[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公布说明书

[21] 申请号 200710004267.8

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101005351A

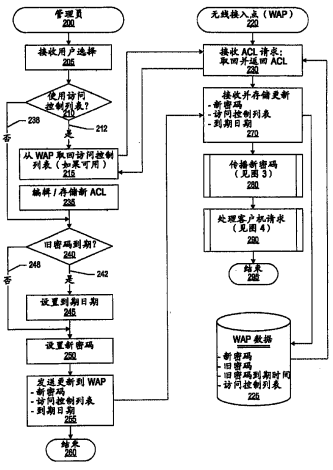
[22] 申请日 2007.1.19
[21] 申请号 200710004267.8
[30] 优先权
[32] 2006. 1.20 [33] US [31] 11/336,205
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 维施瓦纳斯·文卡塔拉马普帕
张佑群 张祐彰
[74] 专利代理机构 北京市金杜律师事务所
代理人 王茂华 胡亚莉
权利要求书 4 页 说明书 11 页 附图 5 页

[54] 发明名称

用于信息处理的系统和方法

[57] 摘要

一种允许管理员在无线接入点如传统 WAP 或者无线路由器设置新密码的系统和方法。 该无线接入点创建包含新密码的消息。 该消息使用先前为无线网络而设置的旧密码进行加密。 加密的消息从无线接入点无线地发送到启用客户机设备(当前访问无线网络的那些客户机)。 这些客户机使用先前提供给客户机的旧密码对该消息进行解密。 客户机从该消息取回新密码。 客户机构造使用新密码进行加密的新消息。 该新消息从客户机无线地发送到无线接入设备并作为确认。



1. 一种计算机实现的方法，包括:

在无线接入点处接收新密码;

创建包含所述新密码的第一消息;

使用用来与所述无线接入点通信的当前密码对所述第一消息进行加密;

将所述加密的第一消息无线地发送到一个或多个客户机;

在所述无线接入点处从所述客户机中的一个或多个客户机接收第一响应无线消息，其中使用所述新密码加密所述第一响应无线消息;

将所述当前密码作为旧密码存储于所述无线接入点中；以及

在所述无线接入点中将所述当前密码替换为所述新密码。

2. 根据权利要求 1 所述的方法，还包括:

在所述无线接入点处从新启用的客户机接收连接消息，其中无线地发送在所述第一消息时将所述新启用的客户机断开，以及其中使用所述旧密码加密所述连接消息;

创建包含所述新密码的第二消息;

使用所述旧密码对所述第二消息进行加密;

将所述加密的第二消息无线地发送到所述新启用的客户机；以及

在所述无线接入点处从所述新启用的客户机接收第二响应无线消息，其中使用所述新密码加密所述第二响应无线消息。

3. 根据权利要求 2 所述的方法，还包括:

在所述无线接入点处取回当前时间和存储的到期时间;

比较所述当前时间与所述存储的到期时间；以及

基于所述比较来确定所述旧密码是否到期，其中仅响应于确定所述旧密码没有到期来执行所述第二消息的发送。

4. 根据权利要求 3 所述的方法，还包括:

在创建所述第一消息之前在所述无线接入点处接收所述到期时间；以及

在可由所述无线接入点访问的非易失性存储区上存储所述到期时间。

5. 根据权利要求 2 所述的方法，还包括:

将对应于所述新启用的客户机的标识符与在访问控制列表（ACL）中列出的一个或多个客户机标识符做比较，其中仅在所述访问控制列表中包含所述新启用的客户机的标识符时才发送所述第二消息。

6. 根据权利要求 1 所述的方法，还包括:

在所述无线接入点处取回包含一个或多个客户机标识符的访问控制列表（ACL），其中所述一个或多个客户机各自对应于在所述 ACL 中包含的所述客户机标识符中的一个客户机标识符。

7. 根据权利要求 1 所述的方法，还包括:

识别从所述客户机中的一个客户机接收的所述第一响应无线消息中的拒绝；以及

停止在所述无线接入点与在所述第一响应无线消息中包含所述拒绝的所述客户机之间的通信。

8. 根据权利要求 1 所述的方法，还包括:

在所述客户机中的一个客户机处从所述无线接入点接收所述加密的第一消息;

使用在可由所述客户机访问的非易失性存储区中存储的无线接入密码对所述加密的第一消息进行解密;

从所述解密的第一消息取回所述新密码;

利用所述新密码更新所述无线接入密码;

在所述非易失性存储区上存储所更新的无线接入密码;

在所述客户机处使用所述新密码对所述第一响应消息进行加密;以及

将所述加密的第一响应消息无线地发送到所述无线接入点；以及

向所述客户机的用户通知所述无线接入密码已经被更新。

9. 一种信息处理系统，包括:

一个或多个处理器;

一个或多个网络适配器，其中所述网络适配器中的至少一个网络适配器是无线网络适配器；

可由所述处理器访问的非易失性存储区；

由所述处理器操作的向客户机设备提供无线密码的处理，所述处理被执行用以：

接收新密码；

创建包含所述新密码的第一消息；

使用用来通过所述无线网络适配器与客户机设备通信的当前密码对所述第一消息进行加密；

使用所述无线网络适配器将所述加密的第一消息无线地发送到一个或多个客户机设备；

在所述无线网络适配器处从所述客户机设备中的一个或多个客户机设备接收第一响应无线消息，其中使用所述新密码加密所述第一响应无线消息；

将所述当前密码作为旧密码存储于所述非易失性存储区中；以及

在所述非易失性存储区中将所述当前密码替换为所述新密码。

10. 根据权利要求 9 所述的信息处理系统，其中所述处理还被执行用以：

在所述无线网络适配器处从新启用的客户机设备接收连接消息，其中在无线地发送所述第一消息时所述新启用的客户机设备断开，以及其中使用所述旧密码加密所述连接消息；

创建包含所述新密码的第二消息；

使用所述旧密码对所述第二消息进行加密；

使用所述无线网络适配器将所述加密的第二消息无线地发送到所述新启用的客户机设备；以及

在所述无线网络适配器处从所述新启用的客户机设备接收第二响应无线消息，其中使用所述新密码加密所述第二响应无线消息。

11. 根据权利要求 10 所述的信息处理系统，其中所述处理还被执行用以：

取回当前时间;

从所述非易失性存储区取回所存储的到期时间;

比较所述当前时间与所述存储的到期时间;以及

基于所述比较来确定所述旧密码是否到期,其中仅响应于确定所述旧密码没有到期来执行所述第二消息的发送。

12. 根据权利要求 11 所述的信息处理系统,其中所述处理还被执行用以:

在创建所述第一消息之前从所述非易失性存储区接收所述到期时间;以及

在所述非易失性存储区中存储所述到期时间。

13. 根据权利要求 10 所述的信息处理系统,其中所述处理还被执行用以:

从在所述非易失性存储区中存储的访问控制列表取回客户机标识符;以及

将对应于所述新启用的客户机的标识符与来自所述访问控制列表(ACL)的所述客户机标识符做比较,其中仅在所述访问控制列表中包含所述新启用的客户机设备的标识符时才发送所述第二消息。

14. 根据权利要求 9 所述的信息处理系统,其中所述处理还被执行用以:

识别从所述客户机设备中的一个客户机设备接收的所述第一响应无线消息中的拒绝;以及

停止与在所述第一响应无线消息中包含所述拒绝的所述客户机设备的通信。

用于信息处理的系统和方法

技术领域

本发明主要地涉及一种用于对用来将设备连接到无线接入点如路由器的密码进行更新的系统和方法。具体而言，本发明涉及一种用于自动地对由客户机用来访问无线接入点的密码进行更新的系统和方法。

背景技术

无线联网在住宅和商务中日益普及。这一点在由于一些建筑物和住宅的设计而难以在设备之间安装网络线缆的环境中尤其如此。此外，计算机用户——尤其是膝上型或者笔记本型计算机用户常常想要在不受特定物理位置约束的情况下连接到计算机网络，如因特网。

无线联网常常允许用户从“无线接入点”或者“WAP”漫游 100 英尺甚至更远。用户的信息处理系统如手持设备（例如 PDA、音乐播放器等）或者笔记本型/膝上型计算机包括无线地发送数据到其它无线网络设备和从其它无线网络设备无线地接收数据的无线网络适配器或者网卡。许多无线设备根据各种标准如 IEEE 802.11 标准来构建。设备所用标准的类型规定了它能够与之通信的其它设备的范围。

无线接入点（WAP 或者 AP）是将无线通信设备“连接”在一起创建无线网络的设备。WAP 通常连接到有线网络，而且可以在每一侧上的设备之间中继数据。许多 WAP 可以连接在一起创建允许“漫游”的更大网络。相比而言，其中客户机设备进行自行管理的网络被称为专用网络。路由器是对使用同一网络路径的两个相似网络进行连接的网络设备。在住宅或者小型商务环境中，路由器常常将用户的局域网（LAN）连接到宽带网络连接，如有线调制解调器，该宽带网络连接

又连接到因特网服务供应商（ISP），由此向局域网上的任何设备提供对因特网的访问。一些路由器包括允许有无线路由器之称的这些路由器也用作无线接入点的无线技术。如这里使用的，“无线接入点”或者“WAP”既包括传统无线接入点以及无线路由器，也包括有助于两个或更多设备的无线连接的任一其它设备。

尽管无线联网向用户提供了更多的移动性和灵活性，但是它也由于潜在地增加了安全风险而受到用户质疑。无线网络常常延伸到用户的住宅或者办公环境以外一百英尺或者更远。除非用户能够保证网络的安全，否则具有无线设备的其它用户都能够连接到该用户的无线网络。为了解决这一安全要求，多数 WAP 提供密码机制。管理员在 WAP 中设置密码，并将该密码提供给将会使用该 WAP 的每个客户机设备。按照惯例，向客户机设备提供密码要求管理员或者设备的用户打开设备上的配置面板并输入密码。WAP 被配置成仅与知道密码的设备通信。WAP 检查它通过无线网络接收的数据分组以查看它们是否使用密码进行了加密。如果分组没有使用密码进行加密则该分组被拒绝。从 WAP 向无线网络上的设备无线发送的分组同样使用该密码进行加密。以这一方式，窥探者在没有获得密码的情况下无法与无线网络通信。

尽管对通过无线网络发送的数据进行加密有助于将窥探者拒之于网络以外，但是它对维护提出了挑战。为了确保安全，许多安全专家建议定期地改变密码。这就要求在使用传统无线网络时改变 WAP 处的密码以及由每个客户机设备使用的密码。如果管理员或者用户忘记改变这些设备中某一设备内的密码，则那一设备将再也无法连接到无线网络。当无线设备的数目很多时加剧了这一挑战。改变较大无线网络上的所有密码可能常常会花费大量时间。此外，在设备数目很多时，一台或多台设备没有更新的可能性增加。由于有这些挑战，无线网络的管理员常常疏于如专家所建议的那样频繁地更新用于无线网络的密码，由此增加了窥探者获得密码并且暗中访问无线网络的可能性。

因此需要一种使密码改变扩散到整个无线网络的系统和方法。另外需要一种提供如下到期时间的系统和方法，在该到期时间之后新密

码不再扩散到客户机设备。

发明内容

已经发现使用一种系统和方法能解决前述挑战，该系统和方法允许管理员在无线接入点如传统 WAP 或者无线路由器处设置新密码。该无线接入点创建包含新密码的消息。该消息使用先前为无线网络而设置的旧密码进行加密。加密的消息从无线接入点无线地发送到启用的客户机设备（当前访问无线网络的那些客户机）。客户机使用先前提供给客户机的旧密码对该消息进行解密。客户机从该消息取回新密码。客户机构造使用新密码进行加密的新消息。该新消息从客户机无线地发送到无线接入设备作为确认。

在一个实施例中，在无线接入点发送包含密码的消息时被断开的客户机试图使用旧密码连接到无线网络（新启用的客户机）。无线接入点通过向新启用的客户机发送消息（利用旧密码进行加密的新密码）做出响应，新启用的客户机取回新密码，并且使用新密码将加密的消息发送回到无线接入点，确认新密码。在一个实施例中，无线接入点检查由新启用的客户机提供的旧密码以确定它是否“到期”。如果它到期，则无线接入点拒绝新启用的客户机的连接请求。如果旧密码没有到期，则无线接入点如上所述将新密码提供给客户机。

以上是发明内容，因此必然包含对细节的简化、概括和省略；而本领域技术人员将认识到该发明内容仅仅是说明性的，本意不在于以任何方式进行限制。仅由权利要求限定的本发明的其它方面、发明特征和优点将在下文阐述的非限制性的具体描述中变得明显。

附图说明

通过参照附图，可以更好地理解本发明，而它的多个目的、特征和优点对于本领域技术人员而言变得更为明显。

图 1 是示出了密码更新如何在管理员、路由器与客户机之间传播的图；

图 2 是示出了当设置新密码和将该密码传播到客户机时在管理员与无线接入点之间采取的步骤的流程图；

图 3 是示出了当无线接入点传播新密码时在无线接入点与在线的客户机设备之间采取的步骤的流程图；

图 4 是示出了当无线接入点传播新密码时在无线接入点与断开（不在线）的客户机设备之间采取的步骤的流程图；以及

图 5 是能够执行在本发明中构想的计算的信息处理系统的框图。

具体实施方式

下文旨在提供对本发明的例子的具体描述，而不应当理解为对本发明本身进行限制。实际上，任一数目的变形都会落入所附权利要求限定的本发明的范围之内。

图 1 是示出了密码更新如何在管理员、无线接入点与客户机之间传播的图。该图示出了时间线，其中较早的事件朝着图顶部的方向出现，而较晚的事件朝着图底部的方向出现。管理员的处理始于 100，在步骤 105 管理员为要使用的无线接入点设置新密码。在一些实施例中，管理员使用直接线路而不是无线地连接到无线接入点来登录到该无线接入点上。这防止了来自物理区域以外的用户改变在无线接入点中存储的安全设置，如密码。

无线接入点处理始于 110，此后在步骤 115，无线接入点从管理员接收新密码并将该密码优选地存储于可由无线接入点访问的非易失性存储设备上。在步骤 120，无线接入点创建含有新密码的消息，并且使用旧（先前的）密码对该消息进行加密（因为客户机当前使用旧密码来连接到无线接入点而还不知道新密码）。在步骤 125，无线接入点将加密的消息无线地发送到所有“启用”客户机。与当前没有连接到无线接入点的断开客户机相反，启用客户机是当前连接到无线接入点的客户机。

启用客户机处理始于 130，此后在步骤 135，启用客户机接收含有新密码的加密消息。客户机使用旧密码对该消息进行解密，然后通过

存储新密码来更新它的配置数据。客户机现在将在对去往/来自无线接入点的消息进行加密/解密时使用新密码。在步骤 140，启用客户机创建使用新密码来加密的新消息。这一消息作为确认。在步骤 145，无线接入点从启用客户机接收该确认。

断开客户机处理始于 150。这些客户机在无线接入点向所有启用客户机发出新密码时没有连接到无线接入点。在此后的某一点，断开客户机使用旧密码连接到无线接入点，因为断开客户机不知道密码已经改变（步骤 155）。在这一点，断开客户机变成“新启用的客户机”，因为它不再与无线接入点断开。

在步骤 160，无线接入点从新启用的客户机接收连接消息并使用旧密码验证该连接。在步骤 165，无线接入点检查旧密码到期时间以查看旧密码是否到期。如果旧密码到期，则连接请求被无线接入点拒绝。然而，如果旧密码还没有到期，则在步骤 170，无线接入点创建包含新密码的消息而且使用旧密码对该消息进行加密。新启用的客户机在步骤 175 接收该消息。新启用的客户机使用旧密码对该消息进行解密并且从解密的消息中取回新密码。在步骤 180，新启用的客户机创建使用新密码加密的消息而且将该新消息发送回到无线接入点。这一消息用作来自新启用的客户机的确认。在步骤 185，无线接入点从新启用的客户机接收该确认。

图 2 是示出了当设置新密码和传播该新密码到客户机时在管理员与无线接入点之间采取的步骤的流程图。管理员处理始于 200，在步骤 205，管理员（用户）输入他的或者她的选择，包括是否将使用访问控制列表（ACL）来进一步保护网络安全以及旧密码是否到期、如果是这样则会将什么到期时间应用于旧密码。关于管理员是否选择使用访问控制列表来进一步保护网络安全进行确定（判断 210）。访问控制列表是能够访问无线接入点的客户机标识符的列表。客户机标识符可以是 MAC 地址，该 MAC 地址是向大多数形式的联网硬件分配的唯一代码。MAC 地址被永久地分配给硬件，由此使无线网络的访问限于硬件地址，如在客户机设备中包含的无线卡，从而进一步保护了网络

安全。然而，有经验的黑客可能能够骗取 MAC 地址，这就是为什么还需要使用密码对去往/来自无线接入点的消息进行加密的原因所在。如果使用访问控制列表，则判断 210 转移到“是”分支 212，此后在步骤 215 从无线接入点请求访问控制列表（如果已经建立访问控制列表）。

无线接入点处理始于 220，此后在步骤 230，无线接入点接收对于访问控制列表的请求并且将访问控制列表返回到管理员。管理员接收访问控制列表并且在步骤 235 编辑（添加和去除）和存储经修正的访问控制列表。回到判断 210，如果管理员选择不使用访问控制列表，则判断 210 转移到“否”分支 238，绕过步骤 215 和 235。

关于管理员是否为旧密码设置到期限制进行确定（判断 240）。在一些实施例中，可以使用缺省到期时间代替从管理员接收到期限制。如果到期限制应用于旧密码，则判断 240 转移到“是”分支 242，由此在步骤 245 为旧密码设置到期日期。另一方面，如果到期日期没有应用于旧密码，则判断 240 转移到“否”分支 248，绕过步骤 245。

在步骤 250，设置由管理员提供的新密码。在步骤 255，将更新发送到无线接入点。这些更新包括无线接入点要使用的新密码、更新的访问控制列表（如果已提供）和对于旧密码的到期限制（如果管理员已提供）。管理员处理随后在 260 结束。

回到无线接入点处理，在步骤 270，无线接入点接收和存储新密码、更新的访问控制列表（如果已提供）和旧密码到期时间（如果已提供）。此数据存储于数据存储器 225 中。在一个实施例中，数据存储器 225 是可由无线接入点访问的非易失性存储区。访问控制列表然后将新密码传播到任何启用客户机，即当前连接到无线接入点的那些客户机（预定义的处理 270，关于处理细节请见图 3 和对应文字）。无线接入点也继续处理客户机请求（预定义的处理 290，关于处理细节请见图 4 和对应文字）。这些请求可以包括来自如下客户机的连接请求，这些客户机在预定义的处理 280 传播新密码时没有收到该新密码。无线接入点处理随后在 295 结束。

图 3 是示出了当无线接入点传播新密码时在无线接入点与在线的客户机设备之间采取的步骤的流程图。无线接入点处理始于 300，此后在步骤 305，无线接入点通过在消息中存储新密码并且使用旧密码对该消息进行加密来创建密码更新消息。关于无线网络是否使用访问控制列表进行确定（判断 310）。如果使用访问控制列表，则判断 310 转移到“是”分支 312，此后在步骤 315，将加密的密码更新消息发送到在访问控制列表中列出的每个客户机。另一方面，如果不使用访问控制列表，则判断 310 转移到“否”分支 318，此后在步骤 320，无线接入点将加密的密码更新消息广播到所有启用客户机（即当前连接到无线接入点的所有设备）。

启用客户机处理始于 325，此后在步骤 330，客户机接收经加密的密码更新消息。关于是接受还是拒绝新密码进行确定（判断 340）。接收新密码的一些设备可能不再需要连接到无线网络。例如，如果管理员计划将客户机设备卖给或者赠给不需要连接到网络的某人，则可以拒绝新密码更新。如果新密码更新消息由客户机接受，则判断 340 转移到“是”分支 342，由此在步骤 345，新密码存储于客户机的配置数据中，使得客户机可以继续访问网络，而在步骤 350，客户机通过使用新密码对确认消息进行加密来创建确认消息。另一方面，如果客户机不希望接受新密码，则判断 340 转移到“否”分支 352，此后在步骤 355，使用旧密码或者新密码对拒绝消息进行加密。在步骤 360，客户机将接受或者拒绝新密码的响应消息发送回到无线接入点。新密码消息的客户机处理随后在 365 结束。在一个实施例中，向用户通知（例如，使用弹出消息）密码已经改变。

回到无线接入点处理，在步骤 370 接收客户机的响应。关于客户机是否接受新密码进行确定（判断 375）。如果客户机不接受新密码，则判断 375 转移到“否”分支 378，此后在 380 从访问控制列表（如果使用了访问控制列表）去除该客户机。另一方面，如果密码已由客户机接受，则判断 375 转移到“是”分支 385，绕过步骤 380。则无线接入点处理在步骤 395 返回到调用例程。

图 4 是当无线接入点传播新密码时在无线接入点与断开（不在线）的客户机设备之间采取的步骤的流程图。客户机处理始于 400，此后在步骤 405，客户机使用最后已知的密码对消息进行加密。如果客户机没有收到新密码，则最后已知的密码不同于由管理员建立的并且正在由无线接入点使用的新密码。然而，如果客户机已经收到新密码，则最后已知的密码与新密码相同。在步骤 410，客户机将加密的消息无线地发送到无线接入点。

无线接入点处理始于 420，此后在步骤 425，无线接入点从数据存储器 225 中读取它的安全设置。安全设置包括正在由无线接入点使用的新密码、在新密码建立之前由无线接入点使用的先前的或者“旧”的密码、旧密码的到期日期或者时间以及可选的访问控制列表。在步骤 430，无线接入点接收由客户机发送的加密消息。

关于无线接入点是否正在使用访问控制列表进行确定（判断 435）。如果正在使用访问控制列表，则判断 435 转移到“是”分支 438，此后在步骤 440，将客户机与访问控制列表做比较。关于是否在访问控制列表中找到客户机进行确定（判断 445）。如果客户机不在访问控制列表中，则判断 445 转移到“否”分支 452，此后在步骤 480，拒绝来自该客户机的消息，无线接入点处理在 499 返回。另一方面，如果客户机在访问控制列表中（此后判断 445 转移到“是”分支 448）或者如果没有正在使用访问控制列表（此后判断 435 转移到“否”分支 446），则在步骤 450，使用由管理员建立的当前的或者“新”的密码对消息进行解密。

关于新密码是否成功地对消息进行解密进行确定（判断 455）。如果新密码成功地对消息进行解密，则判断 455 转移到“是”分支 458，此后在步骤 460，允许来自该客户机的消息。另一方面，如果新密码没有成功地对消息进行解密，则判断 455 转移到“否”分支 462 以进一步分析消息。

关于是否已经出现针对旧密码的使用而建立的到期日期以及旧密码的使用是否因此到期进行确定（判断 465）。如果旧密码到期，则判

断 465 转移到“是”分支 466，此后在步骤 480，拒绝来自该客户机的消息，无线接入点处理在 499 返回。

另一方面，如果旧密码没有到期，则判断 465 转移到“否”分支 468，此后在步骤 470，使用旧密码对从该客户机接收的消息进行解密。关于旧密码是否成功地对消息进行解密进行确定（判断 475）。如果旧密码没有成功地对消息进行解密，则判断 475 转移到“否”分支 478，此后在步骤 480，拒绝来自该客户机的消息，无线接入点处理在 499 返回。另一方面，如果旧密码成功地对消息进行了解密，则判断 475 转移到“是”分支 488，此后将新密码传播到该客户机（预定义的处理 490，关于处理细节请见图 3 和对应文字）。在一个实施例中，可以利用各自具有它自己的密码到期标准的多个旧密码来支持两个或多个“旧密码”。无线接入点处理随后在 499 返回。

暂时回到客户机处理，在步骤 485 客户机从无线接入点接收响应（接受消息、拒绝消息或者密码更新消息，该密码更新消息利用旧密码进行加密并且包含新密码）。客户机相应地处理该响应，客户机处理在 495 结束。

图 5 图示了信息处理系统 501，该系统是能够执行这里描述的计算操作的计算机系统的简化例子。计算机系统 501 包括耦合到主机总线 502 的处理器 500。二级（L2）高速缓存存储器 504 也耦合到主机总线 502。主机到 PCI 桥接器 506 耦合到主存储器 508，包括高速缓存存储器和主存储器控制功能，并且提供用以对于在 PCI 总线 510、处理器 500、L2 高速缓存 504、主存储器 508 和主机总线 502 之间的传送进行处理的总线控制。主存储器 508 耦合到主机到 PCI 桥接器 506 以及主机总线 502。由一个或多个主机处理器 500 独自使用的设备如 LAN 卡 530 耦合到 PCI 总线 510。服务处理器接口和 ISA 访问通过（Access Pass-through）512 在 PCI 总线 510 与 PCI 总线 514 之间提供接口。按照这种方式，PCI 总线 514 与 PCI 总线 510 相隔离。设备如闪存 518 耦合到 PCI 总线 514。在一个实施方式中，闪存 518 包括 BIOS 代码，该 BIOS 代码结合了用于各种低级系统功能和系统引导功能的

可由处理器执行的必要代码。

PCI 总线 514 为由一个或多个主机处理器 500 和服务处理器 516 所共享的各种设备（例如包括闪存 518）提供了接口。PCI 到 ISA 桥接器 535 提供了用以对于在 PCI 总线 514 与 ISA 总线 540 之间的传送、通用串行总线（USB）功能 545、电源管理功能 555 进行处理的总线控制，而且可以包括未示出的其它功能单元，比如实时时钟（RTC）、DMA 控制、中断支持和系统管理总线支持。非易失性 RAM 520 附接到 ISA 总线 540。服务处理器 516 包括用于在初始化步骤期间与一个或多个处理器 500 通信的 JTAG 和 I2C 总线 522。JTAG/I2C 总线 522 也耦合到 L2 高速缓存 504。主机到 PCI 桥接器 506 和主存储器 508，在处理器、服务处理器、L2 高速缓存、主机到 PCI 桥接器与主存储器之间提供通信路径。服务处理器 516 也访问系统电源资源以使信息处理设备 501 掉电。

外围设备和输入/输出（I/O）设备可以附接到各种接口（例如耦合到 ISA 总线 540 的并行接口 562、串行接口 564、键盘接口 568 和鼠标接口 570）。作为选择，许多 I/O 设备可以通过附接到 ISA 总线 540 的超级 I/O 控制器（未示出）来提供。也作为外围设备来连接实时时钟（RTC）560 而且由信息处理系统使用该实时时钟来执行定时操作。

为了将计算机系统 501 附接到另一计算机系统以通过网络拷贝文件，LAN 卡 530 耦合到 PCI 总线 510。类似地，为了将计算机系统 501 连接到 ISP 以使用电话线连接来连接到因特网，调制解调器 575 连接到串行端口 564 和 PCI 到 ISA 桥接器 535。

尽管在图 5 中描述的计算机系统能够执行这里描述的本发明，但是这一计算机系统只不过是计算机系统的一个例子。本领域技术人员将理解到许多其它计算机系统设计能够执行这里描述的本发明。

本发明的优选实施之一是客户机应用，即在代码模块中的指令集（程序代码），该代码模块例如可以驻留于计算机的随机访问存储器中。在计算机需要之前，该指令集可以存储于另一计算机存储器中，例如存储于硬盘驱动器中或者可移动存储器如光盘中（用于最终使用

在 CD ROM 中）或者软盘（用于最终使用在软件驱动器中）中，或者经由因特网或者其它计算机网络进行下载。因此，本发明可以实施为用于在计算机中使用的计算机程序产品。此外，虽然描述的各种方法方便地实施于通过软件有选择地启用或者重新配置的通用计算机中，但是本领域技术人员也将认识到这样的方法可以实施于硬件中、固件中、或者构造为执行所需方法步骤的更专用的装置中。

尽管已经示出和描述了本发明的特定实施例，但是对于本领域技术人员不言而喻，基于这里的教导，在不脱离本发明及其更广泛方面的情况下可以做出多种变换和改型。因此，所附权利要求将在它们的范围之内涵盖所有这些落入本发明的真实思想和范围之内的变换和改型。另外将理解到，本发明仅由所附权利要求进行限定。本领域技术人员将理解到，如果意图在于所引入的权利要求要素的具体数目，则这样的意图将明确地记载于权利要求中，而在没有这样的记载时就不存在这样的限制。作为非限制性的例子，为了帮助理解，后附权利要求包含对引导词语“至少一个”和“一个或多个”的运用以便引入权利要求要素。然而，对这种词语的运用不应当理解为意味着，通过不定冠词“一个”来引入权利要求要素会将包含这样引入的权利要求要素的任何特定权利要求限制为仅含一个这种要素的发明，即使同一权利要求包括引导词语“一个或多个”或者“至少一个”和不定冠词如“一个”时仍然不应当做此理解；这一点对于定冠词“该”或“所述”在权利要求中的运用而言同样适用。

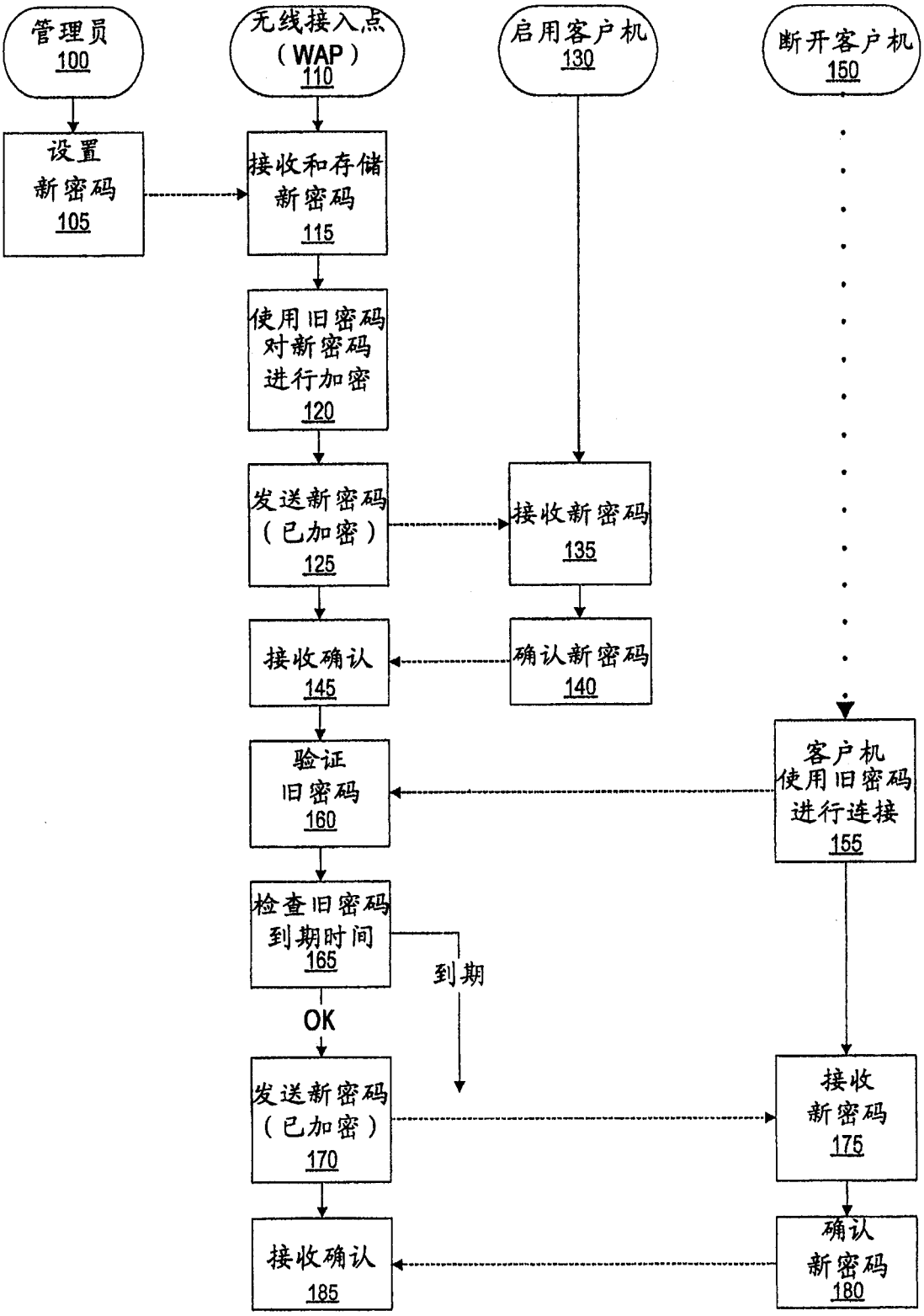

管理员
100
无线接入点
（WAP）
110
启用客户机
130
断开客户机
150
设置
新密码
105
接收和存储
新密码
115
使用旧密码
对新密码
进行加密
120
发送新密码
（已加密）
125
接收新密码
135
接收确认
145
确认新密码
140
验证
旧密码
160
客户机
使用旧密码
进行连接
155
检查旧密码
到期时间
165
到期
OK
发送新密码
（已加密）
170
接收
新密码
175
接收确认
185
确认
新密码
180

图 1

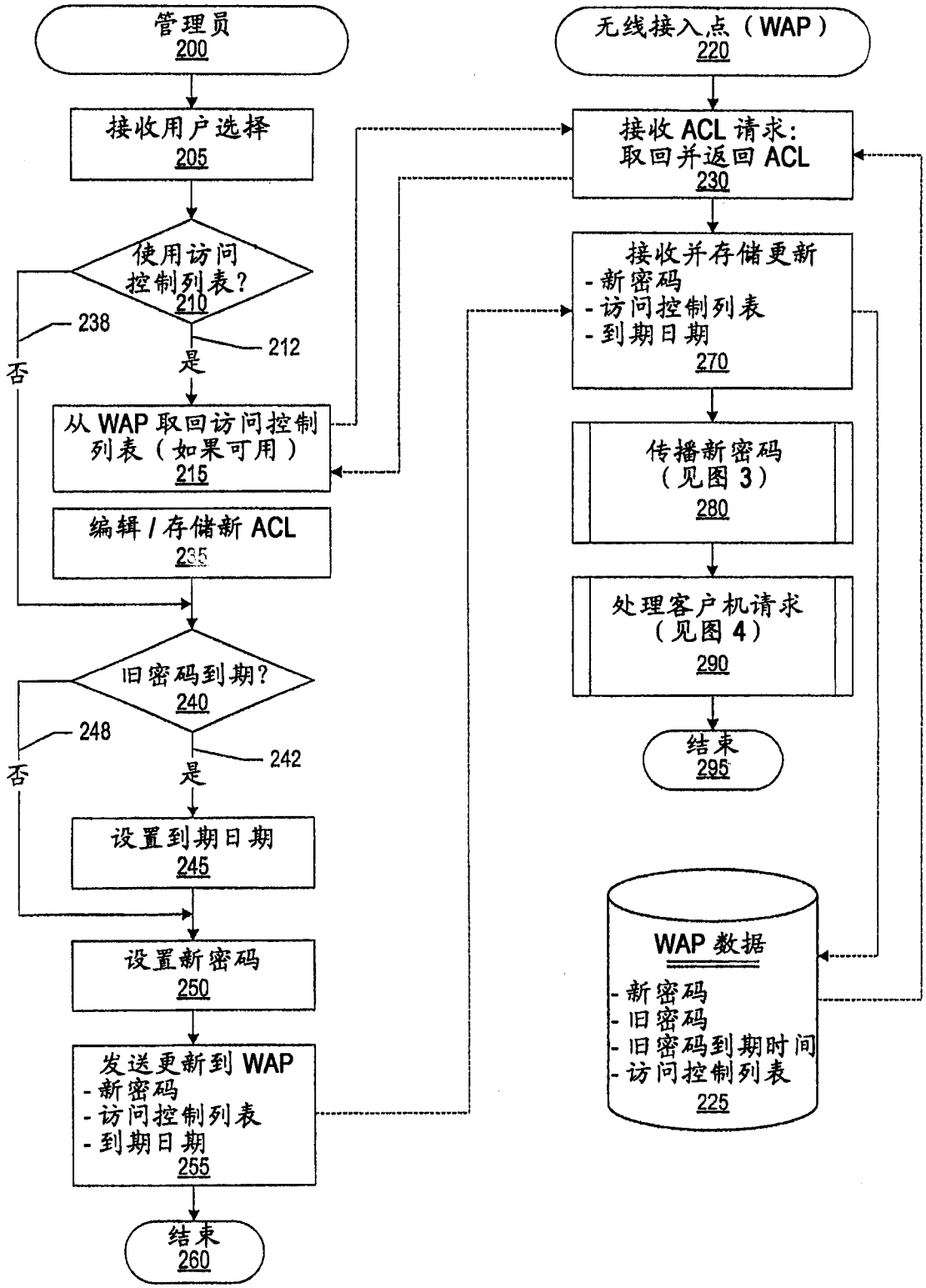

管理员
200
接收用户选择
205
使用访问控制列表?
210
238
否
212
是
从 WAP 取回访问控制列表（如果可用）
215
编辑 / 存储新 ACL
235
旧密码到期?
240
248
否
242
是
设置到期日期
245
设置新密码
250
发送更新到 WAP
- 新密码
- 访问控制列表
- 到期日期
255
结束
260
无线接入点（WAP）
220
接收 ACL 请求:
取回并返回 ACL
230
接收并存储更新
- 新密码
- 访问控制列表
- 到期日期
270
传播新密码
（见图 3）
280
处理客户机请求
（见图 4）
290
结束
295
WAP 数据
- 新密码
- 旧密码
- 旧密码到期时间
- 访问控制列表
225

图 2

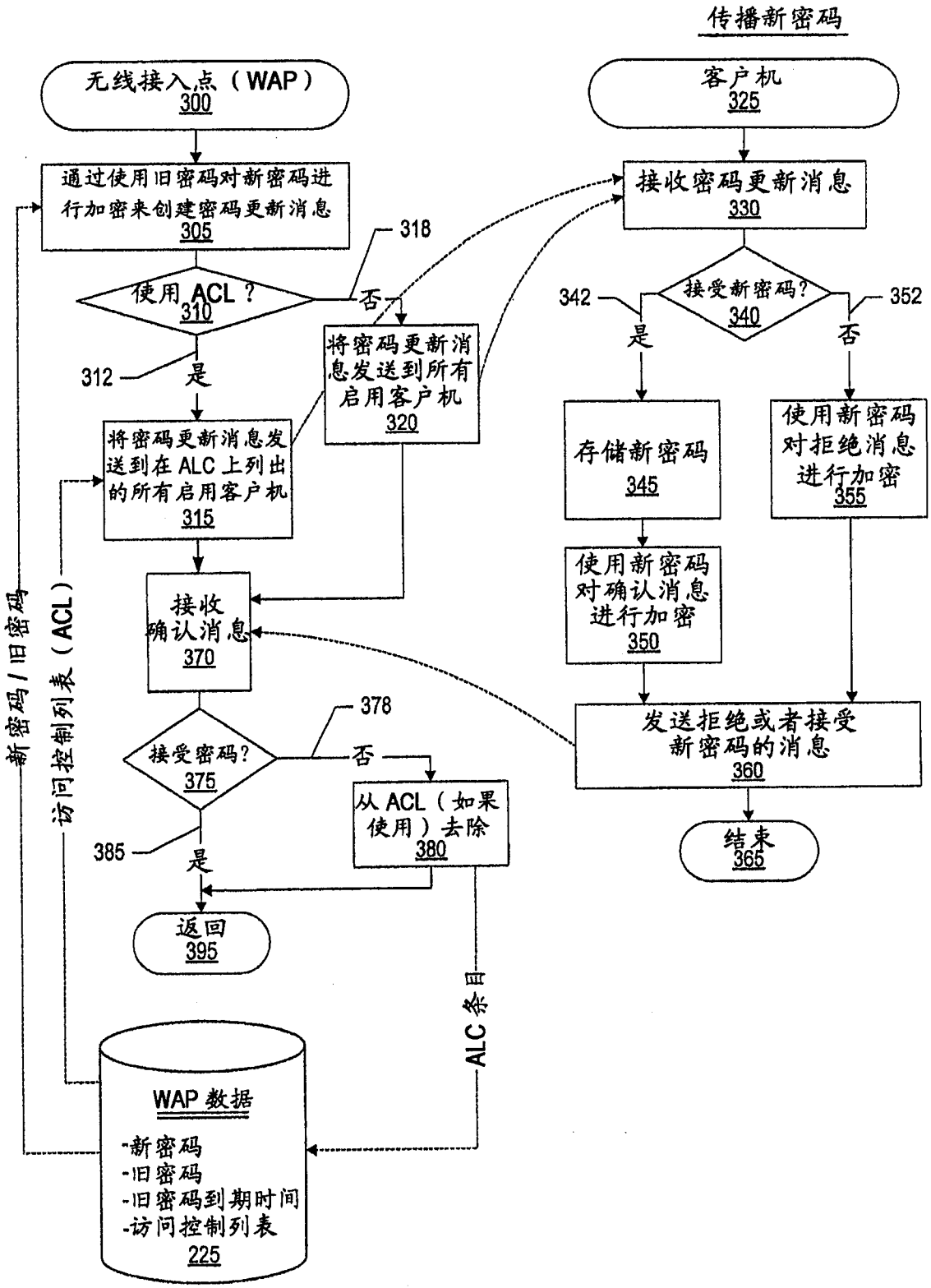

传播新密码
无线接入点（WAP）
300
客户机
325
通过使用旧密码对新密码进行加密来创建密码更新消息
305
接收密码更新消息
330
318
使用 ACL？
310
否
342
接受新密码？
340
352
是
312
是
否
将密码更新消息发送到所有启用客户机
320
存储新密码
345
使用新密码对拒绝消息进行加密
355
将密码更新消息发送到在 ALC 上列出的所有启用客户机
315
使用新密码对确认消息进行加密
350
接收确认消息
370
发送拒绝或者接受新密码的消息
360
378
接受密码？
375
否
从 ACL（如果使用）去除
380
结束
365
385
是
返回
395
新密码 / 旧密码
访问控制列表（ACL）
ALC 条目
WAP 数据
-新密码
-旧密码
-旧密码到期时间
-访问控制列表
225

图 3

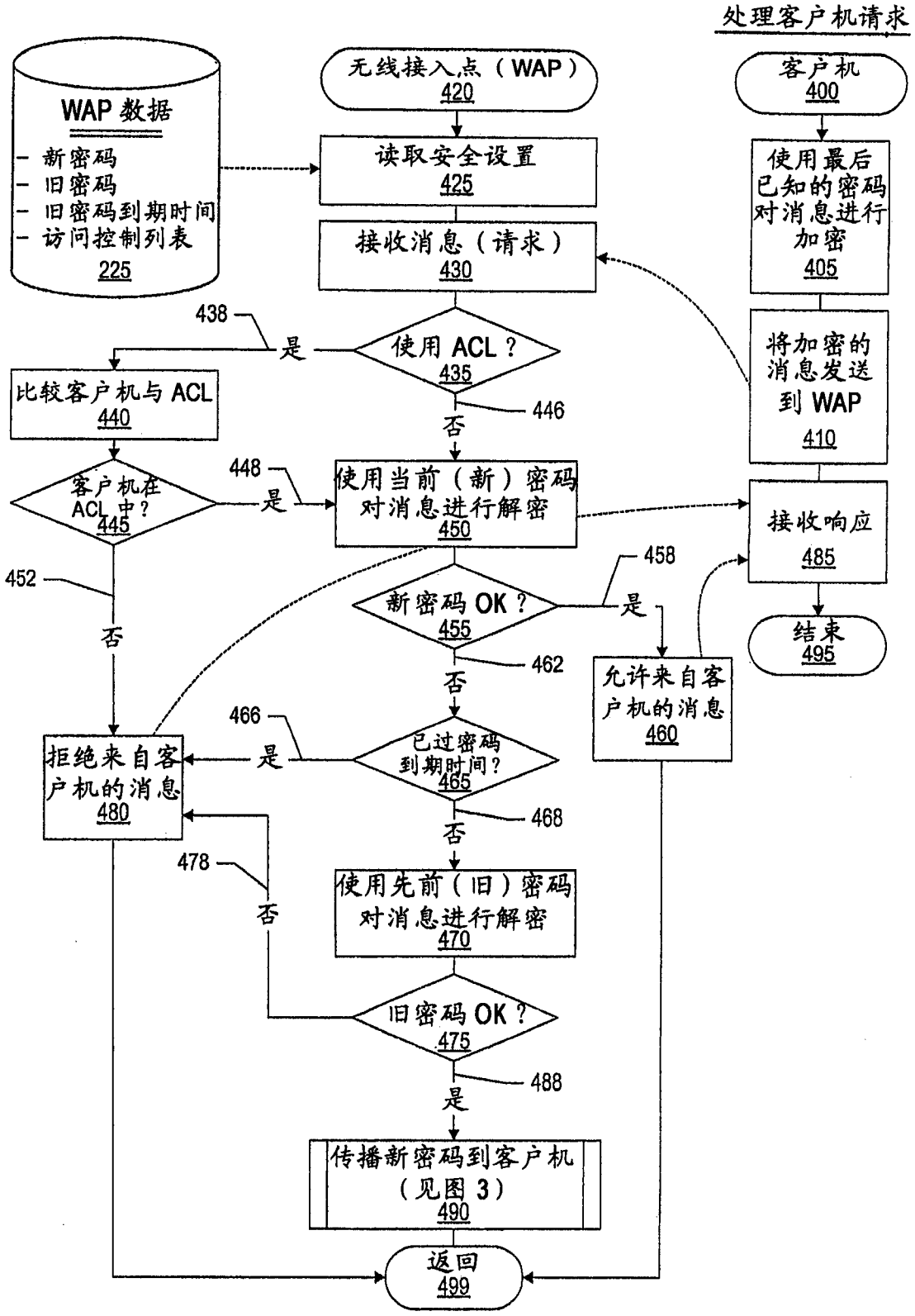

处理客户机请求
WAP 数据
- 新密码
- 旧密码
- 旧密码到期时间
- 访问控制列表
225
无线接入点（WAP）
420
客户机
400
读取安全设置
425
使用最后已知的密码对消息进行加密
405
接收消息（请求）
430
438
是
使用 ACL？
435
446
否
将加密的消息发送到 WAP
410
比较客户机与 ACL
440
客户机在 ACL 中？
445
448
是
使用当前（新）密码对消息进行解密
450
接收响应
485
452
否
458
新密码 OK？
455
是
结束
495
462
否
允许来自客户机的消息
460
466
已过密码到期时间？
465
是
拒绝来自客户机的消息
480
468
否
478
否
使用先前（旧）密码对消息进行解密
470
旧密码 OK？
475
488
是
传播新密码到客户机（见图 3）
490
返回
499

图 4

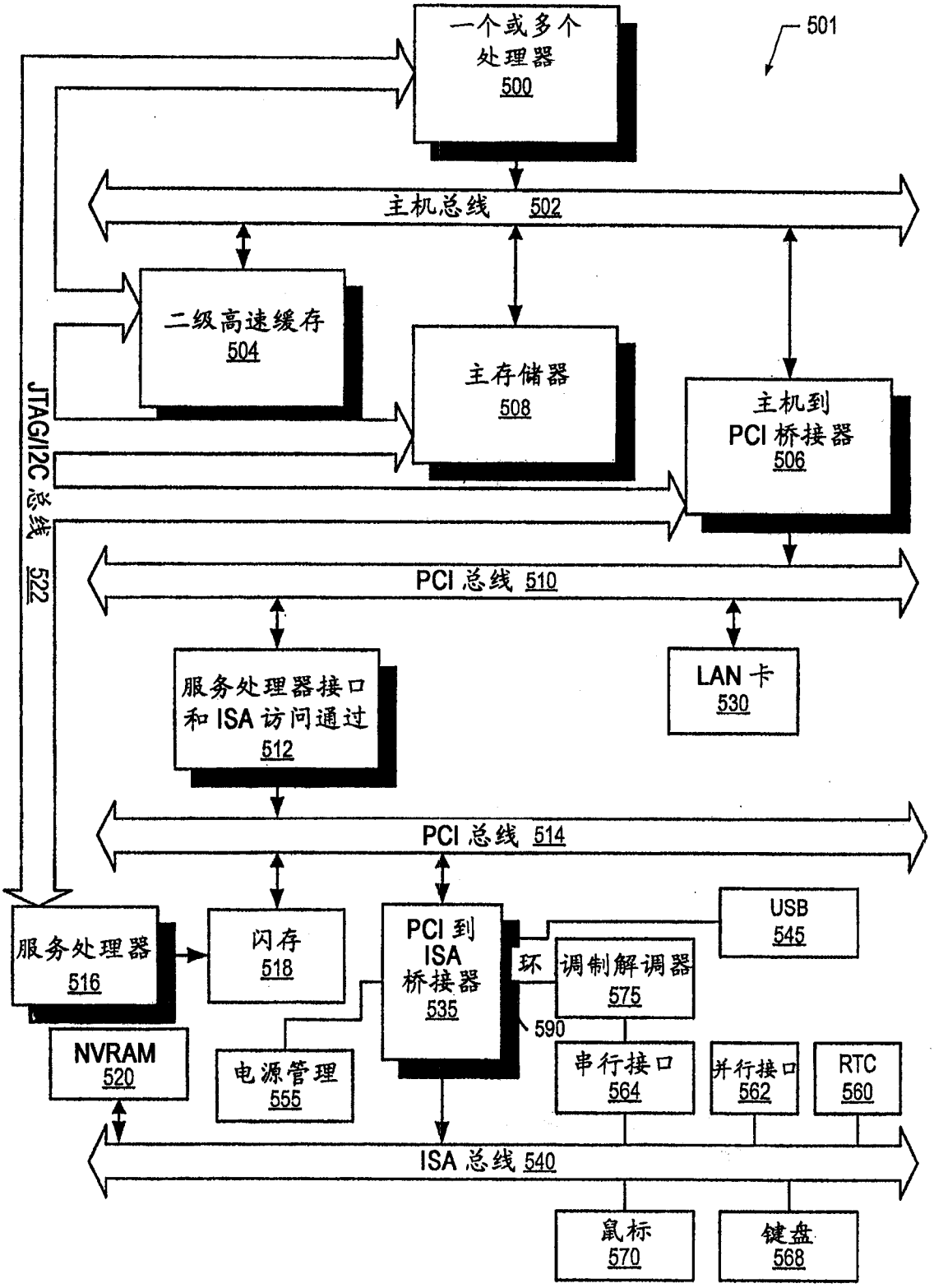

501
一个或多个处理器 500
主机总线 502
二级高速缓存 504
主存储器 508
主机到 PCI 桥接器 506
JTAG/I2C 总线 522
PCI 总线 510
服务处理器接口和 ISA 访问通过 512
LAN 卡 530
PCI 总线 514
服务处理器 516
闪存 518
PCI 到 ISA 桥接器 535
环
调制解调器 575
USB 545
590
NVRAM 520
电源管理 555
串行接口 564
并行接口 562
RTC 560
ISA 总线 540
鼠标 570
键盘 568

图 5