[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/66 (2006.01)
H04L 12/28 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510076484.9

[45] 授权公告日 2008 年 11 月 26 日

[11] 授权公告号 CN 100438516C

[22] 申请日 2005.6.14
[21] 申请号 200510076484.9
[30] 优先权
[32] 2004. 6.15 [33] JP [31] 2004 - 176976
[73] 专利权人 日本电气株式会社
地址 日本东京都
[72] 发明人 藤野庄三
[56] 参考文献
WO01/56251A2 2001.8.2
US6704768B1 2004.3.9
CN1402451A 2003.3.12
CN1398375A 2003.2.19
审查员 冯 楠

[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 朱进桂

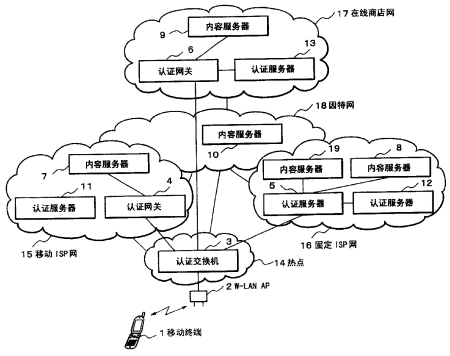
权利要求书 3 页 说明书 14 页 附图 5 页

[54] 发明名称

网络连接系统、网络连接方法、及所使用的交换机

[57] 摘要

无线 LAN 接入点从移动终端接收目的地 URL，并将目的地 URL 提供给认证交换机。 认证交换机连接到与目的地 URL 关联的认证网关，并将目的地 URL 提供给认证网关。 连接到认证交换机的认证网关使与目的地 URL 关联的认证服务器对移动终端(1)进行认证。 认证服务器认证移动终端(1)之后，认证服务器向移动终端(1)提供 IP 地址。 从而使移动终端连接到 URL 指定的内容服务器。



1.一种网络连接系统，包括：

多个内部网，各包含内容服务器，认证服务器，和连接到所述内容服务器和所述认证服务器的认证网关，所述认证服务器认证移动终端，并允许所述移动终端连接内容服务器；和

连接所述移动终端和所述多个内部网中的每一个，并包括无线局域网接入点的热点，所述无线局域网接入点从所述移动终端接收目的地内容服务器信息和认证信息；

其中所述热点还包括：

认证交换机，与由来自所述无线局域网接入点的目的地内容服务器信息识别的内容服务器相关联的认证网关连接，并向由目的地内容服务器信息识别的认证网关发送所述认证信息。

2.根据权利要求1所述的网络连接系统，其中认证交换机包括：

存储器，用于存储与和内容服务器信息关联的内容服务器的所述认证网关进行连接的连接信息；和

连接部分，用于根据目的地服务器信息选择所述连接信息的一部分，并连接所述移动终端和与所选择的连接信息对应的认证网关。

3.根据权利要求2所述的网络连接系统，其中内容服务器信息包括内容服务器的统一资源定位器。

4.根据权利要求2所述的网络连接系统，其中内容服务器信息包括与该内容服务器对应的字符串。

5.根据权利要求1所述的网络连接系统，其中认证网关包括无线局域网接入网关。

6.一种用于网络连接系统的网络连接方法，

所述系统包括：

多个内部网，各包含内容服务器，认证服务器，和连接到所述内容服务器的认证网关；和

连接移动终端和所述多个内部网中的每一个，并包括无线局域网接入

点和认证交换机的热点；

所述网络连接方法包括步骤：

接收步骤，所述无线局域网接入点从所述移动终端接收目的地内容服务器信息和认证信息；

认证网关连接步骤，所述认证交换机向与所述目的地内容服务器信息对应的认证网关发送认证信息；和

在认证服务器认证移动终端之后，认证网关连接所关联的认证服务器和移动终端，并向移动终端提供网际协议地址以允许移动终端连接到内容服务器的步骤。

7. 根据权利要求6所述的网络连接方法，其中：

认证交换机包括存储器，用于存储内容服务器信息的多个部分和与内容服务器信息指定的内容服务器关联的认证网关的多个连接信息；和

所述认证网关连接步骤根据目的地内容服务器信息在所述存储器中选择连接信息，并把所述移动终端连接到由所选择的连接信息识别的认证网关。

8. 根据权利要求7所述的网络连接方法，其中内容服务器信息包括内容服务器的统一资源定位器。

9. 根据权利要求7所述的网络连接方法，其中内容服务器信息包括与该内容服务器对应的字符串。

10. 一种在网络连接系统中包括的热点中使用的认证交换机，所述系统包括：

多个内部网，各包含内容服务器，认证服务器，和连接到内容服务器和认证服务器的认证网关；和

连接移动终端和所述多个内部网中的每一个，并包括无线局域网接入点和认证交换机的热点，

所述认证交换机包括：

存储器，用于存储与内容服务器信息关联的内容服务器相关联的认证网关进行连接的连接信息；和

连接部分，当无线局域网接入点接收到目的地内容服务器信息时，根据目的地内容服务器信息选择存储器中存储的连接信息，并把移动终端连

接到所选择的连接信息指示的认证网关。

11. 根据权利要求10所述的认证交换机，其中内容服务器信息包括内容服务器的统一资源定位器。

12. 根据权利要求10所述的认证交换机，其中内容服务器信息包括与该内容服务器对应的字符串。

网络连接系统、网络连接方法、及所使用的交换机

技术领域

本发明涉及一种网络连接系统，特别是涉及移动终端通过无线接入点连接到需要移动终端的认证的内容服务器的网络连接系统，以及在该系统中所实施的方法。

背景技术

提供热点（hot spot）的服务是已知的。热点通过无线 LAN 接入点把终端设备连接到因特网以便向无数的用户提供服务。近年来，开发了双重终端设备，其中符合个人数字蜂窝（PDC）系统和第三代合作伙伴计划（3GPP）的蜂窝终端设备被装备了无线 LAN 接口（WLAN I/F），提高了将来更广泛地使用热点的期待。

无线局域网（LAN）接入点连接到与热点供应商签有合同的因特网服务供应商（ISP）的内部网。热点供应商也可以作为 ISP 服务。

需要用户终端设备，例如移动终端执行下列过程来通过热点连接到需要在因特网上认证的内容服务器。首先，用户终端设备经过 ISP 认证，以便通过热点连接到因特网（具体地讲，是 ISP 的内部网）。接下来，用户终端设备指定要求认证的内容服务器的统一资源定位器（URL），然后由要求认证的内容服务器进行内容使用认证。例如，在 JP2003-318922A 和 JP2002-152276A 中公开了上述技术。

当用户终端设备通过热点连接到热点供应商（ISP）的内部网时，热点供应商的认证服务器经常使用诸如 L2TP 之类的隧道协议来认证用户终端设备（用户）。

图 7 示出了移动终端 20 通过热点 25 接入也作为 ISP 的热点供应商的内部网 25 的例子。换句话说，图 7 是说明移动终端 20 通过热点 25 连接到因特网的例子的示意图。

在图 7 中，热点 25 具有无线 LAN 接入点 21，并且可以连接到因特网 27。内部网 26 包括可连接到因特网 27 的认证网关 22，需要信用分数等项目的安全内容服务器 23，和认证服务器 24。

下面描述从移动终端 20 通过热点 25 接入到内部网 26。移动终端 20 经无线 LAN 接入点（W-LAN AP）21 和因特网 27 接入认证网关 22。这种情况下，移动终端 20 和认证网关 22 作为虚拟专用网络（VPN）终端。

认证服务器 24 根据诸如 L2TP 之类的隧道协议进行两个隧道端的认证。例如，认证服务器 24 通过从移动终端 20 获得用户 ID 和密码并参考其自身的数据库来认证移动终端 20。当认证服务器 24 已经认证移动终端 20 时，认证服务器 24 向移动终端 20 分配 IP 地址。认证网关 22 向移动终端 20 提供由认证服务器 24 分配的 IP 地址，并把移动终端 20 连接到内部网 26。从认证服务器接收到其自身的 IP 地址的移动终端 20 识别已经允许了其到所需内容服务器的连接。

在连接到内部网 26 的移动终端 20 接入内部网 26 上的内容服务器 23 之前，由内容供应商通过诸如安全套接字协议层（SSL）之类的过程认证移动终端 20。

在大多数情况下，热点服务的收费是固定的（包括免费）。

当用户终端设备（移动终端）尝试通过热点连接到要求认证的内容服务器时，用户首先在热点中执行 ISP 认证过程。另外，用户指定要求认证的内容服务器的 URL，并进行内容服务器的认证。这意味着用户必须执行两个不同的认证过程来通过热点接入内容服务器。这给用户造成了不便。

发明内容

本发明的一个典型的方面是提供一种网络连接系统和网络连接方法，在移动终端通过无线 LAN（热点）连接到需要在因特网上认证的内容服务器时，能够减少所需的认证过程的数量。

根据本发明的一个方面，本发明的网络连接系统，包括：多个内部网，各包含内容服务器，认证服务器，和连接到所述内容服务器和所述认证服务器的认证网关，所述认证服务器认证移动终端，并允许所述移动终端连接内容服务器；和连接所述移动终端和所述多个内部网中的每一个，并包括无线局域网接入点的热点，所述无线局域网接入点从所述移动终端接收目的地内容服务器信息和认证信息；其中所述热点还包括：认证交换机，与由来自所述无线局域网接入点的目的地内容服务器信息识别的内容服务器相关联的认证网关连接，并向由目的地内容服务器信息识别的认证网关发送所述认证信息。

移动终端从无线 LAN 接入点向热点提供信息（内容服务器信息），该信息指定了移动终端要连接的内容服务器。然后，热点的认证交换机把信息传送到与所需的内容服务器关联的认证网关，认证网关请求认证服务器执行移动终端的认证。当认证服务器认证该移动终端时，允许该移动终端连接到内容服务器。

根据这一方面，当移动终端发送内容服务器信息时，根据内容服务器信息选择认证网关，所选择的认证网关把移动终端连接到与内容服务器信

息对应的认证服务器。认证服务器认证该移动终端后，向移动终端提供 IP 地址，并允许其连接到内容服务器。

于是，由与内容服务器关联的认证服务器进行的认证也作为 ISP 认证，使得认证过程的数量减少。

于是，即使在移动终端发送内容服务器信息而没有被 ISP 认证时，移动终端也能够连接到内容服务器。

在上述方面中，认证交换机优选地包括存储器和连接部分。存储器针对内容服务器信息的每个部分存储用于与多个连接侯选（内容服务器）中的每一个关联的认证网关进行连接的信息。当无线接入点接收内容服务器信息时，连接部分选择存储器中存储的、与内容服务器信息关联的连接侯选中的一个。连接部分把移动终端连接到存储器中存储的、与所选择的侯选关联的认证网关。

根据本发明的另一个方面，提供一种用于网络连接系统的网络连接方法，所述系统包括：多个内部网，各包含内容服务器，认证服务器，和连接到所述内容服务器的认证网关；和连接移动终端和所述多个内部网中的每一个，并包括无线局域网接入点和认证交换机的热点；所述网络连接方法包括步骤：接收步骤，所述无线局域网接入点从所述移动终端接收目的地内容服务器信息和认证信息；认证网关连接步骤，所述认证交换机向与所述目的地内容服务器信息对应的认证网关发送认证信息；和在认证服务器认证移动终端之后，认证网关连接所关联的认证服务器和移动终端，并向移动终端提供网际协议地址以允许移动终端连接到内容服务器的步骤。

根据本发明的再一个方面，提供一种在网络连接系统中包括的热点中使用的认证交换机，所述系统包括：多个内部网，各包含内容服务器，认证服务器，和连接到内容服务器和认证服务器的认证网关；和连接移动终端和所述多个内部网中的每一个，并包括无线局域网接入点和认证交换机的热点，所述认证交换机包括：存储器，用于存储与内容服务器信息关联的内容服务器相关联的认证网关进行连接的连接信息；和连接部分，当无线局域网接入点接收到目的地内容服务器信息时，根据目的地内容服务器信息选择存储器中存储的连接信息，并把移动终端连接到所选择的连接信息指示的认证网关。

通过下面结合优选实施例的描述将使本发明的其他实施例变得更加清楚。

附图说明

在附图中，

图 1 是表示根据本发明实施例的网络连接系统的示意图；

图 2 是表示认证交换机 3 的实例的方框图；

图 3 是表示存储器 31 中存储的信息的实例的示意图；

图 4 是由移动终端 1 发送/接收的数据的实例的示意图；

图 5 是说明网络连接系统的操作的顺序流程图；

图 6 是说明与图所示的认证过程不同的认证过程的示意图；和

图 7 是表示常规网络连接系统的示意图。

具体实施方式

下面参考附图描述本发明的优选实施例。

图 1 是表示根据本发明实施例的网络连接系统的示意图。

在图 1 中，网络连接系统包括移动终端 1，热点 14，移动 ISP 网络 15，固定 ISP 网络 16，在线商店网络 17，和连接这些网络的因特网 18。内容服务器 10 连接到因特网 18。

热点 14 包括与移动终端 1 通信的无线 LAN 接入点（W-LAN AP）2 和连接到无线 LAN 接入点 2 的认证交换机（SW）3。热点 14 通过认证交换机连接到因特网 18。

移动 ISP 网络 15 包括连接到因特网 18 的认证网关（GW）4，连接到认证网关 4 的认证服务器 11，和连接到认证网关 4 的内容服务器 7。

固定 ISP 网络 16 包括连接到因特网 18 的认证网关 5，连接到认证网关 5 的认证服务器 12，和连接到认证网关 5 的内容服务器 8 和 19。

在线商店网络（在线 ISP 网络）17 包括连接到因特网 18 的认证网关（GW）6。连接到认证网关 6 的认证服务器 13，和连接到认证网关 6 的内容服务器 9。

A. 实施例的配置

下面详细描述配置部件。

A-1. 移动终端 1

移动终端 1 是移动电话，个人数字助理（PDA）等。例如，移动终端 1 是符合诸如 PDC 或 3GPP 之类的标准并具有用于可连接到因特网的蜂窝通信和 WLAN 通信二者的接口（I/F）的便携式双重终端。移动终端 1 也可以是具有无线 LAN（WLAN）I/F 的笔记本个人计算机（PC）或 PDA。

移动终端 1 包含安装在其中的 VPN（虚拟专用网）客户软件，VPN 客户软件包含可连接的内容服务器的 URL 的列表。可连接的内容服务器是需要认证的服务器。例如，URL 列表包括内容服务器 7，8，9，和 19 的 URL。

移动终端 1 向热点 14 的无线 LAN 接入点 2 发送由用户从 URL 列表选择的目的地 URL。然后，移动终端 1 与认证交换机 3 和认证 GW 4，5，或 6

建立 VPN 对话。

A-2. 无线 LAN 接入点（WLAN AP）2 和热点 14

热点 14 由无线 LAN 供应商运行，并符合诸如 802.11a/b/g 之类的标准，并包括无线 LAN 接入点 2。无线 LAN 接入点 2 与处在热点 14 的覆盖范围内的移动终端 1 进行无线通信。无线 LAN 接入点 2 向认证交换机 3 提供从移动终端 1 发送的内容服务器的 URL（即内容服务器的信息）。

A-3. 认证交换机 3

图 2 是表示认证交换机 3 的例子的方框图。在图 2 中，用相同的参考标号表示与图 1 中描绘的部件相同的那些部件。在图 2 中，认证交换机 3 包括存储器 31 和连接部分 32。

存储器 31 存储内容服务器的 URL 作为与认证网关（GW）的 IP 地址对应的项，所述认证网关与由 URL 指示的内容服务器相关联。换句话说，存储器 31 存储直接连接到相应的内容服务器的认证网关的 IP 地址。认证网关还连接到内容服务器和认证服务器。存储器 31 中存储的内容服务器的 URL 是移动终端 1 可以连接的多个侯选。

图 3 示出了存储器 31 中存储的信息的实例。

如图 3 所示，存储器 31 包含内容服务器作为条目的 URL31a 和认证网关 GW 的 IP 地址 31b，所述认证网关与由 URL 指示的内容服务器相关联。图 3 示出了内容服务器 7 的 URL 是“www.wg1.soshiki.ne.jp”，内容服务器 8 的 URL 是“pc1.sub2.org.ne.jp”，内容服务器 19 的 URL 是“pc3.sub1.org.ne.jp”。图 3 还示出了与内容服务器 8 和 19 关联的认证网关 5 的 IP 地址是“200.0.0.1”，与内容服务器 7 关联的认证网关 4 的 IP 地址是“60.0.0.3”。

当连接部分从无线 LAN 接入点 2 接受内容服务器的 URL 时，连接部分 32 搜索存储器 31 中存储的内容服务器的 URL 31a，以便选择与从无线 LAN 接入点 2 接受的 URL 最接近匹配的内容服务器的 URL。就是说，连接部分 32 选择与接受的 URL 最可能对应的内容服务器的 URL。然后，连接部分 32 连接到具有存储器 31 中存储的、与所选择的 URL 关联的 IP 地址的认证网关。连接部分 32 向连接的认证网关发送从移动终端 1 接收的内容服务器的 URL。

A-4. 认证网关（GW）4，5，和 6

认证网关 4 是认证服务器 11 和内容服务器 7 的代理，并且管理移动终端 1，认证服务器 11 和内容服务器 7 间的连接。认证网关 4 还是用于移动 ISP 网络 15 的代理。移动 ISP 网络 15 是包括认证服务器 11 和内容服务器 7 的内部网。移动 ISP 网络 15 与认证服务器 11 认证的终端连接。

认证网关 5 是认证服务器 12 以及内容服务器 8 和 19 的代理，并且管理移动终端 1，认证服务器 12，以及内容服务器 8 和 19 之间的连接。认证网关 5 还是固定 ISP 网络 16 的代理。固定 ISP 网络 16 是包括认证服务器 12 以及内容服务器 8 和 19 的内部网。固定 ISP 网络 16 与认证服务器 12 认证的终端连接。

认证网关 6 是认证服务器 13 和内容服务器 9 的代理，并且管理移动终端 1，认证服务器 13 和内容服务器 9 之间的连接。认证网关 6 还是在线商店网络 17 的代理。在线商店网络 17 是包括认证服务器 13 以及内容服务器 9 的内部网。在线商店网络 17 仅与认证服务器 13 认证的终端连接。

当与认证交换机 3 连接时，认证网关 4，5，或 6 从移动终端 1 接收 URL，并向移动终端 1 分配认证网关 ID（Auth GW ID）和对话 ID，以便识别用户。Auth GW ID 是目的地认证网关的标识符。对话 ID 是使用认证网关的用户（移动终端 1）的标识符。对话 ID 在认证网关中是独有的。

认证网关 4，5，和 6 还作用用户数据流的网关操作。可以向认证网关提供“Auth GW ID+对话 ID（Session ID）对话标识符”的分组计数器，以允许移动 ISP 网络 15，固定 ISP 网络 16 等根据分组的数量来收费。

A-5. 移动 ISP 网络 15，认证服务器 11，和内容服务器 7

移动 ISP 网络 15 是包括一组服务器的内部网。提供移动电话服务的公司（提供通信服务的公司）已经构成来提供因特网连接和原始内容服务。

认证服务器 11 与内容服务器 7 和尝试连接到内容服务器 7 的认证客户（例如，移动终端 1）相关联。认证服务器 11 不仅可以认证尝试连接到内容服务器的移动终端，而且可以认证尝试连接到移动 ISP 网络 15 的其它设施的客户（例如移动终端）。内容服务器 7 向认证服务器 11 认证的客户（移动终端 1）提供内容。

A-6. 固定 ISP 网络 16，认证服务器 12，和内容服务器 8 和 19

固定 ISP 网络 16 是包括一组服务器的内部网。提供因特网连接服务的供应商已经构成内部网来提供固有的内容服务。认证服务器 12 与内容服务器 8 和 19 相关联。认证服务器 12 认证尝试连接到内容服务器 8 或 19 的客户（例如，移动终端 1）。认证服务器 12 不仅能够认证尝试连接到内容服务器 8 或 19 的客户，而且可以认证尝试连接到固定 ISP 网络 16 中的其它设施的客户。内容服务器 8 和 19 仅向认证服务器 12 认证的客户（移动终端 1）提供内容。

A-7. 在线商店网络 17，认证服务器 13，和内容服务器 9

在线商店网络 17 是包括一组服务器的内部网。提供诸如音乐，视频，游戏等软件文件的在线下载服务的供应商已经构成内部网来提供其固有的内容服务。

认证服务器 13 与内容服务器 9 相关联，并认证尝试连接到内容服务器 9 的客户（例如，移动终端 1）。认证服务器 13 不仅可以认证尝试连接到内容服务器 9 的客户，而且可以认证尝试连接到在线商店网络 17 中的其它设施的客户。内容服务器 9 向认证服务器 13 认证的客户（移动终端 11）提供内容。

A-8. 因特网 18 和内容服务器 10

内容服务器 10 设置在因特网 18 上。

B. 该实施例的操作

首先描述操作的要点。

移动通信用户（移动 ISP 网络 15 的用户，具有数据通信卡的户外网络的用户等）使用移动终端 1 通过热点 14 接入到特定的内部网，或通信网络，或原始供应商的内容的服务器（需要由认证服务器认证）。移动通信用户向移动终端 1 中输入特定内部网的内容服务器的 URL，或管理原始供应商的内容的内容服务器的 URL。

移动终端 1 利用无线电信号向无线 LAN 接入点 2 发送用户选择的内容服务器 URL。无线 LAN 接入点 2 把从移动终端 1 接收到 URL 提供给认证交换机 3。

认证服务器 3 搜索存储器 31 中存储的内容服务器的 URL 31a，以选择

与从无线 LAN 接入点 2 接受的 URL 最接近匹配的内容服务器的 URL。认证交换机连接到由存储器 31 中存储的 IP 地址指定的、与所选择的 URL 相关联的认证网关。认证交换机 3 向连接的认证网关提供从移动终端 1 提供的内容服务器的 URL。

与认证交换机 3 连接的认证网关使与由认证交换机 3 提供的内容服务器的 URL 对应的认证服务器对移动终端 1 进行认证。认证服务器认证移动终端 1 之后，认证网关向移动终端 1 提供移动终端的 IP 地址。于是，移动终端 1 识别已经允许到由 URL 指定的内容服务器的连接。然后，移动终端能够接入内容服务器中的内容。

在本实施例中，由与内容服务器相关联的认证服务器进行的认证也作为 ISP 认证，从而减少了通过无线 LAN 把移动终端 1 连接到需要认证的内容服务器所需的认证过程的数量。

另外，无线 LAN 供应商能够在热点中快速地向移动终端传递本地服务信息等，或能够在紧急设施的热点中快速执行到移动终端的紧急通信。此外，从维护的观点来看，能够快速地向移动终端通知诸如无线 LAN 接入点之类的通信设备的故障。而现有技术只能向已经经过 ISP 认证的移动终端提供这些服务，本实施例没有这些限制。

下面进一步详细地说明该实施例的认证操作。

B-1. 直接接入到 ISP 的认证

通过 VPN 客户软件的操作向对无线 LAN 接入点 2 发送和从无线 LAN 接入点 2 接收的移动终端 1 的控制数据和用户数据提供 VPN 首部。

图 4 是表示控制数据和用户数据（下文中可以将控制数据和用户数据集中称为“发送/接收数据”）的实例的 示意图。在图 4 中，发送/接收数据 100 包括以太网首部 101，因特网 IP 首部 102，UDP 首部 103，VPN 首部 104，VPN IP 首部 105，和数据 106。

VPN 首部 104 包括 KSC 104a，MC 104b，Auth GW ID 104c，和对话 ID 104d。KSC 104a 是一个序号，并且针对每个分组是递增的。KSC 104a 用于防止未经认证的接入用户重放分组。MC 104b 是防止伪造的分组的检验和（检验的总和）。当发送/接收数据 100 是控制数据时，数据 106 包含目的地 URL 信息。

图5是说明该系统的操作的顺序图。下面参考图5描述该系统的操作。在开始图5的步骤之前假设移动终端1已经通过无线LAN接入点2与认证交换机3建立了连接，而没有在热点中的认证过程。还假设移动终端在图5所示的步骤之前已经获得了认证交换机3的媒体接入控制（MAC）地址。

移动终端1的用户从移动终端1中提供的VPN客户软件中的URL列表中选择目的地URL。信息（URL）存储在移动终端1的高速缓存器中。每当移动终端1接入同一个URL时，移动终端被自动连接到同一个认证网关。当用户指示时，移动终端1可以改变连接目标。

当移动终端1在步骤51选择目的地URL时，把携带所选择的目的地URL的认证开始分组发送到无线LAN接入点2。无线LAN接入点2向认证交换机3提供认证开始分组。

在认证交换机3和认证网关4，5，或6根据认证开始分组来传递移动终端1和认证服务器11，12，或13之间的认证过程。

更具体地讲，在步骤S52，认证交换机3的连接部分32把“最长匹配”搜索从认证开始分组上携带的目的地URL中的服务器地址的最低有效位置施加到存储器31中存储的内容服务器的URL。于是，连接部分32从存储器31中存储的内容服务器的URL中选择向最长匹配提供认证开始分组上携带的URL。连接部分32从存储器31读取存储的、与所选择的URL相关联的存储的认证网关的IP地址。

接下来，认证交换机3连接到被分配了所读取的IP地址的认证网关，并把包括URL的认证开始分组传送到连接的认证网关。

在步骤S53，连接到认证交换机3的认证网关向移动终端1分配Auth GW ID和对话ID。所分配的Auth GW ID和对话ID被通过认证交换机3和无线LAN接入点2提供给移动终端1。

接下来，移动终端1把用户ID和密码通过无线LAN接入点2，认证交换机3，和认证网关发送到认证服务器。从而开始认证过程。例如，在步骤S54，移动终端1向认证服务器发送用户ID和密码。

在步骤S55，认证服务器通过参考其自己的数据库来认证移动终端1（用户）并找到被认证的移动终端1的IP地址。

与认证交换机3连接的认证网关向移动终端1提供分配给移动终端1

的 IP 地址。IP 地址的提供使移动终端能够识别已经允许了到所希望的内容服务器的连接。

移动终端 1 和认证服务器之间的认证过程不限于步骤 S54 和 S55 所示，也可以适当地改变。例如，也可以使用图 6 的步骤 S56 至 S61 所示的过程。

接下来，描述图 6 的步骤 S58 至 S61 所示的认证过程。这些步骤在图 5 的步骤 S53 之后执行。当移动终端在步骤 S53 接收到“Auth GW ID 和对话 ID”时（图 5 中的“是”），移动终端 1 在步骤 S56 通过无线 LAN 接入点 2 和认证交换机 3 向认证网关发送用户 ID。认证网关在步骤 S57 产生随机数，并在步骤 S58 把该随机数发送到移动终端 1。

在步骤 S59，移动终端 1 根据从认证网关接受的随机数以及用户 ID 和密码来计算散列值，并将散列值发送到认证网关。在步骤 S60，认证网关把从移动终端 1 发送的散列值和步骤 S57 产生的随机数发送到认证服务器。

在步骤 S61，认证服务器通过参考从移动终端 1 发送的散列值，从认证网关发送的随机数，和其自己的数据库来对移动终端 1（用户）进行认证。认证移动终端 1 后，认证服务器向移动终端 1 分配 IP 地址。认证网关通过认证交换机向移动终端 1 提供分配的 IP 地址。从而由认证服务器认证移动终端 1（移动终端 1 的用户），并允许移动终端 1 连接到由目的地 URL 指定的内容服务器。

例如，当移动终端 1 设定“http://pc3.sub1.org.ne.jp/index.html”（内容服务器 19 的 URL）作为目的地 URL 时，认证交换机 3 执行最长匹配搜索，并与具有 IP 地址“200.0.0.1”的认证网关 5 连接。认证服务器 12 通过认证网关 5 对移动终端 1 进行认证。

当移动终端 1 设定“pc1.sub2.org.ne.jp”作为目的地 URL 时，认证交换机 3 与具有 IP 地址“200.0.0.1”的认证网关 5 连接。

虽然上面的例子给出了当目的地 URL 中的组名是“org”时认证交换机 3 使用认证网关 5 的操作，可以设置认证交换机 3 中的存储器 31 针对象“sub1”和“sub2”这样的不同子地址使用不同的认证网关。

图 5 的序列示出了当移动终端 1 与认证交换机 3 连接时不需要指定的认证过程。利用该特征，无线 LAN 供应商能够从认证交换机 3 向移动终端

1 传递诸如有关热点区 14 中的商店和有关热点 14 的网络中的内容的折扣信息之类的服务信息（本地服务信息）。例如，认证交换机 3 能够在图 5 中表示为“X”和“Y”的阶段中向移动终端 1 传送本地服务信息。

（1）阶段 X

在阶段 X，移动终端 1 了解认证交换机 3 的 MAC 地址，移动终端 1 和认证交换机 3 因此能够进行通信。认证交换机 3 据此能够向处在热点 14 的覆盖区中具有 VPN 客户的所有移动终端传递本地服务信息。

(2)图 5 的阶段 Y

在阶段 Y，移动终端 1 被分配了 Auth GW ID 和对话 ID，认证 交换机 3 因此能够通过指定对话 ID 而仅向特定的移动终端 1 传递信息。

除了本地服务信息外，认证交换机 3 还能够在紧急设施中向热点中的移动终端 1 提供紧急信息，快速地向移动终端 1 通知通信设备的故障。

当移动终端 1 发送用户数据时，认证交换机 3 根据首部的 Auth GW ID+对话 ID 的组合，把用户数据路由到用户数据的首部指示的目的地认证 GW。

由图 4 所示的 VPN 首部在移动终端 1 和认证 GW 之间包封 Auth GW ID 和对话 ID，但在其它部分解包封。

B-1-1. 当移动终端 1 的用户是移动 ISP 用户时

当用户已经与管理移动 ISP 网络 15 的移动 ISP 签定合同时，用户可以通过在移动终端 1 中设定移动 ISP 网络 15 中的内容服务器 7 的 URL 作为目的地 URL 来通过热点 14 使用签定合同的移动 ISP。

移动 ISP 网络 15 中的认证网关 4 允许认证服务器 11 认证的用户（移动终端 1）连接到移动 ISP 网络 15 固有的内容服务器 7，并根据该服务进行固定内容收费。

例如，内容服务器 7 与移动电话服务协作，并提供可在热点 14 中传递的大容量内容。例如，内容服务器 7 的内容可以是大容量移动电话应用，位置服务等。

当认证网关 4 具有内部分组计数器时，可以针对每个用户，根据原始供应商的内容服务器 7 的使用量进行收费。

移动终端 1 还能够通过认证网关 4 接入因特网 18 上的内容 10。对于内容服务器 10 的使用，认证网关 4 依据移动 ISP 的策略来按量收费。

B-1-2. 移动终端 1 的用户是固定 ISP 用户时

现在描述用户已经与管理固定 ISP 网络 16 的固定 ISP 签定合同的情况。通过在移动终端 1 中设定固定 ISP 网络 16 中的内容服务器 8 或 19 的 URL 作为目的地 URL，在使用热点 14 的同时，用户能够使用签定合同的固定 ISP。

固定 ISP 网络 16 中的认证网关 5 允许经认证服务器 12 认证的用户（移动终端 1）连接到固定 ISP 网络 16 固有的内容服务器 8 或 19，认证网关 5 根据提供的服务进行固定内容收费。例如，即使在移动终端 1 处在户外热点 14 的覆盖服务中时，内容服务器 8 和 19 向移动终端 1 的用户提供用户已经为家庭使用而签定合同的服务计划，通信速率服务，IP 电话服务等。当认证网关 5 具有内部分组计数器时，可以针对每个用户，根据原始供应商内容服务器 8 和 19 的使用量进行收费。

移动终端 1 还能够通过认证网关 5 接入因特网 18 上的内容服务器 10。对于内容服务器 10 的使用，认证网关 5 依据固定 ISP 的策略，按使用量进行收费。

B-2. 直接接入在线商店的认证

下面描述没有与任何 ISP 签定合同的用户想把移动终端 1 连接到线商店网络 17 中的内容服务器 9 的情况的实例。用户能够通过在移动终端 1 中把在线商店网络 17 中的内容服务器 9 的 URL 设定为目的地 URL 而将移动终端 1 连接到在线商店网络 17。

这种情况下，认证交换机 3 使用层 2 路径通过因特网 18 与认证网关 6 连接。这种情况下，在与因特网 18 建立连接之后，在已经按常规执行认证过程的同时，由在第一地点的认证服务器 13 直接在在线商店等处进行认证过程。

在线商店网络 17 中的认证网关 6 允许认证服务器 13 已认证的用户（移动终端 1）连接到在线商店网络 17 固有的内容服务器 9，并对固定内容收费。例如，内容服务器 9 提供诸如音乐，视频，游戏等之类的软件文件（内容）。

在认证网关 6 具有内部分组计数器时，可以针对每个用户，根据内容服务器 9 的使用量进行收费。这种情况下，当认证网关 6 根据数据的下载

量设定软件价格时，能够灵活地处理来自各个用户的订单，并自动计算文件价格。例如，自动设定文件价格以使记录时间较长容量较大的视频软件定价较高。

C.实施例的效果描述

在该实施例中，认证交换机 3 把最长匹配搜索从用户指定的 URL 的最低有效位置施加到存储器 31 中存储的服务器地址，从而自动确定与 URL 相关联的目的地认证网关。因此，能够仅通过指定目标服务（目的地 URL）来针对内容直接认证用户，而没有任何其它管理。

无线 LAN 供应商能够迅速地向热点中的用户传递诸如有关热点地区中的商店或热点网络中的内容的折扣信息之类的服务信息（本地服务信息），而不需要认证。无线 LAN 供应商还能够通过指定对话 ID 而仅向特定的用户传递信息。

无线 LAN 供应商还能够在紧急设施中与热点中的移动终端 1 进行紧急通信。从维护的观点来看，无线 LAN 供应商能够迅速向热点中的移动终端 1 通知例如因特网的过载之类的通信设备的故障。

另外，在现有的系统针对因特网的连接和内容的使用需要分开的认证过程时，本实施例的系统仅需要由为内容的使用给出认证的供应商（例如移动 ISP，固定 ISP，或在线商店）执行的单个认证过程。

此外，按常规，通过热点到因特网的连接需要由运行该热点的供应商进行的 ISP 认证。然而，在本实施例中，可以在用户已经与其签定了家庭使用合同的 ISP 的热点中对用户进行认证和收费。

另外，根据本实施例，由于通过认证网关接收所有用户分组，很容易根据分组的数量进行收费。另外，在认证后，能够使用不能通过因特网连接的供应商原始内容，或提供热点固有的大容量数据下载服务。这种情况下，当根据数据下载量设定了软件的价格时，能够计算文件的价格。

下面描述该实施例的改进。

可以用诸如供应商名称之类的字符串替换输入到移动终端 1 的目的地 URL，认证网关的存储器 31 可以存储字符串与认证网关的 IP 地址之间的对应关系。这种情况下，认证网关不执行最长匹配搜索。

当移动终端 1 通过公司的无线 LAN 热点连接到作为该公司的第三代服务的 IMS（IP 多媒体子系统）网络时，其网络配置可以完整地应用到本实施例的网络配置。因此，可以将该实施例的认证网关引入到根据图 6 所示的 3GPP TS23.234 的 3GPP-WLAN 配置中的 WAG（无线 LAN（WLAN）接入网关）。

虽然已经结合特定实施例描述了本发明，但本发明不限于此，对本发明的改进和改变对本领域技术人员来说是显而易见的。

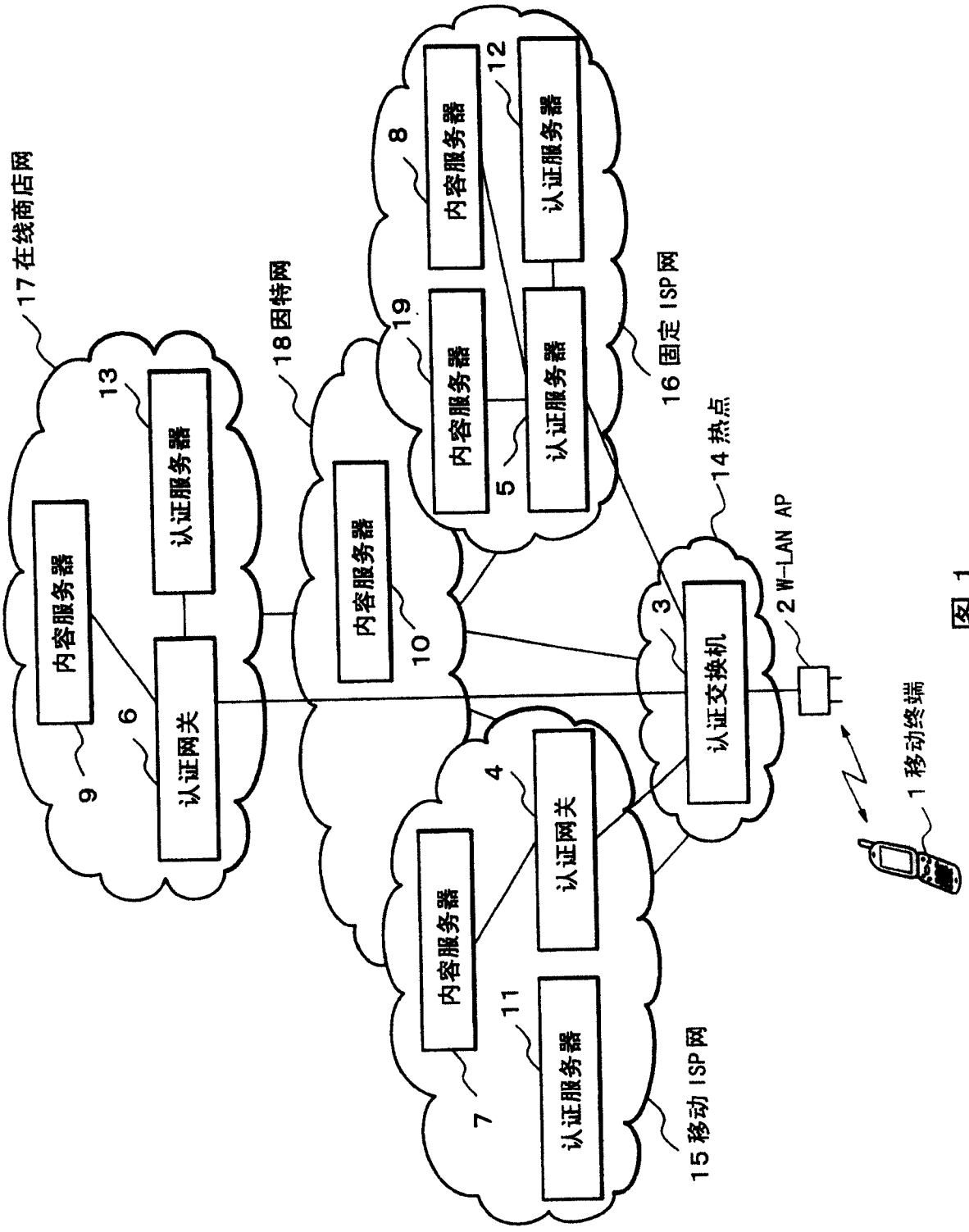

17 在线商店网
内容服务器
9
认证网关
6
认证服务器
13
18 因特网
内容服务器
10
19
内容服务器
5
认证服务器
8
内容服务器
12
认证服务器
16 固定 ISP 网
14 热点
3
认证交换机
2 W-LAN AP
1 移动终端
4
认证网关
内容服务器
7
11
认证服务器
15 移动 ISP 网

图 1

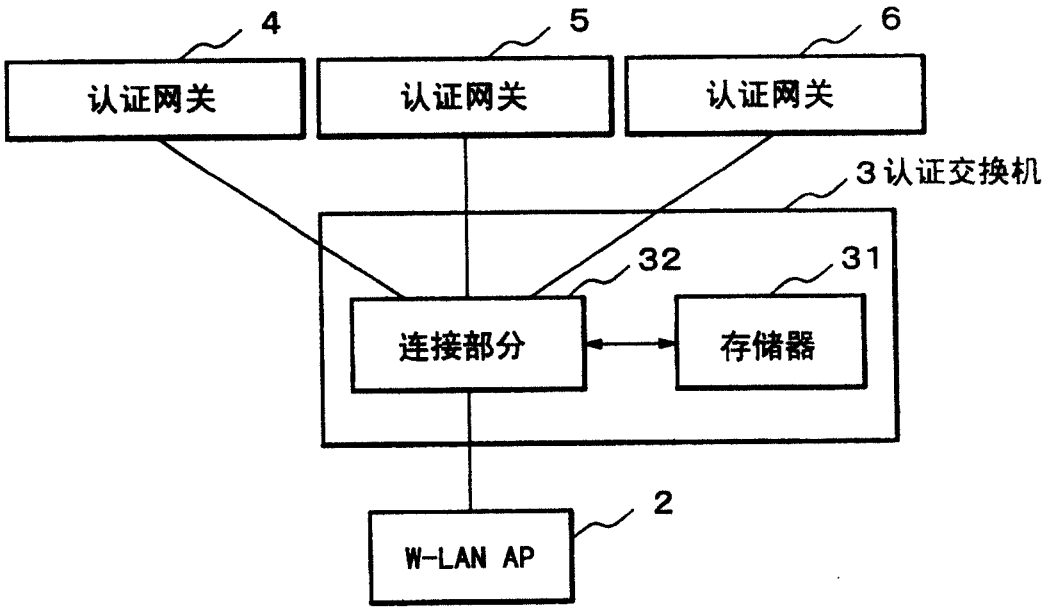

4
5
6
认证网关
认证网关
认证网关
3 认证交换机
32
31
连接部分
存储器
2
W-LAN AP

图 2

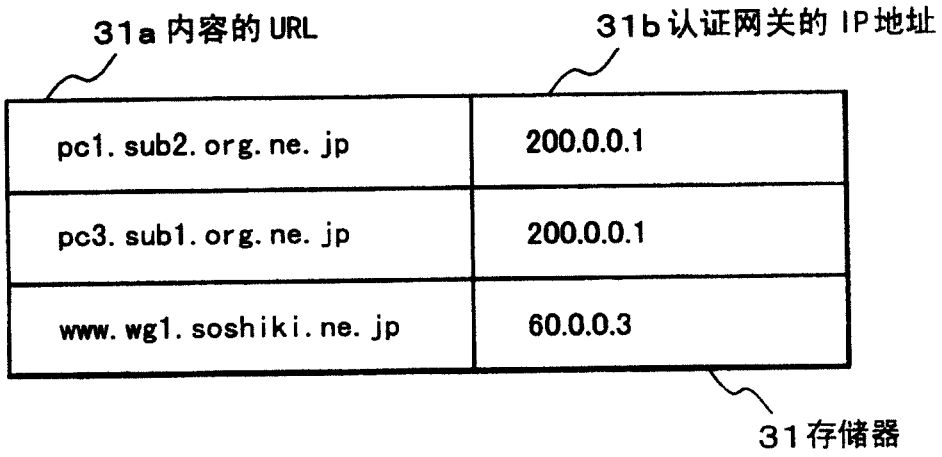

31a 内容的 URL
31b 认证网关的 IP地址
pc1. sub2. org. ne. jp
200.0.0.1
pc3. sub1. org. ne. jp
200.0.0.1
www. wg1. soshiki. ne. jp
60.0.0.3
31 存储器

图 3

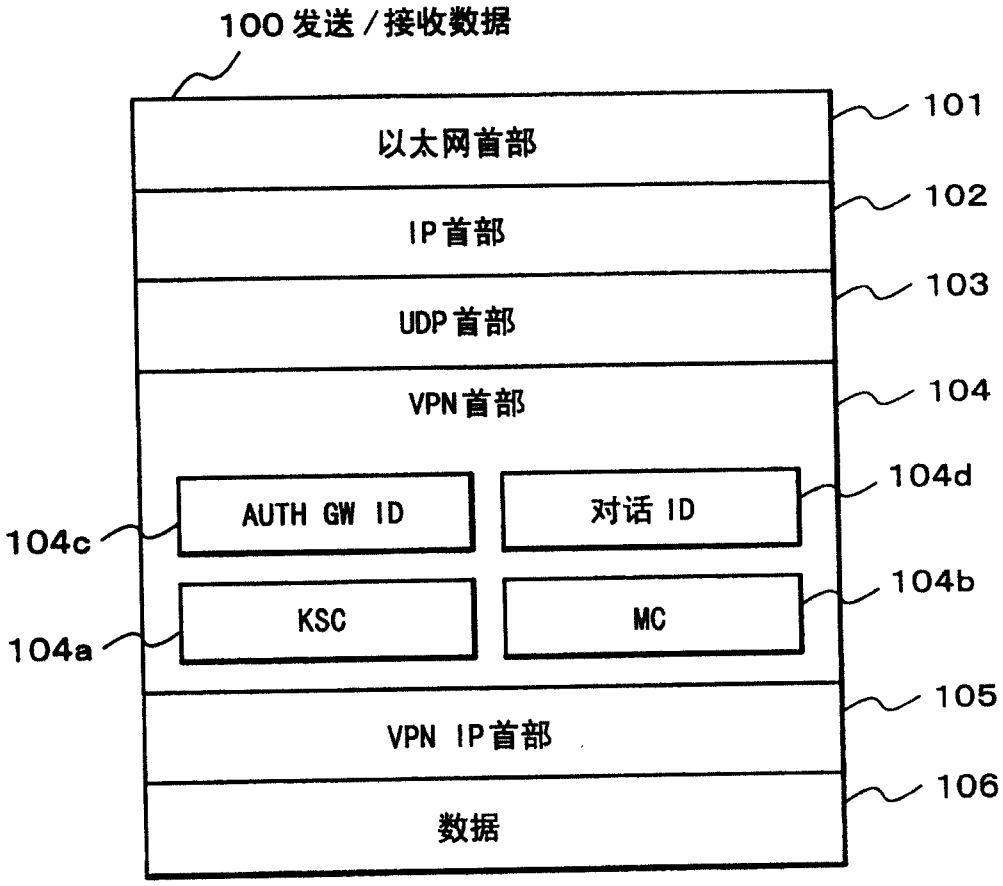

100 发送／接收数据
以太网首部
IP首部
UDP首部
VPN首部
AUTH GW ID
对话 ID
KSC
MC
VPN IP首部
数据
101
102
103
104
104d
104c
104b
104a
105
106

图 4

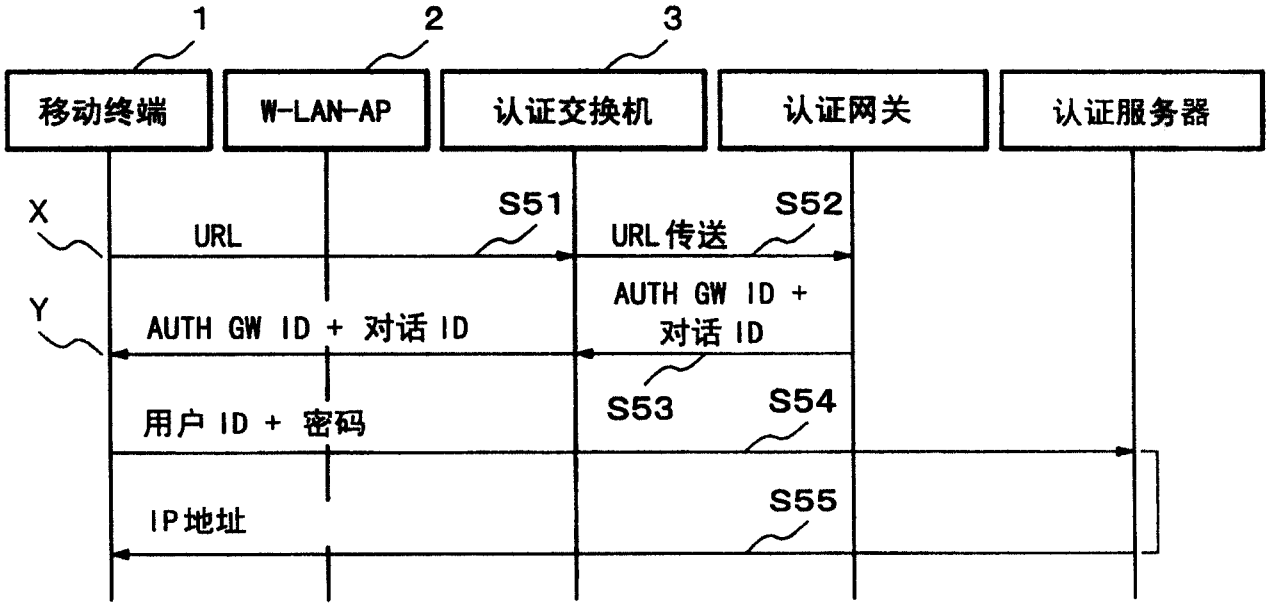

1
2
3
移动终端
W-LAN-AP
认证交换机
认证网关
认证服务器
X
URL
S51
URL传送
S52
Y
AUTH GW ID + 对话 ID
AUTH GW ID + 对话 ID
S53
S54
用户 ID + 密码
IP地址
S55

图 5

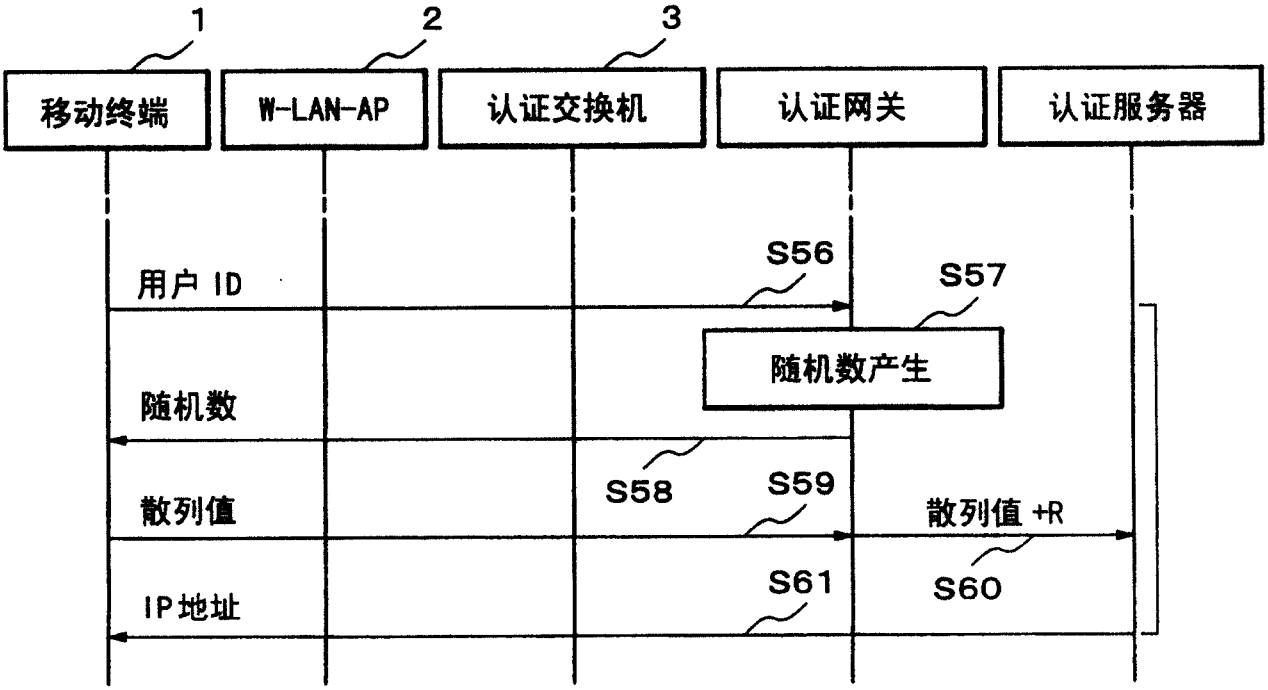

1
2
3
移动终端
W-LAN-AP
认证交换机
认证网关
认证服务器
S56
用户 ID
S57
随机数产生
随机数
S58
S59
散列值
散列值 +R
S60
S61
IP地址

图 6

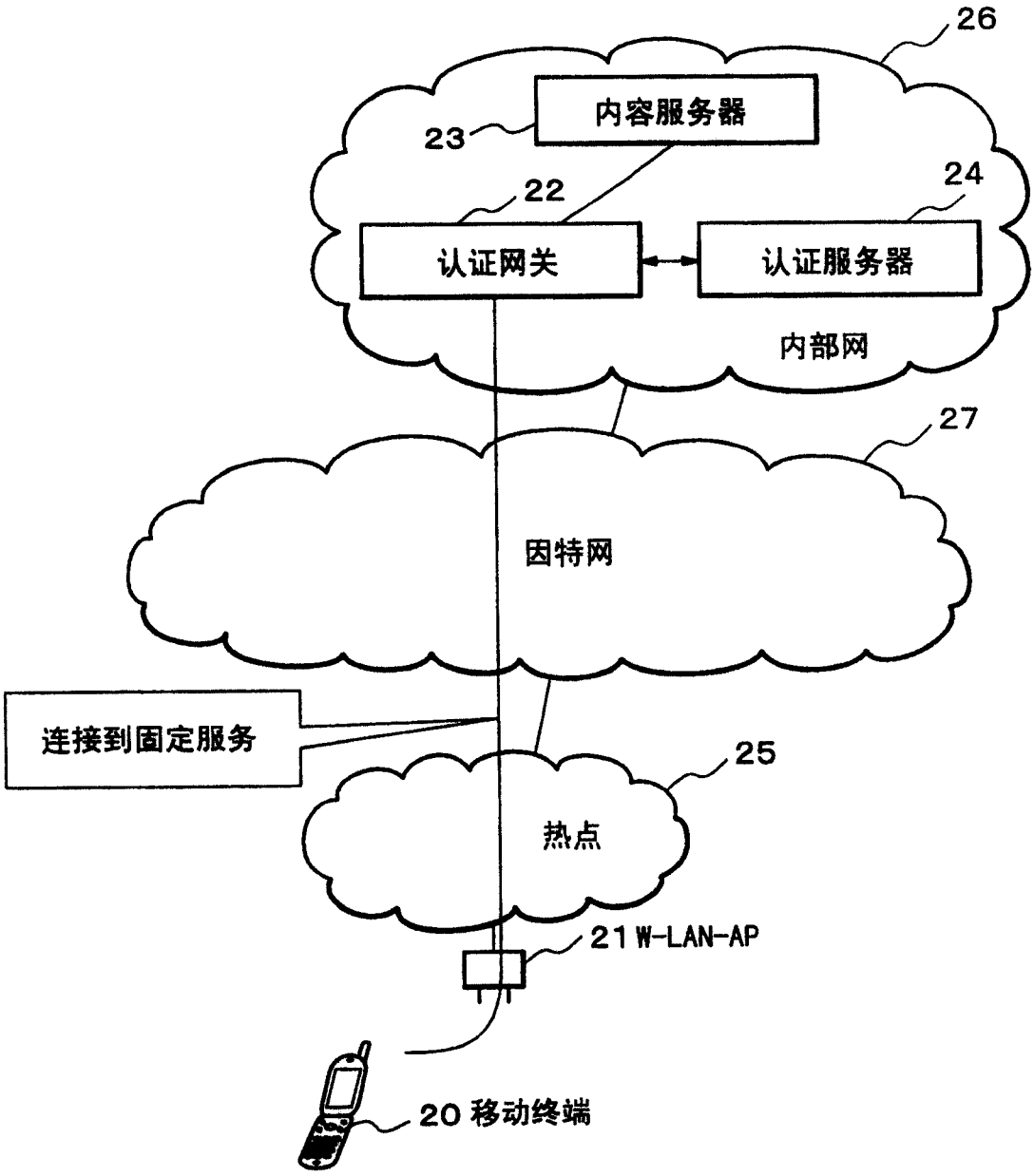

26
内容服务器
23
22
24
认证网关
认证服务器
内部网
27
因特网
连接到固定服务
25
热点
21 W-LAN-AP
20 移动终端

图 7