(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 104980412 A
(43)申请公布日 2015.10.14

(21)申请号 201410148906.8

(22)申请日 2014.04.14

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 修超

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)

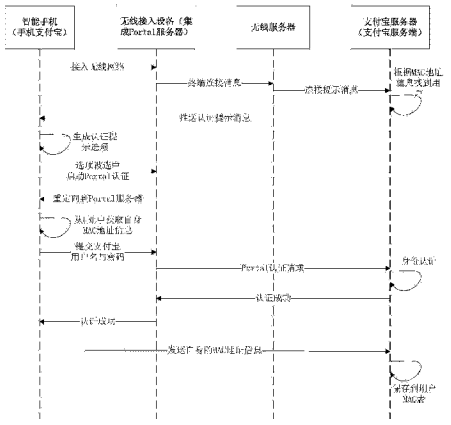
权利要求书3页 说明书11页 附图6页

(54)发明名称

一种应用客户端、服务端及对应的Portal认证方法

(57)摘要

本发明提供一种应用客户端、服务端及对应的Portal认证方法，基于网络与应用系统的联动进行实现，用户便携终端在接收到应用服务器推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；在确定所述认证提示选项被用户选中后启动Portal认证，在Portal认证启动后获取Portal服务器返回的本便携终端的MAC地址信息，并在Portal认证过程中使用在应用服务端进行应用登录的用户名及密码作为Portal认证的用户名及密码；将Portal服务器返回的本便携终端的MAC地址信息发送给所述应用服务器。本发明方便了用户使用Portal认证的操作，在很大程度上避免了用户忘记Portal认证，方便了对Portal认证机制不熟悉的用户。



CN 104980412 A

1. 一种应用客户端，应用于便携终端上，包括：推送处理单元、Portal 代理单元以及 MAC 同步单元，其特征在于：

推送处理单元，用于在接收到应用服务端推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；

Portal 代理单元，用于在确定所述认证提示选项被用户选中后启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回的本便携终端的 MAC 地址信息，并在 Portal 认证过程中使用该应用客户端在应用服务端进行应用登录的用户名及密码作为 Portal 认证的用户名及密码；

MAC 同步单元，用于将 Portal 服务器返回的本便携终端的 MAC 地址信息发送给所述应用服务端。

2. 如权利要求 1 所述的客户端，其特征在于：

Portal 代理单元获取 Portal 服务器返回本便携终端的 MAC 地址信息的方式具体为：从 Portal 服务器返回的重定向 URL 中获取本便携终端的 MAC 地址信息，其中该 MAC 地址信息为该 URL 的传递参数。

3. 如权利要求 1 所述的客户端，其特征在于：

所述 Portal 代理单元，进一步用于在收到浏览器的应用关联组件发送的认证通知时启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回本便携终端的 MAC 地址信息，并在认证过程中使用该应用的用户名及密码作为 Portal 认证的用户名及密码。

4. 如权利要求 1 所述的客户端，其特征在于：所述认证提示消息中还携带有第三方应用标识，所述推送处理单元进一步用于在 Portal 认证成功后根据认证提示消息携带的第三方应用标识启动对应的第三方应用；其中该第三方应用对应于预定商户，该预定商户对应于该便携终端所连接的无线网络。

5. 如权利要求 1 所述的客户端，其特征在于：所述认证提示消息中还携带有与该商户对应的服务信息，所述推送处理单元进一步用于在 Portal 认证成功后展示该服务信息。

6. 如权利要求 1 所述的客户端，其特征在于：所述 Portal 代理单元进一步用于在所述认证提示选项被选中后启动 Portal 认证前先检查用户是否处于应用登录状态，如果是，则继续启动 Portal 认证，否则调用应用登录界面到前台促使用户进行应用登录。

7. 一种 Portal 认证方法，应用于便携终端上，其特征在于，该方法包括：

在接收到应用服务器推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；

在确定所述认证提示选项被用户选中后启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回的本便携终端的 MAC 地址信息，并在 Portal 认证过程中使用在应用服务端进行应用登录的用户名及密码作为 Portal 认证的用户名及密码；

将 Portal 服务器返回的本便携终端的 MAC 地址信息发送给所述应用服务器。

8. 如权利要求 7 所述的方法，其特征在于：其中获取 Portal 服务器返回本便携终端的 MAC 地址信息的方式具体为：从 Portal 服务器返回的重定向 URL 中获取本便携终端的 MAC 地址信息，其中该 MAC 地址信息为该 URL 的传递参数。

9. 如权利要求 7 所述的方法，其特征在于：还包括：

在收到浏览器的应用关联组件发送的认证通知时启动 Portal 认证，在 Portal 认证启

动后获取 Portal 服务器返回本便携终端的 MAC 地址信息，并在认证过程中使用该应用的用户名及密码作为 Portal 认证的用户名及密码。

10. 如权利要求 7 所述的方法，其特征在于：所述认证提示消息中还携带有第三方应用标识，该方法还包括：

在 Portal 认证成功后根据认证提示消息携带的第三方应用标识启动对应的第三方应用；其中该第三方应用对应于预定商户，该预定商户对应于该便携终端所连接的无线网络。

11. 如权利要求 10 所述的方法，其特征在于：所述认证提示消息中还携带有与该商户对应的服务信息，该方法还包括：

在 Portal 认证成功后展示该服务信息。

12. 如权利要求 7 所述的方法，其特征在于：该方法还包括：

在所述认证提示被选中后启动 Portal 认证前先检查用户是否处于应用登录状态，如果是，则继续启动 Portal 认证，否则调用应用登录界面到前台促使用户进行应用登录。

13. 一种应用服务端，应用于服务器上，与应用客户端以及无线服务器进行联动，其中该无线服务器管理至少一个无线网络中的无线接入设备，该应用服务端包括推送管理单元以及 MAC 维护单元，其特征在于：

推送管理单元，用于在接收到无线服务器发送的终端连接消息时，获取该消息中携带的便携终端的 MAC 地址信息，并在自身的用户 MAC 表中查找与该 MAC 地址对应的用户，若查找到对应的用户，则向该用户的应用客户端推送认证提示消息；

Portal 认证单元，用于在接收到 Portal 认证请求时，对该请求中的用户名以及密码是否属于本应用的注册用户，如果是，则确定该用户的 Portal 认证成功；

MAC 维护单元，用于在接收到用户的应用客户端发送的 MAC 地址信息时，将该 MAC 地址信息与该用户之间的对应关系更新到所述用户 MAC 表中。

14. 如权利要求 13 所述的服务端，其特征在于：

所述终端连接消息中进一步携带有与用户便携终端当前连接的无线网络对应的商户标识，所述推送管理单元进一步用于，根据该商户标识在自身的商户信息表中查找对应的服务信息，并将查找到的服务信息携带在认证提示消息中发送给查到的用户的客户端。

15. 如权利要求 14 所述的服务端，其特征在于：所述推送管理单元进一步用于，根据该商户标识在自身的商户信息表中查找对应的服务信息，并将该第三方应用标识携带在认证提示消息中发送给查到到的用户的客户端。

16. 一种 Portal 认证服务方法，应用于应用服务器上，与便携终端以及无线服务器进行联动，其中该无线服务器管理至少一个无线网络中的无线接入设备，其特征在于，该方法包括：

在接收到无线服务器发送的终端连接消息时，获取该消息中携带的便携终端的 MAC 地址信息，并在自身的用户 MAC 表中查找与该 MAC 地址对应的用户，若查找到对应的用户，则向该用户推送认证提示消息；

在接收到 Portal 认证请求时，对该请求中的用户名以及密码是否属于本应用的注册用户，如果是，则确定该用户的 Portal 认证成功；

在接收到用户发送的 MAC 地址信息时，将该 MAC 地址信息与该用户之间的对应关系更新到所述用户 MAC 表中。

17. 如权利要求 17 所述的方法，其特征在于：

所述终端连接消息中进一步携带有与用户便携终端当前连接的无线接入设备对应的商户标识，该方法还包括：

根据该商户标识在自身的商户信息表中查找对应的服务信息，并将该服务信息携带在认证提示消息中发送给查到到的用户的客户端。

18. 如权利要求 19 所述的方法，其特征在于：该方法还包括：

根据该商户标识在自身的商户信息表中查找对应的服务信息，并将该第三方应用标识携带在认证提示消息中发送给查到的用户的客户端。

一种应用客户端、服务端及对应的 Portal 认证方法

技术领域

[0001] 本申请涉及互联网技术领域，尤其涉及一种应用客户端以及应用服务端。

背景技术

[0002] 随着移动互联网上下游产业的发展，目前通过移动方式接入网络获得服务的方式已经逐渐成为主流。人们正在使用智能手机或 Pad 类便携终端享受包括网络购物以及社交等各种移动应用。即便在家中，依然有非常多的用户倾向于使用便携终端来接入网络。当用户处于公共场合时，用户可以使用 3G / 4G 这样的移动数据接入技术接入互联网，另一方面当用户所处的公共场合有免费的无线网络接入服务时，用户通常会选择通过 WLAN（无线局域网）方式接入互联网，相对于移动数据接入而言，WLAN 接入方式通常能够提供更为稳定和快速的互联网接入体验，而且可以大幅度节约用户的流量资费。

[0003] 海底捞或者星巴克这样的公众场合通常会为用户提供无线接入服务，作为商户的海底捞或者星巴克需要架设和管理自身的无线网络；比如说部署包括无线接入点 AP 以及无线控制器 AC 在内的无线网络。此时海底捞等商户不仅是无线网络的拥有者也是管理者，其需要考虑无线接入服务的安全性以及服务质量。

[0004] 从安全角度来说，用户身份认证无疑是极为重要的安全机制。WPA / WPA2 等无线认证方式被广泛应用于家庭网络等小型网络，网络的管理员可以将密钥以相对安全的方式告知每一个合法用户。在一些商户部署中型或大型网络中，密钥的逐一通知显然是不可接受的，而且上述机制运行在无线链路层级，兼容性比较差，比如说有的用户的便携终端是比较老的机型，其使用的无线技术可能无法支持 WPA2 这样的认证方式。

[0005] Portal 认证运行在网络层以上，其具有非常好的普适性，与用户便携终端的硬件以及所使用的无线接入技术几乎无关。只要用户能够接入到无线网络，那么用户可以基于标准的 Portal 认证流程来获得上网权限。然而 Portal 认证技术事实上源自 PC 互联网时代，其存在不适应移动互联网使用特点的技术问题。

[0006] 请参考图 1，以中国联通提供的 WLAN 接入互联网服务为例，假设用户的智能手机成功连接到中国联通的 AP（接入无线网络）之后，用户的智能手机屏幕上方的消息提示栏上无线网络连接图标 11 显示已经成功连接到无线网络，然而此时用户刷新微博却无法成功。造成该问题的根本原因是，很多普通用户会习惯性地认为无线网络连接成功之后便能访问外部网络（通常是互联网），但事实上用户只是成功地通过无线的方式连接到联通的无线网络了，在没有通过 Portal 认证之前，除了一些特殊的面认证站点（比如 DHCP 服务器）之外，用户是没有办法访问互联网的。

[0007] 对于用户终端而言，Portal 认证是基于浏览器实现的，很多普通用户并不知道其需要开启浏览器来启动一次 Portal 认证过程，因为这种认证机制与用户家里无线网络的认证方式并不相同。从另一个角度看，即便部分用户知道 Portal 认证的工作原理，但依然会遇到不便利的问题。比如说，由于用户的便携终端通常有自动连接那些曾经连接过的无线网络的功能，而很多智能手机又通常会在无线网络连接成功的情况下自动关闭 3G 等移

动数据连接。一旦用户的智能手机自动连接到该无线网络，而用户又没有注意到该状况，则用户不会通过浏览器发起 Portal 认证，那么此时用户终端由于移动数据连接被关闭将无法访问互联网，很多需要时刻在线进行数据交换的应用将出现问题。

发明内容

[0008] 有鉴于此，本申请提供一种应用客户端，应用于便携终端上，包括：推送处理单元、Portal 代理单元以及 MAC 同步单元，其中：

[0009] 推送处理单元，用于在接收到应用服务端推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；

[0010] Portal 代理单元，用于在确定所述认证提示选项被用户选中后启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回的本便携终端的 MAC 地址信息，并在 Portal 认证过程中使用该应用客户端在应用服务端进行应用登录的用户名及密码作为 Portal 认证的用户名及密码；

[0011] MAC 同步单元，用于将 Portal 服务器返回的本便携终端的 MAC 地址信息发送给所述应用服务端。

[0012] 本申请还提供一种 Portal 认证方法，应用于便携终端上，该方法包括：

[0013] 步骤 A，在接收到应用服务器推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；

[0014] 步骤 B，在确定所述认证提示选项被用户选中后启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回的本便携终端的 MAC 地址信息，并在 Portal 认证过程中使用在应用服务端进行应用登录的用户名及密码作为 Portal 认证的用户名及密码；

[0015] 步骤 C，将 Portal 服务器返回的本便携终端的 MAC 地址信息发送给所述应用服务器。

[0016] 本申请还提供一种应用服务端，应用于服务器上，与应用客户端以及无线服务器进行联动，其中该无线服务器管理至少一个无线网络中的无线接入设备，该应用服务端包括推送管理单元以及 MAC 维护单元，其中：

[0017] 推送管理单元，用于在接收到无线服务器发送的终端连接消息时，获取该消息中携带的便携终端的 MAC 地址信息，并在自身的用户 MAC 表中查找与该 MAC 地址对应的用户，若查找到对应的用户，则向该用户的应用客户端推送认证提示消息；

[0018] Portal 认证单元，用于在接收到 Portal 认证请求时，对该请求中的用户名以及密码是否属于本应用的注册用户，如果是，则确定该用户的 Portal 认证成功；

[0019] MAC 维护单元，用于在接收到用户的应用客户端发送的 MAC 地址信息时，将该 MAC 地址信息与该用户之间的对应关系更新到所述用户 MAC 表中。

[0020] 本申请还提供一种 Portal 认证服务方法，应用于应用服务器上，与便携终端以及无线服务器进行联动，其中该无线服务器管理至少一个无线网络中的无线接入设备，该方法包括：

[0021] 步骤 a，在接收到无线服务器发送的终端连接消息时，获取该消息中携带的便携终端的 MAC 地址信息，并在自身的用户 MAC 表中查找与该 MAC 地址对应的用户，若查找到对应的用户，则向该用户推送认证提示消息；

[0022] 步骤 b，在接收到 Portal 认证请求时，对该请求中的用户名以及密码是否属于本应用的注册用户，如果是，则确定该用户的 Portal 认证成功

[0023] 步骤 c，在接收到用户发送的 MAC 地址信息时，将该 MAC 地址信息与该用户之间的对应关系更新到所述用户 MAC 表中。

[0024] 相较于现有技术，本申请极大地方便了用户使用 Portal 认证的操作，在很大程度上避免了用户忘记 Portal 认证无法通过无线网络上网，或者因为不知道 Portal 认证机制无法通过无线网络上网的问题；本申请更加适应移动互联网环境下的用户需求。

附图说明

[0025] 图 1 是用户忘记 Portal 认证时刷新微博的结果示意图。

[0026] 图 2 是一种典型的 Portal 认证组网示意图。

[0027] 图 3 是本申请一种实施方式中联动系统中各节点的硬件以及逻辑结构图。

[0028] 图 4 是本申请一种实施方式处理流程图。

[0029] 图 5 是本申请一种实施方式中详细处理流程图。

[0030] 图 6 是本申请一种实施方式中为商户与用户提供便捷交互过程示意图。

具体实施方式

[0031] 在介绍本申请具体实施方式之前，先描述 Portal 认证机制以便本领域普通技术人员更清晰地了解本申请的技术优势。请参考图 2 的组网示例，在该组网环境下，智能手机在成功连接到无线网络之后，用户通过访问外部网络（比如互联网上的某个站点）将触发 Portal 认证，Portal 认证过程可以简述如下：

[0032] 步骤 I，用户使用浏览器访问任意一个网址，比如 www.weibo.com，由于该站点的 IP 地址通常不在 AC（无线接入控制服务器）的例外名单（免认证）中，且该用户的 IP 地址也不 AC 的用户白名单中，流程转入步骤 II；

[0033] 步骤 II，无线接入设备使用 HTTP 重定向方式将用户的访问重定向到 Portal 服务器（通常集成在 AC 中）上，Portal 服务器返回 Portal 认证页面给浏览器；

[0034] 步骤 III，用户在 Portal 认证页面上输入用户名和密码并提交认证请求，Portal 服务器转而将认证请求提交给无线接入设备；

[0035] 步骤 IV，无线接入设备向认证服务器发起 Portal 认证，以验证用户输入的用户名和密码是否匹配一个合法用户；

[0036] 步骤 V，若用户 Portal 认证通过，无线接入设备将用户的 IP 地址加入用户白名单中；

[0037] 步骤VI，用户再次访问任意互联网站点，由于用户的 IP 地址已经在用户白名单中了，因此用户的访问将会被允许通过。

[0038] 步骤 I 到步骤VI描述了一次典型的 Portal 认证的过程，这一过程与 PC 上的 Portal 认证过程大致相同。为了适应移动互联网的需求，方便用户使用，在更加优化的解决方案中，基于无线接入设备（比如前述的 AC）与应用服务器之间联动，Portal 认证过程可以被简化。在步骤 II 中，Portal 服务器返回的 Portal 认证页面上携带有应用关联组件（比如支付宝关联组件）；支付宝关联组件在浏览器上加载之后其将执行手机支付宝的调用操

作，将手机支付宝调用到手机前台，通知手机支付宝代理执行 Portal 认证。假设用户此时已经登录手机支付宝，那么手机支付宝根据该通知，使用用户的支付宝用户名以及密码进行 Portal 认证。在步骤 IV 中，由于使用了支付宝的用户名和密码，此时对应的认证服务器这个角色将由应用服务器（支付宝服务器）来承担，这样一来可以免去用户记忆 Portal 认证用户名和密码的过程，转而用支付宝用户名和密码进行替代。

[0039] 考虑到手机支付宝这一应用可能经常性地保持登录状态，因此在很多时候用户可以不用再打开浏览器，而且在 Portal 认证过程中省掉输入支付宝用户名和密码的操作。更为重要的是，由于支付宝通常与很多商户都建立合作关系，因此，用户去很多商户的场所都可以使用统一的用户名和密码来实现 Portal 认证。当然，如果一个用户不是支付宝用户，那么该用户依然可以通过传统的 Portal 认证方式来进行 Portal 认证，只是其可能需要事先通过注册获得 Portal 用户名和密码，或者通过短信等其他方式获得一个临时性的 Portal 用户名和密码，对于这类用户，其 Portal 用户名和密码的认证仍然在认证服务器上进行。这个方案方便了支付宝用户或类似应用下的注册用户的 Portal 认证。但是这样的实现仍然没有能够深入地解决背景技术所提出的技术问题。

[0040] 请继续参考图 2，本申请在上述 Portal 认证实现方式的基础上继续进行深度优化。在一种实施方式中，本申请基于网络系统与应用系统的深度联动。其中网络系统在物理上包括位于商户无线网络中的无线接入设备以及用来管理每个无线接入设备的无线服务器；而应用系统在物理上则包括便携终端以及应用服务器。其中无线接入设备为便携终端提供无线网络接入服务。无线接入设备可能被运营商或者餐饮商等各类商户拥有，其通常部署在商户提供商业服务的物理区域内。

[0041] 请参考图 3，为了方便描述本申请将服务器以及便携终端这些主机的硬件架构进行了简化抽象，各个主机在硬件层面均包括处理器、内存、非易失性存储器以及网络接口。从业务层面来看，图 3 中的应用客户端以及应用服务端均可理解为对应主机上的处理器将计算机程序读取到内存中然后执行所形成的逻辑装置（也称为“虚拟装置”）。当然本申请并不排除软件实现以外其他实现方式，比如可编程逻辑器件这样的实现方式等等，也就是说后续描述的各个处理步骤的执行主体可以采用硬件或逻辑器件等方式实现。在本实施方式中，所述客户端包括推送处理单元、MAC 同步单元以及 Portal 代理单元，所述应用服务端包括 MAC 维护单元、Portal 认证单元以及推送管理单元。请参考图 4，所述客户端、无线接入设备、无线服务器以及应用服务端在运行过程中相互配合执行如下处理流程。

[0042] 步骤 401，无线接入设备在确定便携终端连接到自身的无线网络时，向无线服务器上报终端连接消息，该消息携带该无线接入设备标识以及连接到无线网络的便携终端的 MAC 地址信息；

[0043] 步骤 402，在收到终端连接消息后，无线服务器向应用服务端发送连接提示消息；该连接提示消息中携带有所述便携终端的 MAC 地址信息；

[0044] 步骤 403，应用服务端的推送管理单元在接收到无线服务器发送的终端连接消息时，获取该消息中携带的便携终端的 MAC 地址信息，并在自身的用户 MAC 表中查找与该 MAC 地址对应的用户，若查找到对应的用户，则转步骤 404，否则结束当前处理流程；

[0045] 步骤 404，应用服务端的推送管理单元向查找到的用户的应用客户端推送认证提示消息；

[0046] 步骤 405，应用客户端的推送处理单元在接收到应用服务端推送的认证提示消息时，在便携终端的消息提示栏中输出与该认证提示消息对应的认证提示选项；

[0047] 步骤 406，应用客户端的 Portal 代理单元在确定所述认证提示选项被用户选中或者收到浏览器关联组件通知后启动 Portal 认证，在 Portal 认证启动后获取 Portal 服务器返回的本便携终端的 MAC 地址信息，并在 Portal 认证过程中使用该应用客户端在应用服务端进行应用登录的用户名及密码作为 Portal 认证的用户名及密码；

[0048] 步骤 407，应用服务端的 Portal 认证单元在接收到 Portal 认证请求时，对该请求中的用户名以及密码是否属于本应用的注册用户，如果是，则确定该用户的 Portal 认证成功；

[0049] 步骤 408，应用客户端的 MAC 同步单元将 Portal 服务器返回的本便携终端的 MAC 地址信息发送给所述应用服务端。

[0050] 步骤 409，应用服务端的 MAC 维护单元在接收到用户的应用客户端发送的 MAC 地址信息时，将该 MAC 地址信息与该用户之间的对应关系更新到所述用户 MAC 表中。

[0051] 在本申请中，便携终端可以是智能手机、PDA 或平板电脑等便于用户携带的终端设备，以下仅以智能手机为例进行说明。本申请的应用客户端可以是一款运行在便携终端上的应用软件，其可以是各种需要用户通过输入用户名和密码进行应用登录的客户端，比如手机支付宝、手机淘宝、新浪微博或来往等手机应用客户端，以下仅以手机支付宝这一客户端为例进行说明。应用服务端则是运行在应用服务器为应用客户端提供相应的应用服务的服务软件，以下仅以支付宝服务端为例。无线接入设备可以是胖 AP，也是可以 AC+ 瘦 AP 架构中的 AC，或其他类似的具有无线接入功能的网络设备，以下仅以 AC 为例进行说明。

[0052] 在大部分情况下，一个智能手机通常有一个唯一的 MAC 地址，因此一个 MAC 地址通常能与一个使用手机支付宝的用户具有相对稳定的对应关系。当智能手机连接到某个 AC 管理的无线网络时，也可以大致确定一个对应的用户试图通过该无线网络接入互联网。此时通过步骤 402 的联动机制，支付宝服务端将可以通过无线服务器发送的终端连接消息得知此事件。相应地支付宝服务端根据该消息中携带的 MAC 地址信息找到对应的支付宝用户，此时可以推定该支付宝用户正在使用上述连接到所述 AC 的智能手机。基于该推定，支付宝服务端向该用户的支付客户端推送认证提示消息。手机支付宝根据认证提示消息生成认证提示选项，用户只要选中该认证提示选项，手机支付宝则可以自动代理用户进行 Portal 认证，整个过程对于用户而言只需要通过点击或类似简单的操作来选中认证提示选项即可快速完成 Portal 认证，而且很重要的是，本申请的上述机制可以很大程度上避免用户忘记进行 Portal 认证这样的问题。以下通过具体的实施方式来详细地介绍本申请的优势。

[0053] 在本申请中，智能手机首次接入无线网络的认证过程与非首次接入无线网络的认证过程存在一定的差异，但无论是首次还是非首次，步骤 406 到步骤 409 都会被执行，事实上首次和非首次的 Portal 认证过程只是触发认证的方式不同而已。

[0054] 1) 用户首次连接支付宝合作商户无线网络时的处理流程：

[0055] 假设从用户 (Tony) 首次进入与某个与支付宝的合作商户 (假定是商户 A)。用户使用自身的智能手机 (MAC 地址为 MAC3) 搜寻到商户 A 的无线网络，完成无线网络的连接。用户连接商户 A 无线网络的操作将触发步骤 401 到步骤 403 的执行，在步骤 403 中支付宝

服务端根据 MAC3 查找自身的用户 MAC 表，请参考表 1 示例，由于用户首次来到支付宝服务端进行 Portal 认证，因此 MAC3 在表 1 中不存在，此时应用服务端的流程处理在此结束。应用服务端并不知道哪个用户使用智能手机连接到商户 A 的无线网络，因此无法推送认证提示消息。也就是说，用户首次连接支付宝合作商户的无线网络时，步骤 404 并不会执行，用户的手机不会受到认证提示消息。在这种情况下，需要用户手动触发一次 Portal 认证。

[0056]

MAC 地址	用户名
MAC1	Tom
MAC2	Jack
MAC4	Zhangs an
……	……
MAC131	Wangwu
……	……

[0057] 表 1

[0058] 用户手动触发 Portal 认证的过程与现有技术一致，比如访问任意一个不在例外站点名单中的网址即可实现，或者简单来说，用户使用浏览器上网即可触发 Portal 认证。如前所述，在此过程中，手机支付宝这一应用客户端将会被浏览器上运行的支付宝关联组件调用。相应地，手机支付宝的 Portal 代理单元会收到该关联组件的认证通知。优选的方式中，在 Portal 代理单元启动 Portal 认证之前，可以先检查用户是否处于应用登录状态，如果用户 Tony 没有处于应用登录状态，则将手机支付宝登录界面调用到前台，供该用户输入支付宝的用户名以及密码，用户提交之后由支付宝服务端进行身份验证以完成应用登录。当然这个过程并不是必须的，因为 Portal 代理单元此时可以不关心支付宝这一应用本身的安全机制，比如说，支付宝应用本身存在登录超时机制，但是这不影响 Portal 认证使用支付宝身份信息（支付宝用户名和密码）来进行代替认证。只要支付宝客户端内部保存了用户的用户名和密码即可启动 Portal 认证。在 Portal 认证启动之后，最终 Portal 认证请求将到达支付宝服务端，由支付宝服务端的 Portal 认证单元来检查 Portal 认证请求中的用户名和密码是否属于某个支付宝的注册用户，如果是则可以返回给无线接入设备认证成功通知，无线接入设备再通知智能手机认证成功。这里值得注意的是，支付宝服务端对外提供应用服务所使用的 IP 地址通常会被配置在商户 A 的 AC 的例外站点名单中，也就是说任何用户通过该 AC 访问该 IP 地址获取应用服务都是不受限制的，与用户是否通过认证无关。

[0059] 步骤 406 中，Portal 认证的启动触发条件有两种，一种是认证提示选项被用户选中，另一种是收到浏览器关联组件的通知。在用户首次连接支付宝合作商户的无线网络时，这个触发条件将是浏览器关联组件的通知。也就是说，在用户首次连接时，步骤 401 到步骤 409 只是部分被执行，其中步骤 404 和步骤 405 将不会执行，这两个步骤的目标被用户手动

操作所实现。除了在步骤 406 启动 Portal 认证之外，本申请中手机支付宝将还执行步骤 408 以及步骤 409 的处理；这一点是与现有技术迥然不同的。

[0060] 在步骤 408 中，手机支付宝获取 MAC 地址的方式与现有技术是有较大差异的。按照传统的设计思路，应用开发人员通常会考虑去操作系统中直接读取 MAC 地址，然后发送给服务端，因为 MAC 地址是手机硬件的一个属性。在传统 PC 互联网环境下，以 Windows 操作系统为例，普通用户都可以通过“ipconfig / all”这样的命令行得到主机的 MAC 地址。但是在移动互联网的环境下，这种传统实现思路却有着不易被察觉的技术缺陷。首先，移动操作系统提供商出于用户信息安全等各种原因的考量，对此读取手机的 MAC 地址设置诸多障碍，在 Goo gle 公司提供的 Android 操作系统中，虽然也允许读取智能手机的 MAC 地址，但却是有附加条件的，要满足这些附加条件需要进行更多的复杂的开发工作。而在苹果公司提供的 IOS 这样的操作系统中，目前手机应用直接读取智能手机的 MAC 地址并不被操作系统允许，若需要读取则可能需要绕过这一限制，这意味着更多且复杂的开发工作量，而且即便成功绕过系统限制间接读取到 MAC 地址，有可能会导致手机应用在 IOS 应用商店中遭受安全质疑，可实施性较差。这也就是说按照传统思路从智能手机上读取 MAC 地址，虽然技术上可行，但实施效果却大打折扣。

[0061] 本申请则在尽量保障用户信息安全的基础下通过更为便捷的方式获得用户的 MAC 地址，由于智能手机连接到 AC 之后，AC 因为转发报文给智能手机的需求而天然保存着该智能手机的 MAC 地址，因此 AC 可以将该智能手机的 MAC 地址在 Portal 认证过程中传递给 Portal 服务器，由 Portal 服务器返回给手机支付宝。在很多流行的实现方案中，Portal 服务器一般会集成在 AC 内部，因此 MAC 地址的传递相对比较容易。在传递方式的优选实现上，本申请将手机的 MAC 地址作为重定向 URL 的传递参数返回给手机支付宝。Portal 服务器发送的重定向 URL 示例如下：

[0062] WWW.portalabc.com / default.asp?id=50-E5-49-BB-3F-BE

[0063] 其中 WWW.portalabc.com / default.asp 表征 Portal 认证页面的 URL，而其后携带的则是可以变的传递参数，当着这个参数是 MAC 地址时，这个参数对于 Portal 认证过程本身并无实质意义，但本申请借用该过程将用户 Tony 的智能手机的 MAC 地址作为 URL 传递参数回传给手机支付宝，此时手机支付宝从该 URL 解析得到 MAC 地址 50-E5-49-BB-3F-BE(MAC3)，然后将该 MAC3 通知给支付宝服务端，优选的方式中，可以在 Portal 认证成功之后再通知支付宝服务端。支付宝服务端收到 MAC3 之后相应保存该用户与其使用的智能手机的 MAC 地址的对应关系，相应地，此时表 1 将更新为表 2。

[0064]

MAC 地址	用户名
MAC1	Tom
MAC2	Jack
MAC3	Tony
MAC4	Zhangs an

……	……
MAC131	Wangwu
……	……

[0065] 表 2

[0066] 考虑到部分无线接入设备处于用户信息安全的考量，其可能将 MAC 地址进行加密形成一个加密字符串，将该加密字符串作为 MAC 地址信息返回给智能手机，对于这种情况，手机支付宝并不需要特别处理，其上的 MAC 同步单元只需要将这个加密后的数据发送给应用服务端即可。而应用服务端一侧需要特殊处理，在步骤 409 中，MAC 维护单元在将 MAC 地址信息保存之前先判断该 MAC 地址信息是否为加密数据，如果不是，将该 MAC 地址信息与用户的对应关系保存即可，如果是加密数据，则需要根据传递参数中额外携带的厂商标识来调用对应的解密算法将该加密数据进行解密获得明文的 MAC 地址信息，然后将该 MAC 地址信息与用户的对应关系保存。一般来说，由于无线接入设备提供商通常与支付宝有着合作关系，因此，支付宝服务端保存了设备的厂商标识以及与该标识对应的加解密算法（如果）。通过双方共享同样加解密算法，既实现 MAC 地址信息联动，又提高了用户信息的安全性。

[0067] 2) 用户非首次连接支付宝合作商户无线网络时的处理流程：

[0068] 请参考图 5，在用户 Tony 在支付宝合作商户 A 完成首次 Portal 认证之后，支付宝服务端将保存有该用户手机 MAC 地址与用户之间的对应关系。有了该对应关系以及步骤 401 到步骤 409 的处理。用户 Tony 后续在任何支付宝的合作商户使用无线网络时将获得极大的便利。假设用户数日之后再次来到商户 B，用户 Tony 使用自身的智能手机搜寻到商户 B 的无线网络，完成无线网络的连接。如前所述，用户连接商户 B 无线网络的操作将触发步骤 401 到步骤 403 的执行，此时支付宝服务端在查询自身的用户 MAC 表（此时是表 2）时发现使用 MAC3 的用户是 Tony，于是应用服务端转入步骤 404 向该用户推送认证提示消息。

[0069] 如前所述，支付宝服务端在 AC 的例外站点名单中，手机支付宝与支付宝服务端的互访是不受限制的，而手机支付宝这些应用通常会在后台与支付宝服务端保持着连接，以便及时互相传递重要的数据。正因如此，该认证提示消息将可以顺利地被推送到用户 Tony 的手机支付宝。手机支付宝在收到该消息后相应地执行步骤 405，在消息提示栏（比如手机屏幕最上方）输出认证提示选项，该选项的输出方式可以采用新浪微博等社交应用的消息提示选项的设计或其他类似设计，具体不再赘述。为了达到更好的提示效果，手机支付宝同样也可以相应地输出声音或者震动提示来提醒用户。用户在手机的消息提示栏中发现该认证提示选项之后即可通过下拉和点击操作来选中该认证提示选项。一旦认证提示选项被选中，此时手机支付宝将执行步骤 406 来代理用户完成 Portal 认证，认证成功之后，用户的 IP 地址就会被 AC 加入到白名单之中，于是用户可以在几乎无感知的情况下通过 Portal 认证进而实现互联网的访问。

[0070] 由此可见，对于任意一个支付宝用户而言，其首次连接支付宝合作商户的无线网络时，需要手工打开浏览器输入网址来触发一次 Portal 认证。此后用户在来到任何支付宝的合作商户并成功连接无线网络之后，用户会在极短的时间内收到认证提示，只需要通过

下拉点击这样的选中认证提示选项便可轻松地完成 Portal 认证，这一方面省去了用户打开浏览器输入网址这些相对繁琐的操作；另一方面由于用户获得了认证提示，避免用户忘记 Portal 认证，而且对于那些不熟悉 Portal 认证技术的用户来说显得更有意义。

[0071] 以上实施方式中，围绕着用户使用固定一个智能手机的情况进行描述的，这基本可以满足绝大大部分用户的使用需求。本申请对于用户使用多个便携终端的情况一样适用。假设用户 Tony 使用两个智能手机，其中手机 1 的 MAC 地址是 MAC3，手机 2 的 MAC 地址是 MAC256。假设用户 Tony 使用手机 2 重复上述使用过程，服务端只要针对一个用户保存一份唯一表项即可，也就是说 Tony 的表项被更新，其 MAC 地址被更新为 MAC256；假设 Tony 再次使用手机 1，则 Tony 的表项会再次被刷新。另外假设 Tony 不再使用手机支付宝，那么意味着 MAC3 所在的表项长期没有被更新命中，因此可以根据定时老化机制来删除掉该表项。也就是说如果一个表 3 中由于第三个表项一直都没有在步骤 409 被更新命中过，因此可以推定用户不再使用该 MAC 地址，因而可以删除该表项。假设 Tony 再次启用该 MAC 地址（比如重新使用旧手机），那么本申请依旧可以按照前述流程进行正常的处理。

[0072]

MAC 地址	用户名
MAC1	Tom
MAC2	Jack
……	……
MAC131	Wangwu
MAC256	Tony
……	……

[0073] 表 3

[0074] 在以上实施方式的基础上，本申请的联动机制可以进一步为用户以及商户提供交互便利。请参考图 6，假设图 6 中的 AC（设备标识为 AC100）与标识为 HDL 的商户具有对应关系，AC100 有可能是商户 HDL 购买或租用的设备，总而言之在无线服务器一端这两者之间具有对应关系即可，这个对应关系通常保存在无线服务器的数据库中，如表 4 的示例。

[0075]

设备标识	商户标识
AC1	XBK
AC2	XBK
……	……

[0076]

AC100	HDL
AC101	HDL
……	……

[0077] 表 4

[0078] 无线服务器根据终端连接消息中携带的 AC 标识 AC100 查找到对应的商户标识 HDL，将该商户标识 HDL 携带在连接提示消息中发送给支付宝服务端。支付宝服务端则保存有商户 HDL 对应的服务信息和 / 或对应的第三方应用标识。从实施的角度来说，支付宝服务端可以进一步包括商户接口单元，商户接口单元可以是一个 WEB 服务窗口，商户使用对应的企业账号登录之后，发送商户配置的服务信息以及第三方应用标识给商户接口单元，商户接口单元将服务信息以及第三方应用标识保存在商户信息表中。商户 HDL 可以不定期地通过商户接口单元来更新自身在应用服务端商户信息表中的服务信息，比如商品促销信息以及新品上市信息等等。而第三方应用标识则可以是与商户 HDL 对应的应用客户端的标识，比如 HDL 自己开发的点餐客户端，或者 HDL 合作者开发的适合 HDL 使用的应用客户端，比如手机淘宝等等。

[0079] 支付宝服务端的推送管理单元根据连接提示消息中的商户标识 HDL 查找自身的商户信息表（参考表 5）的示例，确定对应的服务信息和 / 或第三方应用标识。推送管理单元将查找到的服务信息和 / 或第三方应用标识携带在认证提示消息中推送给手机支付宝。手机支付宝在收到之后，推送处理单元从认证提示消息中获取服务信息并展示，在优选的实施方式中，推送处理单元可以在 Portal 认证通过之后展示服务信息，因为服务信息中可能包括有链接，用户点击链接需要访问对应的站点，Portal 认证通过之前，用户可能无法访问这些站点，除非这些站点也在例外站点白名单中。

[0080] 如果认证提示消息中还携带有第三方应用标识，则推送处理单元可以进一步根据该标识查找智能手机本地是否有对应的第三方应用，如果有，则启动该第三方应用。如果没有，则放弃，或者推荐用户下载该第三方应用。请参考表 5，用户在商户 HDL 连接无线网络过程中，本申请除了快捷地协助用户完成认证之外，还可以将商户 HDL 的最新服务信息展示给用户，这样可以方便用户及时了解最新的商户服务信息。其次，假设 HDL 是一个餐饮商户，其开发了点餐客户端“HDL 点餐”，则推送管理单元在认证通过后调用该应用客户端可以方便正在打算在 HDL 消费用户进行自助点餐，这些服务信息的展示和第三方应用的调用，无疑大大便利了用户在商户 HDL 的消费活动，降低了消费者与商户之间的沟通成本。

[0081]

商户标识	服务信息	第三方应用标识
XBK	周末半价	
KDJ	X 商品买一送一	KDJ 外卖
……	……	……
HDL	消费满 300 返抵用券 90，详情访问 www.hdlxxx.com	HDL 点餐
……	……	……

[0082] 表 5

[0083] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

图 1

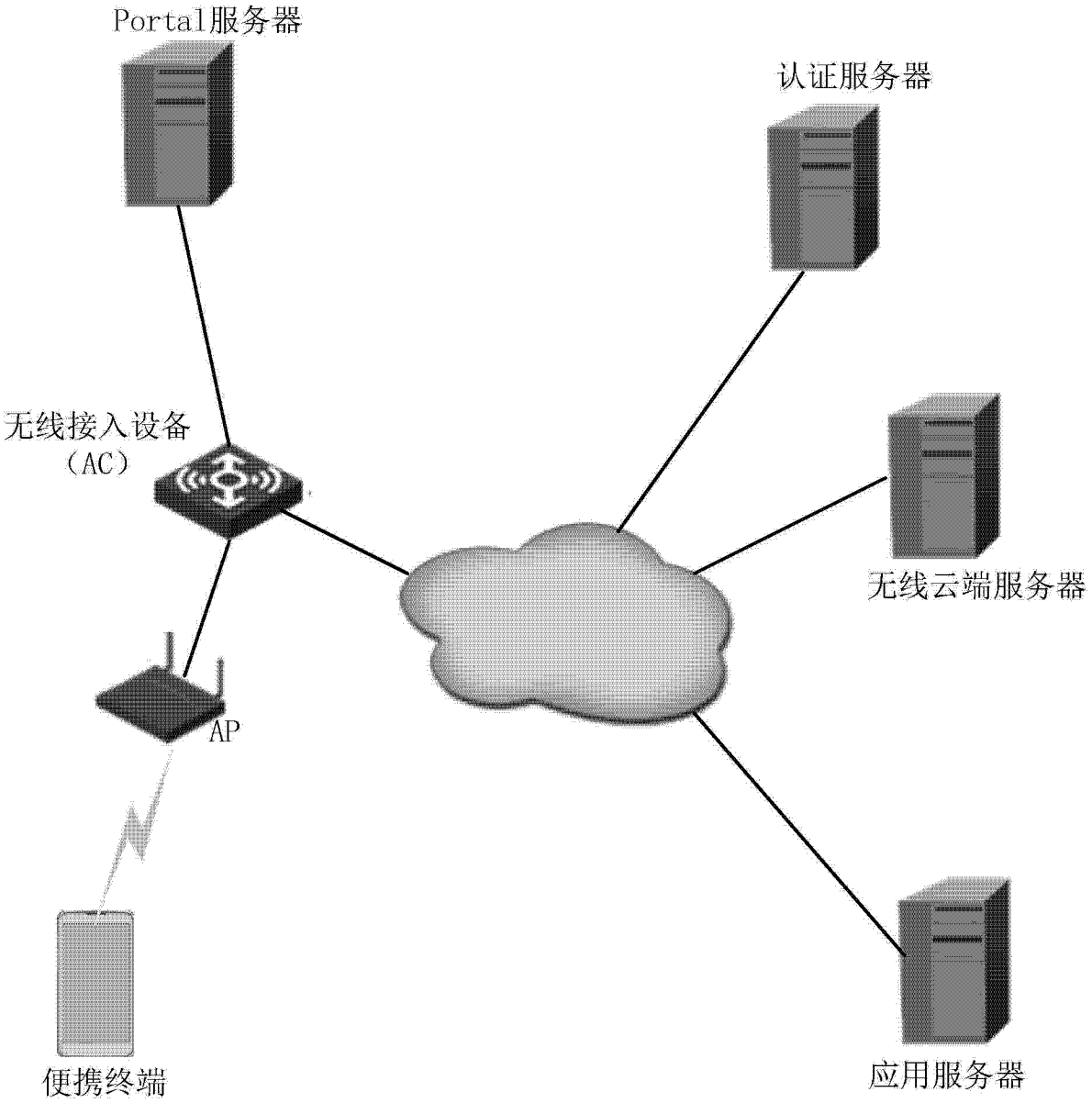


图 2

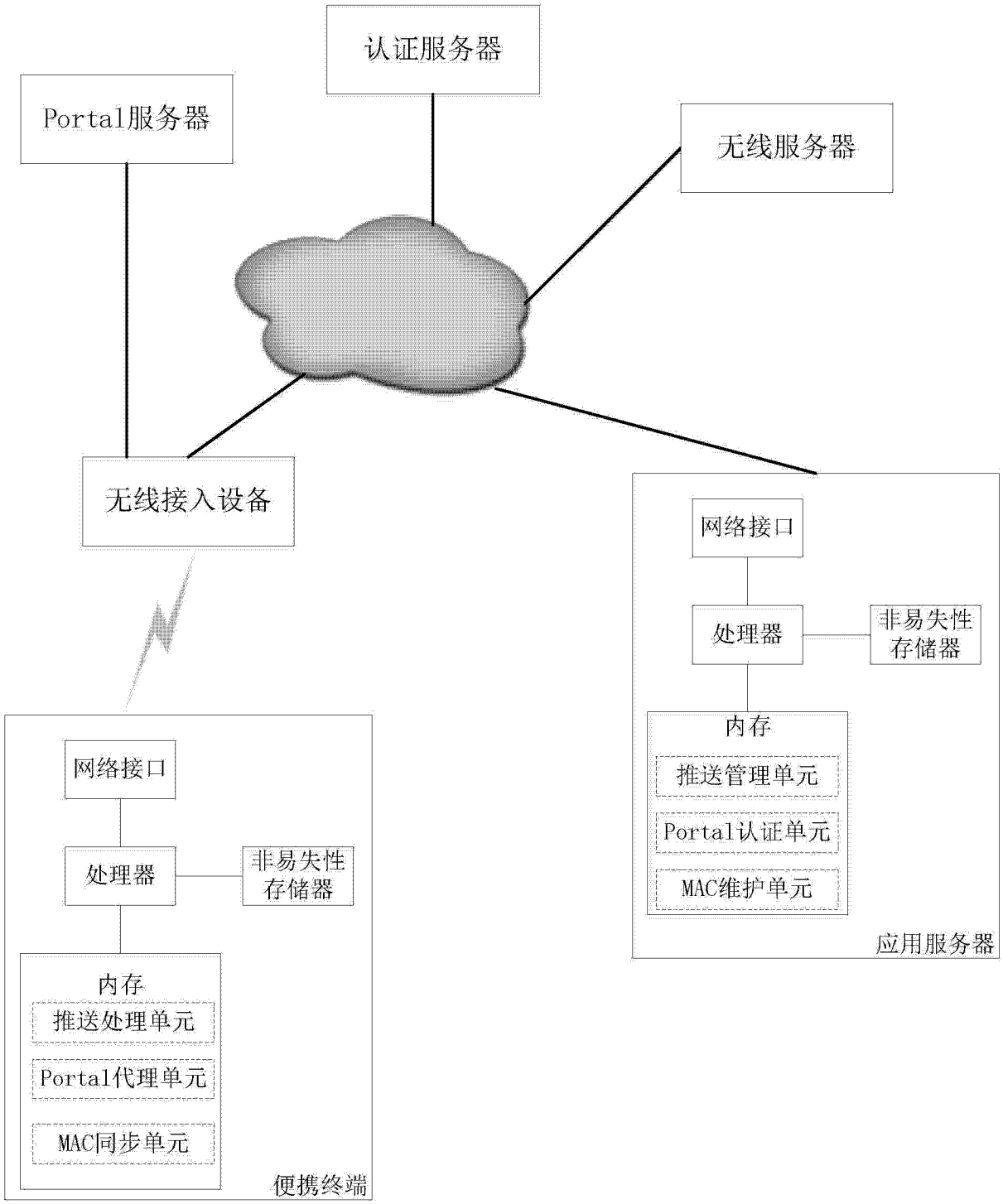

认证服务器
Portal服务器
无线服务器
无线接入设备
网络接口
处理器
非易失性存储器
内存
推送管理单元
Portal认证单元
MAC维护单元
应用服务器
网络接口
处理器
非易失性存储器
内存
推送处理单元
Portal代理单元
MAC同步单元
便携终端

图 3

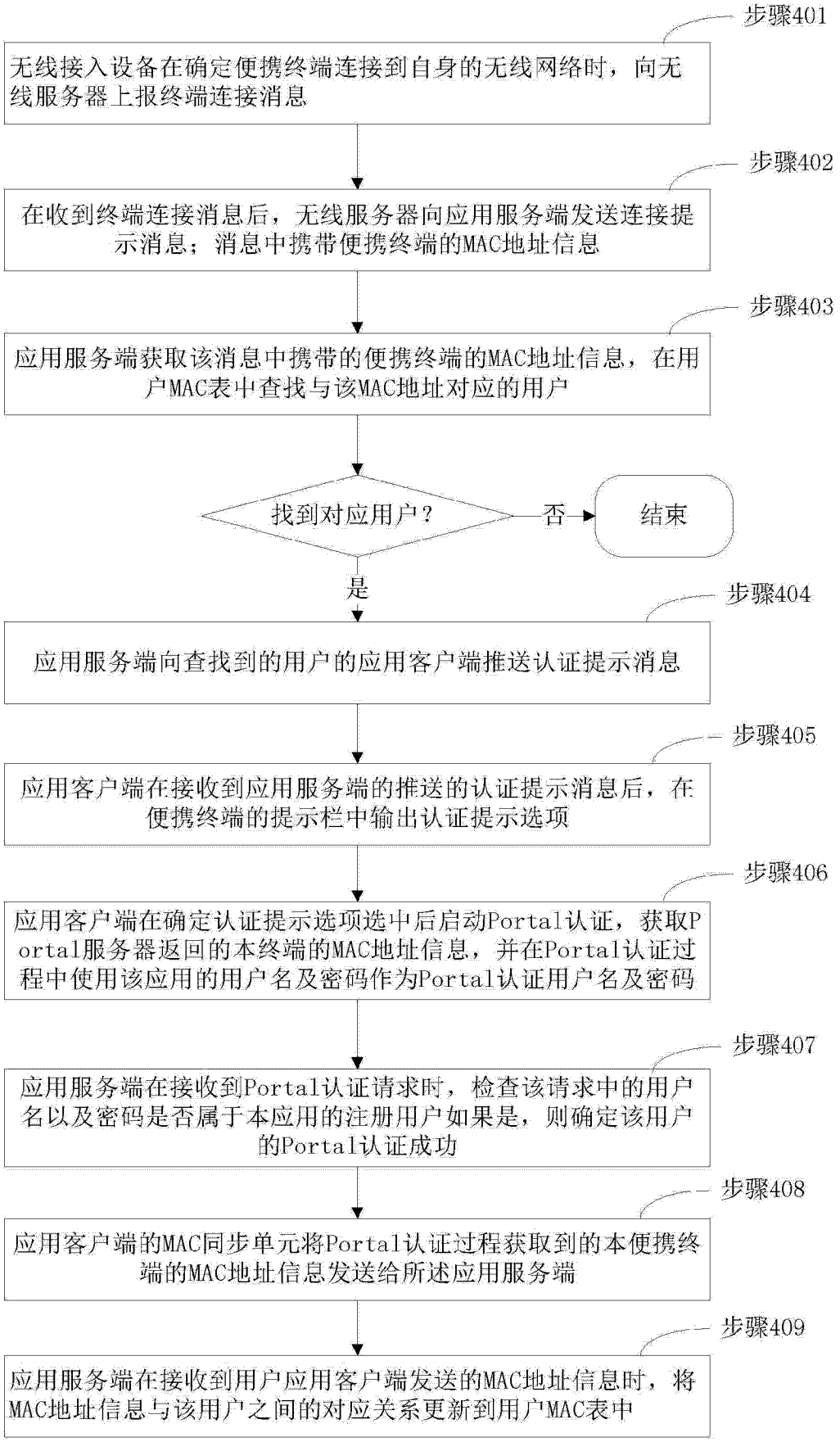

步骤401
无线接入设备在确定便携终端连接到自身的无线网络时，向无线服务器上报终端连接消息
步骤402
在收到终端连接消息后，无线服务器向应用服务端发送连接提示消息；消息中携带便携终端的MAC地址信息
步骤403
应用服务端获取该消息中携带的便携终端的MAC地址信息，在用户MAC表中查找与该MAC地址对应的用户
找到对应用户？
否
结束
是
步骤404
应用服务端向查找到的用户的应用客户端推送认证提示消息
步骤405
应用客户端在接收到应用服务端的推送的认证提示消息后，在便携终端的提示栏中输出认证提示选项
步骤406
应用客户端在确定认证提示选项选中后启动Portal认证，获取Portal服务器返回的本终端的MAC地址信息，并在Portal认证过程中使用该应用的用户名及密码作为Portal认证用户名及密码
步骤407
应用服务端在接收到Portal认证请求时，检查该请求中的用户名以及密码是否属于本应用的注册用户如果是，则确定该用户的Portal认证成功
步骤408
应用客户端的MAC同步单元将Portal认证过程获取到的本便携终端的MAC地址信息发送给所述应用服务端
步骤409
应用服务端在接收到用户应用客户端发送的MAC地址信息时，将MAC地址信息与该用户之间的对应关系更新到用户MAC表中

图 4

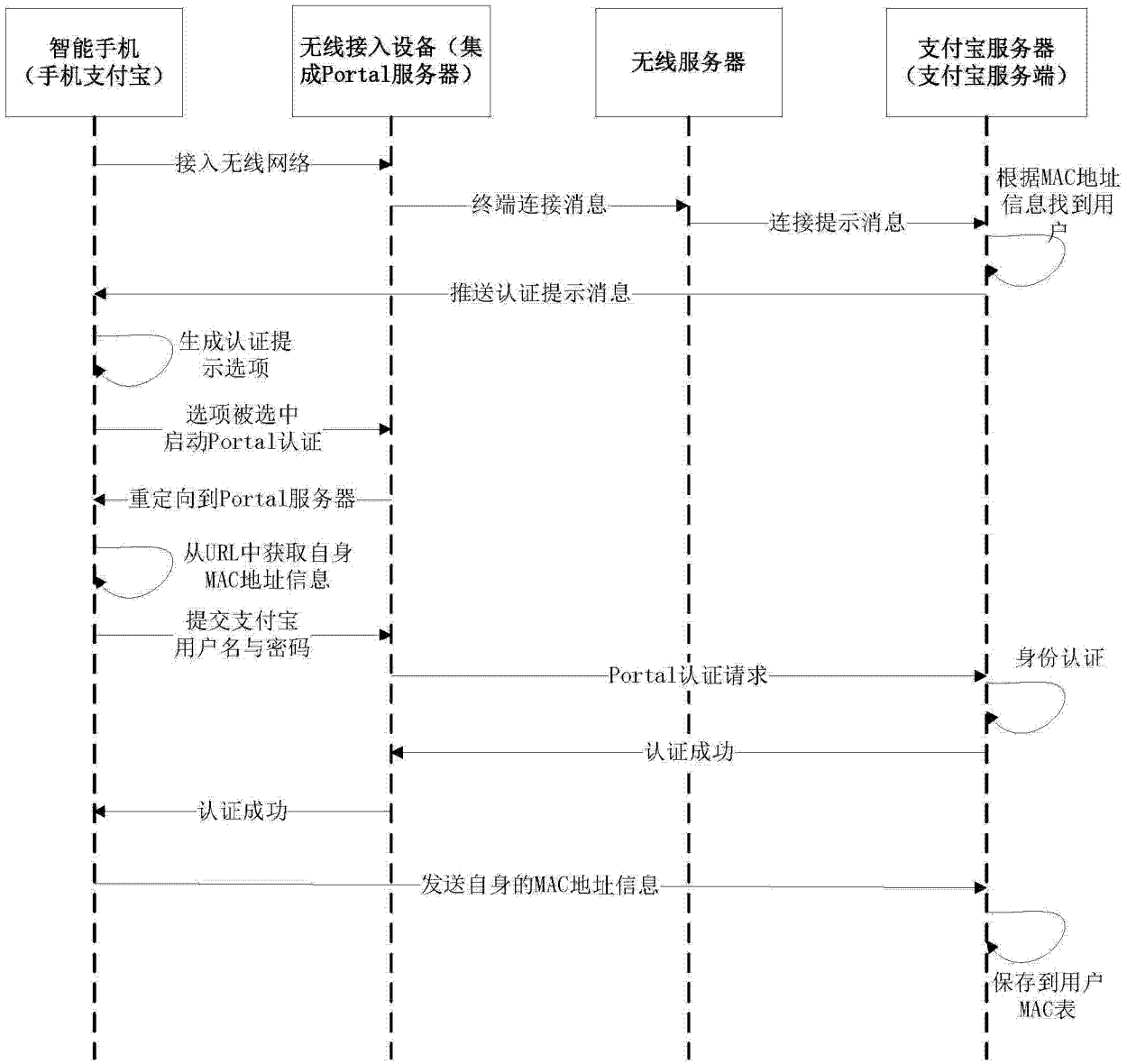

智能手机
（手机支付宝）
无线接入设备（集成Portal服务器）
无线服务器
支付宝服务器
（支付宝服务端）
接入无线网络
终端连接消息
连接提示消息
根据MAC地址信息找到用户
推送认证提示消息
生成认证提示选项
选项被选中
启动Portal认证
重定向到Portal服务器
从URL中获取自身MAC地址信息
提交支付宝用户名与密码
Portal认证请求
身份认证
认证成功
认证成功
发送自身的MAC地址信息
保存到用户MAC表

图 5

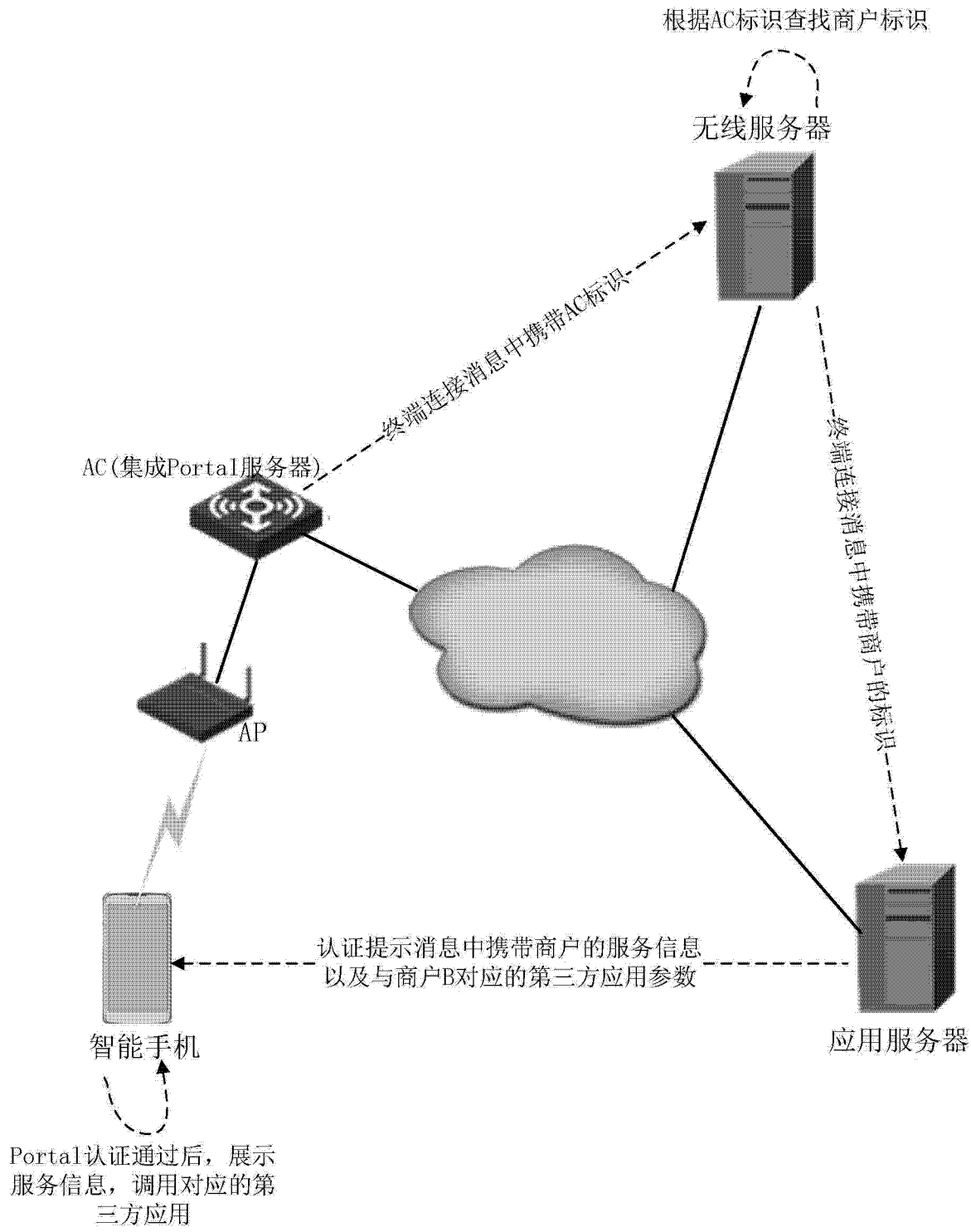

根据AC标识查找商户标识
无线服务器
终端连接消息中携带AC标识
终端连接消息中携带商户的标识
AC(集成Portal服务器)
AP
认证提示消息中携带商户的服务信息
以及与商户B对应的第三方应用参数
智能手机
应用服务器
Portal认证通过后，展示
服务信息，调用对应的第
三方应用

图 6