[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 9/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710001788.8

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101005503A

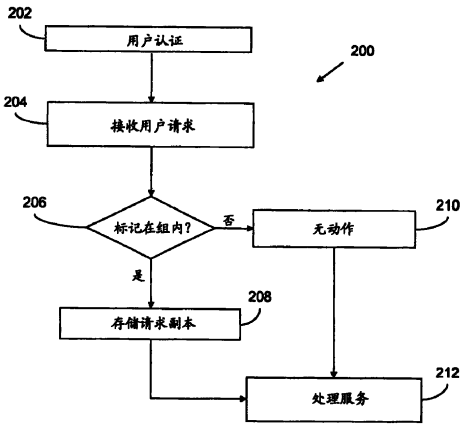
[22] 申请日 2007.1.16
[21] 申请号 200710001788.8
[30] 优先权
[32] 2006. 1.16 [33] EP [31] 06100369.5
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 托马斯·冯库莱萨 斯蒂芬·海因吉里·安德烈斯
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森
权利要求书 4 页 说明书 13 页 附图 7 页

[54] 发明名称

用于侦听客户端和服务之间的通信的方法和数据处理系统

[57] 摘要

提供了一种侦听客户端和服务之间的通信的方法，其中该方法包括执行所述客户端的用户的用户认证的步骤以及由所述服务从所述客户端的用户接收请求的步骤。 所述请求包括用户特有标记，并且该用户特有标记包括唯一的用户标识符。 该用户特有标记由于所述用户认证而能够被分配给所述用户的请求。 如果所述唯一用户标识符等于一组唯一用户标识符的一个用户标识符，则存储所述请求的副本，其中，将所述唯一用户标识符用作密钥。 所述服务发送与所述请求有关的响应，如果所述响应涉及的请求的唯一用户标识符被包括在这组唯一用户标识符中，则存储其副本。



1. 一种侦听客户端(102)和服务(124)之间的通信的方法，所述方法包括:

执行所述客户端(102)的用户(104)的用户认证;

在所述服务(124)处从所述客户端(102)的所述用户(104)接收请求(116)，所述请求(116)包括用户特有标记(118)，所述用户特有标记(118)包括唯一的用户标识符(126)，所述用户特有标记(118)由于所述用户认证而能够被分配给所述用户的所述请求(116);

如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述请求(116)的副本。

2. 如权利要求 1 所述的方法，所述方法还包括:

从所述服务(124)向所述客户端(102)发送响应(128)，所述响应(128)与包括所述用户特有标记(118)的所述请求(116)有关，其中所述用户特有标记(118)包括所述唯一用户标识符(126);

如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述响应(128)的副本。

3. 如权利要求 1 或 2 所述的方法，其中，由认证组件(108)来执行所述用户认证，其中，所述认证组件(108)将所述用户特有标记(118)添加到所述请求(116)中，其中，侦听器插件(112)将所述唯一用户标识符(126)与所述一组唯一用户标识符(122)进行比较，其中，所述侦听器插件(112)被插入代理服务器(110)，所述代理服务器(110)位于所述服务(124)和所述客户端(102)之间，其中，所述侦听器插件(112)包括侦听控制列表(120)，所述侦听控制列表(120)包含所述一组唯一用户标识符(122)，其中，所述侦听器插件(112)链接到侦听管理器(114)，其中，所述请求(116)和所述响应(128)被存储在所述侦听管理器(114)上。

4. 如权利要求 3 所述的方法，其中，所述请求(116)和所述响应(128)被存储在消息队列(402)上，其中，所述消息队列(402)被包括在所述侦听器插件中，或者其中，所述请求(116)和所述响应(128)被存储在所述侦听器插件(112、332)上，由此，所述请求(116)和所述响应(128)通过加密的端到端通信(338)而

被所述消息队列(402)或者从所述侦听器插件(112、332)传递到所述侦听管理器(114、334)。

5. 如权利要求 3 或 4 所述的方法，其中，将所述侦听控制列表(120)永久存储在所述侦听管理器(114、506)上，并且其中，所述方法还包括:

在所述代理服务器(502)的启动之后，将所述侦听器插件(504)加载到所述代理服务器(502)中;

在所述代理服务器(502)的所述启动之后，将所述侦听控制列表从所述侦听管理器(506)加载到所述侦听器插件(504)中。

6. 如权利要求 3、4 或 5 所述的方法，所述方法包括:

利用更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表;

将所述更新的侦听控制列表加载到所述侦听插件中。

7. 如权利要求 2 至 6 中的任一项所述的方法，其中，从所述服务(124)或从所述代理服务器(110)的高速缓冲存储器接收所述响应(128)。

8. 如权利要求 1 至 7 中的任一项所述的方法，其中，以加密的方式将所述请求(116)和所述响应(128)与对应的唯一用户标识符(126)一起存储。

9. 如权利要求 3 至 8 中的任一项所述的方法，其中，在所述侦听插件(332)和所述侦听管理器(334)之间的所述连接(338)是加密的端到端通信。

10. 如权利要求 3 至 9 中的任一项所述的方法，其中，所述认证组件(314)、所述代理服务器(316)、所述侦听器插件(332)、所述侦听管理器(334)以及所述服务(306)是网络宿主环境的组件或服务提供商基础设施(302)的组件。

11. 如权利要求 3 至 10 中的任一项所述的方法，其中，所述侦听管理器和所述侦听器插件采用加密方法来存储所述侦听控制列表。

12. 如权利要求 3 至 11 中的任一项所述的方法，其中，所述侦听管理器(334)通过安全线路(342)链接到执法机构的网络，其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务提供商的所选择的职员访问所述侦听控制列表。

13. 一种计算机程序产品，包括用于执行根据前述权利要求中的任一项的方法的计算机可执行指令。

14. 一种侦听客户端(102)和服务(124)之间的通信的数据处理系统，所述

数据处理系统包括:

用于执行所述客户端(102)的用户(104)的用户认证的部件;

用于在所述服务(124)处从所述客户端(102)的所述用户(104)接收请求(116)的部件，所述请求(116)包括用户特有标记(118)，所述用户特有标记(118)包括唯一的用户标识符(126)，所述用户特有标记(118)由于所述用户认证而能够被分配给所述用户的所述请求(116);

用于如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述请求(116)的副本的部件。

15. 如权利要求 14 所述的数据处理系统，所述数据处理系统还包括:

用于从所述服务(124)向所述客户端(102)发送响应(128)的部件，所述响应(128)与包括所述用户特有标记(118)的所述请求(116)有关，所述用户特有标记(118)包括所述唯一用户标识符(126);

用于如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述响应(128)的副本的部件。

16. 如权利要求 14 或 15 所述的数据处理系统，其中，由认证组件(108)来执行所述用户认证，其中，所述认证组件(108)将所述用户特有标记(118)添加到所述请求(116)中，其中，侦听器插件(112)将所述唯一用户标识符(126)与所述一组唯一用户标识符(122)进行比较，其中，所述侦听器插件(112)被插入代理服务器(110)，所述代理服务器(110)位于所述服务(124)和所述客户端系统(102)之间，其中，所述侦听器插件(112)包括侦听控制列表(120)，所述侦听控制列表(120)包含所述一组唯一用户标识符(122)，其中，所述侦听器插件(112)链接到侦听管理器(114)，其中，所述请求(116)和所述响应(128)被存储在所述侦听管理器(114)上。

17. 如权利要求 16 所述的数据处理系统，其中，所述请求(116)和所述响应(128)被存储在消息队列(402)上，其中，所述消息队列(402)被包括在所述侦听器插件(112、332)中，或者其中，所述请求(116)和所述响应(128)被存储在所述侦听管理器(114、334)上，由此，将所述请求(116)和所述响应(128)通过加密的端到端通信(338)而从所述消息队列(402)传递到所述侦听管理器(114、334)。

18. 如权利要求 16 或 17 所述的数据处理系统，其中，所述侦听管理器(114、506)包括用于存储所述侦听控制列表(120)的部件，并且其中，所述数据处理系统还包括:

用于在所述代理服务器(502)的启动之后将所述侦听器插件(504)加载到所述代理服务器(502)中的部件;

用于在所述代理服务器(502)的所述启动之后将所述侦听控制列表(120)从所述侦听管理器(506)加载到所述侦听器插件(504)中的部件。

19. 如权利要求 16 至 18 中的任一项所述的数据处理系统，所述数据处理系统包括:

用于通过更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表的部件;

用于将所述更新的侦听控制列表加载到所述侦听插件中的部件。

20. 如权利要求 16 至 19 中的任一项所述的数据处理系统，其中，所述侦听管理器包括用于建立到执法机构的网络的安全网络连接的部件，并且其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务提供商的所选择的职员访问所述侦听控制列表。

用于侦听客户端和服务之间的通信的方法和数据处理系统

技术领域

本发明一般地涉及一种用于侦听客户端和服务之间的通信的方法和数据处理系统，并且具体涉及一种用于侦听客户端和服务之间的嫌疑人的通信的方法和数据处理系统。

背景技术

在大多数国家中，法律强制通信或服务提供商使得能够为象特务机关、刑事调查部门以及国家和国际犯罪打击和犯罪防范组织的执法机构侦听顾客的通信。因此，电信服务提供商必须提供电信和IT基础设施，以便使执法部门能够侦听语音和数据流量。基本上，必须确保以下主要原则：

1. 该侦听对于其通信被侦听的人来说必须是不可见的和不可识别的。
2. 该侦听对于服务提供商的职员来说必须是不可见的和不可识别的。
3. 仅仅允许侦听合法确定的嫌疑人的通信。

然而，传统的语音通信基于电路交换网络技术，并且在接入点处，侦听相当容易实现，基于分组交换技术的IP数据流量暴露了关于上述原则的障碍。通常使用的用于侦听数据流量的方法是在特定的侦听点记录若干用户会话的所有IP流量，随后进行过滤器分析，以便重新产生完整的用户会话。三个原因主要地说明这一实践的低效：需要存储、管理和分析巨量数据。此外，记录数据流量不一定记录到所有通信数据，因为分组交换网络可以使用不可预测的路由和节点。侦听不是实时的，并且可能影响法律问题，原因是存储比所需的更多的用户数据。

因此，在互连交换机中，诸如公共交换电话网和公共陆地移动网络的电话网络中进行侦听。所述交换机被互连到与执法机构相连接的传达设备。交换机使用电话号码(ISDN/MSISDN)作为侦听依据。在交换机处侦听对于某个电话号码的呼入或呼出通话。该交换机复制通信内容。除了呼叫者和被叫者之间的传输之外，经由传达设备将数据传递给执法机构。

在基于TCP/IP的网络中，侦听与电话网络非常相似。交换机与连接到执法机构的传达设备相连接。使用IP地址的源地址字段、IP地址的目的地地址字段或者二者取代电话号码作为侦听依据。通常的实践是记录来自或去往给定IP地址的所有连接数据(但不一定是全部内容)。存在若干种类型的信息源，从该信息源中，例如从IP路由器日志文件、从HTTP服务器日志文件、从网络协议分析器或从动态流量过滤，可以提取通信数据记录。

已经知道一些专利，其描述用于合法侦听分组无线网络的侦听方法和系统。那些仅适用于网络运营商，原因是他们需要与其核心网络的交换基础设施进行深入交互。最接近的5个专利列出如下:

美国专利申请US220/0049913A1和US220/0051457A1——侦听系统和方法——涉及一种用于在诸如通用分组无线服务(GPRS)或通用移动通信系统(UMTS)的分组网络中进行合法侦听的侦听系统和方法。

名称为侦听方法和系统的美国专利申请US2002/0078384A1涉及一种侦听方法和系统，用于在诸如通用分组无线服务(GPRS)或通用移动通信系统(UMTS)的分组网络中进行合法侦听的侦听系统和方法。

美国专利申请US2002/0068582A1——用于向执法机构报告信息的方法、系统和传达设备——涉及蜂窝对电信网络用户通信的监控，并且特别涉及一种用于向执法机构报告所监控的信息的方法、系统和传达设备。

在名称为——用于使用基于实时内容的网络监控来检测和报告在线活动的系统和方法的美国专利申请2002/0128925中描述了关于监控的更普通的方法。其一般地涉及通过诸如因特网、万维网或公司局域网(LAN)的公共或专用网络报告在线活动的系统。该专利仅适用于基于URL的过滤，并且不进行整个用户会话。它明确排除了对诸如图像的特定内容类型的侦听，因此不适用于合法侦听。

基于IP的侦听使用定义的IP地址来侦听来自或去往特定IP地址的通信。然而，如果用户不具有诸如由例如因特网接入提供商的第三方提供的动态分配的IP地址的公知/固定IP地址，则基于IP地址的侦听并不够。要利用这样的IP地址侦听的用户建立的应用程序会话将不会被记录到。基于IP的侦听可以记录特定应用程序或整个基础设施的所有通信。然而，对于大量应用程序/网站来说，将记录的数据量是巨大的。这些数据的管理和处理需要大量的努力和例如以大量数据存储设备形式的资源。由于在此情况中将侦听所有应

用程序会话，因此隐私问题确实存在，并且法律方面确实适用。为了从所记录的数据中获得所感兴趣的应用程序会话的内容，必须进行过滤。由于这涉及大量数据，因此所述过滤是耗时和耗费资源的。

此外，可以使用传输层安全协议(TLS)或安全套接字层(SSL)来加密通过IP地址侦听所记录的数据。对诸如HTTP网络服务器日志或应用程序日志的标准应用程序和基础设施日志的分析不包含通信的全部内容。为了获得全部应用程序会话内容，需要修改应用程序以实现所需的日志记录。

因此，确实存在对于用于侦听数据流量的改进的方法和数据处理系统的需要。

发明内容

根据本发明的实施例，提供了一种侦听客户端和服务之间的通信的方法，其中，该方法包括执行所述客户端的用户的用户认证的步骤，以及由所述服务从所述客户端的用户接收请求的步骤。所述请求包括用户特有标记(token)，并且该用户特有标记包括唯一的用户标识符。由于所述用户认证，可以将该用户特有标识符分配给用户的请求。如果该唯一用户标识符与一组唯一用户标识符中的一个用户标识符相等，则存储该请求的副本，其中，将该唯一用户标识符用作密钥。

将用户特有标记添加到从客户端发送给服务的所有请求。用户特有标记包括唯一的用户标识符。通过使用该用户特有标记，可以识别该用户。检查所述唯一的用户标识符是否等于包括在一组唯一用户标识符中的一个用户标识符。如果是这种情况，则记录请求的副本，从而将用户标识符用作密钥以便识别该用户。因此，通过将包括在标记中的用户标识符和一组唯一用户标识符进行比较来窃听客户端和服务之间的通信。在这组唯一用户标识符中，包含可疑的并且将被窃听的所有用户的用户标识符。

根据本发明的实施例，所述方法还包括将来自服务的响应发送给客户端的步骤，其中，所述响应与包括用户特有标记的请求有关，所述用户特有标记包括唯一的用户标识符。如果该唯一用户标识符等于一组唯一用户标识符中的一个用户标识符，则在所述方法的另一步骤中，将所述响应的副本与作为密钥的唯一用户标识符一起存储。

因此，不仅仅侦听从客户端发送到服务的请求。从服务发送给客户端的

响应也被侦听。如果响应与包括标记的请求有关、其中所述标记具有也包括在该组唯一用户标识符中的唯一用户标识符，则存储该响应的副本。

当仅仅对于在该组唯一用户标识符中存储了其用户标识符的用户的请求和响应进行侦听时，所述方法尤其有利。所有其它用户不受根据本发明的方法影响。因此，根据本发明的方法满足仅仅允许侦听合法确定的人的通信的法律要求。此外，被侦听的人不会觉察到他或她已经被侦听。

根据本发明的实施例，通过认证组件来执行用户认证，其中，认证组件将用户特有标记添加到所述请求中，其中，侦听器插件将唯一的用户标识符与一组唯一用户标识符进行比较，其中，该侦听器插件被插入代理服务器，其中，该代理服务器位于服务和客户端之间，其中，侦听器插件包括侦听控制列表，其中，侦听控制列表包含该组唯一用户标识符，其中，侦听器插件连接到侦听管理器，其中，将所述请求和响应存储在侦听管理器上。

典型为服务提供商的基础设施的第一组件并且从客户端接收消息的认证组件对用户进行认证，并且将用户特有标记添加到所述请求中。如上所述，用户特有标记包括唯一的用户标识符。所述请求还被传递给位于服务和客户端之间的代理服务器。侦听器插件被插入包括侦听控制列表的代理服务器。侦听控制列表保存该组唯一用户标识符。针对该组唯一用户标识符检查被包括在消息的标记中的用户标识符。如果唯一用户标识符被包括在该组唯一用户标识符中，则将响应副本存储在侦听管理器上。因为可以简单地将侦听器插件插入代理服务器，所以使用侦听器插件识别是否从应该被侦听的用户发送请求特别有利。然而，这要求服务提供商的基础设施包括代理服务器。还有可能在另一组件中使用侦听器插件。例如，可以将侦听器插件集成到认证组件中，此外，使用容留该侦听器插件的分离组件也是可行的。然后，将把这一组件布置在认证组件和服务之间。

根据本发明的实施例，将所述请求和响应存储在消息队列中，其中，在侦听器插件中比较该消息队列，或者其中，将所述请求和响应存储在侦听器插件中，由此通过加密的端到端通信将所述请求和响应从消息队列或从侦听器插件传递到侦听管理器。

根据本发明的实施例，将侦听控制列表永久存储在侦听管理器上，并且在代理服务器启动之后将侦听器插件加载到代理服务器中，并且在该代理服务器启动之后，将侦听控制列表从侦听管理器加载到侦听器插件中。

根据本发明的实施例，利用被加载到侦听器插件中的更新的侦听控制列表来更新侦听控制列表，从而刷新所存储的侦听控制列表。

根据本发明的实施例，从服务或从代理服务器的高速缓冲存储器接收所述响应。

根据本发明的实施例，以加密的方式将所述请求和响应与对应的唯一用户标识符一起存储。这确保了将不会向未被授权访问被侦听的响应和请求的任何人授予访问权。

根据本发明的实施例，侦听器插件和侦听管理器之间的连接是加密的端到端通信。当将被侦听的响应和请求从侦听插件传递到侦听管理器时，这阻止未被授权访问被侦听的请求和响应的任何人。

根据本发明的实施例，认证组件、代理服务器、侦听器插件、侦听管理器和服务本身是网络宿主环境的组件或服务提供商的基础设施的组件。例如但不唯一的是，所述服务与提供服务的服务器或者设备盒有关。

根据本发明的实施例，侦听管理器和侦听器插件采用加密方法来存储侦听控制列表。以加密的方式存储被侦听的请求和响应以及侦听控制列表的优点在于防止未被授权访问这些敏感数据中的任一个的任何人这么做。当法律要求未被授权的任何人都不能访问这些敏感数据中的任一个时，这特别有利。因此，根据本发明的方法满足法律所要求的必要条件。

根据本发明的实施例，侦听管理器通过安全线路连接到执法机构的网络，其中，仅仅执法机构的职员被特许访问存储在侦听管理器上的侦听控制列表以及被侦听的响应和请求，并且其中，仅仅准许服务提供商的被选中的职员访问侦听控制列表。

在另一方面，本发明涉及一种计算机程序产品，其包括用于执行根据本发明的方法的计算机可执行指令。

在另一方面，本发明涉及一种侦听客户端和服务之间的通信的数据处理系统，其中，所述数据处理系统包括用于执行客户端的用户的用户认证的部件和用于在服务处从客户端的用户接收请求的部件，其中，所述请求包括用户特有标记，其中该用户特有标记包括唯一的用户标识符，其中，由于所述用户认证，可以将该用户特有标记分配给该用户。该数据处理系统还包括用于如果所述唯一的用户标识符与一组唯一用户标识符中的一个用户标识符相等则使用所述唯一的用户标识符作为密钥来存储所述请求和相关响应的副

本。

附图说明

下面，将仅仅参考附图、作为示例来更详细地描述本发明的优选实施例，在附图中：

图 1 示出了连接到被适配为侦听通信的服务提供商的基础设施的客户端系统的方框图，

图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图，

图 3 在方框图中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端和服务之间的数据流量，

图 4 示出了侦听设施的可扩充(scalable)设置的方框图，

图 5 是示出在侦听器插件启动期间由各个组件处理的步骤的顺序图，

图 6 是图示当侦听通信时各个组件的交互的顺序图，以及

图 7 示出了图示当更新侦听控制列表时执行的步骤的顺序图。

具体实施方式

图 1 示出了连接到被适配为侦听通信的服务提供商 106 的基础设施的客户端系统 102 的方框图 100。服务提供商基础设施 106 包括认证组件 108、代理服务器 110、侦听管理器 114 和服务 124。用户 104 登录到客户端系统 102 中。客户端系统 102 例如是诸如 PC、移动电话或 PDA 的、运行浏览器应用程序的设备，其连接到服务提供商基础设施 106。服务提供商知晓用户 104，因此服务提供商准许用户 104 访问服务提供商基础设施 106。

认证组件 108 从客户端 102 接收请求 116。在那里，将带有用户标识符 126 的标记 118 添加到请求 116 中。可以通过用户标识符 126 来识别用户 104。请求 116 被发送给服务 124。代理服务器 110 位于认证组件 108 和服务 124 之间，使得请求 116 在它到达服务 124 之间通过代理服务器 110。代理服务器 110 包括侦听器插件 112。在此示例中，侦听器插件 112 是被插入代理服务器 110 中的插件。侦听器插件 112 保存列出一组用户标识符 122 的侦听控制列表(ICL)120。侦听器插件 112 从请求 116 读取用户标识符 126。如果用户标识符 126 被包括在侦听控制列表 120 中，则将请求 116 的副本与用户标识符 126 一起发送到侦听管理器 114，在那里，将请求 116 的副本与用户标识符 126

一起存储。

服务 124 接收请求 116。服务 124 将响应 128 发送回客户端。当响应 128 通过代理服务器 110 时，侦听器插件 112 检查该响应是否与被侦听的请求有关。如果是这样，则将响应 128 的副本与用户标识符 126 一起存储在侦听管理器 114 中。响应 128 被进一步发送给客户端系统 102，使得用户最终接收到根据其请求 116 的响应 128。由此，用户不知道他可能已被侦听。

图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图 200。在步骤 202 中，执行客户端系统的用户的用户认证。在步骤 204 中，在侦听器插件处从客户端的用户接收请求，其中，该请求包括含有唯一用户标识符的用户特定标记，其中，由于所述用户认证，可以将用户特有标记分配给该用户的请求。在步骤 206 中，检查该唯一用户标识符是否被包括在一组唯一用户标识符中。如果是这种情况，则根据本发明的方法继续进行步骤 208，其中，存储所述请求的副本。否则，根据本发明的方法继续进行步骤 210，其中，不进一步考虑动作。在步骤 208 或 210 的处理之后，在步骤 212 中，将所述请求传递到所述服务，在那里它被处理。

图 3 在方框图 300 中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端 312 和服务提供商基础设施 302 之间的数据流量。概念服务提供商基础设施是非常笼统的术语，并且它应当被理解为：在此文档的语境中，它指的是在最广泛的意义上向用户提供通信服务的服务提供商的基础设施。如先前所述，服务提供商只需要通过使用认证组件来识别该用户的方式。下面，将专注于与通信服务提供商所提供的基础设施不同的服务提供商的基础设施。通常，通信服务提供商通过使用分配给客户端的动态 IP 地址来授权用户的访问，并且允许到 IP 网络的通信。另一方面，服务提供商具有固定 IP 地址以及被用来获得服务的公知域名，所述服务例如可以是在线银行服务或者在更广的意义上为相同 IP 网络上的网络服务。

客户端 312 可以是具有浏览器应用程序的设备，所述设备经由网络 310 连接到也被称为服务提供商所在地(premise)的服务提供商基础设施 302。客户端 312 也可以是使用包括语音浏览器(例如 VoiceXML 浏览器)的交互式语音响应(IVR)系统的电话，其中，通过服务提供商基础设施 302 通过网络 310 向其提供服务。语音浏览器应用网络技术，以便使用户能够经由言语和双音多频(DTMF)的组合而从电话访问服务。

网络 310 可以是由通信服务提供商提供的所有类型访问信道的代表实体。如上所述，服务提供商和通信服务提供商通常不是相同的。这意味着服务提供商不知道除了客户端的 IP 地址以外的用户细节。服务提供商不能在没有通信服务提供商的帮助的情况下识别或认证用户。由于这一事实，诸如在线银行的由服务提供商所提供的大多数网络应用要求用户在访问所述服务时认证他们自己。

服务提供商基础设施302通常由3个组件组成，它们是HTTP服务器304、应用程序服务器 306 和目录服务 308。此外，服务提供商基础设施通常包括所谓的边缘组件 313，其包括认证组件 314 和代理服务器 316。

客户端 312 经由连接 318 和 320，通过网络 310 而连接到服务提供商基础设施 302。在认证组件 314 处接收来自客户端 312 的请求。认证组件 314 经由连接 330，针对目录服务 308 验证证书。认证组件 314 仅仅将可被证实的请求经由连接 322、324 和 326 转发到代理服务器 316、HTTP 服务器 304 或应用程序服务器 306。

认证组件 314 还将用户特有标记添加到请求中。该用户特有标记包括可用以唯一地识别用户的唯一的用户标识符。

将所述请求继续传递到代理服务器 316。代理服务器 316 包括侦听器插件 332，其分析所述标记，并且针对在侦听控制列表中列出的一组用户标识符来检查用户标识符。如果在侦听控制列表中列出了所述用户标识符，则将该请求的副本存储在例如侦听器插件的高速缓冲存储器中。

所述请求被进一步传递给 HTTP 服务器 304 和应用程序服务器 306，由此，将与目录服务 308 的连接 328 用于授权的目的和用户细节。从应用程序服务器 326 产生响应，所述响应随后经由 HTTP 服务器 304 和边缘组件 313 而被发送回客户端系统 312。如果以前请求过所述请求，那么也可以直接由代理服务器 316 部分或全部地产生所述请求。

代理服务器 316 的侦听器插件 332 还分析所述响应是否与带有标记的用户标识符的请求有关，其中所述用户标识符也被包括在侦听控制列表中列出的一组用户标识符中。如果在侦听控制列表中列出了所述用户标识符，则将所述响应的副本存储在例如侦听器插件的存储器中。

通常，以加密的方式将被侦听的请求和响应存储在侦听器插件的存储器中，使得服务提供商的未被授权的服务职员不能访问所述请求和响应。此外，

出于相同的原因，以加密的方式存储该侦听控制列表。

侦听管理器 334 经由连接 338 连接到代理服务器 316，并且可以直接与侦听器插件 332 通信。可以使用连接 338 来在侦听器插件 332 和侦听管理器 334 之间建立加密的端到端通信。例如，可以周期性地建立连接 338，然后，可以将存储在侦听器插件 332 的存储器中的请求和响应从侦听器插件 332 传递到侦听管理器 334。

或者，可以永久地建立连接 338，并且可以将被侦听的响应和请求从侦听器插件 332 直接传送到侦听管理器 334，在侦听管理器 334 中，它们将以加密的方式而被永久存储。侦听控制列表也以加密的方式被存储在那里。

此外，在侦听器插件和侦听管理器组件之间可以使用消息队列，以便提高可用性和适用性。在这么做的时候，实现了侦听器插件 332 和侦听管理器 334 之间的有保证的传送，并且在服务中断的情况下避免了数据丢失。

侦听管理器 334 经由连接 342 与网络 340 通信。连接 342 最好也是永久或临时建立的加密的端到端连接。网络 340 由执法机构控制。可以将被侦听地响应和请求从侦听管理器传递到网络 340，以便由执法机构的授权职员作进一步分析。

如之前已经提到的那样，将用户特有标记添加到从客户端接收的所有请求中，在该客户端上该用户特定标记所涉及的用户访问服务提供商所在地。利用被包括在该侦听控制列表中的用户标识符来检查该用户特有标记。服务提供商知道该用户标识符。因此，执法机构必须向帮助建立侦听控制列表的服务提供商的职员中的几个人授权，因为这些人必须提供用户特有标识符。

图 4 示出了侦听设施的可扩充设置的方框图 400。该设置基本上与如图 3 所述的相同，并且根据本发明的用于侦听用户请求和响应的方法也是相同的。将水平扩充(scaling)技术应用于认证组件 314、代理服务器 316 和对应的侦听器插件 332。消息队列 402 被置于侦听器插件 332 和侦听管理器 334 之间。在侦听器插件 332 和侦听管理器组件 334 之间使用消息队列 402，以便如上所述提高可用性和适用性。

图 5 是示出在侦听器插件 504 启动期间由各个组件(即代理服务器 502、侦听器插件 504 和侦听管理器 506)处理的步骤的顺序图 500。在步骤 508 中，启动代理服务器 502。侦听器插件 504 被加载到代理服务器中。它被插入代理服务器 502。在步骤 510 中，侦听器插件将它自己初始化。它从侦听管理

器 506 请求侦听控制列表，所述侦听控制列表被加载到侦听器插件 504 的存储器中。侦听器插件 504 将“准备工作”信号发送回代理服务器 502。在步骤 512 中，完成代理服务器 502 的启动，并且该代理服务器将其状态设置为“准备工作”。

图 6 是图示当侦听嫌疑用户的通信时各个组件(即客户端系统 602、认证组件 604、代理服务器 606、服务 608、侦听器插件 610、侦听管理器 612 和执法机构(LEA)614)的交互的顺序图 600。

在步骤 630 中，客户端 602 将请求发送给认证组件 604。认证组件 604 在步骤 616 中对用户进行认证，将带有用户标识符的用户特有标记添加到该请求中，并且在步骤 632 中将该请求发送给代理服务器 606。在步骤 634 中，调用侦听器插件 610。针对侦听控制列表检查用户标识符，并且如果它被保存在侦听控制列表中，则在步骤 618 中侦听该请求。在步骤 636 中，将该请求的副本发送到侦听器管理器 612，所述侦听器管理器 612 在步骤 620 中存储该请求。在步骤 638 中，它被进一步发送给执法机构 614，或者更准确地说，它被进一步发送给该机构的网络。在步骤 640 中，代理服务器 606 还将所述请求转发给服务 608，在那里，在步骤 622 中，执行该服务自身。在步骤 642 中，将与所述请求有关的响应发送回代理服务器 606。该代理服务器在步骤 644 中调用侦听器插件。在步骤 624 中，如果所述响应与被侦听的请求有关，那么它也被侦听。所述响应的副本被发送给侦听管理器 612，在那里，在步骤 628 中将其存储。在步骤 648 中，它被进一步发送给执法机构 614。代理服务器 606 还在步骤 650 中将所述响应转发到认证组件 604，在步骤 652 中，将所述响应发送给客户端。用户在不知道他可能已经被侦听的情况下接收到该响应。

图 7 示出了图示被执行以便更新侦听控制列表(ICL)的步骤的顺序图 700。在步骤 710 中，授权的管理员 702 维护和更新存储在侦听管理器 704 上的侦听控制列表(ICL)。在步骤 712 中，分发更新的侦听控制列表。在步骤 718 中将该侦听控制列表发送到侦听器插件 706。在步骤 714 中，更新的侦听控制列表刷新所存储的侦听控制列表。在步骤 720 中，将向侦听管理器 704 通知已经成功地进行了该更新的消息从侦听器插件 706 发送到侦听管理器 704。在步骤 716 中，将更新信息发送给执法机构(LEA)708。在步骤 722 中，向 LEA 708 通知允许对侦听控制列表(ICL)的改变。

参考标号列表

100	方框图
102	客户端系统
104	用户
106	服务提供商基础设施
108	认证组件
110	代理服务器
112	侦听器插件
114	侦听管理器
116	请求
118	标记
120	侦听控制列表
122	一组用户标识符
124	服务
126	用户标识符
128	响应
200	流程图
202	用户认证
204	在侦听器插件处接收用户的请求
206	检查是否设置了标记
208	存储请求的副本
210	无动作
212	处理服务
300	方框图
302	服务提供商基础设施
304	HTTP 服务器
306	应用程序服务器
308	目录服务
310	网络
312	客户端

313	边缘组件
314	认证组件
316	代理服务器
318	连接
320	连接
322	连接
324	连接
326	连接
328	连接
330	连接
332	侦听器插件
334	侦听管理器
336	连接
338	连接
340	网络
342	连接
400	方框图
402	消息队列
500	顺序图
502	代理服务器
504	侦听器插件
506	侦听管理器
600	顺序图
602	客户端系统
604	认证组件
606	代理服务器
608	服务
610	侦听器插件
612	侦听管理器
614	执法机构

700	顺序图
702	管理员
704	侦听管理器
706	侦听器插件
708	执法机构

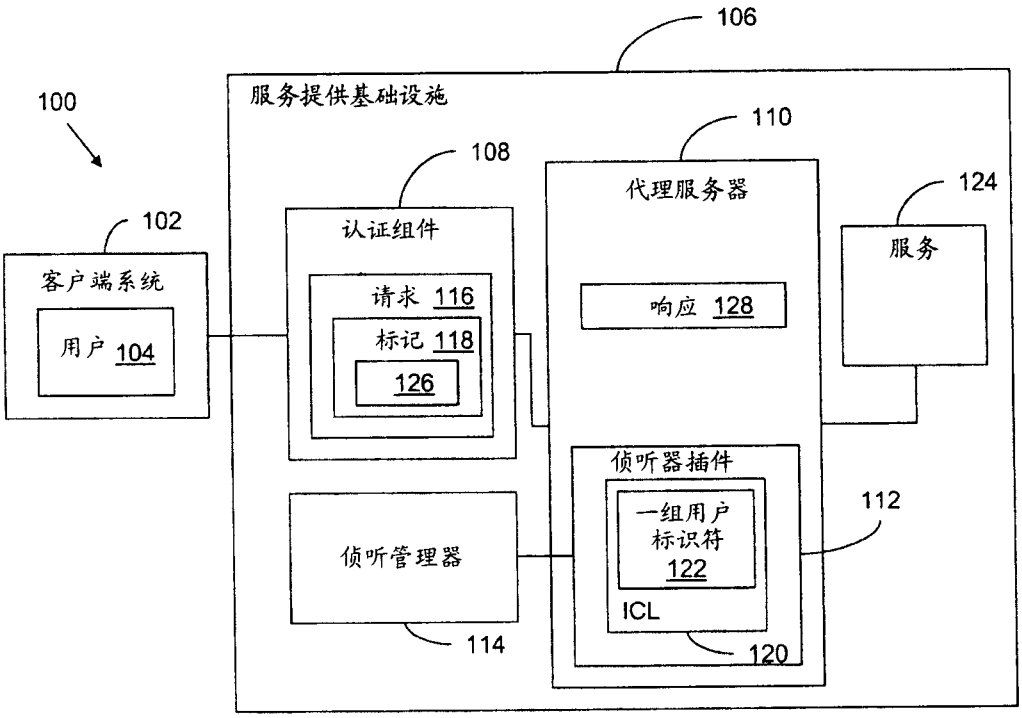

106
服务提供基础设施
100
110
108
代理服务器
124
102
认证组件
服务
客户端系统
请求 116
响应 128
用户 104
标记 118
126
侦听器插件
112
一组用户
标识符
122
侦听管理器
ICL
114
120

图 1

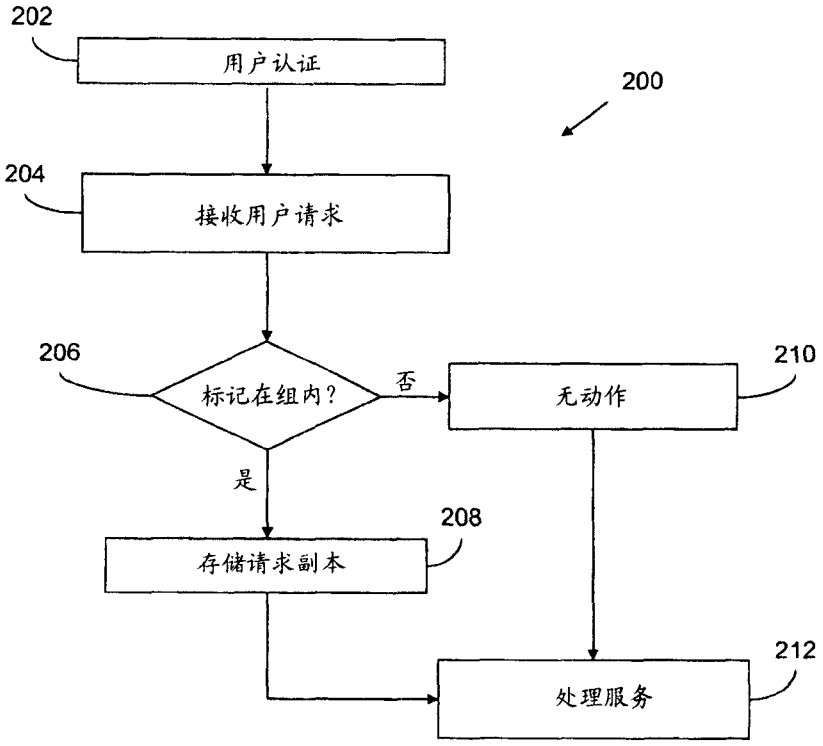

202
用户认证
200
204
接收用户请求
206
标记在组内?
否
210
无动作
是
208
存储请求副本
212
处理服务

图 2

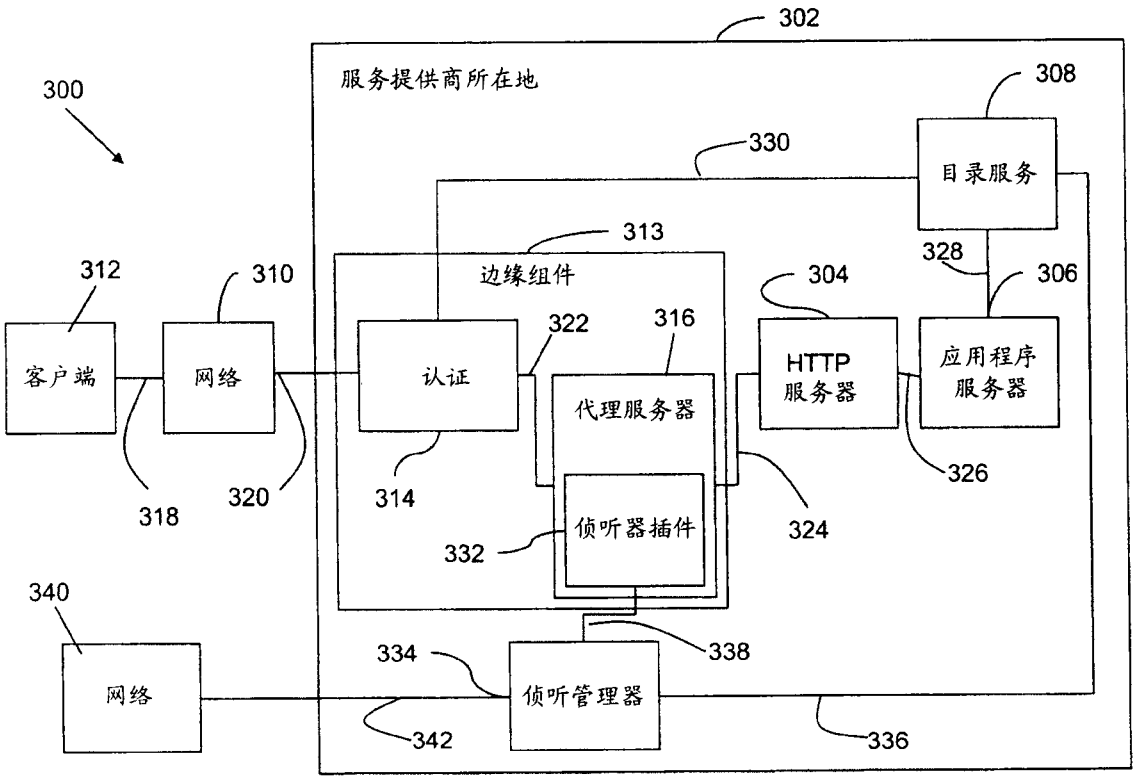

300
302
服务提供商所在地
308
目录服务
330
313
边缘组件
328
306
312
310
304
客户端
网络
认证
322
316
代理服务器
HTTP
服务器
应用程序
服务器
326
318
320
314
324
侦听器插件
332
340
网络
334
338
侦听管理器
342
336

图 3

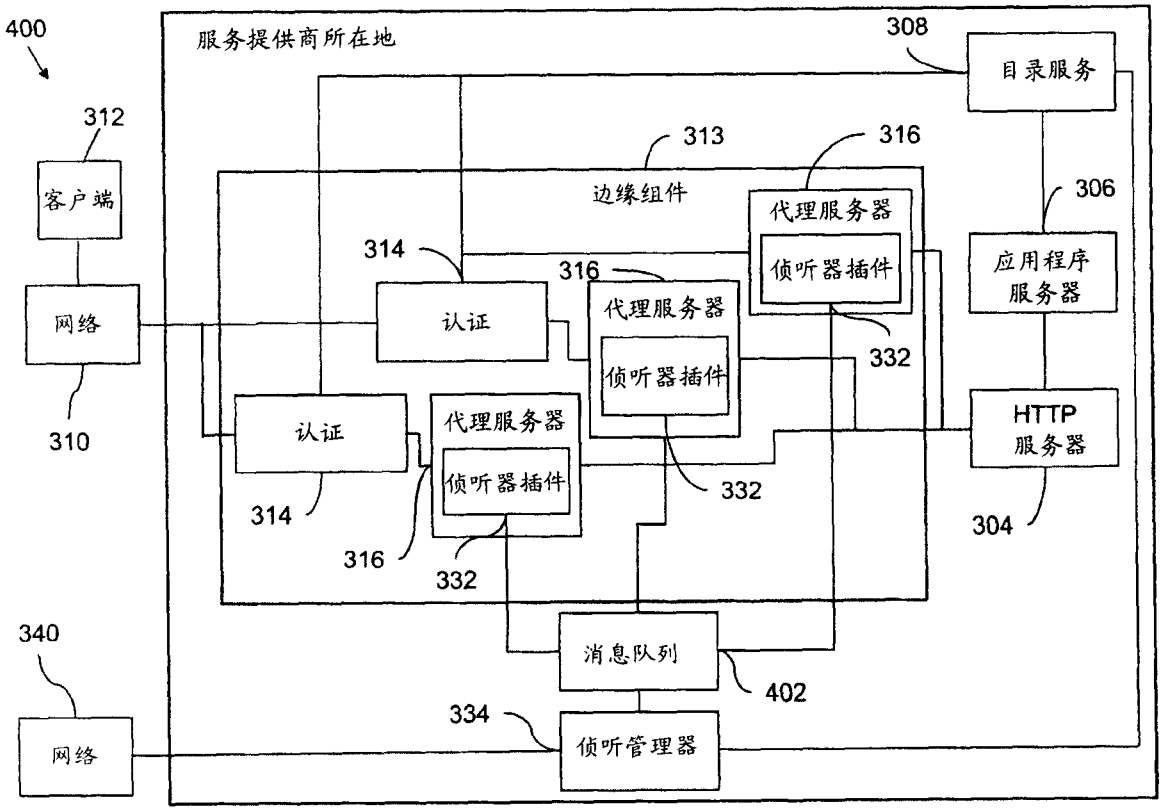

400
服务提供商所在地
308
目录服务
312
客户端
313
316
边缘组件
306
代理服务器
侦听器插件
314
316
应用程序
服务器
网络
认证
代理服务器
侦听器插件
332
310
认证
代理服务器
侦听器插件
HTTP
服务器
332
314
316
332
304
340
消息队列
402
334
网络
侦听管理器

图 4

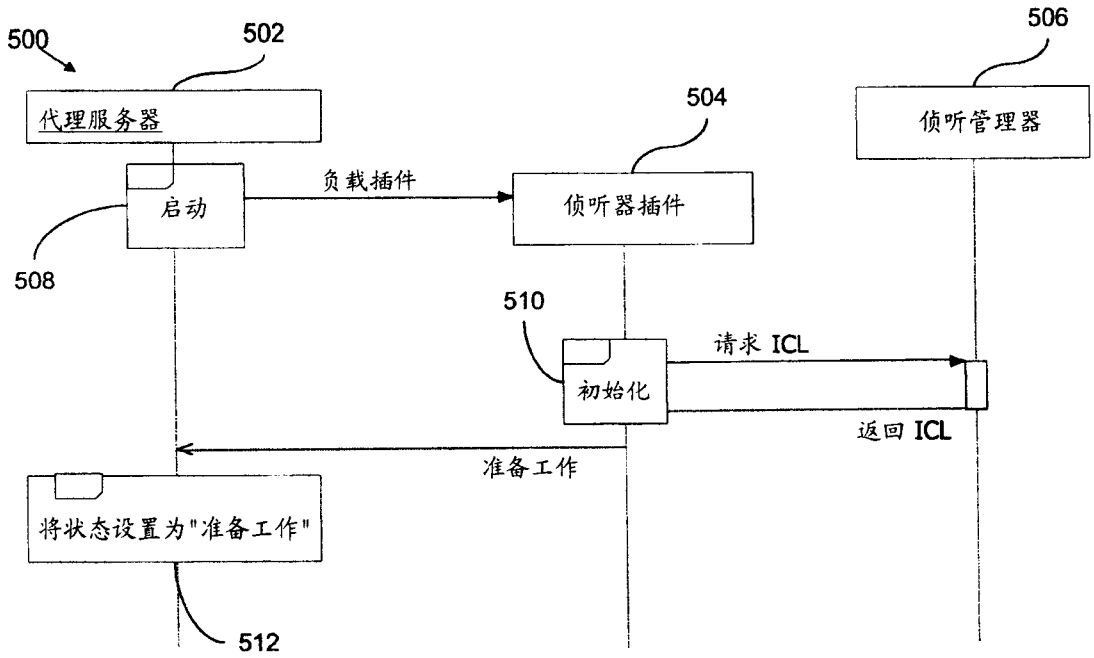

500
502
506
代理服务器
504
侦听管理器
启动
负载插件
侦听器插件
508
510
请求 ICL
初始化
返回 ICL
准备工作
将状态设置为"准备工作"
512

图 5

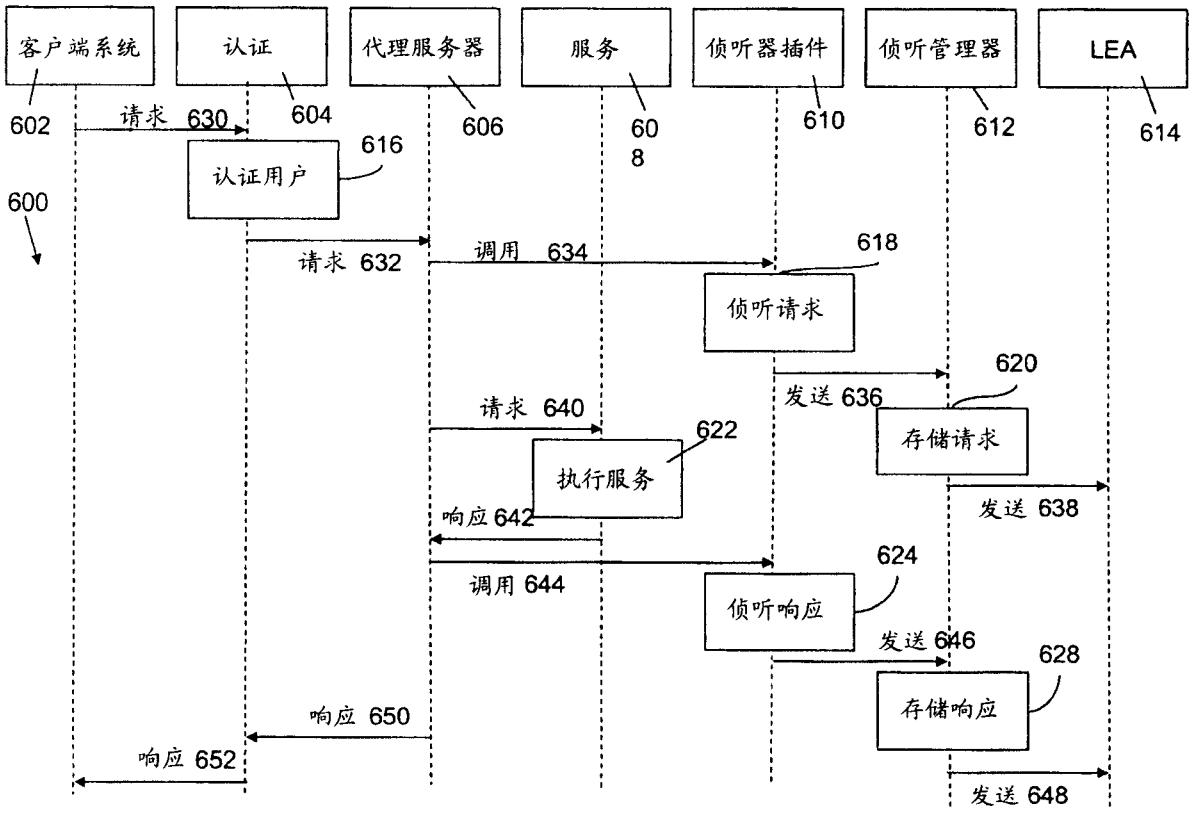

客户端系统
认证
代理服务器
服务
侦听器插件
侦听管理器
LEA
602
604
606
608
610
612
614
600
请求 630
认证用户
616
请求 632
调用 634
618
侦听请求
620
发送 636
存储请求
请求 640
622
执行服务
发送 638
响应 642
调用 644
624
侦听响应
发送 646
628
存储响应
响应 650
响应 652
发送 648

图 6

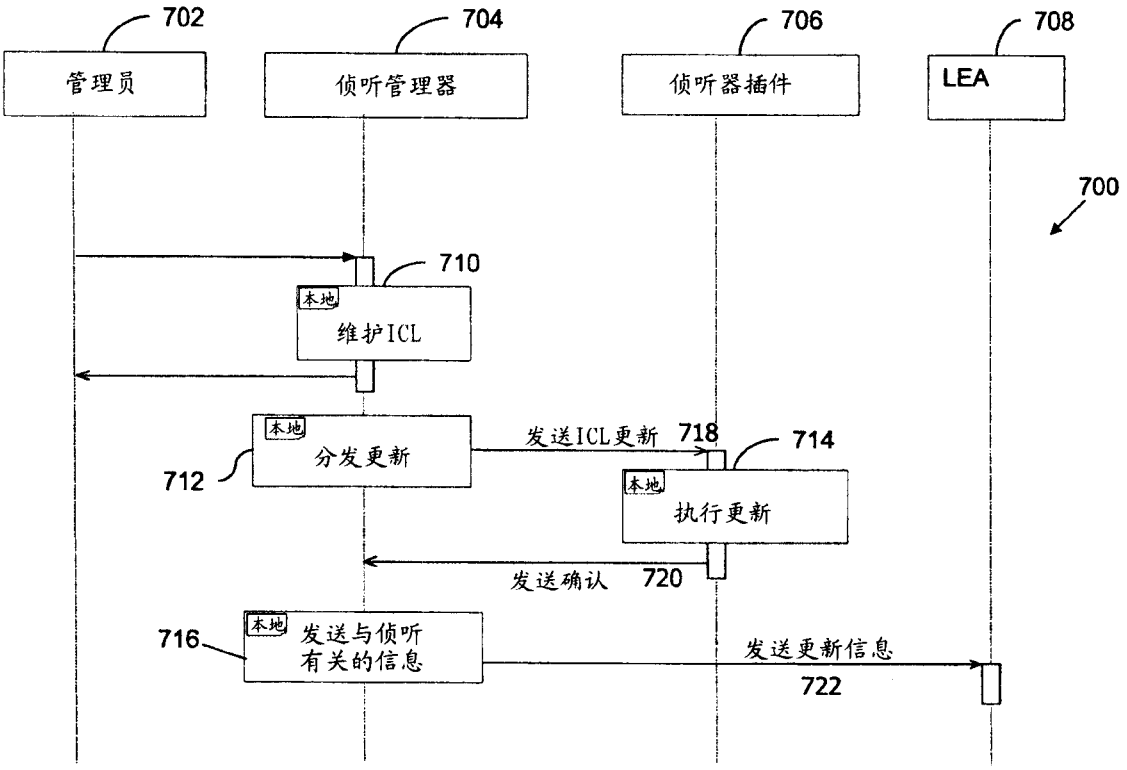

702
704
706
708
管理员
侦听管理器
侦听器插件
LEA
700
710
本地
维护ICL
本地
分发更新
712
发送ICL更新
718
714
本地
执行更新
发送确认
720
716
本地
发送与侦听
有关的信息
发送更新信息
722

图 7