

(12) 发明专利申请

(10) 申请公布号 CN 102446257 A

(43) 申请公布日 2012. 05. 09

(21) 申请号 201110252298. 1

(22) 申请日 2011. 08. 30

(30) 优先权数据

12/903, 605 2010. 10. 13 US

(71) 申请人 国际商业机器公司

地址 美国纽约

(72) 发明人 R · D · 罗伯茨 B · S · 泰里斯

R · A · 韦尔普

(74) 专利代理机构 北京市中咨律师事务所

11247

代理人 于静 杨晓光

(51) Int. Cl.

G06F 21/20 (2006. 01)

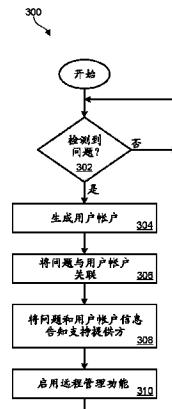
权利要求书 1 页 说明书 6 页 附图 5 页

(54) 发明名称

基于问题的帐户生成方法和装置

(57) 摘要

本发明涉及一种基于问题的帐户生成方法和装置。此处披露了一种提供对计算设备的基于问题的访问的方法。在本发明的一个实施例中，此类方法包括检测计算设备上的问题。所述方法响应于检测到问题而在所述计算设备上自动生成用户帐户。将所述问题与所述用户帐户关联。然后，将所述问题和与所述问题关联的所述用户帐户通知支持提供方。此用户帐户可以被分配给服务技术人员以使能访问所述计算设备。所述服务技术人员然后可以使用所述用户帐户登录到所述计算设备并解决所述问题。此处还披露了相应的装置和计算机程序产品。



1. 一种提供对计算设备的基于问题的访问的方法,所述方法包括:  
检测计算设备上的问题;  
响应于检测到问题而在所述计算设备上自动生成用户帐户;  
将所述问题与所述用户帐户关联;以及  
将所述问题和所述用户帐户通知支持提供方,从而允许将所述用户帐户分配给服务技术人员,以使得所述服务技术人员能够登录到所述计算设备并解决所述问题。
2. 如权利要求 1 中所述的方法,其中将所述问题与所述用户帐户关联包括将所述问题与所述用户帐户唯一地关联。
3. 如权利要求 1 中所述的方法,其中自动生成用户帐户进一步包括生成所述用户帐户的密码。
4. 如权利要求 3 中所述的方法,其中生成密码进一步包括加密所述密码。
5. 如权利要求 3 中所述的方法,其中将所述用户帐户通知支持提供方进一步包括将所述密码发送给所述支持提供方。
6. 如权利要求 1 中所述的方法,还包括在解决所述问题之后立即关闭所述帐户。
7. 如权利要求 1 中所述的方法,还包括在所述用户帐户中记录解决所述问题而采取的操作。
8. 如权利要求 1 中所述的方法,还包括将所述用户帐户复制到与所述计算设备交互的至少一个设备。
9. 如权利要求 1 中所述的方法,还包括在创建所述用户帐户时启用所述计算设备的远程管理功能。
10. 一种提供对计算设备的基于问题的访问的装置,所述装置包括:  
检测模块,用于检测计算设备上的问题;  
帐户生成模块,用于响应于检测到问题而在所述计算设备上自动生成用户帐户;  
关联模块,用于将所述问题与所述用户帐户唯一地关联;以及  
通信模块,用于将所述问题和为了解决所述问题而创建的所述用户帐户通知支持提供方。
11. 如权利要求 10 中所述的装置,其中所述帐户生成模块进一步被配置为生成所述用户帐户的密码,并且所述通信模块被配置为将所述密码发送给所述支持提供方。
12. 如权利要求 11 中所述的装置,还包括用于加密所述密码的加密模块。
13. 如权利要求 10 中所述的装置,还包括用于在解决所述问题之后立即关闭所述帐户的帐户终止模块。
14. 如权利要求 10 中所述的装置,还包括用于在所述用户帐户中记录解决所述问题而采取的操作的记录模块。
15. 如权利要求 10 中所述的装置,还包括用于将所述用户帐户复制到与所述计算设备交互的至少一个设备的复制模块。
16. 如权利要求 10 中所述的装置,还包括用于在创建所述用户帐户时启用所述计算设备的远程管理功能的启用模块。

## 基于问题的帐户生成方法和装置

### 技术领域

[0001] 本发明涉及一种用于控制对诸如服务器和存储系统之类的计算系统的访问的装置和方法。

### 背景技术

[0002] 在现今的服务环境中,许多系统使用提供机器访问权限的单个预定义服务帐户来实现。通常会建立用于登录到此类帐户中的密码。这不会提供高度安全性,因为通常跨产品线和服务人员而共享密码。也可能在很长一段时间内不更改此类密码。这为偶然得到用户帐户和密码的攻击者提供了攻击途径或者可能允许前任员工在未获授权的情况下访问系统。频繁地更改密码也会带来问题,因为可能需要将新密码告知适当的服务人员。此过程非常耗时并将带来管理问题。

[0003] 在许多服务环境中,客户拥有设备并具有对用户帐户和密码的控制。这在由诸如产品供应商或第三方之类的外方提供技术支持时会产生问题。允许客户控制用户帐户和密码具有一个缺点,即经常需要客户介入来获取对客户设备的访问(现场访问或远程访问)。这会在提供支持时导致不必要的延误,从而可能导致不必要的中断和服务延迟。

[0004] 鉴于上述问题,需要更有效地管理诸如服务器、存储设备和其他计算硬件之类的计算产品上的用户帐户和密码的装置和方法。还需要防止攻击者、前任员工或其他人员对此类计算产品进行未授权访问的装置和方法。理想情况下,此类装置和方法几乎不需要来自计算产品的所有者的介入(即使介入,介入也非常少)。

### 发明内容

[0005] 响应于本领域的当前状态,具体地说,响应于本领域中尚未被当前可用的装置和方法完全解决的问题和需求,开发了本发明。相应地,开发本发明以提供一种装置和方法,所述装置和方法用于提供对诸如服务器、存储系统之类的计算设备的基于问题的访问。从下面的说明和所附权利要求,本发明的特性和优点将变得更加显而易见,或者可以通过实施下面所述的本发明,了解本发明的特性和优点。

[0006] 根据以上问题,此处披露了一种提供对计算设备的基于问题的访问的方法。在本发明的一个实施例中,此类方法包括检测计算设备上的问题。所述方法响应于检测到问题而在所述计算设备上自动生成用户帐户。将所述问题与所述用户帐户关联。然后,将所述问题和与所述问题关联的所述用户帐户通知支持提供方。此用户帐户可以被分配给服务技术人员以使能访问所述计算设备。所述服务技术人员然后可以使用所述用户帐户登录到所述计算设备并解决所述问题。

[0007] 此处还披露并要求保护相应的装置和计算机程序产品。

### 附图说明

[0008] 为了便于理解本发明的优点,将参考附图中示出的特定实施例呈现上文简单介绍

的本发明的更具体的说明。应该理解，这些附图仅示出本发明的典型实施例，因此不能被认为是限制本发明的范围，将使用附图描述和解释本发明额外的特征和细节，这些附图是：

- [0009] 图 1 是示出包括不同类型的计算设备的网络环境的一个实例的高级方块图；
- [0010] 图 2 是示出提供对计算设备的基于问题的访问的系统的一个实施例的高级方块图；
- [0011] 图 3 是示出提供对计算设备的基于问题的访问的方法的一个实施例的流程图；
- [0012] 图 4 是示出记录针对与用户帐户关联的问题执行的操作的方法的一个实施例的流程图；
- [0013] 图 5 是提供对多个计算设备的基于问题的访问的系统的一个实施例的高级方块图；以及
- [0014] 图 6 是提供对计算设备的基于问题的访问的系统的一个实施例的高级方块图，其中计算设备与支持提供方之间的通信中断。

### 具体实施方式

[0015] 将理解，此处的图中总体描述和示出的本发明的组件可以按照各种不同的配置排列和设计。因此，图中表示的下面对本发明实施例的更详细的描述并非旨在限制如要求保护的本发明的范围，而是只是表示根据本发明的目前构想的实施例的特定实例。通过参考附图，可以最佳地理解目前所描述的实施例，在所述附图中，相同的部件由相同的标号指定。

[0016] 本领域的技术人员将理解，本发明可以体现为装置、系统、方法或计算机程序产品。此外，本发明可以采取硬件实施例、被配置为操作硬件的软件实施例（包括固件、驻留软件、微代码等）或组合了在此通常被称为“模块”或“系统”的软件和硬件方面的实施例的形式。此外，本发明可以采取体现在任何有形表达介质（其中存储有计算机可用程序代码）中的计算机可用存储介质的形式。

[0017] 可以使用一个或多个计算机可用或计算机可读存储介质的任意组合来存储计算机程序产品。所述计算机可用或计算机可读存储介质例如可以是（但不限于）电、磁、光、电磁、红外线或半导体系统、装置或设备。计算机可读存储介质的更具体实例（非穷举列表）可以包括以下项：具有一条或多条线的电连接、便携式计算机软盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦写可编程只读存储器（EPROM 或闪存）、光纤、便携式光盘只读存储器（CDROM）、光存储设备或磁存储设备。在本文档的上下文中，计算机可用或计算机可读存储介质可以是任何能够包含、存储或传输由指令执行系统、装置或设备使用或与所述指令执行系统、装置或设备结合的程序的介质。

[0018] 用于执行本发明的操作的计算机程序代码可以使用包含一种或多种编程语言的任意组合来编写，所述编程语言包括诸如 Java、Smalltalk、C++ 或类似语言之类的面向对象的编程语言以及诸如“C”编程语言或类似的编程语言之类的常规过程编程语言。用于实现本发明的计算机程序代码还可以使用诸如汇编语言之类的低级编程语言编写。

[0019] 下面可参考根据本发明的各实施例的方法、装置、系统和计算机程序产品的流程图和 / 或方块图对本发明进行描述。将理解，所述流程图和 / 或方块图的每个方块以及所述流程图和 / 或方块图中的方块的组合可以由计算机程序指令或代码来实现。这些计算机

程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器，以便通过所述计算机或其他可编程数据处理装置的处理器执行的所述指令产生用于实现在一个或多个流程图和 / 或方块图方块中指定的功能 / 操作的装置。

[0020] 所述计算机程序指令也可以被存储在可引导计算机或其他可编程数据处理装置以特定方式工作的计算机可读存储介质中，以便存储在所述计算机可读存储介质中的所述指令产生一件包括实现在一个或多个流程图和 / 或方块图方块中指定的功能 / 操作的指令的制品。所述计算机程序指令还可被加载到计算机或其他可编程数据处理装置，以导致在所述计算机或其他可编程装置上执行一系列操作步骤以产生计算机实现的过程，从而在所述计算机或其他可编程装置上执行的指令提供用于实现在一个或多个流程图和 / 或方块图方块中指定的功能 / 操作的过程。

[0021] 参考图 1，其中示出了网络体系结构 100 的一个实例。提供了网络体系结构 100 以示出可以从此处披露的装置和方法中获益的各种类型的计算设备。网络体系结构 100 仅作为实例示出，并非旨在进行限制。实际上，此处披露的装置和方法适用于多种不同的计算设备，并不限于此处所示的这些设备。

[0022] 如图所示，网络体系结构 100 包括一个或多个通过网络 104 互连的计算机 102、106。网络 104 可包括例如局域网 (LAN) 104、广域网 (WAN) 104、因特网 104、内联网 104 等。在特定实施例中，计算机 102、106 可包括客户端计算机 102 和服务器计算机 106（也称为“主机系统”106）两者。通常，客户端计算机 102 发起通信会话，而服务器计算机 106 等待来自客户端计算机 102 的请求。在特定实施例中，计算机 102 和 / 或服务器 106 可与一个或多个内部或外部直连存储系统 112（例如，硬盘驱动器、固态驱动器、磁带等）相连。这些计算机 102、106 和直连存储系统 112 可以使用诸如 ATA、SATA、SCSI、SAS、光纤通道之类的协议通信。

[0023] 在特定实施例中，网络体系结构 100 可包括位于服务器 106 之后的存储网络 108，例如存储区域网络 (SAN) 108 或 LAN 108（例如，当使用网络连接的存储设备时）。此网络 108 可将服务器 106 连接到一个或多个存储系统 110，例如硬盘驱动器或固态驱动器的阵列 110a、磁带库 110b、单独的硬盘驱动器 110c 或固态驱动器 110c、磁带驱动器 110d、CD-ROM 库、虚拟磁带库等。为了访问存储系统 110，主机系统 106 可通过从主机 106 上的一个或多个端口到存储系统 110 上的一个或多个端口的物理连接进行通信。连接可以通过交换机、光纤通道网络、直接连接等实现。在特定实施例中，服务器 106 和存储系统 110 可以使用诸如光纤通道 (FC) 之类的联网标准进行通信。

[0024] 参考图 2，其中示出了提供对计算设备 202 的基于问题的访问的系统 200 的一个实施例。计算设备 202 可包括服务器 106、存储系统 110、112、个人计算机 102、工作站 102 或诸如图 1 中所示的其他计算设备。如图所示，计算设备 202 包括提供对计算设备 202 的基于问题的访问的一个或多个模块。这些模块可包括检测模块 210、帐户生成模块 212、关联模块 214、通信模块 216、启用模块 218、记录模块 220 以及帐户终止模块 222 中的一个或多个。

[0025] 检测模块 210 被配置为检测计算设备 202 上的问题或与计算设备 202 相关的问题。出于描述目的，“问题”可包括各种类型的错误或其他预料之外或不希望出现的情况。一旦检测到问题，帐户生成模块 212 就在计算设备 202 上生成用户帐户。帐户生成模块 212

包括密码生成模块 224 和加密模块 226 两者。密码生成模块 224 生成用户帐户的密码。该密码可以随机生成，也可以根据某些预定义的算法生成。加密模块 226 对密码进行加密，以便密码可以被安全地传送给支持提供方 204。

[0026] 关联模块 214 将问题与新生成的用户帐户关联。在选定实施例中，问题被唯一地关联到用户帐户，这意味着问题与用户帐户之间存在一对一的关联。在其他实施例中，可以将诸如多个相关问题之类的多个问题分配给同一用户帐户。这允许将多个相关问题分配给同一技术人员并一起解决这些问题（而非逐个解决）。

[0027] 一旦将问题关联到用户帐户，通信模块 216 就将问题告知支持提供方 204，例如计算设备 202 的供应商或被雇佣的为计算设备 202 提供技术支持的第三方。通信 236 可通过诸如因特网、专用网、广域网 (WAN)、通过调制解调器的拨号连接之类的网络 208 进行。通信 236 可包括内含前面所述的加密密码的用户帐户信息 234。通信 236 还可包括分析和 / 或解决问题所需的信息，例如踪迹、转储文件、日志、文件和 / 或硬件或代码配置设置。

[0028] 在发送通信 236 之时或接近发送通信 236 之时，启用模块 218 启用计算设备 202 的远程管理功能。这将允许服务技术人员 206 从远程位置登录并访问计算设备 202。例如，启用模块 218 可启用诸如 Tivoli Assist-On-Site 之类的功能以允许技术人员 206 从远程位置访问计算设备 202。

[0029] 当在支持提供方 204 处接收到通信 236 时，记录生成模块 228 生成与问题关联的问题管理记录 232。与问题关联的用户帐户信息可存储在问题管理记录 232 中。该问题管理记录 232 可被分配给服务技术人员 206 以使其能够访问计算设备 202 并解决问题。可以提供解密模块 230 以对密码进行解密。在解决问题期间，记录模块 220 可记录技术人员 206 在解决问题时所执行的所有维护操作。

[0030] 一旦问题得到解决，所指定的服务技术人员 206 就可关闭与问题关联的问题管理记录 232。当问题管理记录 232 被关闭时，帐户终止模块 222 将终止计算设备 202 上的用户帐户。此时可以禁用远程管理功能。当关闭帐户时，可生成记录解决问题时所执行的所有维护操作（如记录模块 220 所记录的）的数据包并将其发送给支持提供方 204。该数据包可供支持提供方 204 用于记录保留、培训和 / 或评估目的。

[0031] 上述基于问题的用户帐户不仅提供用于根据问题事件来控制对计算设备 202 的访问的机制，而且还充当用于记录解决问题时所采取的维护操作的存储库。一旦问题得到解决并关闭帐户，就终止通过用户帐户和密码对计算设备 202 的访问。这会阻止攻击者、前任员工或其他未授权的用户使用所述用户帐户和密码访问计算设备 202。

[0032] 如果再次打开与问题关联的问题管理记录 232，则可以重新启用用户帐户和密码。在这种情况下，技术人员可再次有权访问计算设备 202，直到问题得到解决，并且问题管理记录 232 和用户帐户被关闭。在特定实施例中，如果在一段指定时间内未检测到问题管理记录 232 的活动，则自动禁用用户帐户和密码。这将通过阻止用户帐户长时间保持活动而减少未授权的访问。在特定实施例中，客户可配置触发帐户禁用的不活动周期。

[0033] 应该指出，图 2 中所示的模块可以使用硬件、可在硬件上执行的软件或固件或它们的组合实现。所述模块仅作为实例示出，并非旨在进行限制。实际上，备选实施例可以包括比所示数量更多或更少的模块。还应认识到，在某些实施例中，某些模块的功能可以细分为多个模块，或者相反地，将若干模块的功能组合为单个模块或更少的模块。还应认识到，

所述模块不一定在示出它们的位置中实现。例如，在计算设备 202 中示出的某种功能可以实际上在支持提供方设备 204 中实现，反之亦然。其他模块可以跨多个设备分布，而不是包含在单个设备中。因此，所述模块的位置仅作为实例示出，并非旨在进行限制。

[0034] 参考图 3，其中示出提供对计算设备的基于问题的访问的方法 300 的一个实施例。此方法 300 可由计算设备 202 实现。如图所示，方法 300 初始地判定 302 计算设备 202 上是否出现问题。如果出现问题，则方法 300 在计算设备 202 上生成 304 用户帐户。这可以包括生成密码以及对密码进行加密以传送给支持提供方 204。方法 300 然后将问题关联 306 到用户帐户并将问题和用户帐户信息告知 308 支持提供方 204。方法 300 还启用 310 远程管理功能以使得技术人员能够从远程位置解决问题。

[0035] 参考图 4，其中示出记录针对与用户帐户关联的问题所执行的操作的方法 400 的一个实施例。如图所示，一旦创建用户帐户，方法 400 就判定 402 是否已采取与问题相关的操作。如果是，则方法 400 在与问题关联的用户帐户中记录 404 操作。此过程可以一直继续，直到解决问题为止。一旦问题得到解决，如步骤 406 所判定，方法 400 就关闭 408 与问题关联的用户帐户。这将阻止通过用户帐户和密码对计算设备 202 进行未授权的访问。方法 400 还禁用为解决问题而许可的远程管理功能。方法 400 然后将记录的操作发送 412 给支持提供方 204 以用于记录保留、培训和 / 或评估目的。

[0036] 参考图 5，其中示出提供对计算设备的基于问题的访问的系统 200 的一个备选实施例。在该实施例中，客户计算设备 202a 包括复制模块 500 以及上述其他模块。该复制模块 500 可以在问题涉及多个计算设备 202，或多个计算设备 202 与出现问题的计算设备 202 交互的情况下使用。如果在计算设备 202a 上检测到问题，则以上述方式在所述计算设备上生成用户帐户并将帐户信息 234 发送给支持提供方 204。如果问题与其他计算设备相关（例如，问题涉及若干计算设备 202 之间的交互或其他计算设备 202 包含信息或需要进行修改以解决问题），则也可以将帐户信息 234 复制到其他计算设备 202。

[0037] 例如，如图 5 中所示，如果在计算设备 202a 上发生的问题涉及第二计算设备 202b，则将帐户信息 234 从第一计算设备 202a 复制到第二计算设备 202b。这允许第二计算设备 202b 建立用户帐户和密码以允许对其的访问。在特定实施例中，与问题关联的问题管理记录 232 识别与问题关联的每个计算设备 202，以及每个计算设备 202 的用户帐户和密码。在选定的实施例中，每个相关计算设备 202 上生成的用户帐户和密码是相同的，因为它们均与同一问题关联。技术人员 206 然后可以访问与问题关联的每个计算设备 202，可能使用同一用户帐户和密码。当问题被解决后，以上述方式关闭与问题关联的问题管理记录 232 以及关闭多个计算设备 202 上的用户帐户。

[0038] 参考图 6，其中示出提供对计算设备的基于问题的访问的系统 200 的一个备选实施例。在该实施例中，客户计算设备 202 包括用户接口模块 602 以及上述其他模块。用户接口模块 602 可以在计算设备 202 不能与支持提供方 204 通信（例如，发生间断 600 或中断 600）的情况下使用。在这种情况下，用户接口模块 602 可提供用户接口以允许用户针对计算设备 202 上发生的问题手动生成和 / 或确定用户帐户和密码。

[0039] 然后，用户可以使用备用通信手段（例如，使用电话 604 或其他设备 604）联系支持提供方 204。支持提供方 204 然后可针对问题创建问题管理记录 232。此时可以将用户帐户信息和密码传送给支持提供方 204 以包含在问题管理记录 232 中。然后可以将问题管

理记录 232 分配给技术人员 206 以便提供修复问题的服务。如果可以通信，技术人员可尝试远程修复问题。如果不能通信，技术人员可到达计算设备 202 的现场以解决问题。

[0040] 附图中的流程图和方块图示出了根据本发明的各种实施例的系统、方法和计算机可用介质的可能实施方式的架构、功能和操作。在此方面，所述流程图或方块图中的每个方块都可以表示代码的模块、段或部分，所述代码包括用于实现指定的逻辑功能（多个）的一个或多个可执行指令。还应指出，在某些备选实施方式中，在方块中说明的功能可以不按图中说明的顺序发生。例如，示为连续的两个方块可以实际上被基本同时地执行，或者某些时候，取决于所涉及的功能，可以以相反的顺序执行所述方块。还应指出，所述方块图和 / 或流程图的每个方块以及所述方块图和 / 或流程图中的方块的组合可以由执行指定功能或操作的基于专用硬件的系统或专用硬件和计算机指令的组合来实现。

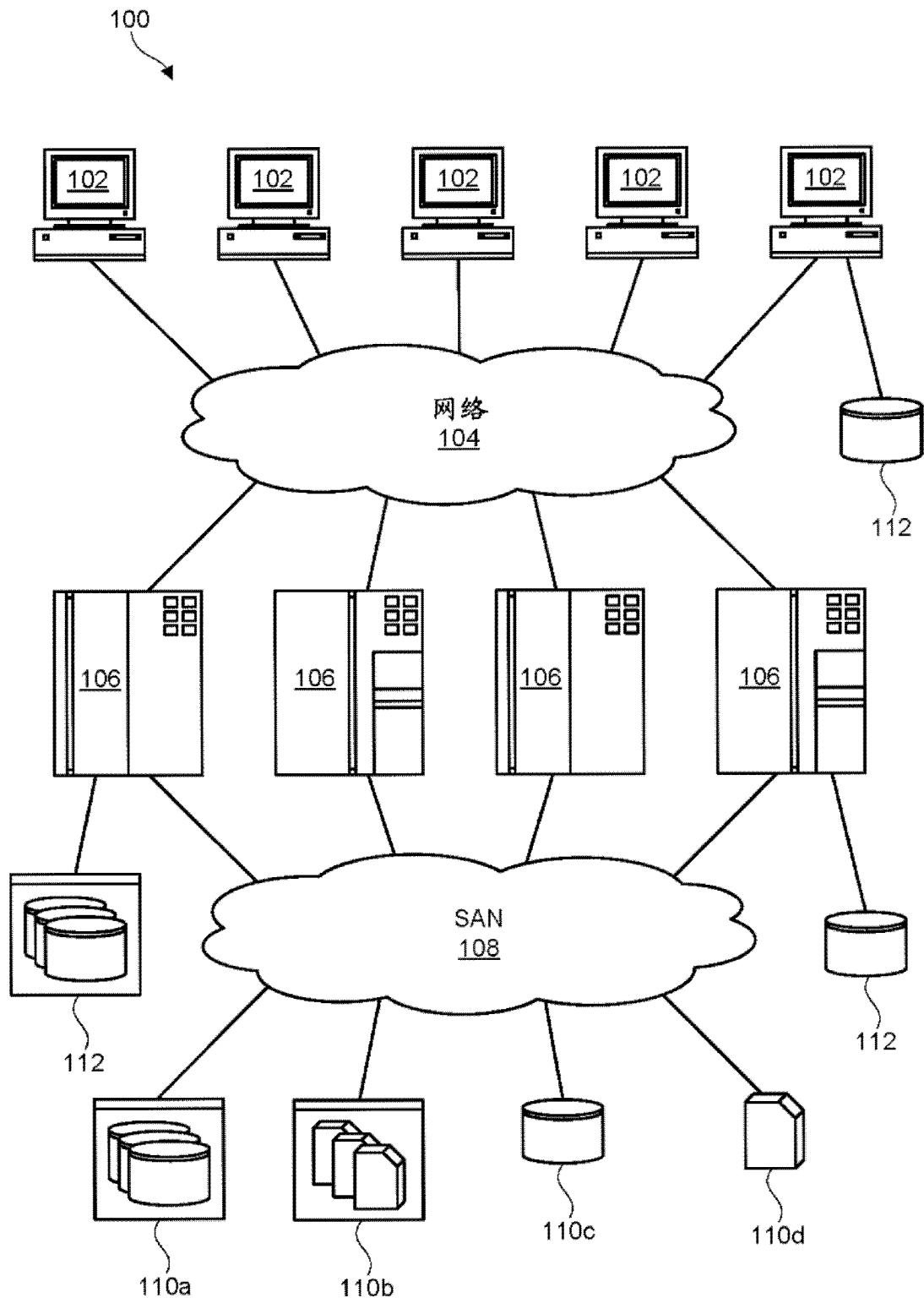


图 1

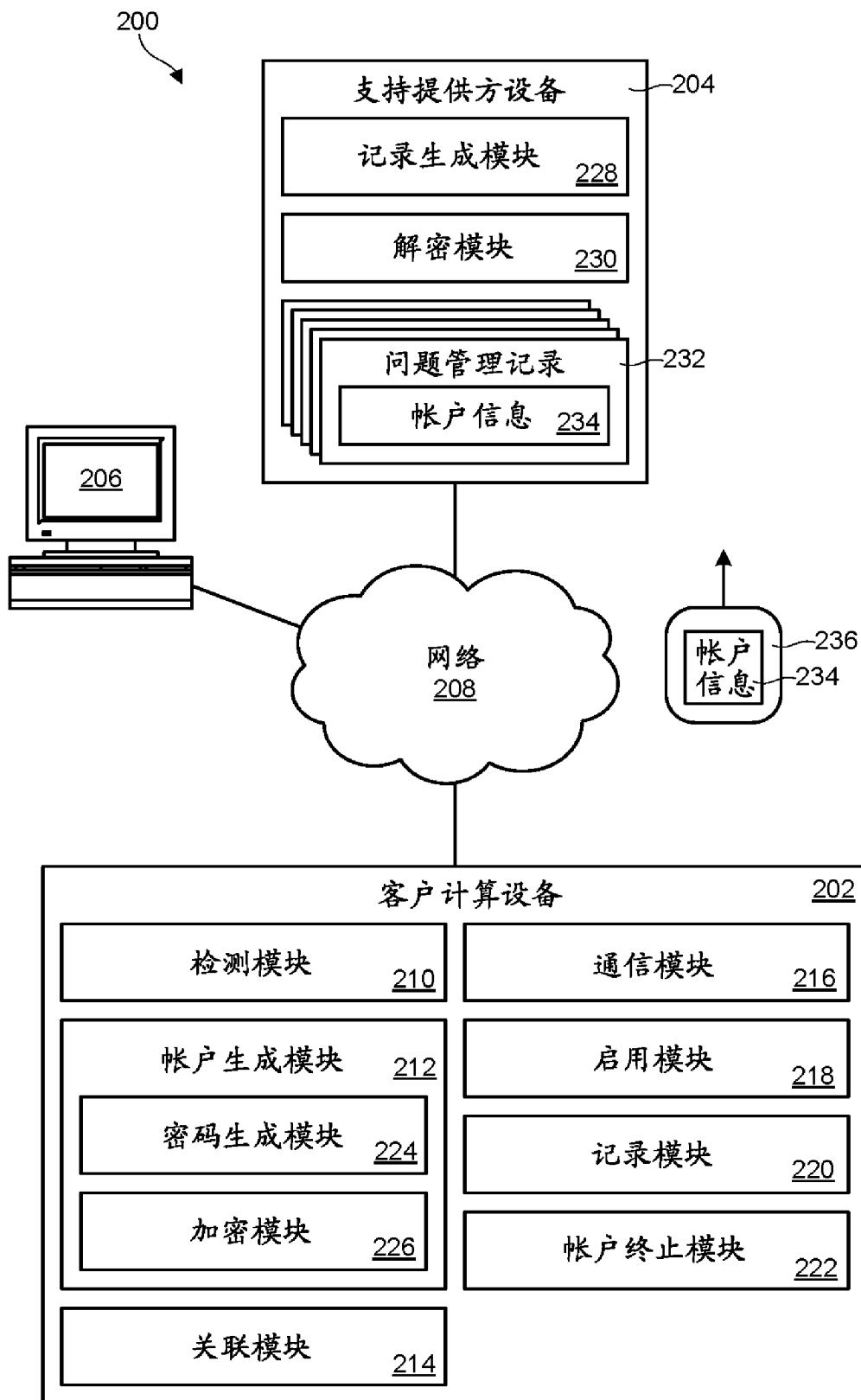
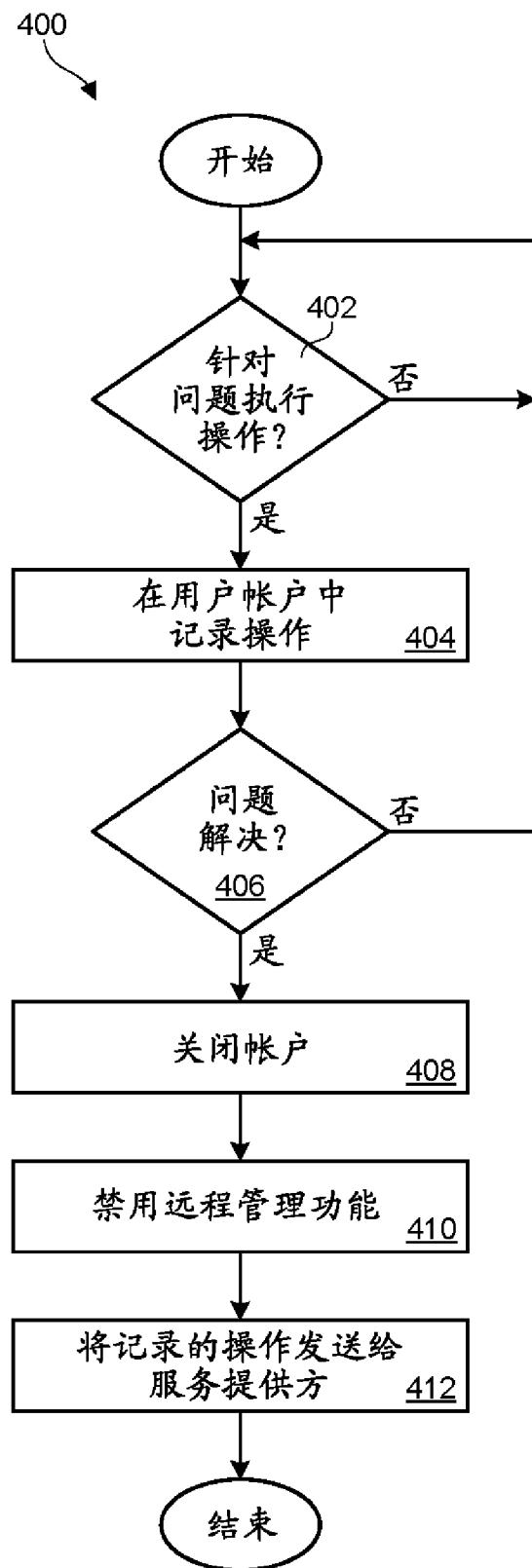
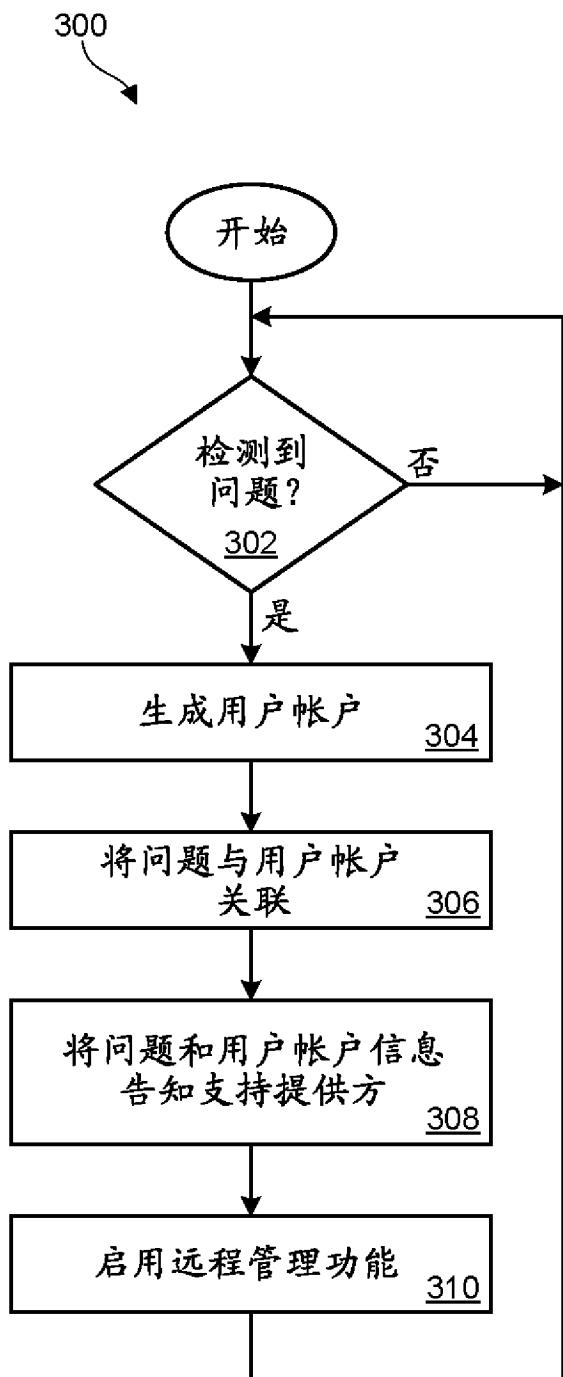


图 2



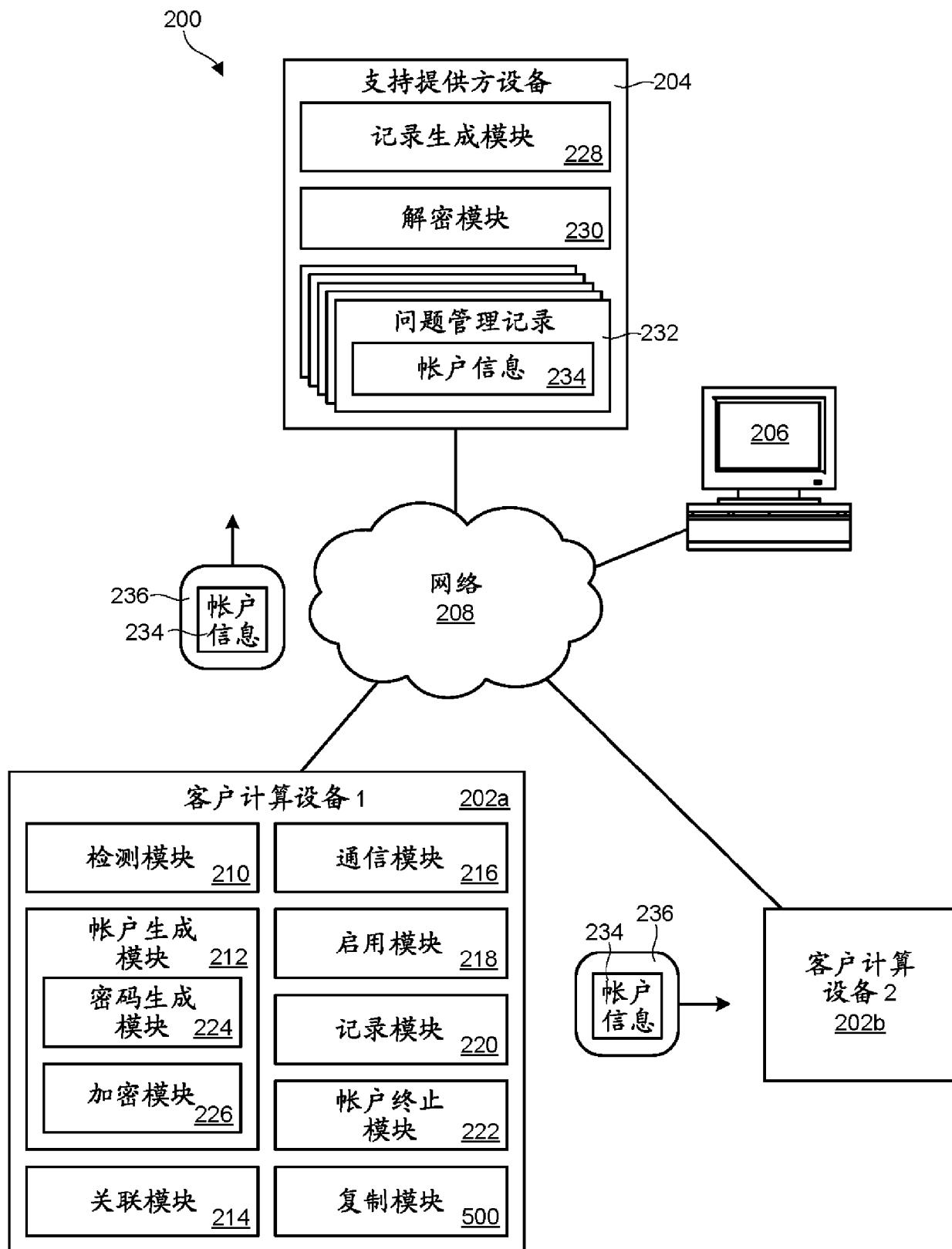


图 5

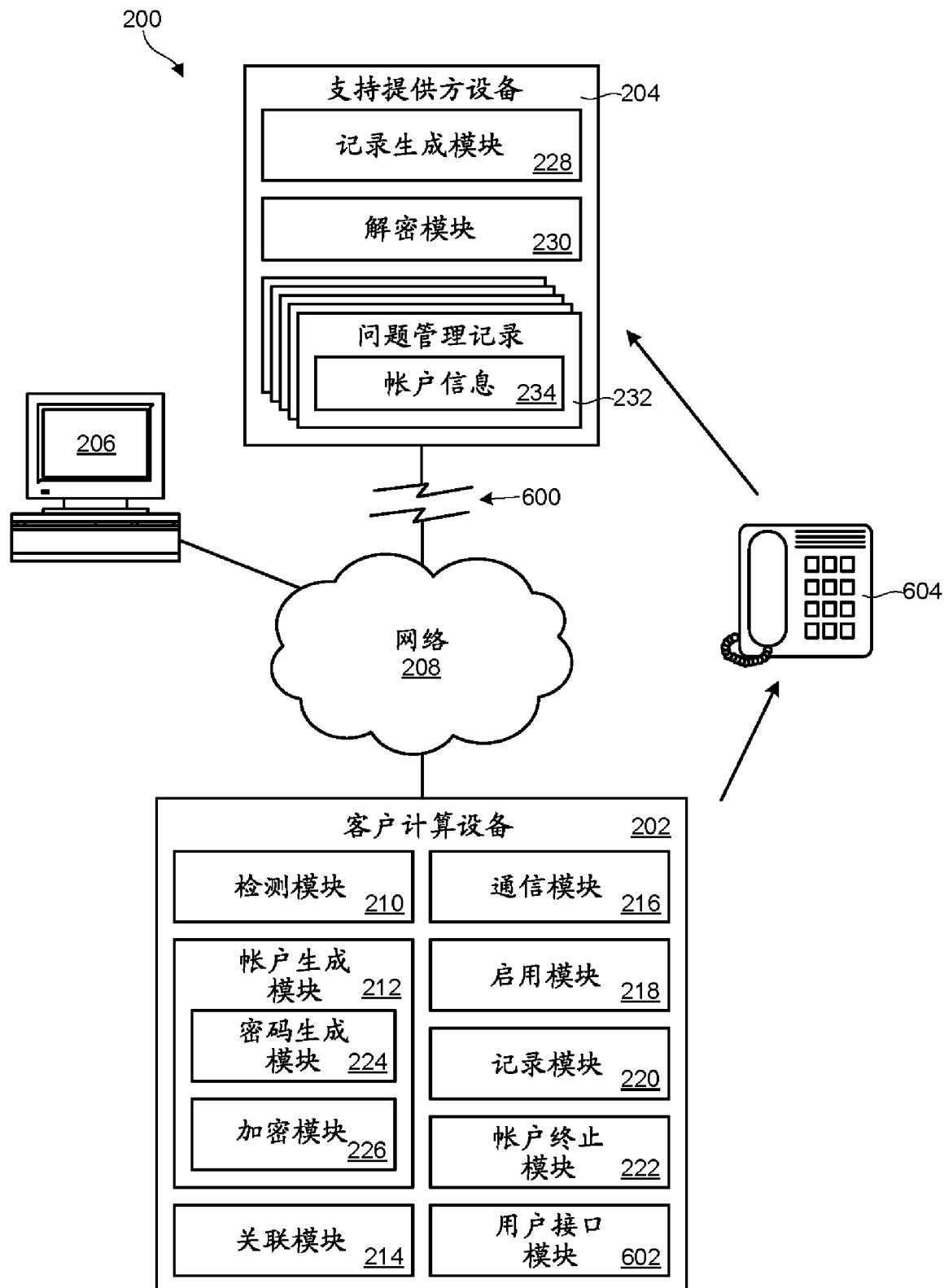


图 6