动用户的 IP 地址转换信息，所述 IP 地址转换信息包括移动用户的私有 IP 地址和公有 IP 地址；

关联信息存储模块，用于将获取的移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

身份标识查询模块，用于根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台；

业务标识码生成模块，用于获取移动用户访问的服务商提供的网页地址，并生成唯一的业务标识码，将所述业务标识码作为附加参数，重新定向移动用户到访问的服务商的页面地址；

所述关联信息存储模块，还用于将所述业务标识码与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

所述身份标识查询模块，具体用于接收业务平台发送的业务标识码，从所述关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台；

用户归属地识别模块，用于根据业务平台发送的查询请求中移动用户的公有 IP 地址，确定移动用户归属的移动用户身份标识管理装置，将所述业务平台发送的查询请求定向到移动用户归属的移动用户身份标识管理装置。

5. 根据权利要求 4 所述的移动用户身份标识管理装置，其特征在于，所述身份标识查询模块，具体用于接收业务平台发送的移动用户的公有 IP 地址，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

6. 根据权利要求 4 所述的移动用户身份标识管理装置，其特征在于，还包括：

业务鉴权模块，用于对发送查询请求的业务平台进行鉴权，以在业务平台鉴权后，将移动用户的身份标识提供给业务平台。

7. 根据权利要求 4 所述的移动用户身份标识管理装置，其特征在于，还包括：

伪码获取模块，用于从 BSS 获取移动用户的身份标识对应的伪码信息；

所述关联信息存储模块，还用于将所述伪码信息与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中。

移动用户身份标识管理方法和装置

技术领域

[0001] 本发明涉及通信技术，尤其涉及一种移动用户身份标识管理方法和装置。

背景技术

[0002] 数据业务已成为移动通信的重要应用，且当前数据业务的提供商大部分是通过传统的互联网为用户提供超文本传输协议（HyperText Transfer Protocol，HTTP）业务或非HTTP业务，而移动网络与传统的互联网，即公网之间是两种不同的网络系统，因此，移动用户使用数据业务时，通常需要访问公网，而公网上的业务平台在为用户提供数据业务时，需要获得移动用户的身份标识，以对移动用户进行识别和计费，为移动用户提供数据业务。

[0003] 移动用户在访问数据业务时，移动运营商所在的移动网络会为移动用户分配一个私有网络之间互连的协议（Internet Protocol，IP）地址和端口号，并与移动用户的身份标识对应，其中，移动用户的身份标识是用来对移动用户进行识别的标识信息，可以为移动用户的电话号码、移动用户国际号码（Mobile Subscriber International ISDN/PSTN number，MSISDN）等；同时，移动用户的数据包到达公网时，移动用户的数据包内携带的私有IP地址就会被转换成公有IP地址，以便访问公网。现有技术中对移动用户访问公网时身份标识的管理一般是通过业务网关，或者在移动终端内设置cookie封装身份标识的方式，来对移动用户的身份标识进行管理，以便公网上的业务平台获取移动用户的身份标识，便于对移动用户进行计费，为移动用户提供数据业务。下面将分别对两种现有移动用户的身份标识管理方法进行说明。

[0004] 图1为现有采用业务网关对移动用户身份标识进行管理的流程示意图。如图1所示，现有业务网关对移动用户的身份标识管理方法主要包括以下步骤：

[0005] 步骤100、用户开机时，网关GPRS支持节点（Gateway GPRS Support Node，GGSN）通过无线网络接收到移动用户终端的信息后，向无线应用协议（Wireless Application Protocol，WAP）网关发送远程用户拨号认证服务（Remote Authentication Dial In User Service，RADIUS）用户接入鉴权请求包；

[0006] 步骤200、当WAP网关收到认证请求包后，对GGSN发送认证授权/拒绝包；

[0007] 步骤300、GGSN接收到认证授权/拒绝包，确认认证授权通过时，GGSN给用户终端分配一个私有IP地址，由GGSN向WAP网关发送开始请求包，该开始请求包中包括移动用户的私有IP地址及手机号；

[0008] 步骤400、WAP网关从开始请求包中获得移动用户的私有IP地址和手机号对应关系等信息后，将其存储下来，并向GGSN发送RADIUS开始响应消息，这里的手机号即是作为移动用户的身份标识的MSISDN号；

[0009] 步骤500、GGSN收到WAP网关的RADIUS开始响应消息后，向WAP网关开始发送HTTP用户数据包；

[0010] 步骤600、WAP网关接收到用户数据包后，查询本地数据库中存储的IP地址和手机号对应关系，然后将手机号插入到HTTP包中，再将这些数据包转发给防火墙做网络地址转

换(Network Address Translation,NAT)转换；

[0011] 步骤700、公网上的防火墙接收到WAP网关发送来的移动用户的数据包后，会把用户的私有IP地址转换为公有IP地址，并将移动用户的手机号会包含在转换后的数据包中；

[0012] 步骤800、防火墙将转换过IP地址的HTTP包发送到应用服务器，应用服务器就可以获得数据包中的手机号，即获得移动用户的身份标识，从而可以根据获得移动用户的身份标识对移动用户进行验证，对移动用户计费，并将HTTP业务提供给移动用户。

[0013] 该种基于业务网关，即WAP网关对移动用户的身份标识进行管理方法中，由于需要在HTTP头中插入用户手机号来传递给网站即业务平台，而流媒体等非HTTP业务，则无法通过该种方式将用户手机号码传递给业务平台，因此，该种方法仅能适用于HTTP业务，不适用于移动用户访问非HTTP业务；而且，WAP网关在对移动用户的身份标识进行管理时，需要存储移动用户的私有IP地址和手机号对应关系，并需要将手机号插入到IP数据包中，导致WAP网关开销较大。

[0014] 现有采用在移动终端内置cookie封装身份标识的管理方法，可以实现流媒体等大流量数据的非HTTP业务，但是这种身份标识管理中，当用户在使用互联网业务的时间段内关闭浏览器，保存的cookie文件将会被删除，此时应用服务器端就无法继续获得移动用户的身份标识，而且这种移动用户身份标识管理存在较大的安全隐患，无法保证业务的安全性。

[0015] 综上可以看出，现有对移动用户的身份标识管理方法，要么仅能实现HTTP业务的访问，要么仅能实现非HTTP业务的访问，不利于用户使用数据业务；而且，目前移动用户访问公网上提供的业务时，业务平台记录的均是移动用户的公有IP地址，无法通过该公有IP地址对移动用户进行IP地址溯源，导致网络的安全性能较差。

发明内容

[0016] 本发明提供一种移动用户身份标识管理方法和装置，可有效对移动用户的身份标识进行管理，实现对HTTP业务或非HTTP业务的访问，提高数据业务访问的便利性，实现IP地址溯源，提高网络的安全性。

[0017] 本发明提供一种移动用户身份标识管理方法，包括：

[0018] 从接入网关获取移动用户的身份标识和私有IP地址；

[0019] 从公网上的防火墙获取移动用户的IP地址转换信息，所述IP地址转换信息包括移动用户的私有IP地址和公有IP地址；

[0020] 将获取的移动用户的身份标识、私有IP地址和公有IP地址关联起来，并存储在关联信息数据库中；

[0021] 根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0022] 本发明提供一种移动用户身份标识管理装置，包括：

[0023] 身份标识获取模块，用于从接入网关获取移动用户的身份标识和私有IP地址；

[0024] IP地址获取模块，用于从公网上的防火墙获取移动用户的IP地址转换信息，所述IP地址转换信息包括移动用户的私有IP地址和公有IP地址；

[0025] 关联信息存储模块，用于将获取的移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

[0026] 身份标识查询模块，用于根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0027] 本发明提供的移动用户身份标识管理方法和装置，通过将移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中，从而可以为移动用户访问的业务平台提供身份标识，以便于业务平台对移动用户身份进行识别，实现对移动用户进行计费，为移动用户提供业务；而且，本发明技术方案可由业务平台主动查询移动用户的身份标识，可应用于 HTTP 业务或非 HTTP 业务应用，便于提高移动用户访问数据业务的便利性；同时，本发明技术方案由于保存有移动用户的私有 IP 地址，可有效实现 IP 地址溯源，提高整个业务网络使用的安全性。

附图说明

[0028] 图 1 为现有采用业务网关对移动用户身份标识进行管理的流程示意图；

[0029] 图 2 为本发明移动用户身份标识管理装置实施例的结构示意图；

[0030] 图 3 为本发明移动用户身份标识管理方法实施例一的流程示意图；

[0031] 图 4 为本发明移动用户身份识别管理装置实际应用的结构示意图；

[0032] 图 5 为本发明图 4 中各功能模块交互的流程示意图。

具体实施方式

[0033] 图 2 为本发明移动用户身份标识管理装置实施例的结构示意图。如图 2 所示，本实施例管理装置包括身份标识获取模块 1、IP 地址获取模块 2、关联信息存储模块 3 和身份标识查询模块 4，其中，身份标识获取模块 1 用于从接入网关获取移动用户的身份标识和私有 IP 地址；IP 地址获取模块 2 用于从公网上的防火墙获取移动用户的 IP 地址转换信息，该 IP 地址转换信息包括移动用户的私有 IP 地址和公有 IP 地址；关联信息存储模块 3 与身份标识获取模块 1 和 IP 地址获取模块 2 连接，用于将获取的移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；身份标识查询模块 4 与关联信息存储模块 3 连接，用于根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0034] 本实施例移动用户身份标识管理装置可以从移动用户的接入网关，以及公网上的防火墙，获取移动用户的身份标识、私有 IP 地址和公有 IP 地址，并可将它们关联起来，存储在关联信息数据库中，这样，移动用户在访问业务平台的数据业务时，由于移动用户的身份标识、私有 IP 地址和公有 IP 地址均由移动用户身份标识管理装置存储，这样，当用户发送业务请求至业务平台时，业务平台可以根据该移动用户身份标识管理装置获取移动用户的身份标识，从而可实现访问 HTTP 业务或非 HTTP 业务的移动用户的身份标识的获取，提高移动用户身份标识管理的便利性，可实现对 HTTP 业务或非 HTTP 业务的访问；同时，由于该移动用户身份管理装置存储了移动用户的私有 IP 地址、公有 IP 地址以及身份标识的关联信息，因此，还可实现 IP 地址溯源，可有效提供业务网络的安全性和可靠性。

[0035] 实际应用中，为便于业务平台从本实施例移动用户身份标识管理装置中，获取移

动用户的身份标识，还可以在移动用户访问 HTTP 业务时，生成使用该 HTTP 业务的业务标识码，以便业务平台可根据该业务标识码从移动用户身份标识管理装置获取移动用户的身份标识。具体地，如图 2 所示，本实施例装置包括业务标识码生成模块 5，用于获取移动用户访问的服务商提供的网页地址，生成唯一的业务标识码，并将业务标识码作为附加参数，重新定向移动用户到访问的服务商的页面地址；上述的关联信息存储模块 3 还可用于业务标识码与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；身份标识查询模块 4 具体可用于接收业务平台发送的业务标识码，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台，如此，移动用户访问 HTTP 业务时，业务平台就可以在查询请求中携带该业务标识码，以获取移动用户的身份标识；本实施例移动用户身份标识管理装置接收到该查询请求后，就可以根据查询请求中携带的业务标识码，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0036] 本领域技术人员可以理解的是，当移动用户访问非 HTTP 业务时，业务平台可以通过移动用户携带的公有 IP 地址，实现对移动用户的身份标识的查询，具体地，本实施例上述的身份标识查询模块 4 具体可用于接收业务平台发送的移动用户的公有 IP 地址，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台，如此，移动用户在访问非 HTTP 业务时，业务平台就可以在查询请求中携带移动用户的公有 IP 地址，以获取移动用户的身份标识；本实施例移动用户身份标识管理装置接收到该查询请求后，就可以根据查询请求中携带的公有 IP 地址，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0037] 实际应用中，如图 2 所示，本实施例管理装置还可包括业务鉴权模块 6，用于对发送查询请求的业务平台进行鉴权，以在业务平台鉴权后，身份标识查询模块 4 可将移动用户的身份标识提供给业务平台。如此，只有在对业务平台鉴权通过后，本实施例移动用户身份标识管理装置才将移动用户的身份标识提供给业务平台，可有效保证移动用户信息的安全性，防止业务平台恶意获取移动用户信息，对移动用户进行扣费等情况。

[0038] 实际应用中，由于每个区域的移动用户均归属自身所在区域的移动网络管理，每个区域的移动网络可分别配置有本实施例移动用户身份标识管理装置，从而使得每个移动用户的身份标识与私有 IP 地址、公有 IP 地址等的关联信息均被自身所归属的移动用户身份标识管理装置所管理，因此，在移动用户访问其它区域的网络中的数据业务时，相应的，位于其他区域的业务平台在查询移动用户的身份标识时，只能发送到移动用户所在地的移动用户身份标识管理装置进行查询，因此，为使得移动用户身份标识查询的有效性，本实施例移动用户身份标识管理装置还可将业务平台的查询请求定向到其需要查询的移动用户归属的管理装置。具体地，如图 2 所示，本实施例装置还可包括有用户归属地识别模块 7，用于根据业务平台发送的查询请求中移动用户的公有 IP 地址，确定移动用户归属的移动用户身份标识管理装置，将业务平台发送的查询请求定向到移动用户归属的移动用户身份标识管理装置，这样，业务平台查询的移动用户不归属本地移动用户身份标识管理装置时，就可以通过用户归属地识别模块 7 将业务平台的查询请求重定向到其归属的移动用户身份标识管理装置，以便由其归属的移动用户身份标识管理装置处理该查询请求，其中，用户归属地识别模块 7 与业务鉴权模块 6 连接，以便业务鉴权模块 6 接收到业务平台发送的查询

请求信息后，并通过身份标识查询模块 4 查询不属于本地用户后，可将业务平台发送的查询请求发送至用户归属地识别模块 7 进行处理。

[0039] 实际应用中，为保证移动用户身份信息的安全性，本实施例还可通过获取移动用户的伪码信息，并将其与移动用户的身份标识、私有 IP 地址和公有 IP 地址等信息关联起来，以便为业务平台提供移动用户的伪码信息，避免移动用户相关信息被窃取。具体地，如图 2 所示，本实施例装置还可包括有伪码获取模块 8，用于从 BSS 获取移动用户的身份标识对应的伪码信息；上述的关联信息存储模块 3，还可用于将伪码信息与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中。这样在业务平台查询移动用户的身份标识时，可将移动用户的伪码信息提供给业务平台，以保证移动用户身份信息的安全性。

[0040] 本实施例移动用户身份标识管理装置中，通过将移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中，从而可以为移动用户访问的业务平台提供身份标识，以便于业务平台对移动用户身份进行识别，实现对移动用户进行计费，为移动用户提供业务；而且，本实施例技术方案可由业务平台主动查询移动用户的身份标识，可应用于 HTTP 业务或非 HTTP 业务应用，便于提高移动用户访问数据业务的便利性；同时，本实施例身份标识管理装置保存有移动用户的私有 IP 地址，可有效实现 IP 地址溯源，提高整个业务网络使用的安全性。

[0041] 图 3 为本发明移动用户身份标识管理方法实施例一的流程示意图。如图 3 所示，本实施例移动用户身份标识管理方法可包括如下步骤：

[0042] 步骤 101、从接入网关获取移动用户的身份标识和私有 IP 地址；

[0043] 步骤 102、从公网上的防火墙获取移动用户的 IP 地址转换信息，该 IP 地址转换信息包括移动用户的私有 IP 地址和公有 IP 地址；

[0044] 步骤 103、将获取的移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中；

[0045] 步骤 104、根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0046] 本实施例可应用于移动用户访问公网上的数据业务时，对移动用户的身份标识进行管理，以提高移动用户身份标识管理的便利性，满足移动用户对 HTTP 业务或非 HTTP 业务的访问，提高移动用户访问数据业务的便利性，而且可以实现 IP 地址溯源，确保整个业务网络使用的安全性和可靠性。

[0047] 本实施例中，为便于移动用户对 HTTP 业务的访问和计费，在移动用户访问 HTTP 业务的服务商时，可为该访问的业务生成唯一的业务标识码，以便根据该业务标识码查询移动用户的身份标识，实现对移动用户的计费，以便于为移动用户提供业务。具体地，通过获取移动用户访问的服务提供商提供的网页地址，生成唯一的业务标识码，并将业务标识码作为附加参数，重新定向移动用户到访问的服务商的页面地址；同时，将生成的业务标识码与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联起来，并存储在关联信息数据库中，这样，当接收到业务平台发送的业务标识码，即可根据该业务标识码从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。

[0048] 本实施例中，对非 HTTP 业务访问时，为便于业务平台获取移动用户的身份标识信

息，上述的根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台还可为：接收业务平台发送的移动用户的公有 IP 地址，根据该公有 IP 地址从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台。这样，在移动用户访问非 HTTP 业务时，即可以根据业务平台发送的查询请求中的移动用户的公有 IP 地址，查询并获得移动用户的身份标识。

[0049] 本实施例中，为提高移动用户身份的安全性，将移动用户的身份标识提供给业务平台之前还可包括：对发送查询请求的业务平台进行鉴权，以在业务平台鉴权后，将移动用户的身份标识提供给业务平台。

[0050] 本实施例中，为便于获取不同归属地移动用户的身份标识，当接收到业务平台的查询请求后，还可根据业务平台发送的查询请求中移动用户的公有 IP 地址，确定移动用户归属的移动用户身份标识管理装置，并将业务平台发送的查询请求定向到移动用户归属的移动用户身份标识管理装置。

[0051] 本实施例中，还可通过获取移动用户的伪码信息，并将其与移动用户的身份标识、私有 IP 地址和公有 IP 地址等信息关联起来，这样，在业务平台查询移动用户的身份标识时，可直接将移动用户的伪码信息提供给业务平台，以保证移动用户身份的安全性和可靠性。

[0052] 为对本发明实施例技术方案有更好的了解，下面将以本发明的具体应用为例进行说明。

[0053] 图 4 为本发明移动用户身份识别管理装置实际应用的结构示意图；图 5 为本发明图 4 中各功能模块交互的流程示意图。如图 4 所示，本实施例移动用户身份识别管理装置可单独设置，并与接入网关 10 和公网防火墙 20 连接，使得移动用户身份识别管理装置 30 可从接入网关 10 获取移动用户的身份标识、私有 IP 地址及私有端口信息；并从公网防火墙 20，也即 Internet 防火墙获取 IP 地址转换前移动用户的私有 IP 地址，以及 IP 地址转换后的公有 IP 地址和公有端口信息；同时，该移动用户身份识别管理装置 30 还可与业务支撑系统 40 连接，用于从基站子系统（Base Station Subsystem，BSS）获取移动用户的身份标识对应的伪码信息，并可将该伪码信息与移动用户的身份标识、私有 IP 地址和公有 IP 地址关联并存储起来。可以看出，移动用户通过接入网连接公网时，移动用户身份标识管理装置 30 会将移动用户的身份标识、私有 IP 地址、私有端口信息、公有 IP 地址、公有端口信息以及伪码信息关联起来，这样，移动用户身份标识管理装置 30 就可以存储移动用户访问公网时，其处于移动网络册的相关身份识别信息，以及进入公网时对应的相关身份识别信息（即公有 IP 地址及公有端口信息）。

[0054] 如图 4 所示，移动用户身份标识管理装置 30 具体可以包括 RADIUS 代理模块 301、BSS 接口模块 302、NAT 接口模块 303、标识鉴权模块 304 和标识关联存储模块 305 组成，其中，RADIUS 代理模块 301 即相当于上述本发明装置实施例中的身份标识获取模块，BSS 接口模块 302 相当于上述的伪码获取模块，NAT 接口模块 303 相当于上述的 IP 地址获取模块，标识鉴权模块 304 相当于上述的业务鉴权模块、业务标识码生成模块和身份标识查询模块的集成模块，标识关联存储模块 305 相当于上述的关联信息存储模块。

[0055] 结合上述图 4 所示，对移动用户使用业务时的步骤进行说明，具体地，如图 5 所示，在移动用户发起 HTTP 业务请求后，需要使用业务时各功能模块之间的交互的具体过程如

下：

[0056] 步骤 201、当移动用户通过接入网关 10 接入公网时，可向 RADIUS 代理模块启动计费鉴权流程，将移动用户的身份标识及私有 IP 地址等 RADIUS 信息发送到 RADIUS 代理模块；

[0057] 步骤 202、RADIUS 代理模块接收到 RADIUS 信息后，将 RADIUS 信息发送至标识关联存储模块，将移动用户的身份标识、私有 IP 地址及私有端口信息存储在关联信息数据库中；

[0058] 步骤 203、当移动用户的业务请求发送到公网防火墙时，公网防火墙会将 IP 地址转换信息发送给 NAT 接口模块，其中，IP 地址转换信息包括转换前后的移动用户的私有 IP 地址、以及转换后的公有 IP 地址及公有端口信息；

[0059] 步骤 204、NAT 接口模块会从公网防火墙接收 NAT 转换前的私有 IP 地址，以及转换后的公有 IP 地址及公有端口信息，并将这些信息发送给标识关联存储模块；

[0060] 步骤 205、标识关联存储模块将接收到的移动用户的身份标识、私有 IP 地址、私有端口信息、公有 IP 地址以及公有端口信息关联并存储；

[0061] 步骤 206、移动用户要访问的服务商，会将其要访问的网页地址 URL 编码后，作为参数重定向到标识鉴权模块；

[0062] 步骤 207、标识鉴权模块将会为移动用户访问本地业务计费生成唯一的业务使用标识码 S — KEY；

[0063] 步骤 208、标识鉴权模块将 S — KEY 发送到标识关联存储模块，由标识关联存储模块将 S — KEY、移动用户的身份标识、私有 IP 地址和公有 IP 地址关联并存储；

[0064] 步骤 209、标识鉴权模块将 S — KEY 作为附加参数，重定向移动用户到初始访问的服务页面；

[0065] 步骤 210、服务商根据 S — KEY 向标识鉴权模块请求查询移动用户的身份标识；

[0066] 步骤 211、标识鉴权模块对服务商鉴权后，将移动用户的身份标识返回给服务商，服务商获得移动用户的身份标识后，即可实现对移动用户的识别、计费。

[0067] 上述为移动用户访问 HTTP 业务时的流程，当移动用户请求非 HTTP 业务时，服务商可以将移动用户请求信息中的公有 IP 地址及公有端口信息作为查询请求信息的一部分，发送给移动用户身份标识管理装置，以便移动用户身份标识管理装置根据查询请求信息中的移动用户的公有 IP 地址，对服务商进行鉴权、查询移动用户的身份标识，并将移动用户的身份标识提供给服务商。

[0068] 如图 4 所示，考虑到网络实际需要，移动用户身份标识管理装置 30 还可包括有计费标识网关服务器 306，具体可包括计费标识代理模块 3061 和路由分发模块 3062，当标识鉴权模块 304 接收到业务平台的查询请求，发现无相应的移动用户时，可将其发送到计费标识网关服务器 306，由其中的计费标识代理模块 3061 确认所要查询的移动用户归属的移动用户身份标识管理装置，并通过路由分发模块 3062 将查询请求定向到移动用户归属的移动用户身份标识管理装置进行处理；或者，业务平台每次发送的查询请求均可发送到计费标识网关服务器 306，由计费网关服务器 306 确认移动用户归属地后，再将其查询请求发送给本地或发送到其归属的移动用户身份标识管理装置。

[0069] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过

程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0070] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

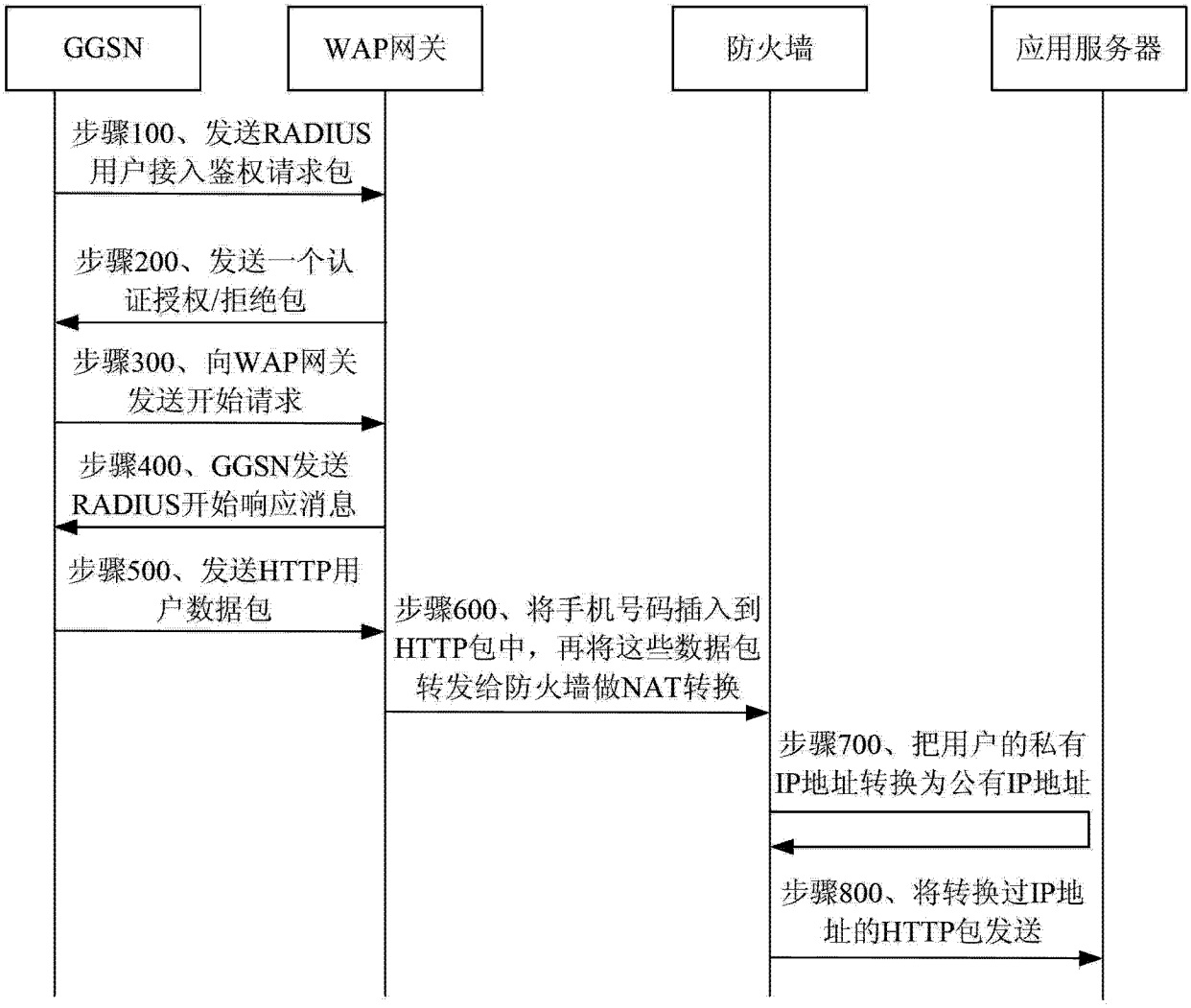

GGSN
WAP网关
防火墙
应用服务器
步骤100、发送RADIUS用户接入鉴权请求包
步骤200、发送一个认证授权/拒绝包
步骤300、向WAP网关发送开始请求
步骤400、GGSN发送RADIUS开始响应消息
步骤500、发送HTTP用户数据包
步骤600、将手机号码插入到HTTP包中，再将这些数据包转发给防火墙做NAT转换
步骤700、把用户的私有IP地址转换为公有IP地址
步骤800、将转换过IP地址的HTTP包发送

图 1

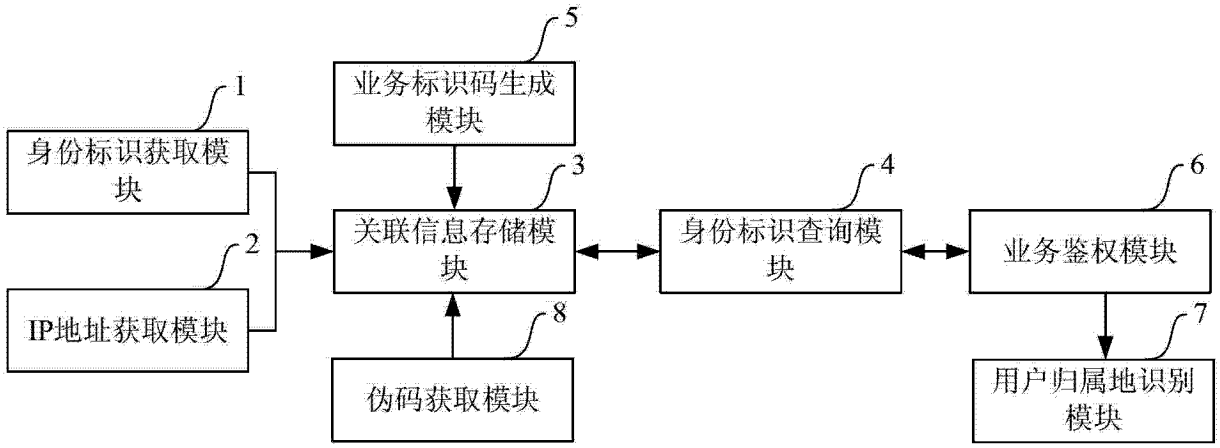

1
身份标识获取模块
2
IP地址获取模块
5
业务标识码生成模块
3
关联信息存储模块
8
伪码获取模块
4
身份标识查询模块
6
业务鉴权模块
7
用户归属地识别模块

图 2

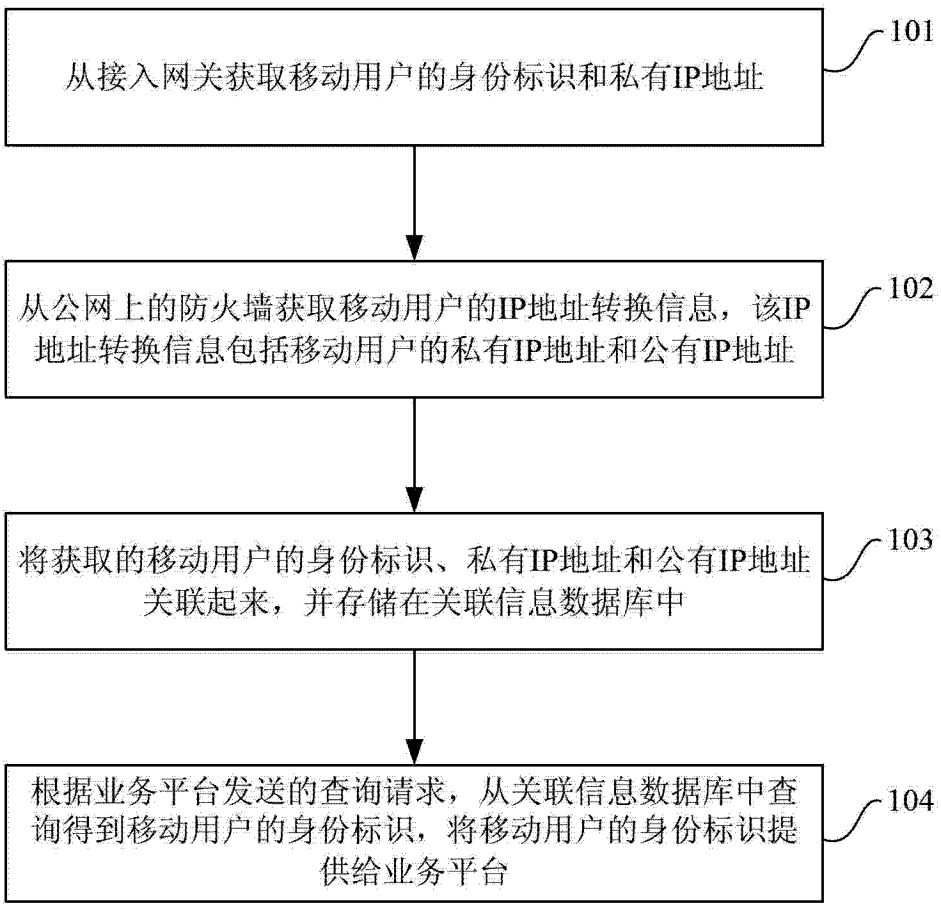

从接入网关获取移动用户的身份标识和私有IP地址
101
从公网上的防火墙获取移动用户的IP地址转换信息，该IP地址转换信息包括移动用户的私有IP地址和公有IP地址
102
将获取的移动用户的身份标识、私有IP地址和公有IP地址关联起来，并存储在关联信息数据库中
103
根据业务平台发送的查询请求，从关联信息数据库中查询得到移动用户的身份标识，将移动用户的身份标识提供给业务平台
104

图 3

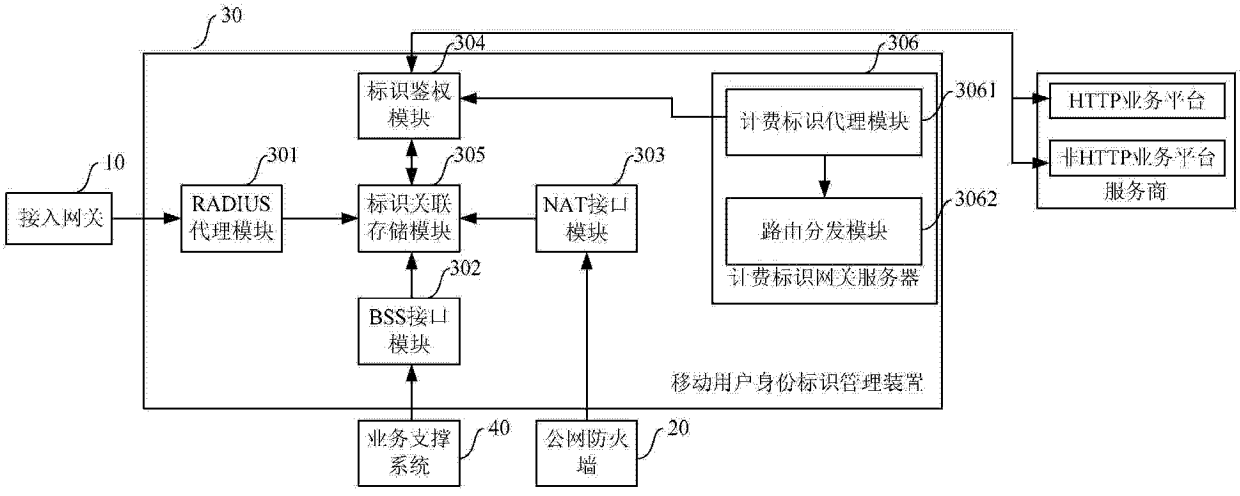

30
304
306
标识鉴权模块
计费标识代理模块
3061
HTTP业务平台
非HTTP业务平台
服务商
10
接入网关
301
RADIUS代理模块
305
标识关联存储模块
303
NAT接口模块
3062
路由分发模块
计费标识网关服务器
302
BSS接口模块
移动用户身份标识管理装置
业务支撑系统
40
公网防火墙
20

图 4

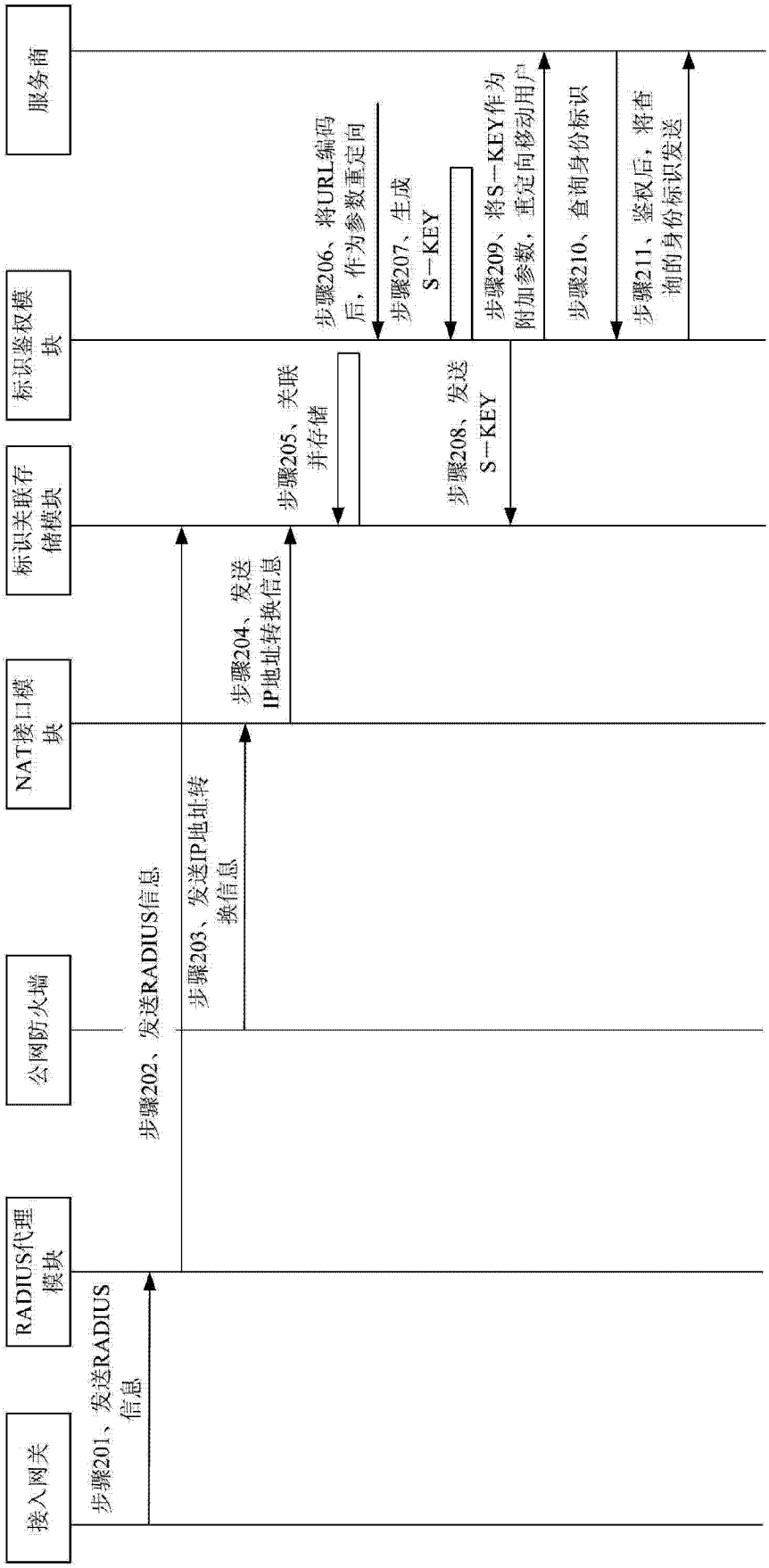

接入网关
RADIUS代理模块
公网防火墙
NAT接口模块
标识关联存储模块
标识鉴权模块
服务商
步骤201、发送RADIUS信息
步骤202、发送RADIUS信息
步骤203、发送IP地址转换信息
步骤204、发送IP地址转换信息
步骤205、关联并存储
步骤206、将URL编码后，作为参数重定向
步骤207、生成S－KEY
步骤208、发送S－KEY
步骤209、将S－KEY作为附加参数，重定向移动用户
步骤210、查询身份标识
步骤211、鉴权后，将查询的身份标识发送

图 5