[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04Q 7/30
H04L 29/06
H04L 12/56
H04L 12/28

[12] 发明专利申请公开说明书

[21] 申请号 03824001.7

[43] 公开日 2005 年 10 月 26 日

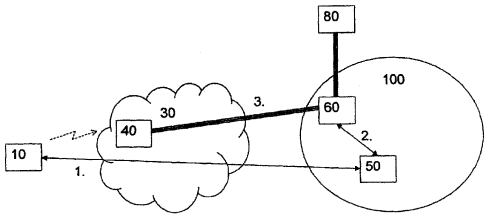
[11] 公开号 CN 1689369A

[22] 申请日 2003.9.26 [21] 申请号 03824001.7
[30] 优先权
[32] 2002.10. 8 [33] US [31] 10/265,760
[86] 国际申请 PCT/IB2003/004217 2003.9.26
[87] 国际公布 WO2004/034720 英 2004.4.22
[85] 进入国家阶段日期 2005.4.8
[71] 申请人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 凯莉·阿玛瓦阿拉
塞伯·维斯特里宁
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李德山
权利要求书 4 页 说明书 16 页 附图 5 页

[54] 发明名称 用于经由接入网建立连接的方法和系统

[57] 摘要

本发明涉及经由与至少一个用户终端和至少一个骨干网络(100)通信的接入网(30)来建立连接的系统和方法，所述骨干网络(100)至少包括用户终端认证和授权装置(50)以及至少一个用户数据处理节点(60，62)，其中，用户终端(10)到接入网(30)的连接被认证，并且基于在认证信令中传递的选择信息来选择至少一个用户数据处理节点(60，62)中的一个。 然后，所选的用户数据处理节点的隧道参数信息被通知给接入网(30)，并且基于隧道参数信息在接入网(30)与所选的用户数据处理节点(60)之间建立隧道连接。 通过基于与隧道两个端点有关的网络信令建立隧道连接，可以在初始彼此不相知的两个网络单元之间建立隧道连接。 这样，就可以在不提供情境激活程序或相应控制平面信令功能的接入网上接入蜂窝分组交换服务。



ISSN1008-4274

知识产权出版社出版

1. 一种经由与至少一个用户终端和至少一个骨干网络（100）通信的接入网（30）来建立连接的方法，所述骨干网络（100）至少包括用户终端认证和授权装置（50）以及至少一个用户数据处理节点（60，62），所述方法包括如下步骤：

a）认证用户终端（10）经由所述接入网（30）的连接；

b）在所述认证步骤中选择所述至少一个用户数据处理节点（60，62）中的一个（60）；

c）将所述所选的用户数据处理节点的隧道参数信息通知给所述接入网（30）；以及

d）基于所述隧道参数信息，在所述接入网（30）与所述所选的用户数据处理节点（60）之间建立隧道连接。

2. 根据权利要求 1 的方法，还包括使用至少一个通知的隧道参数作为所述建立的隧道连接内的标识符的步骤。

3. 根据权利要求 2 的方法，其中，所述至少一个隧道参数是隧道分配标识。

4. 根据权利要求 2 或 3 的方法，其中，所述所建立的隧道连接是 GRE 类型的。

5. 根据权利要求 4 的方法，还包括使用所述至少一个隧道参数作为所建立的 GRE 隧道的密钥参数的步骤。

6. 根据前述权利要求中任何一个的方法，其中，所述接入网是无线局域网（30）。

7. 根据前述权利要求中任何一个的方法，其中，所述至少一个骨干网络是蜂窝分组交换网络（100）。

8. 根据权利要求 7 的方法，其中，所述蜂窝分组交换网络是 GPRS 网络（70；100）。

9. 根据前述权利要求中任何一个的方法，其中，所述认证是基于 EAP 信令的。

10. 根据前述权利要求中任何一个的方法，其中，所述选择信息包括至少一个 APN 参数。

11. 根据权利要求 10 的方法，其中，所述至少一个 APN 参数包括 APN、用户名和口令。

12. 根据前述权利要求中任何一个的方法，其中，所述隧道参数信息在 AAA 接入接受消息中被通知给所述接入网（30）。

13. 根据权利要求 12 的方法，其中，所利用的 AAA 协议是 RADIUS。

14. 根据权利要求 12 的方法，其中，所利用的 AAA 协议是 Diameter。

15. 根据前述权利要求中任何一个的方法，其中，所述隧道参数信息包括隧道类型、隧道介质、隧道服务器地址和隧道分配标识中的至少一个。

16. 根据前述权利要求中任何一个的方法，其中，所述用户数据处理节点是 WLAN 网关（60，62）。

17. 根据权利要求 1 至 15 中任何一个的方法，其中，所述用户数据处理节点是 GGSN。

18. 根据前述权利要求中任何一个的方法，其中，所述选择信息在所述选择步骤中被辨别成 AAA 域名。

19. 根据前述权利要求中任何一个的方法，其中，所述选择信息是服务选择信息。

20. 根据权利要求 19 的方法，还包括在所述所选的用户数据处理节点（60）存储外部服务器域名、隧道参数和过滤参数中的至少一个的步骤。

21. 根据权利要求 20 的方法，还包括基于所述选择信息检查是否将所述选择信息通知给所述外部服务器的步骤。

22. 一种用于提供认证机制的认证服务器设备，所述认证服务器设备（50）被设置成用于：

a）基于在来自连接到接入网（30）的终端设备（10）的认证信

令中接收的选择信息，选择用户数据处理节点（60）；

b）从与所述用户数据处理节点（60）相关的信令中获得隧道参数信息；以及

c）将所述隧道参数信息通知给所述接入网（30）的接入服务器设备（40）。

23. 根据权利要求 22 的认证服务器设备，其中，所述认证信令是基于 EAP 协议的。

24. 根据权利要求 22 或 23 的认证服务器设备，其中，所述认证服务器是独立的 WLAN 认证服务器（50）。

25. 根据权利要求 22 或 23 的认证服务器设备，其中，所述认证服务器是 GGSN。

26. 根据权利要求 22 至 25 中任何一个的认证服务器设备，其中，所述服务选择信息包括至少一个 APN 参数。

27. 根据权利要求 22 至 26 中任何一个的认证服务器设备，其中，所述认证服务器（50）被设置成用于在 AAA 接入接受消息中通知所述隧道参数信息。

28. 根据权利要求 22 至 27 中任何一个的认证服务器设备，其中，所述隧道参数信息包括隧道类型、隧道介质、隧道服务器地址和隧道分配标识中的至少一个。

29. 根据权利要求 28 的认证服务器设备，其中，所述隧道类型是 GRE，和/或所述隧道介质是 IPv4 或 IPv6。

30. 根据权利要求 27 的认证服务器设备，其中，所述认证服务器（50）被设置成将 EAP 成功消息合并到所述 AAA 接入接受消息中。

31. 一种用于控制对接入网（30）的接入的接入控制设备，终端设备（10）连接到所述接入网（30），所述接入控制设备（40）被设置成用于从接收自认证服务器设备（50）的信令消息中获得隧道参数信息，以及用于建立到用户数据处理节点（60）的隧道连接以提供对所述终端设备（10）的服务接入。

32. 根据权利要求 31 的设备，其中，所述所接收的信令消息是

AAA 接入接受消息。

33. 根据权利要求 31 或 32 的设备，其中，所述隧道参数信息包括隧道类型、隧道介质、隧道服务器地址和隧道分配标识中的至少一个。

34. 根据权利要求 33 的设备，其中，所述接入控制设备（40）适于使用所述隧道分配标识作为所述所建立的隧道连接的流标识。

35. 根据权利要求 34 的设备，其中，所述流标识在密钥 GRE 属性中被通知。

36. 一种用于经由与至少一个用户终端（10）和至少一个骨干网络（100）通信的接入网（30）来建立连接的系统，所述骨干网络（100）至少包括根据权利要求 22 至 30 中任何一个的认证服务器设备（50）以及根据权利要求 31 至 35 中任何一个的接入控制设备（40）。

用于经由接入网建立连接的方法和系统

技术领域

本发明涉及经由接入网建立连接的方法和系统，所述接入网例如无线局域网（WLAN），其与至少一个用户终端和至少一个骨干网络通信，所述骨干网络例如通用分组无线业务（GPRS）网或通用移动电信系统（UMTS）网，并至少包括用户终端认证和授权装置以及至少一个用户数据处理节点。

背景技术

近年来，无线通信的市场已经有了巨大的发展。无线技术现在已经到达或者能够到达几乎地球上的每一个角落。随着无线电话和消息服务的巨大成功，无线通信正开始被应用于个人和商务计算领域，这几乎不会让人感到惊奇了。不再受有线网络设施的限制，人们在他们敢于到达的几乎任何地方都将能够接入和共享全球范围内的信息。

发展 WLAN 的主要动机和好处是增加移动性。网络用户可以几乎没有限制地到处移动，并且可以从几乎任何地方接入 LAN。除了增加的移动性之外，WLAN 提供增加的灵活性。会议可以如下安排，在会议中，雇员使用小型计算机和无线链路来共享和讨论未来的设计计划和产品。如果需要，这种“ad hoc”网络可以在很短的时间内构建或拆卸掉，在会议桌旁和/或世界各处都可以。WLAN 提供有线 LAN 的连接性和方便性，而不需要昂贵的布线或再布线。

但是，即使是最快的膝上型电脑，在旅行时的生产率也可能由于对互联网或公司内联网的较差接入而下降。尽管全球移动通信系统（GSM）在演变，但是膝上型电脑用户需要更快速的接入，以快速下载大的文件并同步他们的邮件。逐渐形成的移动信息社会要求数据在任何时间和任何地点都可得到。作为该问题的解决方案，已经提出了

运营商 WLAN（OWLAN）解决方案，即在特定地方例如机场、会议中心、饭店和会议室提供对膝上型电脑或终端设备的宽带接入。这样，移动网络运营商能够从世界上几乎任何地方提供对互联网、公司内联网或其他服务机器的宽带接入。这样，可以提供具有自身 WLAN 漫游特征的公共 WLAN 服务。

在分组交换蜂窝网络中，例如在 GPRS 或 UMTS 网络中，用户服务描述由接入点名称（APN）指定。GPRS 是用于 GSM 和 UMTS 网络两者的公共包域核心网络。该公共核心网络提供分组交换服务，并且被设计用于支持几个服务质量等级，以允许非实时流和实时流的有效传递。服务 GPRS 支持节点（SGSN）被提供用于跟踪移动终端的单独位置，并执行安全功能和接入控制。此外，网关 GPRS 支持节点（GGSN）提供与外部分组交换网络的接口，并且经由基于 IP 的包域骨干网络与 SGSN 连接。在骨干网络中，APN 实际上是指将要使用的 GGSN。此外，在 GGSN 中，APN 可以识别外部网络以及可选地将要被提供的服务。与 APN 的使用和结构有关的进一步的细节在例如 3GPP 规范 TS 23.003 中定义。

在 GPRS 中，用户可以接入位于由其 APN 识别的接入点之后的家庭网服务。当用户连接到 GPRS 服务时，即建立起如在例如 3GPP 规范 TS 23.060 中指定的包数据协议（PDP）情境时，在 PDP 情境建立信令中，由终端设备或用户装备（UE）或终端设备的用户选择的 APN 信息被从终端设备发送到网络。该信息包括 APN，以及可选地如果需要的话包括用户名和口令以便接入所选 APN 之后的服务。在 GPRS 网络中，该信息被用来选择合适的 GGSN。信息还到达所选的 GGSN，并且 GGSN 进一步使用该信息来建立到 GGSN 之后的网络节点即公司内联网或运营商服务节点的连接。如果提供了用户名和密码，那么它们就被传送到 GGSN 之后的有关网络节点，以允许连接的授权。

但是，在所提出的公共或运营商 WLAN 系统中，没有提供与 GPRS PDP 情境激活类似的操作。具体而言，没有专用的信令来在 WLAN 终端设备即 WLAN UE 与 WLAN 网络或 WLAN 网络之后的

网络之间建立服务。这种服务可以是例如对用户公司内联网的接入、第三方 ISP 型服务、移动运营商服务，到现在为止，用户只能经由本地 WLAN 接入网直接连接到互联网。因此，GPRS 型服务选择和激活是不可能经由 WLAN 网络的，这就构成了所提出的公共或运营商 WLAN 的缺点。

发明内容

因此，本发明的目的是提供使得能从 WLAN 网络或任何其他接入网对更广范围的服务进行接入的方法和系统。

该目的是通过下面的方法实现的，该方法经由接入网建立连接，该接入网与至少一个用户终端和至少一个骨干网络通信，所述骨干网络至少包括用户终端认证和授权装置以及至少一个用户数据处理节点，所述方法包括如下步骤：

——认证用户终端到所述接入网的连接；

——基于在所述认证步骤中传递的选择信息，选择所述至少一个用户数据处理节点中的一个；

——将所述所选的用户数据处理节点的隧道参数信息通知给所述接入网；以及

基于所述隧道参数信息，在所述接入网与所述所选的用户数据处理节点之间建立隧道连接。

此外，上述目的通过提供认证机制的认证服务器设备来实现，所述认证服务器设备被设置成用于：

——基于在来自连接到接入网的终端设备的认证信令中接收的选择信息，选择用户数据处理节点；

——从与所述用户数据处理节点有关的信令中获得隧道参数信息；以及

——将所述隧道参数信息通知给所述接入网的接入服务器设备。

此外，上述目的通过用于控制对接入网的接入的接入控制设备实现，终端设备连接到所述接入网，所述接入控制设备被设置成用于从

接收自认证服务器设备的信令消息中获得隧道参数信息，并用于建立到用户数据处理节点的隧道连接，以提供对于所述终端设备的服务接入。

因此，通过使用认证信令，选择信息被从接入网转发到骨干网络。然后，选择信息可以在骨干网络中被用于选择用户数据处理节点，以建立隧道连接。从而，对第三方网络服务的接入在整个接入网例如WLAN上都是可能的。基于第三单元与隧道两个端点之间的信令，可以在初始彼此不相知的两个网络单元之间建立隧道连接。这样，就能够进行动态服务选择和到不同服务的多个同时连接，并且在不同网络之间，例如在 WLAN 和蜂窝分组交换网络之间，实现服务连续性。从而可以增加网络灵活性和用户移动性，并且可以统一不同网络中的服务逻辑。

主要的优点是标准构建块在它们被用在例如 WLAN 的接入网中时，被以特定方式组合以实现期望的系统等级功能。这使网络供应商例如 WLAN 供应商容易采用这一解决方案。此外，对用户终端的影响被最小化，这同时使互用性最大化。另一个运营商的好处是会节省由于可能重复使用用于 WLAN 解决方案的蜂窝供应系统而引起的与用户相关的运营商支出。所提出的解决方案的优势在于当前的服务描述机制，例如 GPRS 中的 APN 机制，可以在新的运营商 WLAN 中使用，从而支持遗留的解决方案。

至少一个通知的隧道参数可以在所述建立的隧道连接内用作标识符。该至少一个隧道参数可以是隧道分配 ID。此外，所建立的隧道连接可以是 GRE 类型的。那么，至少一个隧道参数可以用作所建立 GRE 隧道的密钥参数。

认证信令可以是根据可扩展认证协议（EAP）的信令。具体而言，认证信令可以包括 EAP 响应消息。服务选择信息可以包括至少一个 APN 参数。该至少一个 APN 参数可以包括期望服务的 APN、用户名和口令。此外，APN 参数可以在认证消息中加密。对不同 APN 参数应用的加密可以进行不同的选择，使得所选的 APN 参数可以以加密格

式由认证服务器转发到所选的接入点，并且所选的 APN 参数只在接入点或所选的服务网络处被解密。

隧道参数信息可以在 AAA 接入接受消息中被通知给接入网。AAA 协议可以是 RADIUS 或 Diameter。隧道参数信息可以包括隧道类型、隧道介质、隧道服务器地址和隧道分配标识中的至少一个。

此外，用户数据处理节点可以是 WLAN 网关或 GGSN。

选择信息可以在选择步骤中被辨别为 AAA 域名。具体而言，选择信息可以是服务选择信息。

在所选的用户数据处理节点，外部服务器域名、隧道参数和过滤参数中的至少一个可以被存储。然后可能基于选择信息检查是否将选择信息信号通知给外部服务器。

认证服务器可以被设置成用于在 AAA 接入接受消息中通知隧道参数信息。该隧道参数信息可以包括隧道类型、隧道介质、隧道服务器地址和隧道分配标识中的至少一个。例如，隧道类型可以是 GRE，和/或隧道介质可以是 IPv4 或 IPv6。认证服务器可以被设置成用于将 EAP 成功消息合并到所述 AAA 接入接受消息中。该 EAP 成功消息然后可以通过认证信令被通知给请求例如服务连接的终端设备。

接入控制设备可以适于使用隧道分配标识作为所建立的隧道连接的流标识。作为实例，该流标识然后可以以密钥 GRE 属性被通知。

进一步的有利的修改在所附权利要求中限定。

附图说明

下面，将参照附图基于优选实施例更详细地描述本发明，其中：

图 1 示出了指示本发明基本原理的示意框图；

图 2 示出了根据优选实施例的网络体系结构的示意框图，其中，WLAN 经由 WLAN 网关被连接到 GPRS 网络；

图 3 示出了指示根据本发明优选实施例的 EAP 信令的信令图；

图 4 示出了根据优选实施例的增强 EAP 响应查询包的格式；

图 5 示出了指示根据本发明优选实施例的 RADIUS 认证信令的

信令图；

图6示出了根据本发明优选实施例的在认证服务器与认证服务器数据库之间的接口体系结构；

图7示出了指示根据本发明优选实施例的数据库询问信令的信令图；

图8示出了指示根据本发明优选实施例在WLAN网关与认证服务器之间进行隧道参数传递的RADIUS信令的信令图；

图9示出了指示根据本发明优选实施例在外部服务器与WLAN网关之间进行隧道参数传递的RADIUS信令的信令图；以及

图10示出了指示根据优选实施例用于提供对服务的接入的连接建立信令的信令图。

具体实施方式

现在将基于如图1和图2指示的网络体系结构来描述优选实施例，在图1和图2中，WLAN用户通过EAP认证被认证以接入WLAN网络，从而可以接入蜂窝分组交换服务。

图1示出了网络体系结构的示意框图，该网络体系结构包括WLAN 30和家庭网100，例如GPRS网络或任何其他蜂窝分组交换网络。被预订给家庭网服务并希望可以接入该服务的终端设备或WLAN UE 10，首先通过使用认证信令例如授权请求消息，将指示至少一个APN参数以及可选的用户名和口令的服务选择信息经由WLAN 30传递给家庭网100的认证服务器50（第一步）。然后，认证服务器50选择设置在家庭网100中的WLAN网关60，将服务信息通知给WLAN网关60，并且作为响应从WLAN网关60接收用于在WLAN 30的接入服务器40与应用服务器80之间建立连接的连接信息，应用服务器80提供被请求的服务且由至少一个APN参数标识（第二步）。具体而言，认证请求可以与用户名和口令一起被进一步转发到应用服务器80或其他外部AAA服务器，而WLAN网关60首先从那里接收响应，然后将该响应代理给接入服务器40。

图 2 示出了 OWLAN 用户平面体系结构的更详细的框图，在该体系结构中可以实现本发明的优选实施例。

在图 2 中，WLAN UE 10 经由无线连接例如基于 IEEE 802.1x WLAN 协议被连接到 WLAN 的接入点 20。要注意，接入点 20 具有一些与在通用蜂窝网络中的基站类似的基本功能，例如在空中接口上提供到移动 UE 的连接。接入点 20 不是移动的，并且形成有线网络基础结构的一部分。与 WLAN 网络的体系结构和功能有关的进一步的细节可以从例如 IEEE 规范 802.11 中收集。

此外，WLAN 包括用于建立到外部网络的连接的 WLAN 接入服务器 40，所述外部网络例如家庭网 100 或其他分组交换网络，例如互联网或运营商或公司内联网。家庭网 100 可以是 GPRS 网络或 WLAN 骨干网络并且包括认证服务器 50，其具有分派的认证服务器数据库 55，用户信息例如每一个被连接的终端设备或 UE 的服务简档信息在其从永久用户数据库 110 中被检索出之后就被存储在认证服务器数据库 55 中，所述永久用户数据库 110 例如归属位置寄存器（HLR）或家庭用户服务器（HSS），其可以通过 MAP（媒体访问协议）信令接入。要注意，认证服务器 50 的功能还可以位于其他网络，例如 WLAN 骨干或子系统。在 UE 10 中使用 GSM SIM 卡的情况中，与 UE 10 有关的认证信令可以基于 EAP SIM 认证协议。或者，在 UE 10 中使用 UMTS SIM 卡的情况中，认证可以基于 EAP AKA（认证和密钥协议）认证协议。

EAP 协议机制被用于通过 GSM SIMS 或 USIM 的认证和会话密钥分发。认证基于查询响应机制，其中，在 SIM 或 USIM 卡上运行的认证算法可以被给予随机数（RAND）作为查询。SIM 或 USIM 卡运行特定于运营商的秘密算法，该算法将存储在 SIM 或 USIM 上的 RAND 和私钥作为输入，并产生响应（SRES）和密钥作为输出。该密钥最初旨在在空中接口上被用作加密密钥。认证服务器 50 具有到 UE 10 的 GSM 或 UMTS 家庭网 100 的接口，并且作为分组交换 AAA（认证、授权和计费）网络与 GEM 或 UMTS 认证基础结构之间的网

关。在接收包括可映射到用户的国际移动用户识别号（IMSI）的用户标识的 EAP 身份响应之后，授权服务器 50 从在用户家庭网 100 的归属位置寄存器（HLR）或家庭用户服务器（HSS）110 处的认证中心得到 n 个三位字节或五位字节。从三位字节中，认证服务器 50 基于密码算法得到密钥材料。

根据优选实施例，WLAN 认证信令被用来将 GPRS 服务预订或选择信息经由认证服务器 50 通知给家庭网 100。GPRS 服务信息或服务选择信息包括期望服务的 APN 以及经由所指示的 APN 连接到服务所需的可选用户名和口令。认证服务器 50 使用所获得的服务选择信息来选择与 GGSN 具有类似功能的 WLAN 网关 60，从这里用户可以接入预订的服务。预订的服务可以是例如对公司内联网或者移动运营商的服务的接入。

OWLAN 用户平面处理使得能够对由家庭网 100 经由 WLAN 提供的服务进行受控和强制的接入。这是在已经提供的直接互联网接入服务之外的新特征。由家庭网 100 提供的服务可以是家庭运营商自身的服务或者是第三方服务，如公司内联网接入。所提供的服务可以与经由 GPRS 接入点提供的那些服务相同。

这些家庭网服务可以经由 OWLAN 家庭网 100、经由由其接入点名称（APN）标识的 WLAN 网关 60 接入。与特定用户的家庭网服务有关的信息配置在数据库 55 中，在下文中将数据库 55 称为认证服务器数据库，其对于认证服务器 50 以及所有其他家庭网认证服务器来说都是可接入的。在认证服务器数据库 55 中的信息是 HLR GPRS 简档中信息的子集。认证服务器数据库 55 可通过由 MAP 更新位置程序或者经由 O&M（操作和维护）功能从 HLR 110 中拷贝来建立。

当家庭认证服务器 50 对用户进行认证时，其从认证服务器数据库 55 中检查用户是否已经预订家庭网服务。如果没有，那么认证服务器 50 继续正常地进行 EAP 认证。

如果用户被预订给家庭网服务，那么认证服务器 50 等待来自 WLAN UE 10 的 APN 信息。WLAN UE 10 可以在 EAP-SIM 响应消

息中通知期望的 APN。APN 信息由 APN 以及可选的 APN 的用户名和口令组成。如果用户不在 EAP-SIM 响应消息中包括任何 APN 信息，那么认证服务器 50 继续正常地进行 EAP 认证，并采用普通互联网接入。当用户通过 APN 参数指示他正连接到特定 APN 时，认证服务器 50 从检索出的预订信息中检查到用户被授权接入所指示的 APN。当检查成功后，认证服务器 50 将 APN 名辨别成 WLAN 网关 AAA 服务器域名，例如 RADIUS（远程认证拨入用户服务）域名，并请求允许由其 IMSI（国际移动用户识别号）标识的用户接入 WLAN 网关 60。与被用于执行认证的 RADIUS 协议有关的进一步的细节，在网络接入服务器与共享认证服务器之间的授权和配置信息，可以从 IETF（互联网工程任务组）规范 RFC 2138 中收集。

认证服务器 50 请求 WLAN 网关 60（或 WLAN 网关 60 之后的网络）分配合适的隧道参数，并授权用户接入 APN。这是通过向所指示的 WLAN 网关 RADIUS 服务器发送 AAA 接入请求例如 RADIUS 接入请求来完成的。取决于所利用的 AAA 域名，WLAN 网关 60 检测被请求的服务。

如果服务是由家庭网服务器 120 提供的移动运营商（MO）服务，那么各 WLAN 网关 62 从服务的内部数据库中选择适当的隧道和过滤参数，分配隧道分配 ID，并将 AAA 接入接受消息发回认证服务器 50。

如果服务是第三方服务，WLAN 网关 60 基于所利用的 AAA 域名选择各外部 AAA 服务器，例如 RADIUS 服务器 130，并在那里轨发 AAA 接入请求，例如具有用户名和口令的请求。在接收 AAA 接入接受消息并建立所指示的到外部网络的隧道之后，WLAN 网关 60 选择到 WLAN 接入服务器 40 的隧道参数，分配隧道分配 ID，并将 RADIUS 接入接受消息发送到认证服务器 50。认证服务器 50 将 EAP 成功消息和密钥材料添加到 AAA 接入接受消息中，并将其转发到 WLAN 接入服务器 40。

如果 WLAN UE 10 支持 IP 多重连接（multihoming）并因此支持与不同 IP 地址的同时连接，那么就可能以这里描述的相同方式来建

立与已经存在的连接并行的多个连接。每一个连接将具有其自身的WLAN UE IP地址，其自身的WLAN网关，以及在各自的WLAN网关与WLAN接入服务器40之间的其自身的隧道。然后，可以使用计费功能来检测用户平面隧道的存在。

图3示出了信令图，其指示在UE 10与认证服务器50之间的EAP-SIM认证信令。由网络发出的第一EAP请求（未示出）是EAP身份请求。客户机或UE 10通过包括假名或IMSI的EAP身份响应来作出响应（步骤1）。在身份隐私支持正被UE 10使用时使用假名。响应于EAP身份响应消息或包，认证服务器50发送包括n随机数RAND和其他参数的EAP查询请求（步骤2）。响应于此，UE 10发出包括计算出的响应值SRES的EAP查询响应。此外，根据本发明的优选实施例，EAP查询响应还包括至少一个加密的APN参数，该参数指定将被接入的期望GPRS服务。加密的APN参数可以包括期望服务的APN以及可选的用于可以接入该服务的用户名和口令（步骤3）。对不同APN参数应用的加密可以不同地选择，即APN本身可以是AP选择所需的唯一APN参数，因此只有这个参数必须是将被接入服务器解密和/或读的格式。用户名和口令参数可以以加密的格式由认证服务器被转发到所选的接入点，并且这些参数只在接入点或所选的服务网络处被解密。因此，就不可能在它们经由第一网络被传递时来接入它们。如果认证程序是成功的，那么认证服务器50用EAP成功消息来作出响应（步骤4）。

上面的认证信令程序使得能够将服务选择参数通知给认证服务器50而不需要任何额外的情境激活功能，而在没有WLAN功能的传统GPRS网络中是需要这种功能的。为了实现认证信令的这一增强功能，在UE 10处的客户机软件被修改或编程，以将各服务选择信息添加到EAP查询响应消息中。具体而言，如果用户已经选择要连接到由其APN标识的特定服务，那么服务信息或服务选择信息在UE 10处的客户机软件中配置。对每一个服务，都可以进行下面的设定。第一，可以设置为用户识别服务的自由文本入口。第二，APN，即公共陆地

移动网络（PLMN）的标识加上由移动运营商（MO）分配的域名服务器（DNS）名称可以被设置以指向特定的服务，第三，可以在客户机软件中进行指示是否需要用户名和口令的设置（例如是/否设置）。第三个设置可以包括指示预定的还是动态的用户名的设置或/和密码设置。

最迟在接收 EAP 请求消息之后，UE 10 从用户那得到与所需的服务选择相关的信息，并如由所利用的信令协议例如 EAP-SIM 规定的那样，将其加密。UE 10 然后将 APN 参数信息插入到 EAP 查询响应消息中，并将其发送到认证服务器 50。

图 4 示出了如在 SIM 中产生的根据优选实施例的增强 EAP SIM 查询响应消息的格式。“码”字段被用来将消息标识为响应消息。“标识符”字段是一个八位字节，帮助匹配对响应的应答。具体而言，“标识符”字段必须匹配作为响应向其发送的消息的“标识符”字段。“长度”字段指示 EAP 消息或包的长度。“类型”和“子类型”字段被设置为指定 EAP SIM 查询响应消息的特定值。“预留”字段在发送时被设置为 0，而在接收时忽略不计。“AT_SRES”字段指示属性值，其后是指示下一个 SRES 值的长度的另一个“长度”字段，再然后是“预留”字段。最后，所提出的指定被请求服务的 APN 参数可以例如作为加密值被添加。

图 5 示出了指示根据本发明优选实施例的 RADIUS 认证信令的信令图。当 WLAN 接入服务器 50 接收 RADIUS 接入接受消息时，其检查与隧道设置有关的参数。如果在 IETF 规范 RFC 2868 中定义的隧道类型属性存在，那么就可以对用户应用隧道。具体而言，隧道类型属性 9（GRE）可以被 WLAN 接入服务器 40 利用，而 IP（互联网协议）地址可以作为一个可选的字段被添加。然后，WLAN 接入服务器 40，可以在 IP 地址没有在 RADIUS 信令中被传送时作为引导协议延迟，或者可以作为 DHCP（动态主机配置协议）服务器，用于分配由 RADIUS 信令给出的 IP 地址。

隧道介质类型可以由在 RFC 2868 中定义的隧道介质类型属性指示。所支持的介质类型是 IPv4（IP 第 4 版）和 IPv6（IP 第 6 版）。

然后，建立到所指示的隧道服务器端点地址的隧道。该信息在RADIUS接入接受中的在RFC 2868中定义的隧道服务器端点属性中给出。

端点地址可以是FQDN或具有点符号的IP地址。取决于隧道基站协议（IPv4或IPv6），端点地址也可以是IPv4或IPv6格式的。

RADIUS隧道分配ID可以被WLAN接入服务器40用作将要建立的到所指示隧道服务器端点地址的GRE隧道的流ID。在GRE中，流ID由密钥GRE属性提供。

在建立GRE隧道之后，WLAN接入服务器40将从WLAN UE 10接收的所有用户数据都映射到向着隧道服务器的隧道。这包括任何DHCP请求。

在RADIUS接入接受消息中没有设置任何隧道参数的情况下，WLAN接入服务器40可以利用内部DHCP服务器进行IP地址分配，并根据局部路由策略将即将到来的用户数据直接路由到互联网。

下面，描述在认证服务器50与认证服务器数据库55之间的服务预订检索信令。

图6示出了在认证服务器50与认证服务器数据库55之间的接口体系结构。认证服务器50与认证数据库55之间的接口可以支持多对一连接，即多个认证服务器可以能够使用相同的认证服务器数据库。特别地，认证服务器数据库功能可以相应于如在相应的3GPP第6版规范中定义的即将具有的HSS的特定于WLAN的功能。认证服务器50与认证服务器数据库55之间的接口因此可以类似于由3GPP指定的即将到来的Wx接口。Wx应用可以在认证服务器与认证服务器数据库55之间的RADIUS连接上使用。此外，向着HLR 110的MAP接口可以逻辑地处于认证数据库55与HLR 110之间。

图7示出了指示用于在认证服务器数据库55处的询问的信令的信令图。最迟在用户在EAP-SIM响应消息内提供APN信息时，认证服务器50向认证服务器数据库55询问用户的服务预订信息。预订信息可以由RADIUS应用消息请求来进行WLAN用户简档请求。该消

息含有用户的 IMISI。认证服务器数据库 55 用 RADIUS 应用消息 WLAN 用户简档来作出响应。该消息含有所指示用户的预订服务列表。对于每一个预订的服务，都包括下面的信息：

·接入点名称（APN）

·MSISDN 号（用于 MCD）

·SIM 认证，或者额外的用户名和口令认证

如果不存在预订的服务，那么认证服务器数据库 55 可以返回空消息。

下面，描述从外部 RADIUS 服务器 130 经由 WLAN 网关 60 到认证服务器 50 的隧道参数传递。

图 8 示出了指示用于在 WLAN 网关 60 与认证服务器 50 之间的隧道参数传递的 RADIUS 信令的信令图，图 9 示出了指示用于在外部 RADIUS 服务器 130 与 WLAN 网关 60 之间的隧道参数传递的 RADIUS 信令的信令图。在 APN 与 RADIUS 服务器 130 之间是一对一的映射，以授权用户对服务的接入。一般地，RADIUS 服务器 130 或对服务器的 RADIUS 代理位于 WLAN 网关内。认证服务器 50 辨别来自内部数据库而非来自只含有特定于用户的入口的认证服务器数据库 55 的、与所指示的 APN 相关联的 RADIUS 服务器名称。

具体而言，认证服务器 50 将 RADIUS 接入请求消息发到被辨别的 RADIUS 服务器 130。

如果服务依赖于 SIM 认证，那么在 RADIUS 接入请求消息中，认证服务器 50 可以使用被认证的 IMSI 作为用户的身份。

如果服务具有其自身的额外的认证，那么在 RADIUS 接入请求消息内的 EAP SIM 响应中，认证服务器 50 可以使用在 APN 参数内提供的用户名和口令。

在接收 RADIUS 接入请求之后，WLAN 网关 60 即从其内部数据库中检查与所利用的域名相关的服务。在每一个域名与经由 WLAN 网关 60 可得到的服务之间应该是一一映射的。

对于每一个服务，下面的信息都可以存储在 WLAN 网关 60 中：

·外部 RADIUS 服务器域名（如果有的话）

·适当的隧道参数

·适当的过滤参数

WLAN 网关 60 检查 RADIUS 接入请求消息是否将被代理到外部 RADIUS 服务器 130。如果是，那么 WLAN 网关 60 使用从其内部数据库中辨别的域名将消息转发到外部 RADIUS 服务器 130。

在不成功的情况下，认证服务器 50 接收 RADIUS 接入拒绝消息作为应答，并且认证服务器 50 以适当的原因码拒绝来自 WLAN UE 10 的连接。

在成功的情况下，认证服务器 50 接收来自 RADIUS 服务器 130 的 RADIUS 接入接受消息。该消息包括将在外部网络与 WLAN 网关 60 之间被利用的适当的隧道和过滤属性。

隧道参数可以包括:

·隧道类型（GRE）

·隧道介质（IPv4 或 IPv6）

·隧道服务器地址（由 WLAN 网关 60 分配的地址）

·帧化 IP 地址属性（可选）

·隧道分配 ID（由 WLAN 网关 60 分配的唯一标识符）

此外，预先配置的 L2TP（第 2 层隧道协议）隧道可以在 WLAN 网关 60 与外部网络之间得到支持。

然后，WLAN 网关 60 将 RADIUS 接入接受消息转发到认证服务器 50。认证服务器 50 将 EAP 成功消息和会话密钥材料添加到 RADIUS 接入接受消息中，并将其转发到 WLAN 接入服务器 40。

图 10 示出了指示经由 WLAN 30 对 GPRS 服务的服务接入的详细信令图。最初，EAP 身份响应被从 UE 10 传送到接入点 20，接入点 20 产生 RADIUS 接入请求消息并经由 WLAN 接入服务器 40 将该消息转发到认证服务器 50。认证服务器 50 在 WLAN UE 10 的家庭网 100 的 HLR 110 处对恢复用户数据进行处理，HLR 110 用 WLAN UE 10 的用户数据来作出响应。然后，认证服务器 50 向 HLR 110 发出发

送授权信息请求消息，HRL 110 用包括所要求的授权信息的发送授权信息响应消息来作出响应。然后，授权服务器 50 通过使用 UE 10 用户的 IMSI 来从授权数据库 55 请求服务简档信息，并从数据库 55 接收包括指示用户预订服务的 APN 列表的服务简档。然后，认证服务器 50 向 UE 10 发出 EAP 查询请求消息，例如 EAP SIM 请求，并接收增强的 EAP 查询响应消息，例如 EAP SIM 响应，如在图 4 中指定的。

基于 APN 参数信息以及可选的用户名和密码，认证服务器 50 选择 WLAN 网关 60，并将包括用户名和密码的 RADIUS 接入请求消息转发到 WLAN 网关 60，WLAN 网关 60 将 RADIUS 接入请求路由到有关的 APN，例如外部 RADIUS 服务器 130。RADIUS 服务器 130 用 RADIUS 接入接受消息作出响应，该消息包括建立隧道连接以提供所请求服务所需的隧道和过滤参数。WLAN 网关 60 产生 WLAN 接入服务器 40 的接入控制器功能与 WLAN 网关 60 之间的隧道连接所需的隧道和过滤参数以及隧道分配 ID，并将 RADIUS 接入接受消息转发到认证服务器 50。认证服务器 50 向 RADIUS 接入接受消息中添加 EAP 成功消息和会话密钥，并将 RADIUS 接入接受消息转发到 WLAN 接入服务器 40。响应于此，WLAN 接入服务器 40 将包括 EAP 成功消息的 RADIUS 接入接受消息转发到 WLAN 接入点 20，接入点 20 提取出 EAP 成功消息并将其转发到 WLAN UE 10。最后，基于从认证服务器 50 接收的在 RADIUS 接入接受消息中的信息，WLAN 接入服务器 40 使用隧道分配 ID 作为流 ID 或密钥建立到 WLAN 网关 60 的隧道连接。

总之，服务接入是通过在 EAP SIM 或 EAP AKA 认证信令中并入或包括分组交换域类型服务选择信息作为新的加密属性来实现的。当用户希望连接到由 APN 标识的特定服务时，在 WLAN UE 10 中的用户或客户机软件将期望的 APN 以及可选的用户名和口令设置到有关的 EAP 消息中，并且 WLAN 30 使用该信息来选择合适的用户平面网络单元以及建立隧道和过滤策略。

要注意，本发明不限于所描述的 WLAN 和 GPRS 服务，并且可

以在没有在接入网中提供接入分组交换服务所需的控制平面信令的任何网络体系结构中使用。认证服务器 50 和网关 60 的功能不一定必须是 GPRS 功能，而是可以位于任何骨干网络或 WLAN 的子系统或任何其他可由 WLAN 30 接入的网络中。它们可以分别提供在独立的服务器设备中或者在 GPRS GGSN 或 SGSN 功能中。另外，接入的服务不一定是 GPRS 服务。这样，WLAN UE 10 可以是单模 WLAN 终端，该终端没有 GPRS 功能，但是具有经由认证信令，例如通过与 GPRS 服务选择机制类似的机制，来接入外部服务的功能。此外，任何给定的认证消息都可以用来传递服务选择信息。优选实施例因此可以在所附权利要求的范围内改变。

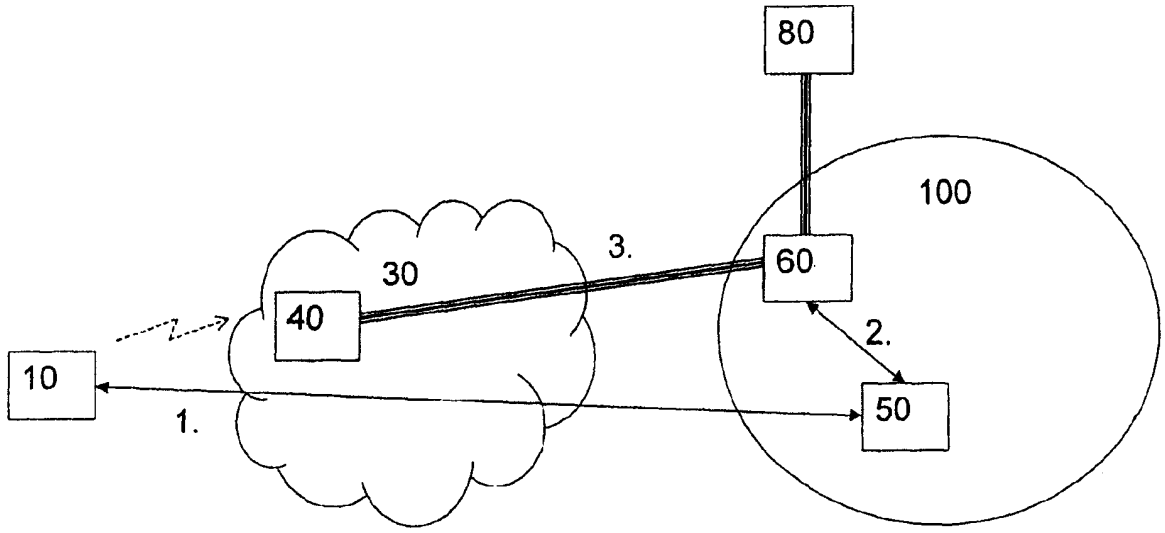

80
100
3.
30
60
40
2.
10
1.
50

图1

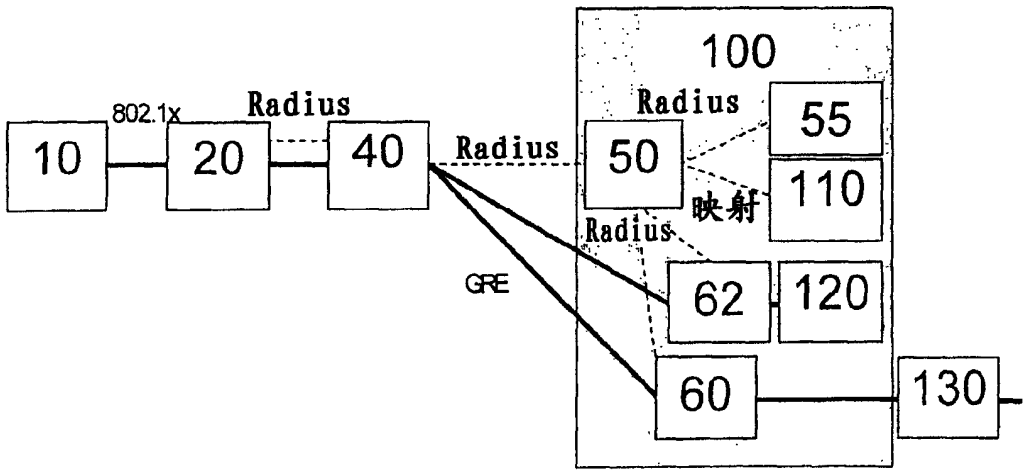

100
802.1x
Radius
Radius
55
10
20
40
Radius
50
110
映射
Radius
GRE
62
120
60
130

图2

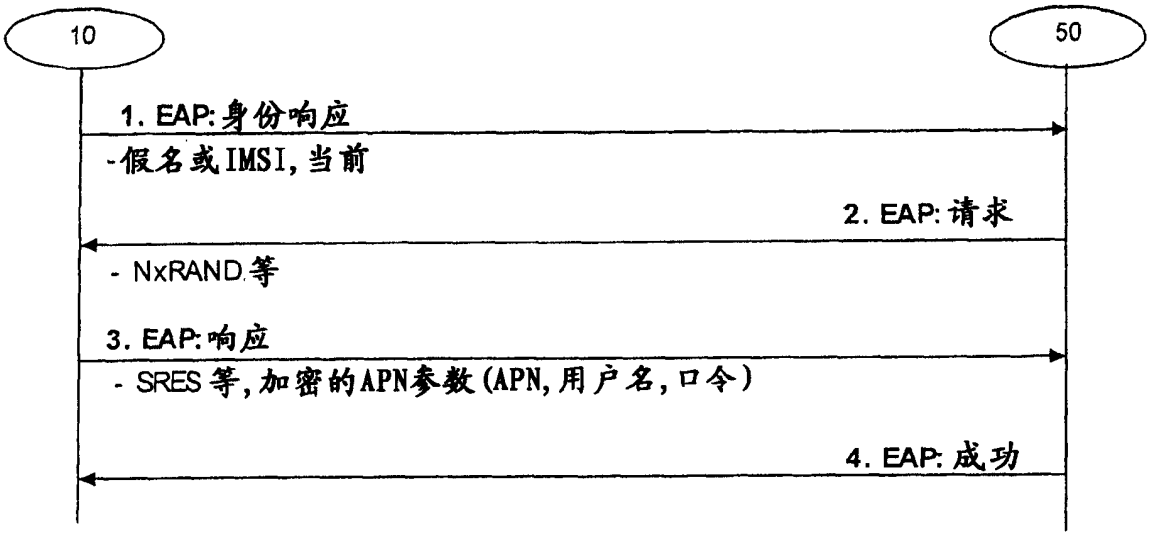


图3

码	标识符	长度
类型	子类型	预留
AT_SRES	长度	预留
SRES		
APN参数		

图4

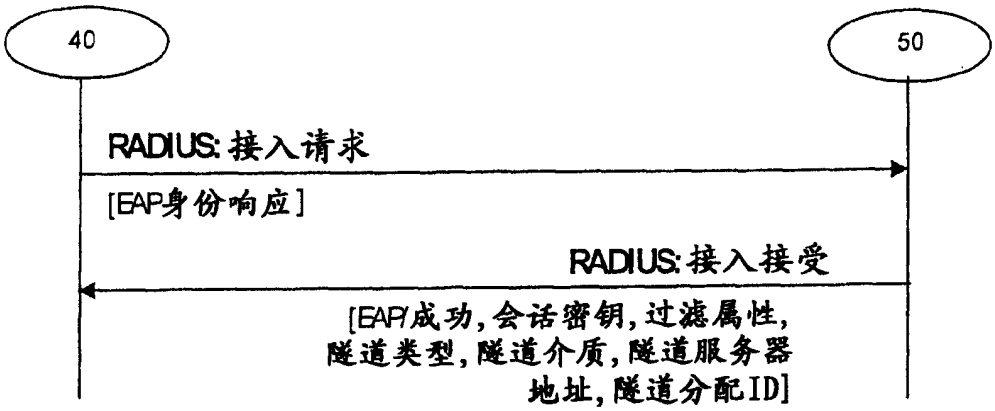

40
50
RADIUS:接入请求
[EAP身份响应]
RADIUS:接入接受
[EAP成功,会话密钥,过滤属性,
隧道类型,隧道介质,隧道服务器
地址,隧道分配ID]

图5

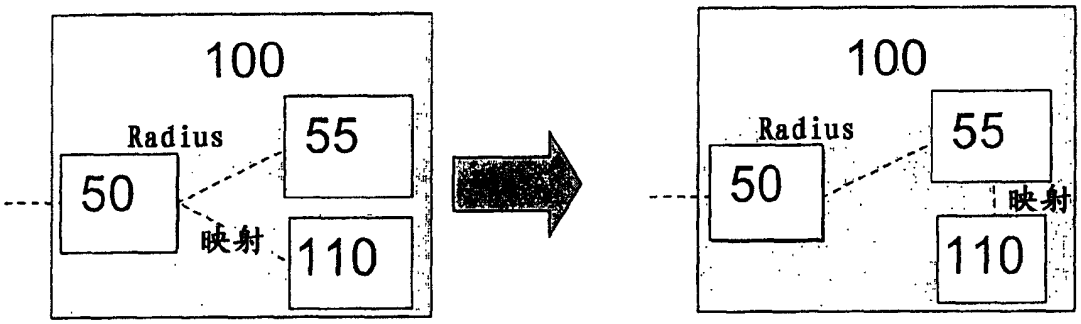

100
Radius
55
50
映射
110
100
Radius
55
50
映射
110

图6

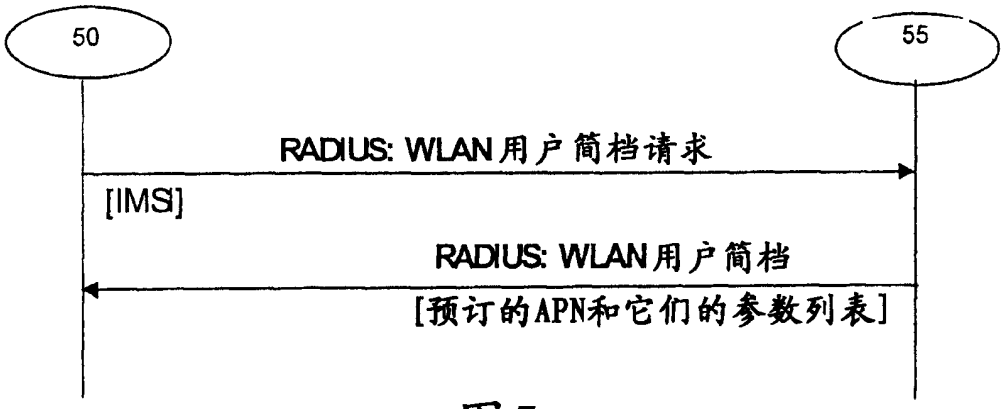

50
55
RADIUS: WLAN用户简档请求
[IMSI]
RADIUS: WLAN用户简档
[预订的APN和它们的参数列表]

图7

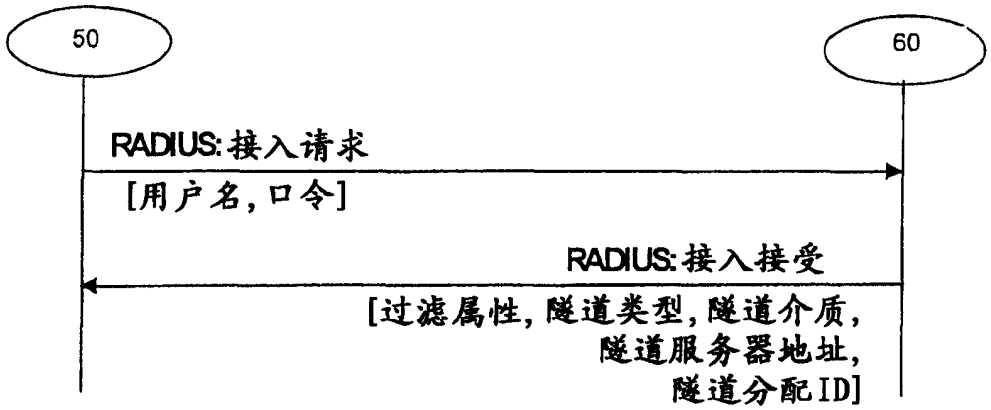

50
60
RADIUS:接入请求
[用户名,口令]
RADIUS:接入接受
[过滤属性,隧道类型,隧道介质,
隧道服务器地址,
隧道分配ID]

图8

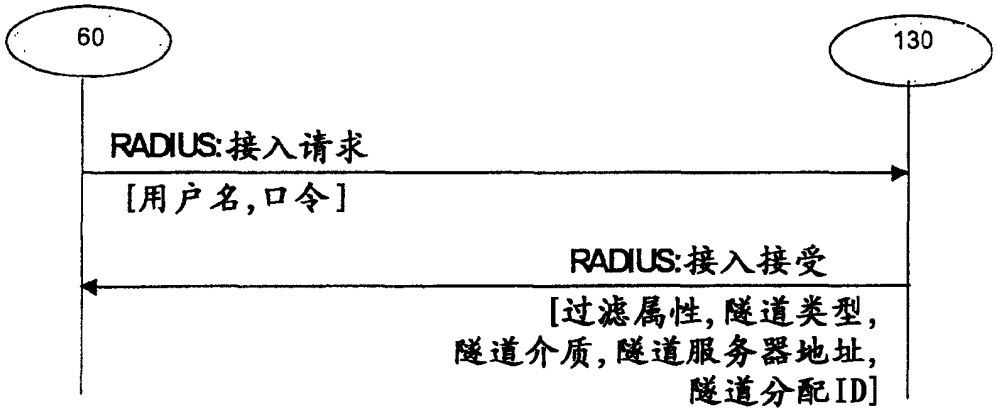

60
130
RADIUS:接入请求
[用户名,口令]
RADIUS:接入接受
[过滤属性,隧道类型,
隧道介质,隧道服务器地址,
隧道分配ID]

图9

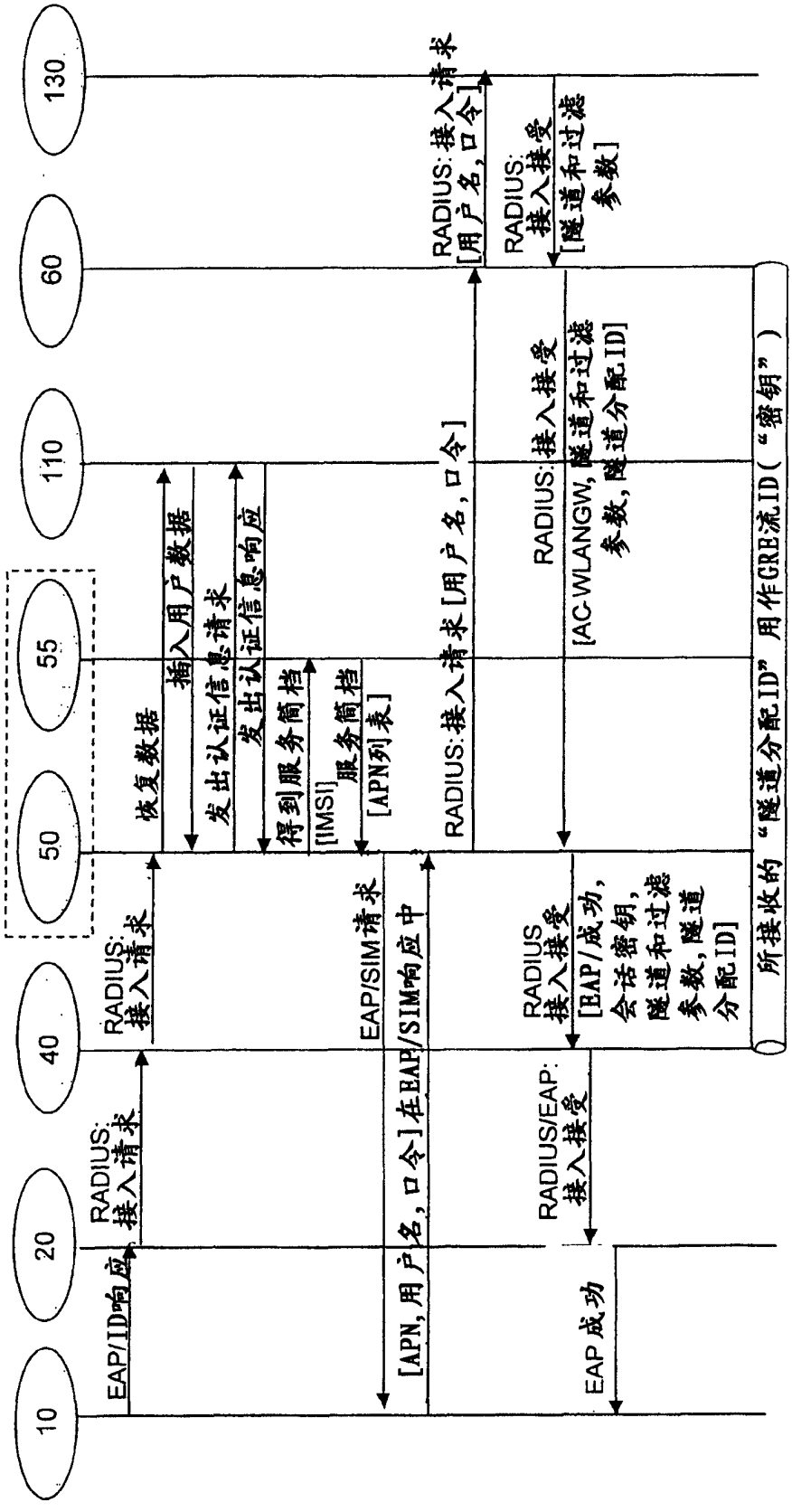

10
20
40
50
55
110
60
130
EAP/ID响应
RADIUS:
接入请求
RADIUS:
接入请求
恢复数据
插入用户数据
发出认证信息请求
发出认证信息响应
得到服务简档
[IMSI]
服务简档
[APN列表]
EAP/SIM请求
[APN,用户名,口令]在EAP/SIM响应中
RADIUS:接入请求[用户名,口令]
RADIUS:
接入请求
[用户名,口令]
RADIUS:
接入接受
[隧道和过滤
参数]
RADIUS:接入接受
[AC-WLANGW,隧道和过滤
参数,隧道分配ID]
RADIUS
接入接受
[EAP/成功,
会话密钥,
隧道和过滤
参数,隧道
分配ID]
RADIUS/EAP:
接入接受
所接收的“隧道分配ID”用作GRE流ID(“密钥”)
EAP 成功

图10