(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 101578828 B
(45)授权公告日 2013.03.27

(21)申请号 200880001509.0
(22)申请日 2008.08.25
(30)优先权数据
60/957,740 2007.08.24 US
12/192,488 2008.08.15 US
(85)PCT申请进入国家阶段日
2009.06.26
(86)PCT申请的申请数据
PCT/CN2008/072126 2008.08.25
(87)PCT申请的公布数据
WO2009/026848 EN 2009.03.05
(73)专利权人 华为技术有限公司
地址 518129 中国广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 约翰·凯帕利马利尔
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张伟
(51)Int.Cl.
H04L 12/66(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)
(56)对比文件
US 2006/0140150 A1,2006.06.29, 全文.
US 2007/0112967 A1,2007.05.17, 全文.
EP 1365621 A1,2003.11.26, 全文.
审查员 王伦杰

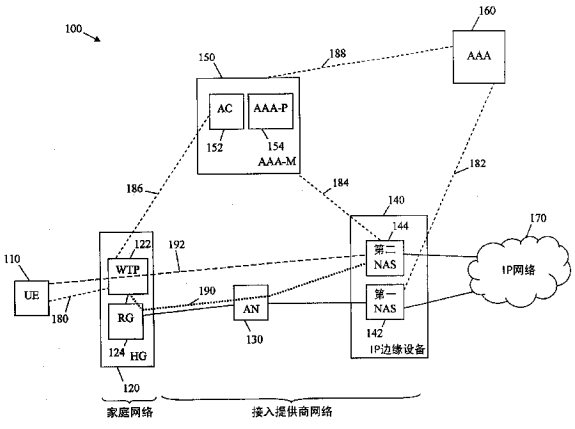
权利要求书 1 页 说明书 9 页 附图 4 页

(54)发明名称

一种网络接入处理方法、装置和系统

(57)摘要

一种包括节点的装置，该节点包括接入控制器(AC)以及认证、授权和计费(AAA)代理(AAA-P)，其中，该AC用于对用户设备(UE)进行认证管理，并且其中，所述AAA-P用于与AAA服务器交换与所述UE有关的认证信息。包括一种网络组件，该网络组件包括至少一个处理器，所述至少一个处理器用于实现一种方法，该方法包括：与家庭网关(HG)建立第一隧道，其中，所述HG与UE进行无线通信；以及在所述UE与网络接入服务器(NAS)之间建立第二隧道。还包括一种网路组件，该网路组件包括至少一个处理器，所述至少一个处理器用于实现一种方法，该方法包括：从AAA中介(AAA-M)接收成对主会话密钥(PMK)；以及使用所述PMK来认证UE。



CN 101578828 B

1. 一种用于网络接入处理的装置，包括：

节点，包括接入控制器 AC 以及认证、授权和计费 AAA 代理 AAA-P

其中，所述 AC 用于对用户设备 UE 进行认证管理；并且

其中，所述 AAA-P 用于与 AAA 服务器交换与所述用户设备 UE 有关的认证信息；

所述认证、授权和计费 AAA 服务器产生主会话密钥 MSK；

其中，所述主会话密钥 MSK 用于导出第一对主密钥 PMK1 和第二对主密钥 PMK2；所述第一对主密钥用于导出第一对临时密钥以在所述用户设备 UE 与家庭网关 HG 之间建立安全无线链路信道；所述第二对主密钥用于导出第二对临时密钥以在所述用户设备 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

2. 如权利要求 1 所述的装置，进一步包括与所述节点进行通信的因特网协议 IP 边缘设备、以及与所述 IP 边缘设备进行通信的接入节点 AN。

3. 如权利要求 2 所述的装置，所述 IP 边缘设备进行与所述 AAA 服务器和所述 IP 网络的通信，所述节点与所述 AAA 服务器进行通信。

4. 如权利要求 2 所述的装置，所述节点和所述 AN 进行与家庭网关 HG 的通信，所述家庭网关 HG 与所述用户设备 UE 进行无线通信。

5. 如权利要求 1 所述的装置，所述节点是 AAA 中介 AAA-M 并且与包括第一网络接入服务器 NAS 和第二 NAS 的因特网协议 IP 边缘设备进行通信。

6. 一种用于网络接入处理的方法，包括：

用户设备 UE 通过家庭网关 HG 从认证、授权和计费 AAA 服务器获取主会话密钥 MSK；

根据所述主会话密钥 MSK 导出第一对主密钥 PMK1 和第二对主密钥 PMK2；

根据所述第一对主密钥导出第一对临时密钥，在所述用户设备 UE 与家庭网关 HG 之间建立安全无线链路信道；

根据所述第二对主密钥导出第二对临时密钥，在所述用户设备 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

7. 如权利要求 6 所述的方法，所述安全无线链路信道是 Wi-Fi 漫游虚拟局域网 VLAN，所述 IP 隧道是因特网协议安全 IPsec 隧道。

8. 如权利要求 6 所述的方法，所述方法进一步包括：

与因特网协议 IP 网络建立通信；以及

控制所述用户设备 UE 与所述 IP 网络之间的会话。

9. 如权利要求 8 所述的方法，所述方法进一步包括对所述会话进行计费。

10. 如权利要求 6 所述的方法，获取所述第一对主密钥和第二对主密钥包括：接收携带在远程认证拨号用户服务 RADIUS 或直径 DIAMETER 会话中的所述第一对主密钥和第二对主密钥。

一种网络接入处理方法、装置和系统

[0001] 相关申请的交叉引用

[0002] 本申请要求 John Kaippallimalil 于 2007 年 8 月 24 日提交的标题为“Roaming Wi-Fi Access in Fixed Network Architectures”的美国临时专利申请 No.60/957,740 和 John Kaippallimalil 于 2008 年 8 月 15 日提交的标题为“Roaming Wi-Fi Access in Fixed Network Architectures”的美国专利申请 No.12/192,488 的优先权，并以引用方式将它们全部并入本文。

[0003] 背景技术

[0004] 在诸如因特网协议 (IP) 网络等固定通信网络中，可以借助诸如 Wi-Fi 等无线技术向移动用户提供漫游或无线接入。许多用于向移动用户设备 (UE) 提供对 IP 网络的漫游接入的机制正在被研究。其中的一些机制可以经由家庭网关 (HG) 在 UE 与本地网络或家庭网络之间建立无线通信，家庭网关 (HG) 可以是住宅用户单元。同样地，UE 最初建立与 HG 的“委托”，从而 HG 与 IP 网络进行通信并且在 UE 与 IP 网络之间转发通信。然而，当 UE 委托 HG 时，可以在 HG 或家庭网络截取 UE 与 IP 网络的通信。

[0005] 此外，HG 负责对通信进行控制，例如设置策略和服务质量 (QoS)，并且 HG 还负责对通信进行计费，例如对连接或时间使用进行计费。然而，在某些情况下，例如，当 HG 不属于 IP 网络服务提供商时，由 HG 负责对通信进行控制和计费可能对 IP 网络服务提供商而言是不期望的或无益的。

[0006] 发明内容

[0007] 在一个实施例中，公开了一种包括节点的装置，该节点包括接入控制器 (AC) 和认证、授权和计费 (AAA) 代理 (AAA-P)，其中，所述 AC 用于对 UE 进行认证管理，并且其中，所述 AAA-P 用于与 AAA 服务器交换与所述 UE 有关的认证信息，所述认证、授权和计费 (AAA) 服务器产生主会话密钥 (MSK)；

[0008] 其中，所述主会话密钥 (MSK) 用于导出第一对主密钥 (PMK1) 和第二对主密钥 (PMK2)；所述第一对主密钥用于导出第一对临时密钥以在所述 UE 与 HG 之间建立安全无线链路信道；所述第二对主密钥用于导出第二对临时密钥以在所述 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

[0009] 在另一个实施例中，公开了一种网络接入处理方法，包括，用户设备 UE 通过 HG 从认证、授权和计费 (AAA) 服务器获取主会话密钥 (MSK)；

[0010] 根据所述主会话密钥 (MSK) 导出第一对主密钥 (PMK1) 和第二对主密钥 (PMK2)；

[0011] 根据所述第一对主密钥导出第一对临时密钥，在所述 UE 与 HG 之间建立安全无线链路信道；

[0012] 根据所述第二对主密钥导出第二对临时密钥，在所述 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

[0013] 在另一个实施例中，公开了一种用户设备，所述 UE 通过 HG 从认证、授权和计费 (AAA) 服务器获取主会话密钥 (MSK)；根据所述主会话密钥 (MSK) 导出第一对主密钥 (PMK1) 和第二对主密钥 (PMK2)；所述第一对主密钥用于导出第一对临时密钥以在所述 UE

与 HG 之间建立安全无线链路信道；所述第二对主密钥用于导出第二对临时密钥以在所述 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

[0014] 在另一个实施例中，公开了一种家庭网关 HG，所述 HG 从认证、授权和计费 (AAA) 服务器获取主会话密钥 (MSK) 后，将所述 MSK 发送给用户设备 UE；所述主会话密钥 (MSK) 用于导出第一对主密钥 (PMK1) 和第二对主密钥 (PMK2)；所述第一对主密钥用于导出第一对临时密钥以在所述 UE 与 HG 之间建立安全无线链路信道；所述第二对主密钥用于导出第二对临时密钥以在所述 UE 与 IP 边缘设备之间建立 IP 隧道进行通信。

[0015] 通过下面给出的具体实施方式以及附图、权利要求书，可以更加清楚地理解本发明的这些和其它特征。

[0016] 附图说明

[0017] 为了更好地理解本申请，现在对附图和具体实施方式进行简要说明，在附图中，相同的附图标记表示相同的部件。

[0018] 图 1 是固定网络漫游接入系统的实施例的示意图；

[0019] 图 2 是固定网络漫游接入系统的另一个实施例的示意图；

[0020] 图 3 是漫游接入方法的实施例的协议图；以及

[0021] 图 4 是通用计算机系统的实施例的示意图。

具体实施方式

[0022] 首先应该理解，虽然下文提供了一个或多个实施例的示例性实现方式，但是可以使用任意数量的当前已知技术或现有技术来实现所公开的系统和 / 或方法。本申请决不限于这些示例性实现方式、附图和下文所述的技术 (包括本文举例说明并且描述的示例性设计和实现方式)，而是可以在所附权利要求的范围内以及所附权利要求的等价要件的全部范围内对本申请进行修改。

[0023] 本文公开的系统和方法用于 UE 漫游接入到诸如 IP 网络等固定网络。为了提供漫游接入，UE 使用无线链路与位于家庭网络中的 HG 进行通信。HG 耦合到包括 IP 边缘设备的接入提供商网络，IP 边缘设备可以与 IP 网络进行通信。因此，HG 可以经由 IP 边缘设备在 UE 与 IP 网络之间转发通信。具体地，HG 可以使用无线链路以及与 UE 共享的第一共享密钥来与 UE 进行通信，并且 HG 可以使用第一隧道与 IP 边缘设备进行通信。此外，UE 可以使用第二安全隧道和第二共享密钥来经由 HG 与 IP 边缘设备进行通信，而无需委托 HG。因此，UE 可以使用第二安全隧道来建立对 IP 网络的漫游接入，而无需将它的通信委托给 HG。这种结构还允许 IP 边缘设备对第二安全隧道的通信进行控制和计费。

[0024] 图 1 示出了固定网络漫游接入系统 100 的实施例。该固定网络漫游接入系统 100 可以包括至少一个 UE 110、HG 120、接入节点 (AN)130、IP 边缘设备 140、AAA-M 150、AAA 服务器 160 和 IP 网络 170。在一个实施例中，HG 120 可以是家庭网络或家庭网络的一部分，家庭网络可以耦合到包括 AN 130 和 IP 边缘设备 140 的接入提供商网络。接着，接入提供商网络经由 IP 边缘设备 140 耦合到 IP 网络 170。在一些实施例中，接入提供商网络也可以包括 AAA-M 150。

[0025] 在一个实施例中，UE 110 可以是使用无线链路 180 与 HG 120 通信的任意用户移动设备、组件或装置。例如，UE 110 可以是蜂窝电话、个人数字助理 (PDA)、便携式计算机或

任意其它无线设备。UE 110 可以包括红外端口、蓝牙接口、符合 IEEE 802.11 的无线接口或使 UE 110 能够与 HG 120 进行无线通信的任意其它无线通信系统。在一个实施例中，无线链路 180 可以是 IEEE 802.11 链路或 Wi-Fi 链路。在其它实施例中，无线链路 180 可以是蓝牙链路、微波存取全球互通 (WiMAX) 链路、近距离通信 (NFC) 链路、红外数据协会 (IrDa) 链路或使用无线技术建立的任意其它通信链路。

[0026] 在一个实施例中，HG 120 是用于允许 UE 110 无线接入到与 IP 网络 170 耦合的家庭网络或接入提供商网络的任意设备、组件或网络。具体地，HG120 可以包括耦合到路由器或住宅网关 (RG) 124 的无线终端点 (WTP) 122。WTP 122 可以是用于与 UE 110 建立无线链路以及在 UE 110 与诸如 RG 124 等另一组件之间转发通信的任意设备、组件或网络。在一个实施例中，WTP 122 可以是经由无线链路 180 与 UE 110 进行通信并且经由诸如以太网链路等固定链路与 RG 124 进行通信的固定设备。WTP 122 也可以用于在 UE 110 与 AAA-M 150 之间转发认证信息。对于在 HG 120 上管理 UE 110 接入到家庭网络而言，需要该认证信息。

[0027] RG 124 可以是允许 UE 110 与所述接入提供商网络上的 IP 边缘设备 140 进行通信的任意设备、组件或网络。例如，RG 124 可以是 IP 路由器，例如客户端设备 (CPE) 路由器或位于用户端并且与网络进行通信的任意路由器设备。例如，RG 124 可以是 DSL 调制解调器、线缆调制解调器或机顶盒。在另一个实施例中，RG 124 可以是将 Ipv4 和 / 或 Ipv6 分组转发到 UE 110 并且转发来自 UE 110 的 Ipv4 和 / 或 Ipv6 分组的节点。

[0028] RG 124 可以经由 WTP 122 与 RG 124 之间的固定链路和 WTP 122 与 UE 110 之间的无线链路 180 与 UE 110 交换通信。此外，RG 124 可以使用隧道 190 与 IP 边缘设备 140 交换通信，该隧道 190 是经由 AN 130 在 HG 120 与 IP 边缘设备 140 之间建立的。例如，隧道 190 可以是在 WTP 122、RG 124、AN 130 和 IP 边缘设备 140 之间建立的 Wi-Fi 漫游虚拟局域网 (VLAN)。隧道 190 可以用于转发 UE 110 与 IP 边缘设备 140 之间的网络设置信息，例如 IP 地址请求和分配。

[0029] 在一个实施例中，AN 130 可以是在 HG 120 与 IP 边缘设备 140 之间传输通信的任意设备。例如，AN 130 可以是交换机、路由器或网桥，例如提供商边缘网桥 (PEB) 或提供商核心网桥 (PCB)。AN 130 可以位于接入提供商网络上并且 AN 130 可以经由诸如以太网链路等固定链路耦合到 HG120 和 IP 边缘设备 140。此外，AN 130 可以使用隧道 190 与 HG 120 和 IP 边缘设备 140 进行通信。

[0030] 在一个实施例中，IP 边缘设备 140 可以是在 HG 120 与 IP 网络 170 之间转发通信的任意设备。例如，IP 边缘设备 140 是由宽带论坛或线缆调制解调器终端服务器 (CMTS) 所定义的宽带路由接入服务器 (BRAS)。IP 边缘设备 140 可以包括第一网络接入服务器 (NAS) 142 和第二 NAS 144。第一 NAS 142 和第二 NAS 144 可以包括网桥、交换机、路由器或它们的组合。在一些实施例中，可以将第一 NAS 142 和第二 NAS 144 组合成一个组件，例如网桥或路由器。例如，第一 NAS 142、第二 NAS 144 或这两者可以是骨干边缘网桥 (BEB)、PEB、PCB 或用户网络接口 (UNI)。可替换地，第一 NAS 142、第二 NAS 144 或这两者可以是独立的有线节点 (Point-oriented Wire-line Node)，例如数字用户线 (DSL) 连接或提供商网络边缘设备。

[0031] 第一 NAS 142 可以经由 AN 130 耦合到 RG 124 以及经由固定链路耦合到 IP 网络 170。第一 NAS 142 可以使用固定链路在 IP 网络 170 与家庭网络或接入提供商网络之间转

发通信。此外，第一 NAS 142 可以与 AAA 服务器 160 交换与家庭网络组件或接入提供商网络组件有关的认证信息。可以使用会话流 182 来交换认证信息，该会话流 182 是使用远程认证拨号用户服务 (RADIUS) 协议建立的。可以使用 DIAMETER 协议来代替本文所述的任意 RADIUS 协议实现方式。

[0032] 第二 NAS 144 还经由固定链路耦合到 IP 网络 170，并且第二 NAS 144 使用会话流 184 与 AAA-M 150 交换认证信息。类似于会话流 182，会话流 184 也是使用 RADIUS 或 DIAMETER 建立的。此外，第二 NAS 144 可以使用安全隧道 192 与 UE 110 进行通信，而不必委托 HG 120，可以在认证 UE 110 以及为 UE 110 分配 IP 地址之后建立该安全隧道 192。例如，安全 隧道 192 可以是因特网协议安全 (IPsec)，该因特网协议安全 (IPsec) 使用因特网密钥交换 (IKE) 在 UE 110 与第二 NAS 144 之间建立安全会话流。

[0033] 在一些实施例中，固定网络漫游接入系统 100 可以包括多个 UE 110，所述多个 UE 110 使用对应于各个 UE 110 的多个安全隧道 192 与第二 NAS144 进行通信。在其它实施例中，IP 边缘设备 140 可以包括多个第二 NAS144，所述多个第二 NAS 144 使用多个安全隧道 192 一对一地与多个 UE 110 进行通信。

[0034] 在一个实施例中，AAA-M 150 可以是对 UE 110 接入到 HG 120 处的家庭网络和接入提供商网络进行管理并且对 UE 接入到 IP 边缘设备 140 处的 IP 网络 170 进行管理的任意设备、组件或服务器。AAA-M 150 包括 AC 152 和 AAA-P 154。AC 152 可以对 UE 110 进行认证管理。例如，经由 WTP 122，AC 152 可以使用无线接入点的控制和配置 (CAPWAP) 协议来与 UE 110 交换认证信息。具体地，可以使用 CAPWAP，经由无线链路 180 在 UE 110 与 WTP 122 之间以及经由会话流 186 在 WTP 122 与 AC 152 之间交换认证信息。

[0035] 在其它实施例中，AC 152 可以使用任意其它适合的管理协议来交换认证信息。例如，AC 152 可以经由 DSL 链路耦合到 WTP 122，并且 AC 152 可以使用宽带论坛技术报告 069(TR-069) 协议来管理转发的认证信息。可替换地，AC 152 可以经由光链路耦合到 WTP 122，并且 AC 152 可以使用光网络终端管理和控制接口 (OMCI) 协议或 OMCI 第二层连接协议 (OMCI/L2CP) 来管理 UE 110 的接入。

[0036] AAA-P 154 是用于将 UE 110 的一些认证信息转发或者中继到 AAA 服务器 160 的 AAA 代理。例如，AAA-M 150 可以使用 RADIUS 或 DIAMETER 来与 AAA 服务器 160 建立会话流 188，以便交换认证信息。此外，AAA-P154 可以用于使用会话流 184 在第二 NAS 144 与 AAA-M 150 之间转发认证信息。在一些实施例中，AAA-P 154 可以用于管理认证信息流。例如，AAA-P 154 可以负责在多个第二 NAS 144 与 AAA 服务器 160 之间复用和转发多个消息。在一些实施例中，AAA-P 154 也可以用于实施一些与资源使用和供应有关的策略。

[0037] 在一个实施例中，AAA 服务器 160 可以是用于实现 AAA 协议的任意 设备、组件或服务器，AAA 协议定义了用于协议认证、授权和计费的各种机制和策略。可以使用 RADIUS 或 DIAMETER(会话流 188 和 184) 经由 AAA-M 150 在 AAA 服务器 160 与第二 NAS 144 之间转发一些与管理 UE110 接入到 IP 网络 170 有关的认证信息。此外，可以使用 RADIUS(会话流 188) 和 CAPWAP(会话流 186) 经由 AAA-M 150 在 AAA 服务器 160 与 HG 120 之间转发与管理 UE 110 接入到家庭网络或接入提供商网络有关的其它认证信息。

[0038] 就认证而言，AAA 服务器 160 可以对 UE 110 声明的标识进行验证。例如，通过将诸如网络地址等数字标识与客户信息数据库相比对，AAA 服务器 160 可以建立认证。在其

它实施例中，AAA 服务器 160 可以将对应于 UE 110 的证书，例如密码、一次性令牌、数字证书或电话号码与客户信息数据库相比对。

[0039] 就授权而言，AAA 服务器 160 判断是否可以将特定权利（例如，访问某些资源）给予 UE 110。例如，AAA 服务器 160 可以基于 UE 110 的认证、UE 110 请求的特权、当前系统状态或其组合来将具体类型的特权（包括“无特权”）给予 UE 110。授权可以是基于限制的，例如，每天定时限制、物理位置限制或对 UE 110 多次登录的限制。给予特权可以包括：提供使用特定类型的服务，例如 IP 地址滤波、地址分配、路由分配、QoS 服务、带宽控制、流量管理、到特定端点的隧道建立、以及加密。

[0040] 就计费而言，AAA 服务器 160 可以对 UE 110 使用的网络资源或者分配给 UE 110 的网络资源进行跟踪。该使用信息可以用于管理、规划、计费或其它目的。在一些实施例中，AAA 服务器 160 可以跟踪实时计费信息，IP 边缘设备 140 可以在利用或消费资源的同时转发该实时计费信息。在其它实施例中，IP 边缘设备 140 可以批处理、存储这种计费信息，并且在稍后的时刻将这种计费信息传送到 AAA 服务器 160。计费信息可以包括 UE110 的标识、传送的服务的种类、服务开始时间和服务结束时间。

[0041] 在一个实施例中，IP 网络 170 可以是与 IP 边缘设备 140、HG 120 和 UE 110 交换 IP 数据分组的任意类型的网络。例如，IP 网络 170 可以是分组交换网络 (PSN)、内联网、因特网或局域网 (LAN)。IP 网络 170 可以是以太网传输网络、骨干网络、接入网络、光网络、有线网络、电气电子 工程师协会 (IEEE)802 标准网络、无线网络或任意其它基于 IP 的网络。

[0042] 图 2 示出了另一个固定网络漫游接入系统 200 的实施例。固定网络漫游接入系统 200 可以包括至少一个 UE 210、HG 220、AN 230、IP 边缘设备 240、路由器边缘设备 (R 边缘设备）250、AAA 服务器 260 和 IP 网络 270。在一个实施例中，HG 220 可以是家庭网络或家庭网络的一部分，家庭网络可以耦合到包括 AN 230 和 IP 边缘设备 240 的接入提供商网络。此外，可以将该接入提供商网络上的 IP 边缘设备 240 耦合到 IP 网络 270。可以将 UE 210、HG 220、AN 230、AAA 服务器 260 和 IP 网络 270 配置为类似于固定网络漫游接入系统 100 的对应组件。此外，在图 2 中，可以将各种组件之间的会话流 280、282、286 和 288 配置为类似于固定网络漫游接入系统 100 的对应会话流。

[0043] 此外，IP 边缘设备 240 可以包括被配置为类似于第一 NAS 142 的单个 NAS 242。同样地，可以将 IP 边缘设备 240 配置为类似于标准或接入提供商网络中的 IP 边缘设备。R 边缘设备 250 可以包括被配置为类似于 AC 152 的 AC 252、被配置为类似于 AAA-P 154 的 AAA-P 254、以及被配置为类似于第二 NAS 144 的 NAS 256。同样地，NAS 256 与 AC 252 和 AAA-P 254 可以一起被放置在另一个提供商网络上，而不是与 IP 边缘设备 240 被放置在同一个提供商网络上。例如，将 NAS 242 放置在与包括 IP 边缘设备 240 的接入提供商网络进行通信的第二提供商网络上。

[0044] NAS 256 可以使用隧道 290 与 HG 220 交换通信，该隧道 290 是经由 AN 230 在 HG 220 与 R 边缘设备 250 之间建立的。可以使用隧道 290 来转发 UE 210 与 IP 边缘设备 140 之间的网络设置信息，例如 IP 地址分配信息。在一个实施例中，隧道 290 可以是在 WTP 222、RG 224、AN 230 和 NAS 256 之间建立的 Wi-Fi 漫游虚拟局域网 (VLAN)。此外，NAS 256 可以使用安全隧道 292 与 UE 210 交换通信，而不必委托 HG 220。在一个实施例中，安全隧道 292 可以是一个 IPsec，IPsec 使用 IKE 经由 R 边缘设备 250 在 UE 210 与 IP 网络 270 之间

建立安全通信。

[0045] 为了在固定或 IP 网络（例如，固定网络漫游接入系统 100 或 200）中建立对移动 UE 的漫游接入，可以使用 CAPWAP 协议来将与 UE 有关的一些认证信息从 HG 转发到 AAA-M。CAPWAP 协议是在 AAA-M 与 HG 之间 的、独立于具体无线技术的互操作协议。可以设计 CAPWAP 协议的元素，以满足标准无线技术的具体要求。可以将 CAPWAP 协议实现为适用于特定的无线技术，其中该特定的无线技术遵从为该技术定义的绑定要求 (bindingrequirement)。该绑定可以包括技术特有的消息的定义和技术特有的消息元素的定义。CAPWAP 可以支持包括多个 HG 的局域网，所述多个 HG 经由基于 IP 的连接与 AAA-M 上的 AC 进行通信。例如，CAPWAP 协议可以借助 IEEE 802.11 绑定来支持包括 UE 和 HG 的、基于 IEEE 802.11 无线 LAN(WLAN) 的网络。同样地，CAPWAP 协议可以使 AC 能够在 HG 上对 UE 接入到网络进行管理。HG 可以作为 AC 控制的接口，例如远程射频 (RF) 接口，用于将 UE 连接到 IP 网络，这需要一组动态的管理和控制功能。一般，在私人企业中使用 CAPWAP 协议，但是如本文所述，可以在公共领域中实施 CAPWAP 协议。

[0046] 在一个实施例中，CAPWAP 协议可以支持分离介质接入控制 (MAC) 操作模式，在该操作模式中，借助 CAPWAP 协议来封装所有第二层 (L2) 的无线数据和管理帧，并且在 AC 与 HG 之间交换所有第二层 (L2) 的无线数据和管理帧。在这种模式中，可以由 HG 直接封装从 UE 接收的无线帧并且将其转发到 AC。可替换地，CAPWAP 协议可以支持本地 MAC 操作模式，在该模式中，HG 对 L2 的无线管理帧进行本地处理，然后将其转发到 AC。因此，CAPWAP 协议可以集中控制无线网络的认证和策略执行功能。CAPWAP 协议可以使高级的协议处理从 HG 转移到 AC，对于无线控制和接入的关键应用而言，这为 HG 留下了时间。此外，CAPWAP 协议可以提供通用封装和传输机制，这使得能够借助具体的无线绑定将 CAPWAP 协议应用于各种接入点类型的技术。

[0047] 根据 CAPWAP 协议，可以传输两种类型的数据或有效负载，包括 CAPWAP 数据消息和 CAPWAP 控制消息。CAPWAP 数据消息可以封装转发的无线帧。CAPWAP 控制消息可以是在 HG 与 AC 之间交换的管理消息。可以将 CAPWAP 数据和控制消息分成可使用单独端口发送的分组。可以使用例如 IPsec 或数据报传输层安全 (DTLS) 来加密或者保护传输的 CAPWAP 控制消息、CAPWAP 数据消息或这两者。IPsec 包括用于保护 IP 通信安全的一套协议，这套协议通过对数据流中的每个 IP 分组进行认证或对数据流 中的每个 IP 分组进行加密，或者同时对数据流中的每个 IP 分组进行认证和加密来保护 IP 通信的安全。IPsec 还包括用于建立密钥的协议。例如，基于本地策略，IPsec 可以使用 IKE 协议来处理协议和算法的协商以及生成加密密钥和认证密钥，并由此建立安全的 IPsec 通信会话。

[0048] 此外，CAPWAP 协议可以允许传输扩展认证协议 (EAP) 有效负载，以便建立安全的 IPsec 通信会话。EAP 可以是在诸如 WLAN 和点对点连接等无线网络中使用的通用认证框架。EAP 可以为期望的认证机制提供一些公共的功能和协商，又被称为 EAP 方法，该 EAP 方法是由 IKE 协议定义的。例如，当调用 EAP 时，EAP 方法可以提供安全认证机制并且协商在一端的 AC 与另一端的 HG 和 UE 之间的安全 PMK。然后，可以使用 PMK 来建立安全的 IPsec 通信会话。

[0049] CAPWAP 协议可以从发现阶段开始，在该发现阶段中，HG 经由 WTP 发送发现请求消息。AC 接收该发现请求消息并且用发现响应消息来响应。HG 接收该发现响应消息，并且作

为响应，HG 与 AC 建立安全的 IPsec（或 DTLS）通信会话。一旦 HG 与 AC 建立了安全的 IPsec 通信会话，则发生配置交换，在该配置交换中，两个组件对信息达成了一致。在该交换期间，HG 可以接收配置设置并且因此能够进行操作。

[0050] 此外，可以使用 RADIUS 协议在 AAA-M、AAA 服务器和 IP 边缘设备之间交换与 UE 有关的一些认证信息。RADIUS 可以用于传输与 UE 有关的认证信息，例如用户名称和密码。因此，IP 边缘设备可以创建“接入请求”，该“接入请求”包括多个属性，例如 UE 的用户名称、UE 的用户密码、IP 边缘设备的标识（ID）、UE 正接入的端口 ID 或其组合。然后，可以经由例如 AAA-M 将接入请求转发到充当 RADIUS 服务器的 AAA 服务器。当在一个时间长度内没有返回响应时，可以多次发送请求。

[0051] RADIUS 服务器接收该请求并且使用客户信息数据库来查找在请求中识别出的 UE。数据库中的 UE 条目可以包括一个要求列表，必须满足这一要求列表才允许 UE 经由 IP 边缘设备接入 IP 网络。该要求可以包括：密码的验证、UE 被允许接入的 IP 边缘设备或端口，或其它要求。如果没有满足要求或条件，则 RADIUS 服务器发送用于指示请求无效的接入拒绝响应。如果满足了要求或条件，则将 UE 的配置值列表放到接入接受响应中。这 些值包括服务类型，例如串行线路因特网协议（SLIP）、点对点协议（PPP）或登录用户、以及传送服务所需要的其它值。对于 SLIP 和 PPP 而言，这包括诸如 IP 地址 / 子网掩码、以太网 MAC ID、最大传输单元（MTU）、期望的压缩、期望的分组滤波标识符、期望的协议和期望的主机之类的值。

[0052] 图 3 示出了漫游接入方法 300 的实施例，该漫游接入方法 300 允许移动 UE 经由家庭网络上的 HG 以及接入提供商网络上的 IP 边缘设备（或 R 边缘设备）无线接入到 IP 网络。具体地，该方法 300 可以通过建立与 HG 的无线链路来使 UE 漫游接入到 IP 网络，而不必将它与 IP 网络的通信委托给 HG。

[0053] 在该方法 300 中，HG 首先与 IP 边缘设备（或 R 边缘设备）交换认证数据，并由此与 IP 边缘设备建立 IP 会话 302。同样地，HG 可以与诸如 Wi-Fi 漫游 VLAN 等 IP 边缘设备建立隧道 304。在一个实施例中，除了 HG 和 IP 边缘设备之外，隧道 304 还可以包括与 HG 和 IP 边缘设备进行通信的 AN。

[0054] 当移动 UE 在 HG 附近漫游时，UE 和 HG 可以建立无线关联或链路 306，该无线关联或链路 306 可以是 802.11 关联。具体地，UE 可以与 HG 上的 WTP 建立无线关联 306。在一个实施例中，在建立了无线关联 306 之后，可以不授权 UE 与 HG 进行通信。例如，可以封锁 HG 上的到 UE 的端口。HG 可以使用无线关联 306 向 UE 请求认证信息。例如，HG 可以使用无线关联 306 将 EAP 请求 308 转发到 UE。接着，UE 利用所请求的认证信息来响应 HG。例如，UE 可以使用无线关联 306 将 EAP 响应 310 转发到 HG。

[0055] 当 HG 接收了包括认证信息的 EAP 响应 310 时，HG 将认证信息转发到 AAA-M。例如，HG 可以使用 CAPWAP 与 AAA-M 交换 EAP 参数 312。EAP 参数 312 可以包括 UE 的认证信息。接着，AAA-M 将认证信息转发到 AAA 服务器。例如，AAA-M 可以使用 RADIUS 来与 AAA 服务器交换 EAP 参数 314，EAP 参数 314 包括认证信息。

[0056] AAA 服务器接收 EAP 参数 314，并且 AAA 服务器使用 EAP 序列 316 对 UE 进行认证。作为 EAP 序列 316 的认证阶段的结果，可以使用例如基于密钥的认证推导来导出主会话密钥（MSK）。例如，在 AAA 服务器和 UE 中，在例如用户初始化期间，首先提供密钥。因此，在认

证阶段期间，UE 可以通过利用认证信息 (EAP 响应 310) 进行响应来向 AAA 服务器证实它知道或拥有该密钥。该认证信息包括额外的密钥资料，AAA 服务器和 UE 两者都使用该密钥资料，以便利用特定的算法导出 MSK。一旦认证成功，AAA 服务器使用 RADIUS 将成功的认证应答 318 转发到 AAA-M，该认证应答 318 包括授权信息或参数和 MSK。AAA-M 可以使用 MSK 导出第一对主密钥 (PMK1) 和第二对主密钥 (PMK2)。

[0057] 然后，AAA-M 使用 CAPWAP 将成功的认证应答 320 转发到 HG。除了 PMK1 以外，成功的认证应答 320 还包括来自 AAA 服务器的授权参数。接着，HG 使用无线关联 306 将成功的认证应答 322 转发到 UE。当 UE 在成功地完成 EAP 序列 316 之后而导出 MSK 时，UE 使用 MSK，例如通过执行算法 324 而导出与 AAA-M 上的 PMK1 和 PMK2 相同的 PMK1 和 PMK2。这样，UE 可以与 HG 共享 PMK1。然后，UE 和 HG 使用共享的 PMK1 和 IEEE 802.11i 协议来实现四次 (4 次) 握手或交换，以便与 HG 建立安全的无线链路信道 326，例如安全的 802.11 信道。在一个实施例中，UE 和 HG 均可以使用 PMK1 来导出第一对临时密钥 (PTK1)，该第一对临时密钥可用于使用 802.11i 4 次交换来建立安全无线链路信道。

[0058] 接着，UE 将 IP 地址请求 328，例如动态主机配置协议 (DHCP) 请求，转发到 IP 边缘设备以便获得用于接入 IP 网络的 IP 地址。可以经由 HG 和隧道 304(Wi-Fi 漫游 VLAN 隧道) 将 IP 地址请求 328 转发到 IP 边缘设备。然后，为了获得对 UE 的授权，IP 边缘设备使用 RADIUS 将授权请求 330 转发到 AAA-M。在一个实施例中，IP 边缘设备将经由隧道 304 接收的任意授权请求直接转发到 AAA-M，而无需处理该授权请求。授权请求 330 包括 UE 连接识别信息，例如 UE 的介质接入控制 (MAC) 地址、线路 ID、VLAN ID 或其组合。

[0059] AAA-M 可以使用连接识别信息来验证 UE 的标识，并且 AAA-M 可以授权 UE 的连接。在一个实施例中，AAA-M 可以与 AAA 服务器进行通信以识别 UE。因此，AAA-M 使用 RADIUS 将授权应答 332 转发到 IP 边缘设备。除了 PMK2 以外，授权应答 332 还包括与 UE 有关的连接授权信息。这样，IP 边缘设备与 UE 共享 PMK2。然后，IP 边缘设备与 DHCP 服务器交换 DHCP 请求和响应 334，并且获得分配给 UE 的 IP 地址。此外，IP 边缘设备可以将从 AAA-M 接收的授权与分配的 IP 地址绑定。接着，IP 边缘设备将包括分配的 IP 地址的 DHCP 响应 336 转发到 UE。

[0060] 然后，IP 边缘设备使用 RADIUS 将计费开始消息 338 转发到 AAA-M。计费开始消息 338 用于以信号向 AAA-M 通知 :通信会话将要在 UE 与 IP 网络之间开始。此外，IP 边缘设备可以利用计费开始消息 338 将分配的 IP 地址转发给 AAA-M。接着，AAA-M 将计费开始消息 340 转发到 AAA 服务器，该计费开始消息 340 包括分配的 IP。同样地，AAA 服务器开始对 UE 的漫游接入连接使用进行计费。在一个实施例中，IP 边缘设备可以使用 RADIUS 经由 AAA-M 从 AAA 服务器接收与 UE 有关的计费策略信息，或者 IP 边缘设备可以使用 RADIUS 从 AAA-M 接收与 UE 有关的计费策略信息。例如，IP 边缘设备可以接收除了授权应答 332 中的连接授权信息之外的计费策略信息。同样地，IP 边缘设备可以对 UE 的漫游接入连接使用进行监管，而 AAA 服务器独立地处理连接使用的计费。IP 边缘设备可以使用分配的 IP 地址来识别以及监管 UE 连接使用，该分配的 IP 地址与计费策略信息绑定。类似地，AAA 服务器可以使用分配的 IP 地址对 UE 连接使用进行识别和计费。

[0061] 当 UE 接收了包括分配的 IP 的 DHCP 响应 336 时，UE 和 IP 边缘设备可以使用 IKE 建立安全的 IP 隧道 342，例如 IPsec。在一个实施例中，UE 和 IP 边缘设备均使用共享的

PMK2 来导出第二对临时密钥 (PTK2)，该第二对临时密钥用于建立安全的 IP 隧道 342，而不必委托 HG。

[0062] 当漫游的 UE 离开 HG 的附近时，断开 UE 与 HG 之间的安全无线链路信道 326。相应地，终止了对 UE 的漫游接入连接使用的计费以及监管。例如，HG 将安全无线链路信道 326 的断开通知给 IP 边缘设备，然后 IP 边缘设备删除或者丢弃 UE 的授权和策略信息，包括 PMK2 和 PTK2。此外，例如，IP 边缘设备或者 AAA-M 将安全无线链路信道 326 的断开通知给 AAA 服务器，并且 AAA 服务器停止对连接使用的计费。在一个实施例中，停止在 AAA 服务器上对连接使用进行计费可以将 CAPWAP 序列触发到 HG，例如，通过 AAA-M，这促使 HG 删除 PMK1 和 PTK1 以及与 UE 有关的其它认证信息。

[0063] 上述的网络组件可以用任意的通用网络组件来实现，例如具有能够处 理施加在其上的必要工作负荷的足够处理功率、存储器资源以及网络吞吐量的计算机或网络组件。图 4 示出了适用于实现本文所公开的组件的一个或多个实施例的典型通用网络组件 400。网络组件 400 包括处理器 402（可以将处理器 402 称为中央处理器单元或 CPU），该处理器 402 与包括辅助存储器 404、只读存储器 (ROM)406、随机存取存储器 (RAM)408 的存储器设备进行通信，并且该处理器 402 还与输入 / 输出 (I/O) 设备 410 和网络连接设备 412 进行通信。可以将处理器 402 实现为一个或多个 CUP 芯片，或者将处理器 402 实现为一个或多个专用集成电路 (ASIC) 的一部分。

[0064] 辅助存储器 404 一般由一个或多个磁盘驱动器或磁带机组成，并且辅助存储器 404 用于数据的非易失性存储，并且如果 RAM 408 不足以容纳全部工作数据，则将辅助存储器 404 用作溢出数据存储设备。当选择执行加载到 RAM 408 中的程序时，辅助存储器 404 可以用于存储这种程序。ROM406 用于存储指令并且还可能存储在程序执行期间读取的数据。ROM 406 是非易失性存储设备，与辅助存储器 404 的大存储容量相比，ROM 406 一般具有小的存储容量。RAM 408 用于存储易失性数据并且还可能存储指令。访问 ROM 406 和 RAM 408 一般比访问辅助存储器 404 快。

[0065] 尽管本申请已经提供了几个实施例，但是应该理解 :在不脱离本申请的精神或范围的前提下，可以以许多其它具体的形式来实现公开的系统和方法。应该将本发明的实例看作是示例性的而非限制性的，并且不限于本文所给出的细节。例如，可以将各种元件或组件组合或集成在另一个系统中，或者可以省略或者不实现某些特征。

[0066] 此外，在不脱离本申请的范围的前提下，可以将各种实施例中描述并且示出的离散或独立的技术、系统、子系统和方法与其它系统、模块、技术或方法进行组合或集成。本文示出或论述的彼此耦合或直接耦合或通信的其它部件可以通过一些接口、设备或中间组件以电子方式、机械方式或其它方式间接地耦合或通信。本领域技术人员可以发现其它的示例性变化、替换和修改并且可以在不脱离本文公开的精神和范围的前提下对它们进行改变、替换和修改。

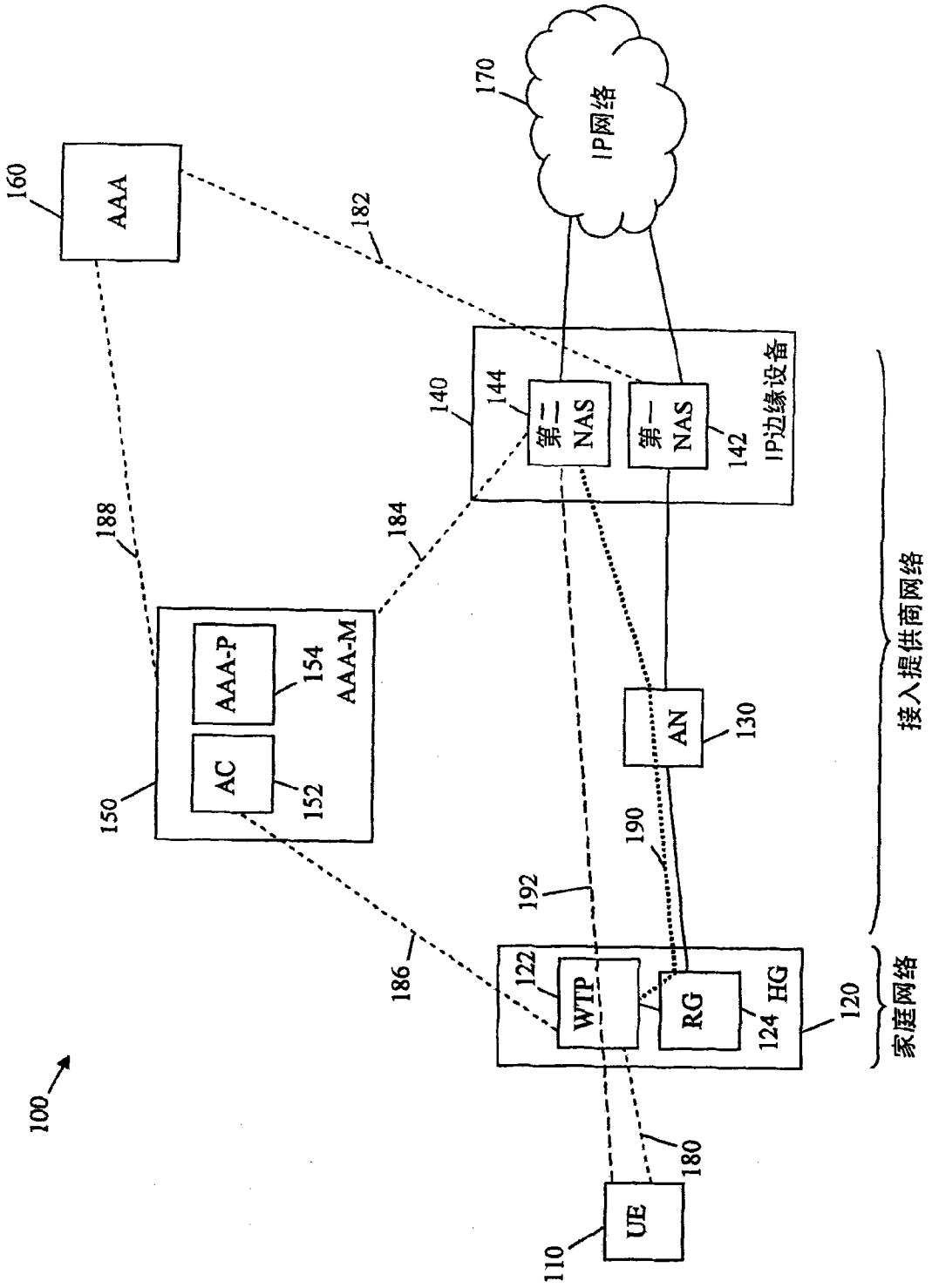

100
AAA
160
IP网络
170
182
第二 NAS
第一 NAS
IP边缘设备
140
144
142
188
184
AAA-P
AAA-M
154
AC
152
150
AN
130
190
192
186
WTP
RG
HG
122
124
120
UE
110
180
接入提供商网络
家庭网络

图 1

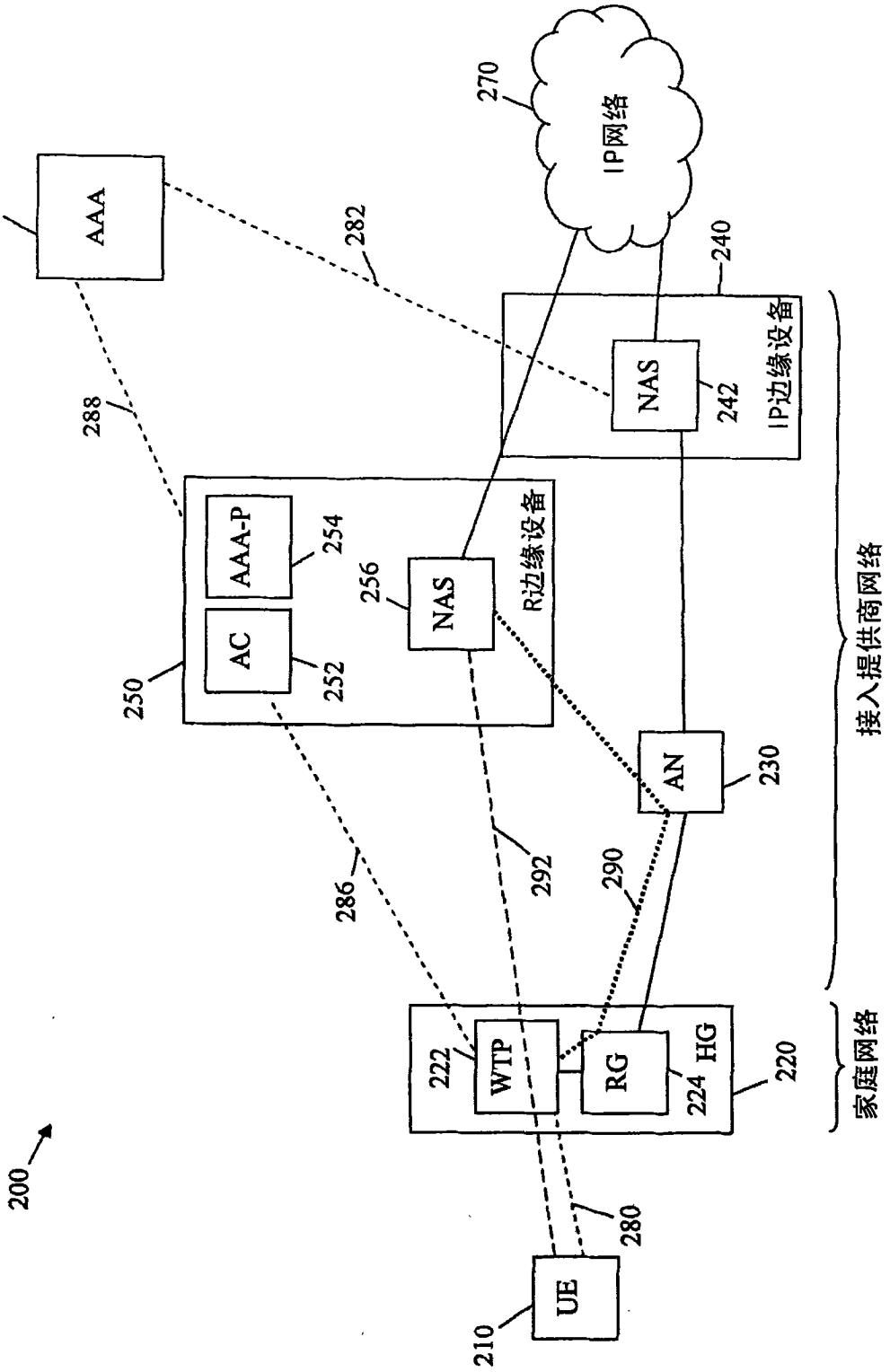

200
260
AAA
270
IP网络
282
240
IP边缘设备
NAS
242
288
AAA-P
254
AC
252
250
256
NAS
R边缘设备
AN
230
接入提供商网络
286
292
290
222
WTP
RG
224
HG
220
家庭网络
280
UE
210

图 2

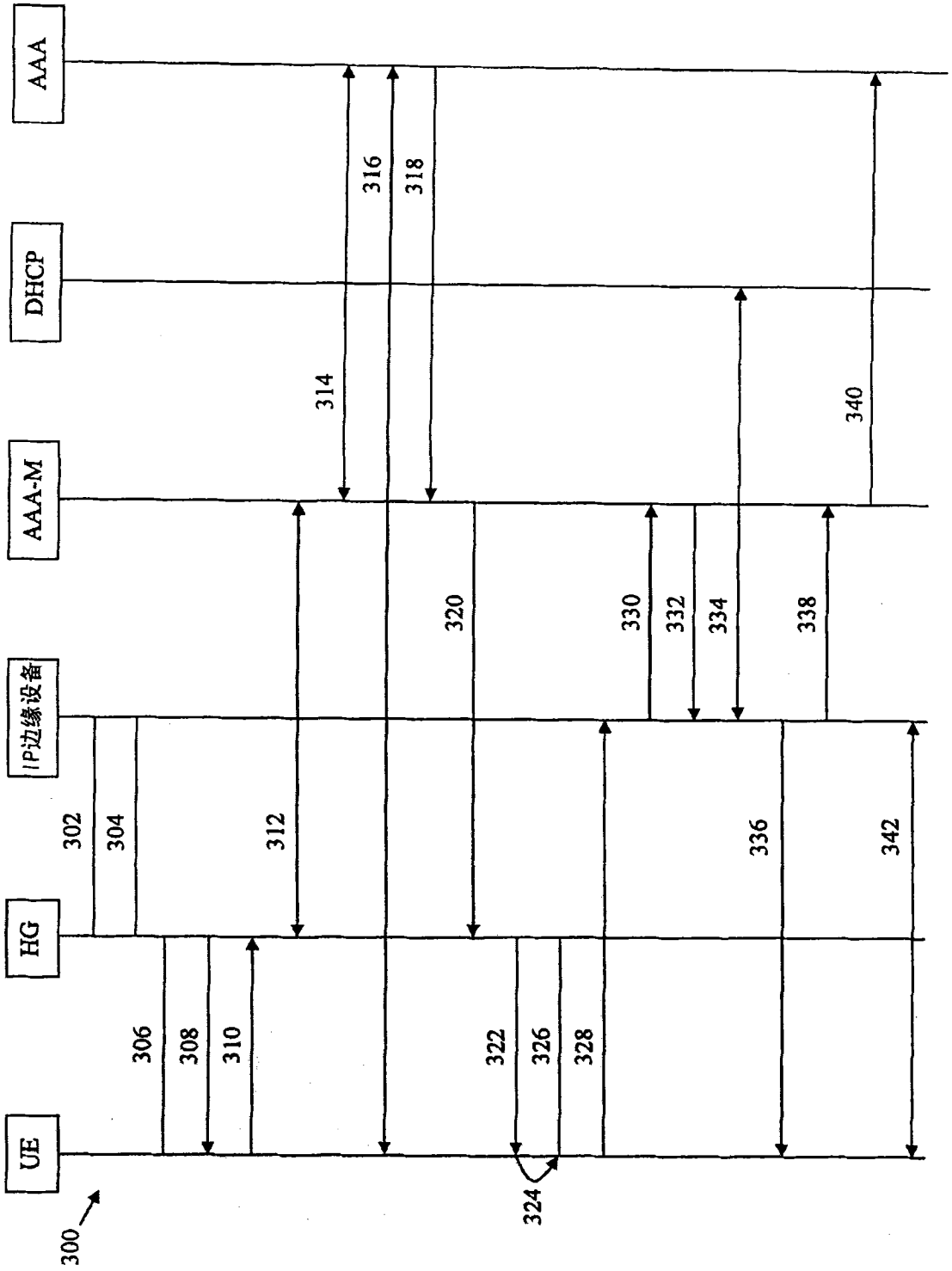

AAA
DHCP
AAA-M
IP边缘设备
HG
UE
300
302
304
306
308
310
312
314
316
318
320
322
324
326
328
330
332
334
336
338
340
342

图 3

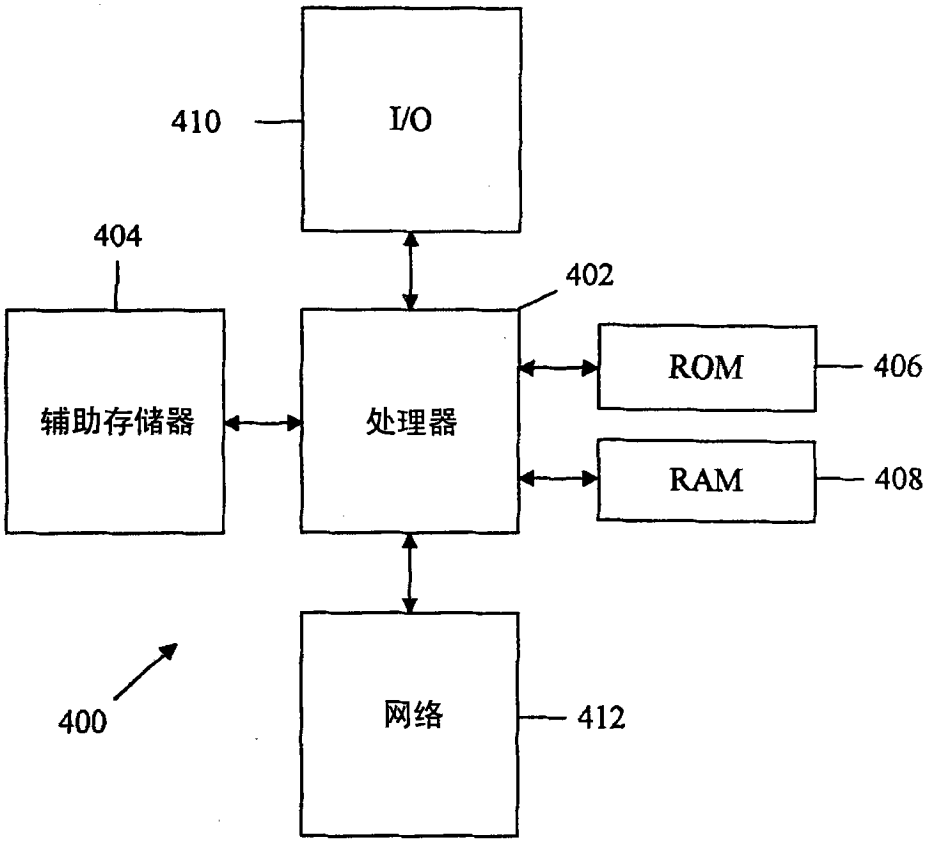


图 4