[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/44 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200480007485.1

[43] 公开日 2007 年 1 月 10 日

[11] 公开号 CN 1894661A

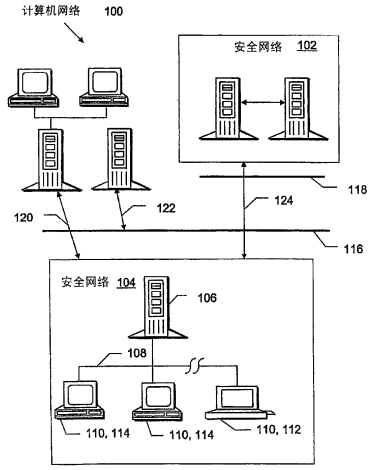
[22] 申请日 2004.3.2
[21] 申请号 200480007485.1
[30] 优先权
[32] 2003. 3.20 [33] US [31] 10/394,447
[86] 国际申请 PCT/US2004/006328 2004.3.2
[87] 国际公布 WO2004/086168 英 2004.10.7
[85] 进入国家阶段日期 2005.9.20
[71] 申请人 派曲林克股份有限公司
地址 美国亚利桑那州
[72] 发明人 S·莫西亚 C·A·H·安德鲁
J·M·戈登 M·培根
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 钱慰民
权利要求书 9 页 说明书 53 页 附图 8 页

[54] 发明名称

非入侵式自动站外补丁指纹识别和更新的系统以及方法

[57] 摘要

提供了方法、系统以及已配置的存储介质，该方法、系统以及已配置的存储介质用于：发现软件更新(232)，找出给定计算机是否能使用该软件更新，然后通过网络(200)用所需的软件来自动更新该计算机。 此外，当检测到故障时(316)，停止该转出(318)并且可以自动地从那些已更新过的计算机中去除该软件。 软件更新最初可存储在经网络防火墙(214)不可访问的一地址处，这是由于该软件更新可中途上载到更新计算机(220)上，其中更新计算机(220)不是网络的一部分但能通过防火墙访问软件包计算机(230)。



1、一种用于在系统中更新软件的自动化的方法，所述系统具有通过网络与处于预更新状态中的更新服务器相连接的处于非更新状态中的第一目标计算机，所述系统也具有所述第一目标计算机不可访问而所述更新服务器可以访问的软件包计算机以及所述第一目标计算机和所述更新服务器都可访问的资源库组件，其特征在于，所述方法包括如下步骤：

把至少一个用来定义特定的软件更新的补丁指纹放入所述的资源库组件；

收集关于所述第一目标计算机的信息；

把所收集到的信息中的至少一部分与所述补丁指纹进行比较，以确定所述特定的软件更新是否不在所述的目标计算机内；

把至少一个任务标识符放置在更新任务列表上，所述任务标识符指定所述第一目标计算机，所述任务标识符也指定至少一个下载地址，该地址是指在所述软件包计算机上的一个位置，所述软件包计算机包含用于所述第一目标计算机的软件更新；

作为对所述任务标识符的响应，把所述软件更新从所述软件包计算机中下载到所述的更新服务器；以及

执行从所述更新服务器到所述第一目标计算机的第二次软件更新下载。

2、如权利要求 1 所述的方法，其特征在于，进一步包括提供补丁定义文件的步骤，所述补丁定义文件是可移植的并可用来在多个网络中复制更新服务器上的补丁。

3、如权利要求 1 所述的方法，其特征在于，所述方法通过在不需要明确管理员命令执行下载步骤的情况下去执行所述下载步骤，提前主动地运行。

4、如权利要求 1 所述的方法，其特征在于，所述方法通过在把所述补丁部署到目标计算机之前把做过标记的补丁高速缓存在所述更新服务器处，提前主动地运行，其中所述补丁标记为关键的、高优先级的以及安全相关的中的至少一种。

5、如权利要求 1 所述的方法，其特征在于，进一步包括来自下列安全

步骤组中的至少两个步骤：利用加密来保护补丁下载；利用循环冗余码来保护补丁下载；利用数字签名来保护补丁下载；利用诸如 SSL 的安全网络协议来保护补丁下载，其中所述安全步骤中的至少一个可用在特定的方法实施例中。

6、如权利要求 1 所述的方法，其特征在于，使用后台下载进程来执行从所述更新服务器到所述第一目标计算机的软件更新下载步骤，由此为所述第一目标计算机用户减少了不便性。

7、如权利要求 1 所述的方法，其特征在于，使用带宽节流下载来执行从所述更新服务器到所述第一目标计算机的软件更新下载步骤，由此允许网络管理员决定在大规模部署期间应如何使用带宽。

8、如权利要求 1 所述的方法，其特征在于，根据限制运行小时数的策略执行下载，所述策略由管理员设置，由此允许所述管理员决定何时允许发生补丁部署。

9、如权利要求 1 所述的方法，其特征在于，进一步包括防止从所述更新服务器到所述软件包计算机的软件更新下载，由此增强了所述软件包计算机的安全性。

10、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括链接式安装特征的使用，所述特征正式地准许管理员把所下载的补丁安装到所述目标计算机上而其重新引导的次数比别它方式所需的要少。

11、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括下载恢复特征的使用，其中所述特征检测下载步骤的中断，然后重新连接，此后在发生所述中断的那个下载步骤中的那一点处或其附近恢复所述下载步骤，由此避免了为完成所述下载重复所述整个下载步骤。

12、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括移动用户支持特征的使用，所述特征允许管理员把补丁部署到所述第一目标计算机，即使在所述任务标识符放置步骤发生时所述第一目标计算机并未连接到所述网络。

13、如权利要求 1 所述的方法，其特征在于，所述方法包括下载源自多家销售商的多个补丁。

14、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括把目

标计算机的合适子集归类以形成一个组的步骤，由此可应用于单台目标计算机的操作也可应用于所述的组。

15、如权利要求 14 所述的方法，其特征在于，所述的归类步骤形成一个包含有由管理员所指定的目标计算机的组。

16、如权利要求 14 所述的方法，其特征在于，所述的归类步骤形成一个包含有由非管理员用户所指定的目标计算机的组。

17、如权利要求 14 所述的方法，其特征在于，所述的归类步骤形成一个包含有通过识别操作系统来指定的目标计算机的组，其中所述操作系统由正在被放入所述的组内的所有目标计算机使用。

18、如权利要求 14 所述的方法，其特征在于，所述的归类步骤形成一个包含有通过识别应用程序来指定的目标计算机的组，其中所述应用程序由正在被放入所述的组内的所有目标计算机使用。

19、如权利要求 14 所述的方法，其特征在于，所述方法进一步包括把有限的管理控制授权给组管理员的步骤，由此所述组管理员仅接收对由所述归类步骤放入所述的组内的那些目标计算机的控制。

20、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括强制性补丁基线策略的使用，其中所述策略至少部分地指定应安装在所述第一目标计算机上的软件，并且所述方法提前主动地下载在所述强制性补丁基线策略中所指定的补丁并将所述补丁安装在所述第一目标计算机上。

21、如权利要求 20 所述的方法，其特征在于，所述强制性补丁基线策略为使用特定应用程序的目标计算机设置基线。

22、如权利要求 20 所述的方法，其特征在于，所述强制性补丁基线策略命令从目标计算机中去除不想要的软件。

23、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括禁用补丁特征的使用，其中所述特征指定不应安装在所述第一目标计算机上的软件，并且所述方法试图防止这种安装的发生。

24、如权利要求 20 所述的方法，其特征在于，所述方法进一步包括在所述补丁中的软件从受所述强制性补丁基线策略影响的目标计算机中丢失之后自动地重装在所述强制性补丁基线策略中所指定的补丁。

25、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括如下步骤：把目标计算机的合适子集归类以形成一个组，以及使用强制性补丁基线策略以至少部分地指定应在所述的组中的目标计算机上安装的软件。

26、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括补丁配合保证特征的使用，其中所述特征指定在所述第一目标计算机上被加锁的软件，并且如果加锁软件被人从所述第一目标计算机中去除，所述方法会提前主动地通知管理员。

27、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括改变控制特征的使用，其中所述特征指定在所述目标计算机上被加锁的至少一个项目，并且所述方法提前主动地通知管理员在所述目标计算机上加锁项目是否被改变，其中所述项目是硬件项目、服务项目和软件项目中的至少一种。

28、如权利要求 1 所述的方法，其特征在于，至少从所述更新服务器到所述第一目标计算机的软件更新下载的步骤会重复，由此至少在所述第一目标计算机上不断地更新特定的文件。

29、如权利要求 1 所述的方法，其特征在于，进一步包括来自灾难恢复步骤组中的至少一个步骤，所述的步骤在系统出故障之后帮助管理员恢复并继续运行，其中所述灾难恢复步骤组包括：创建与出故障的服务器域名相同的另一个服务器；在服务器上重装更新服务器软件；恢复归档数据；以及恢复镜像数据，并且其中所述灾难恢复步骤中的至少一个可用在特定的方法实施例中。

30、如权利要求 1 所述方法，其特征在于，进一步包括维持最近的操作记录以及回退补丁的部署这样的步骤，由此允许管理员撤消已发生问题的目标计算机补丁安装。

31、如权利要求 1 所述的方法，其特征在于，所述方法进一步包括智能多补丁部署特征的使用，其中所述特征使补丁与目标计算机操作系统相匹配，由此正式减轻管理员需要清楚且完全地识别在所述目标计算机上使用的操作系统这样的负担。

32、如权利要求 1 所述方法，其特征在于，所述方法在所述第一目标计算机上安装安全补丁，由此为管理员提供了策略驱动方法以钩连到所述目标计算机的文件系统中并使至少一个特定文件停止在所述目标计算机上的运行。

33、一种已配置的程序存储介质，其配置所代表的数据和指令会使计算机系统的至少一部分来执行用于在所述系统中更新软件的自动化方法中的诸多方法步骤，所述系统具通过网络与处于预更新状态中的更新服务器相连接的处于非更新状态中的第一目标计算机，所述系统也具有所述第一目标计算机不可访问而所述更新服务器可以访问的软件包计算机以及所述第一目标计算机和所述更新服务器都可访问的资源库组件，其特征在于，所述方法包括如下步骤：

把至少一个用来定义特定的软件更新的补丁指纹放入所述的资源库组件；

收集关于所述第一目标计算机的信息；

把所收集到的信息中的至少一部分与所述补丁指纹进行比较，以确定所述特定的软件更新是否不在所述的目标计算机内；

把至少一个任务标识符放置在更新任务列表上，所述任务标识符指定所述第一目标计算机，所述任务标识符也指定至少一个下载地址，其中该下载地址是指在所述软件包计算机上的一个位置，所述软件包计算机包含用于所述第一目标计算机的软件更新；

作为对所述任务标识符的回应，把所述软件更新从所述软件包计算机中下载到所述的更新服务器；以及

执行从所述更新服务器到所述第一目标计算机的第二次软件更新下载。

34、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括提供补丁定义文件的步骤，其中所述的补丁定义文件是可移植的并可用来在多个网络中复制更新服务器上的补丁。

35、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法通过在不需要明确管理员命令执行下载步骤的情况下去执行所述下载步骤，提前主动地运行。

36、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法通过在把所述补丁部署到目标计算机之前把做过标记的补丁高速缓存在所述更新服务器处，提前主动地运行，其中所述的补丁标记为关键的、高优先级的以及安全相关的中的至少一种。

37、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括来自下列安全步骤组中的至少两个步骤：利用加密来保护补丁下载；利用循环冗余码来保护补丁下载;利用数字签名来保护补丁下载;利用诸如 SSL 的安全网络协议来保护补丁下载，其中所述安全步骤中的至少一个可用在特定的方法实施例中。

38、如权利要求 33 所述的已配置的存储介质，其特征在于，使用后台下载进程来执行从所述更新服务器到所述第一目标计算机的软件更新下载步骤，由此为所述第一目标计算机用户减少了不便性。

39、如权利要求 33 所述的已配置的存储介质，其特征在于，使用带宽节流下载来执行从所述更新服务器到所述第一目标计算机的软件更新下载步骤，由此允许网络管理员决定在大规模部署期间应如何使用带宽。

40、如权利要求 33 所述的已配置的存储介质，其特征在于，根据限制运行小时数的策略执行下载，所述策略由管理员设置，由此允许所述管理员决定何时允许发生补丁部署。

41、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括防止从所述更新服务器到所述软件包计算机的软件更新下载，由此增强了所述软件包计算机的安全性。

42、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括链接式安装特征的使用，所述特征正式地准许管理员把所下载的补丁安装到所述目标计算机上而其重新引导次数会比别它方式所需的要少。

43、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括下载恢复特征的使用，所述特征检测下载步骤的中断，然后在重新连接后，在发生所述中断的那个下载步骤中的那一点处或其附近恢复所述下载步骤，由此避免了为完成所述下载重复所述整个下载步骤。

44、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括移动用户支持特征的使用，所述特征允许管理员把补丁部署到所述第一目标计算机，即使在所述任务标识符放置步骤发生时所述第一目标计算机并未连接到所述网络。

45、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法包

括下载源自多家销售商的多个补丁。

46、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括把目标计算机的合适子集归类以形成一个组的步骤，由此可应用于单台目标计算机的操作也可应用于所述的组。

47、如权利要求 46 所述的已配置的存储介质，其特征在于，所述的归类步骤形成一个包含有由管理员所指定的目标计算机的组。

48、如权利要求 46 所述的已配置的存储介质，其特征在于，所述的归类步骤形成一个包含有由非管理员用户所指定的目标计算机的组。

49、如权利要求 46 所述的已配置的存储介质，其特征在于，所述的归类步骤形成一个包含有通过识别操作系统来指定的目标计算机的组，其中所述操作系统由正在被放入所述的组内的所有目标计算机使用。

50、如权利要求 46 所述的已配置的存储介质，其特征在于，所述的归类步骤形成一个包含有通过识别应用程序来指定的目标计算机的组，其中所述应用程序由正在被放入所述的组内的所有目标计算机使用。

51、如权利要求 46 所述的已配置的存储介质，其特征在于，所述方法进一步包括把有限的管理控制授权给组管理员的步骤，由此所述组管理员仅接收对由所述归类步骤放入所述的组内的那些目标计算机的控制。

52、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括强制性补丁基线策略的使用，其中所述策略至少部分地指定应安装在所述第一目标计算机上的软件，并且所述方法提前主动地下载在所述强制性补丁基线策略中所指定的补丁并将所述补丁安装在所述第一目标计算机上。

53、如权利要求 52 所述的配置存储介质，其特征在于，所述强制性补丁基线策略为使用特定应用程序的目标计算机设置基线。

54、如权利要求 52 所述的已配置的存储介质，其特征在于，所述方法进一步包括在所述补丁中的软件从受所述强制性补丁基线策略影响的目标计算机中丢失之后自动地重装在所述强制性补丁基线策略中所指定的补丁。

55、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括如下步骤：把目标计算机的合适子集归类以形成一个组，以及使用强制性补丁基线策略以至少部分地指定应在所述的组中的目标计算机上安装的

软件。

56、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括补丁配合保证特征的使用，其中所述特征指定在所述第一目标计算机上被加锁的软件，并且如果加锁软件被人从所述第一目标计算机中去除，所述方法会提前主动地通知管理员。

57、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括改变控制特征的使用，其中所述特征指定在所述目标计算机上被加锁的至少一个项目，并且所述方法提前主动地通知管理员在所述目标计算机上加锁项目是否被改变，其中所述项目是硬件项目、服务项目和软件项目中的至少一种。

58、如权利要求 33 所述的已配置的存储介质，其特征在于，至少从所述更新服务器到所述第一目标计算机的软件更新下载的步骤会重复发生，由此至少在所述第一目标计算机上不断地更新特定的文件。

59、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括来自灾难恢复步骤组中的至少一个步骤，所述的步骤在系统出故障之后帮助管理员恢复并继续运行，其中所述灾难恢复步骤组包括：创建与出故障的服务器域名相同的另一个服务器；在服务器上重装更新服务器软件；恢复归档数据；以及恢复镜像数据，并且其中所述灾难恢复步骤中的至少一个可用在特定的方法实施例中。

60、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括维持最近的操作记录以及回退补丁的部署这样的步骤，由此允许管理员撤消已发生问题的目标计算机补丁安装。

61、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法进一步包括智能多补丁部署特征的使用，其中所述特征使补丁与目标计算机操作系统相匹配，由此正式减轻管理员需要清楚且完全地识别在所述目标计算机上使用的操作系统这样的负担。

62、如权利要求 33 所述的已配置的存储介质，其特征在于，所述方法在所述第一目标计算机上安装安全补丁，由此为管理员提供了策略驱动方法以钩连到所述目标计算机的文件系统中并使至少一个特定文件停止在所述目标计

算机上的运行。

非入侵式自动站外补丁指纹识别和更新的系统以及方法

版权声明

发明领域

本发明涉及能更新远程网络上现有软件的系统和方法，尤其涉及检查更新的需求然后按客户机服务器系统的需求更新该软件，而不需人工监督，也并不要求目标网络管理机保留软件补丁的副本。

发明背景

计算机软件工业中的“技术发展水平”保持这样：常常交付在它期望性态中包括各种异常的软件。这些异常性态已经称作为“缺陷”。

原始的计算机程序缺陷是在美国哈佛大学 Mark II Aiken Relay 计算器的运行日志，现在保存在史密森。操作员取出已经陷在继电器开关之间的蛾，并记下“发现第一个缺陷的实际情况”条目。以后，计算机的硬件和软件问题称作为“缺陷”，而解决问题的处理过程称作为“缺陷排除”。

每次进行软件“缺陷排除”，对一段程序进行修改---这修改有时导致称作为“补丁”或“修复”另一块软件程序。工业的软件销售商常常由更正式的名称“服务包”或“支撑包”来称呼这些补丁。

这个过程在工业上变得如此地普遍，以致软件销售商用各种命名和编号方案来跟踪他们可用“支撑包”。当销售商未能对命名和编号方案达成一致时，直接增加了跟踪这些支撑包的难度。

微软，例如对操作系统产品的视窗 NT 系列，具有能用于解决用户或许

会经受的问题的不小于6个主要“服务包”。更普遍地，对于任何给定系统，补丁，修复，解决方案，和/或服务包的总数量是巨大的。

当安装应用软件时，它可包括一个或多个这些操作系统文件补丁，连同准则计算机文件。因为应用软件销售商发现在一个或多个操作系统文件中的一些异常运行状态，通常包括这些补丁，并因此按这些麻烦文件中的一个文件的不同版本格式发送一个“修复”。如果仅一个应用软件销售商执行这种服务，或如果由应用软件销售商修改的文件仅由那销售商应用软件使用，这引起的困难相对较少。然而，这常常不是实际情况。

当安装另一个应用软件时，该应用软件可包含更近版本的共享代码块。这些共享操作系统文件的一个子集，称作为DLL（动态链接库），虽然它们可有其他名称。这些共享操作系统文件通常是可执行的，并期望有固定量的参数，某些类型的参数，等等。如果该共享文件的性质已经改变了（例如，参数集不同，名称不同，特性不同），该调用应用软件不再能正确运行。按这种方式涉及例如“打印”的许多公共计算机特性。

许多软件销售商企图提供“最近”版本的操作系统文件。然而，当不同的应用软件装载到计算机内时，它可能重写或精细地（或不那么精细）改变操作系统文件，原应用软件要求该操作系统起到按计划的特性。

假定一个组织的管理员负责维持一百台服务器和运行，同时支持三千个用户连接到这些服务器。该管理员还负责安装用户请求或管理规定的应用软件--- 紧缩套装购买（shrink wrapped purchase）或内部研制应用软件。管理员还有负责时间敏感文件的本地或远程的及时分配。

现在设想：6个服务包必须安装到网络上，并分配给所有客户机。应用这6个服务包能轻易地导致对这百个服务器中的每个和每一个的7次访问，总共有700次访问。这数字包括假定每台机器一次额外访问，因为一个服务包的应用可比它修复能引起更多问题，因此必须撤销这么做。

如果三千个客户机都在运行相同的工作站操作系统，这意味着应用这些补丁的另外的21000次访问。记住：在安装和修补内部研制应用软件和收缩包产品的同时必须完成所有这一切。软件补丁和文件的分配及它们随后的应用变成：可称作为“管理员苦脑”的第一迹象。

当出现所有这些安装时候，还必须监视单个服务器。当一个服务器要求注意时，管理员常常与另一个疯狂报告他们的服务已停机及必须修理的人员接触。如果管理员有某些方法来监视这些设备，他或她变得更负责并能进一步减少问题的影响。监视的要求是“管理员苦脑”的第二迹象。管理员工作中存在很高的翻覆，并这些系统的用户可经受较低的生产力。

传统地，管理员已经受到配以其他职工的帮助。当然，这种补救不可能不存在问题—额外人员将增加他们之间通信信道数。安装和更新人员要求跟踪设备或系统，因此他们不能执行或企图执行相同的工作单元。这种各队员之间缺乏协调性是“管理员苦脑”的第三迹象。

提议的解决方法当前可用在各种格式，执行，及覆盖或完成性中。典型地，这些提议的解决方法可用作为紧缩套装产品，这些可在管理员环境下本地安装(例如，可修补)。某些紧急产品是有帮助的，但许多传统的解决方法是入侵式的，它们要求管理员环境的大块修改。这收缩包解决方法要求在管理员网络中的附加入侵式全产品安装，由此，添加到该问题上，并缺乏集中式的“强制性中心”来协调支持或分配计划。紧急解决方法可提供稍微有些较少程度的入侵，但虽然如此，在管理员和解决方法之间要求特别连接，并它们常不提供用于协调努力的中心。

此外，即便要，也不总是显而易见地确切已经接收什么补丁块给定软件。更新不会总是清楚地宣布它们的存在。因而，不会总是清楚：某一特定计算机是否已经先前接收到某一特定补丁。因此，存在一种要求：用于更新网络计算机的改进工具和技术。这儿描述和声称这样的工具和技术。

发明内容

本发明涉及方法、物件（articles）、信号以及系统，它们用于确定软件是否需要更新，以及如果需要更新则在减少管理员命令的情况下通过网络来更新该软件。如果该更新出现故障，则已安装该更新软件的计算机可恢复到未更新状态。本发明由所附的权利要求书来定义，该权利要求书优先于本发明内容。

在各种实施例中，通过网络本发明基于多个操作系统和设备上的软件和补丁指纹识别（patch fingerprinting）来促进软件部署、软件安装、软件更新以

及文件分配。具有网络连接并具有在其上运行的更新代理的任何计算机都可连接到更新服务器，并接着处理管理员已为该代理指定的无论什么任务。

图 2 示出这样一种系统的概况，网络 200，为了简化描述，仅示出两台目标计算机和一台更新计算机，是由防火墙 214 保护，免受互联网的影响。要求更新网络目标计算机 202 和 208 的软件驻留在软件包计算机 230 和 234 内，这两台计算机位于防火墙的内部或外部，并由防火墙阻挡，避免直接与目标计算机 202、208 进行通信。然而，更新服务器 220 能接入网络 200，潜在地穿过内部防火墙—以及经过防火墙 214 访问。该系统设计成：既作为界内（onside）购买的解决方法，也作为全界外（offside）的解决方法，并能经过防火墙和代理服务器电路（proxy circuit），以内联网/外联网的基础结构内的任何级别运行。

补丁指纹 902 给出一个处方，以允许资源库组件确定某一给定软件包（与补丁指纹 902 相关），补丁，驱动器等是否应当装载进该系统的计算机。这些指纹储存在补丁组件数据库存储位置 900，该数据库存储位置 900 可在防火墙 214 的内部或外部。它可在一个分开位置或它可以安装在更新服务器 528 上。该资源库组件可包括目录库数据库 918，该目录库数据库 918 包括有关每个网络目标计算机 202，208 的基本硬件和软件信息。使用补丁指纹，目录库内的信息，及从每台网络目标计算机收集的特定信息，该系统能够智能地推荐那些补丁和驱动器是某一台给定计算机所要求的。

如图 5 所示，本发明较佳实施例应用称作为发现代理 548 的附加代理，安装在目标计算机 500 上，它例行公事地发现那机器上的硬件和软件。然后，将这目录信息回报给位于目录组件内的某个地方的目录库 918。除了计算机目录外，发现代理还回退补丁指纹的扫描结果，该扫描结果表示它是否适合于安装与每个补丁指纹相关的特定补丁。

这样，目录数据库收集安装在网络内任何特定目标计算机内的软件，硬件和当前补丁指纹的完整目录。用这信息，更新服务器 528 能将网络内所有计算机的当前补丁状态的详细报告呈现给用户。这描述了要求补丁的计算机数量以及已用该补丁安装的计算机。

另外，指纹定义 906 通常也与适合于由系统部署的更新包相关联。一旦

通过扫描网络内所有或任何计算机上的它的签名已经建立了特定补丁的需求，然后通过仅选择日期和时间，由管理员快速地将它部署。

在某些实施例中，指纹定义 906 可与下面中的一个或多个相结合，以形成便携式补丁定义文件：讨论该补丁的销售公告，由本发明实施例为管理员准备的报告，目标计算机 500 的签名，部署包。这补丁定义文件提供能用于更新其他网络的信息。该补丁定义文件（又名为“补丁元文件”）提供一种便携式统一数据表示法，这种表示法可由本发明实施例使用，以移动或复制在不同网络的更新服务器 528 之中的补丁。合适的网络 100 包括未连接到互联网和/或未互相连接的无限制网络，例如，被隔绝以提供更加安全的军用网。这移动/复制可通过电子邮件，磁带读/写，和/或其他传统的数据传送装置来进行。补丁元文件也有助于由不同销售商提供的本发明实施例之间的补丁的交换性和互操作性。

要求装载进特定目标计算机的补丁在更新列表 222 的更新服务器 220 上列出，所述更新列表与更新代理 204，210 相关联；在描述中，列表 224 是与目标 1 202 相关联，而列表 226 与目标 2 208 相关联。该更新列表至少指明一个位置（经过例如通用资源定位器，或 URL），在该位置可找到补丁，并较佳地包括能安装该软件的最早日期。

在运行时，目标 1 202 的更新代理 204 检查在界内或界外更新服务器 220 上的它的更新列表 224，以查看是否应安装一个新包。如果存在一个，更新代理 204 检查以查看更新服务器 220 的存储器内是否已存在该新包。如果是，更新代理 204 企图从更新服务器 220 直接安装该软件补丁。如果否，更新代理 204 企图从软件包计算机位置 232 直接安装软件补丁。在某些情况中，这是成功的，在这种情况中，更新了更新列表 224。

在其他情况中，下载 218 将由防火墙 214 阻止。如果这种情况发生，更新代理 210 通知更新服务器 220，并然后更新服务器 220 本身将企图检索该包，并将它放置在存储器 228 内。从该更新服务器的存储器内将该软件直接安装到目标机内。

监视器检查该软件适当地安装在目标 202，208 上，并然后继续检查（或能被通知），以保证更新软件正确地运行，并保证目标计算机本身不会经受呈

现为不相关区的任何问题。倘若该包未能适当安装，或对要修补的软件程序产生问题，或在目标计算机上产生其他问题，该包能自动地去除并计算机恢复到它先前安装的状态，或更新已被去除或被禁止的另一种可接受状态，并且目标计算机处于可工作状态。如果该包已经安装在多于一台计算机上，他们都能去除。如果在转出到许多计算机的中间发生错误，该次转出可中止并且该软件可去除或禁止。该监视器可位于更新器服务器 220 上，资源库站点 600，至少部分地在更新代理 204，210，和/或在这些位置的组合上。

当安装中存在问题时，或当安装成功时，能通过电子邮件，寻呼机，或通过某些其他通告装置通告管理员。

更新代理 204，210 也能用于调查它自己的目标计算机，并且这信息能储存在数据库界外或其他位置。那么，这信息可用于确定：某一给定目标计算机要求更新什么才能具有量最佳配置。当一个新软件补丁变成可用时，储存的信息能用于确定某一特定目标计算机是否要求该补丁。

应当注意到：目标计算机可包括任何类型的服务器或工作站，不管操作系统或安装的软件。而且，本发明的范畴应用于许多其他装置，包括：无线电装置（移动电话，个人数字助理，便携式计算机等），智能交换机装置，网络集线器，路由器，及任何其他类型的互联网附加装置。

通过下列描述将更能完全明白本发明的其他方面和优点。

附图简述

为了描述能获得本发明优点和特征的方式，将参考附图给出本发明的更特别的描述。这些附图仅描述本发明的所选择的方面，并且这样不限制本发明的范畴，在附图中：

图 1 是一张图，描述依据本发明的适合使用的许多分布式计算系统中的一种；

图 2 是描述依据本发明的系统的一张图；

图 3 是描述依据本发明方法的一张图；

图 4 是进一步描述依据本发明的方法的一张图

图 5 是进一步描述依据本发明的系统的一张图；

图 6 是进一步描述依据本发明的系统的一张图；

图 7 是进一步描述依据本发明的系统的一张图；

图 8 是进一步描述依据本发明的方法的一张图；

图 9 是进一步描述依据本发明的系统的一张图

较佳实施例描述

本发明提供有助于更新远程网络上现有软件的系统，方法，项目，及信号。更特别地，本发明涉及能很少用或不要求人们监督就能更新客户机服务器系统上的软件，并不要求在进行更新的客户机机的网络上的管理机上的软件补丁的复制品。这更新是自动的，并且它能检测某一特定更新内的错误，并自动地将一次故障更新回退（rollback），以将网络保持在可用状态。

这儿讨论的不同的附图描述本发明的各个实施例，但某一给定图的讨论不需限制于某一特定类型的实施例。例如，那些技术熟练人员将理解：这些发明的方法也可用在依据本发明的配置存储介质和/或计算机系统实现。为了防止不要求的重复，这些方法的讨论应用于制品和系统，并反之亦然，除非另外指明。还将理解：方法步骤或系统组件可重命名，重组，重复或省略，并且方法步骤可被不同地排序，和/或按重叠执行地进行，除非按适当理解的权利要求要求特殊步骤或组件和/或要求某一特定的执行顺序。

为了读者的便利，下面提供某些有关例如网络和防火墙的相关技术的信息。本发明越出先前已知技术，但可部分地包括或依赖于计算和连网中的早期发展或/或与这样的早期进展一起使用。

一般系统

如图 1 所示，例如安全计算机网络 102，104 的计算机网络 100 可依据本发明配置。作为例子，适合的计算机网络 100，102，104 包括：局域网，广域网，和/或部分互联网。如这儿所用的“互联网”包括例如私人互联网，安全互联网，增值网，虚拟私人网，或内联网的各种网络。安全网络可用安全边界来保护，所述安全边界是由防火墙 116，118，路由限制，密码，虚拟私人连网，和/或其他装置来定义。网络 100，102，104 也可包括或包括安全内联网，是一种例如内部应用 TCP/IP 和/或 HTTP 协议的局域网的安全网。用于依据本发明

的操作由网络连接的计算机 110 可以是工作站 114，膝上型计算机 112，可断开的移动计算机（例如 PDA（个人数字助理）或其他无线装置），服务器，计算机群，大型机，或其组合。计算机硬件可以是通用，专用，单机，和/或嵌入式。网络 100 可以包括其他网络，例如一个或多个局域网，广域网，无线网络（包括红外线网），互联网络服务器和客户机机，内联网服务器和客户机机，或其组合，这些可由它们自己的防火墙保护。

一个给定网络 100 可以包括 Novell Netware®网络操作系统软件（NETWARE 是一个 Novell 公司的注册商标），NetWare 连接服务器，VINES，视察 NT，视窗 95，视窗 98，视窗 2000，视窗 ME，视窗 XP，视窗 2K3，LAN 管理，或 LANtastic 网络操作系统软件，UNIX，TCP/IP，AppleTalk 和 NFS 基系统，分布式计算环境软件，和/或 SAA 软件，例如（VINES 是 Banyan 系统的商标；NT，视窗 95，视窗 98，视窗 2000，视窗 ME，视窗 XP 和 LAN 管理器是微软件公司的商标；LANTASTIC 是 Artisoft 的商标；SAA 是 IBM 的标记）。网络可包括可通过网关或类似装置可连接到其他网络的局域网。

一种依据本发明的系统包括一个或多台服务器 106，由网络信号线 108 连接到一个或多个网络客户机 110。服务器和网络客户机可由那些技术熟练人员按无数种方法配置，以依据本发明运行。服务器可配置成互联网服务器，内联网服务器，目录服务提供器或名字服务器，软件服务器，文件服务器，或这些和其他特性的组合。这些服务器可以是单处理器或多处理器机器。服务器 106 和客户机机 110 每个包括例如随机存储器的可寻址存储介质和/或例如磁盘或光盘的非易失存储介质。信号线 108 可包括双绞线，同轴线，或光纤电缆，电话线，卫星，微波中继，调制 AC 电源线，和那些技术熟练人员已知的其他数据传输“导线”，包括无线连接。依据本发明的信号可以被体现在这种“导线”和/或在可寻址存储介质内。

除了网络客户机机计算机外，打印机，硬盘阵和其他外围设置可以附加到一个特定系统。一台给定计算机可起客户机机 110 和服务器 106 两者的特性；例如这可以发生在运行微软视窗 NT 软件的计算机上。虽然提到特定的单台或网络计算机系统和组件，那些技术熟练人员将赏识：本发明也与各种其他网络和计算机一起工作。

本发明的合适软件和/或硬件的实现可由那些技术熟练人员使用这儿呈现的技术和编程语言及工具轻易地提供，所述编程语言和工具例如为 Java，Pascal， C++，C，Perl，外壳文稿程序（shell scripts），汇编，固件，微码，逻辑阵，PAL，ASIC，PROMS，和/或其他语言，电路或工具。

一般配置的介质

服务器 106 和网络客户机 110 及单台计算机 110，114 能使用软盘驱动器，磁带驱动器，光驱动器或其他装置以阅读一种存储介质。合适的存储介质包括：磁，光，或其他计算机可读存储装置。合适存储装置包括：软盘，硬盘，磁带，CD-ROM（光盘只读存储器），PROM（可编程只读存储器），RAM（随机存储器）和其他计算机系统存储装置。基底配置表示能使计算机按这儿描述的某一特定和预定方式运行的数据和指令。这样，介质可有形地嵌入可由服务器和/或网络客户机机计算机和/或单台计算机执行的程序，特性，和/或指令，以执行如这儿充分描述的本发明的更新，监视，管理和/或其他步骤。

防火墙

网络管理员一般不允许任何信息进入它们的系统。而是，他们使用防火墙 16，118 以保护网络。防火墙是能屏蔽输入信息（常基于内容，起源，或请求性质）并仅允许确认为安全的那些信息通过硬件和/或软件装置。三种主要类型的防火墙是筛选路由器（也称作为包过滤器），代理服务器电路层网关，代理服务器应用层网关。筛选路由器能底层决定有关网络包的外部信息，例如它的域名和 IP 地，因此，来自可接受域名和 IP 地址的信息允许经过 120，124，同时拒绝来自其他位置 122 的信息。当将信息传递给外部系统时，代理服务器电路层网关伪装有关内部系统的信息。内部计算机的 IP 地址典型地由代理服务器的 IP 地址替代。在这一层，要求鉴定。代理服务器应用层网关提供筛选路由器和电路层网关的所有特性，同时也允许它们自己对包内容进行评估。因为内容以及妨碍安全，可拒绝信息。

软件安装

系统管理员经常要求改变某一特定机器上的软件。因为当一块新应用软件添加到一台机器上时，一个新软件必须第一次安装。因为当在一台特定机器上要安装一个已有软件的新版本时，能更新（升级）一个已安装的软件；这也

称作为“替代”该软件。因为当在记录程序上更新税表时，或当更新防病毒软件时，一块已有软件的数据文件也可更新，而不需另外改变软件配置。如果在一块已有软件中发现问题时，那么能安装一个修复（fix）或补丁。对某台特定机器或多台机器的任何或所有这些改变在这个专利被称作为“安装”。类似地，词“包”，“补丁”，和“更新”应给予最广泛的可能含意。例如，包涉及包括所有必须文件的整个程序，一个或多个数据文件，对已有文件的软件补丁，对配置文件的修改，一个*.dll 文件，用于将一个特定硬件添加到一台计算机和/或计算机网络的驱动文件，等等。“更新”至少涉及企图将一个包安装到一台计算机。

一般方法

参考图 3，4 和 5，依据本发明运行的一种方法的一个实施例包括处于预更新状态的目标计算机 500。该目标计算机 500 是本发明至少企图更新的计算机；不是本发明的每个实施例都要求成功地更新。一台更新服务器 528 跨过网络 524 连接到目标计算机。在某些实施中，目标计算机具有网络连接，例如是经过 Winsock 层的连接。典型地，该目标计算机是由受防火墙 526 保护，如上面解释的，但是该更新服务器能穿过防火墙访问目标计算机。

许多现有企业软件管理工具使用代理。例如包括微软 SMS 软件，微软动态目录软件。IBM Tivoli 产品，Symantec 防病毒软件，McAfee 防病毒软件，及 Novell ZEN 工作软件（它们是各自拥有者的标记）。在大规模网络中，当有信息要报告时，代理可唤醒并且平行地报告给服务器。相反，缺代理的工具依赖远程 API 调用，哪些是由服务器连续地轮询，使它们在性能上可线性地缩放，而不是在较佳实施例中所见的平行地处理。

本发明实施例中的代理能接收压缩文件，以保存网络带宽。压缩也能增强安全性，因为解压缩差错可指明一个补丁已经被损害。

当承载代理的移动目标被断开时，一个本发明的代理也能恢复下载，并然后在另一位置重新连接到网络上，不象缺乏代理的补丁管理工具，并因此在中断后，下载整个服务包或文件。因为补丁被部署，缺代理的工具也可在带宽利用中产生未控制的尖峰信息，然而，本发明的某些实施例允许一台更新服务器由管理员控制，所以，该服务器每次代理连接仅使用指定量的带宽(带宽节

流)。

依赖永久 LAN/域连接和缺乏客户机机代理的传统补丁工具可依赖于远程注册服务，远程注册服务将注册信息提供给远程计算机。远程注册服务不能用在视窗（Windows）95，视窗 98，或视窗 ME 平台。这样，一次服务可能是其客户机计算机是在互联网的组织中的一次安全冒险，因为它们允许远程计算机阅读客户机的注册，由此提供了能用于引导渗透或其他攻击客户机机安全的信息。因为安全风险，本发明实施例较佳地避免使用远程注册服务。

更新代理 508 位于有待更新的每台计算机上。更新代理是软件组件（通常不很大），或按传统方式或通过使用本发明，可以初始安装在例如工作站和/或服务器的网络目标机上。更新代理能在人们管理员的地方运行，在人们管理员的指引下运行，以与如人们管理员实际在该机器上执行时相类似的方式执行操作。更新代理知道怎样执行四种基本任务：1） 怎样接触更新服务器 528 以检索任务列表，2） 怎样启动接收的任务列表内的任务，3） 怎样处理运行数小时的策略信息等，及 4） 怎样向更新服务器登记。

更新代理能更新，配置，或替代它自己，不要求在初始安装后的人工干预。典型地可最初安装一个小的自举代理，但当管理员指示或当请求实现管理员请求时，其能力将增强。不同种类目标计算机 500 的更新代理，例如界内管理员计算机，服务器计算机，和客户机机，都能按与单代理相同版本启动。某一给定网络内的机器都能把一个相同代理安装好，或机器能把唯一的代理安装好。当存在不至一个客户机时，每个客户机最初可有一个不同的更新代理，或当由管理员选择时，或当设置为缺省时，可将代理的混合安装在不同客户机机上。类似地，多台服务器和管理员也可最初把不同代理的混合安装好。因为单台目标计算机的代理的改变，它们都齐声改变，或它们能脱离。在某些实施例中，代理都可不同地出发，并然后在特性上会聚一起。

更新服务器 528 的界外位置是远离于目标计算机的一个位置。该位置可以是在一个完全不同的销售商的界外，或与目标计算机 500 不同物理位置的界外，但在由相同实体管理的位置，在相同物理位置。它也可在离目标计算机 500 不同的出现位置，例如在转包商位置，或在某些其他独特出现位置。 重点是直到涉及单个目标计算机操作系统，工作似乎是界外。一个实施例将更新服务器

定位在目标计算机 500，但以一种方式（例如在一不同分区）出现在界外。

要安装在目标计算机的实际更新材料经常储存在远离更新服务和目标计算机的一个不同位置（称作为软件包计算机）。软件更新本身可以是能在网络上更新的任何广泛的各种软件，例如递增软件补丁，目标计算机上从未安装过的一个新软件程序，对旧程序的一次更新，软件脚本（software script），数据文件，或甚至更新代理的一个更新。

如未满足一个已知条件，在放置步骤 300 期间，一个任务 id 放置在更新任务列表 222 上。该已知条件可以是：补丁当前未在计算机上，管理员已经给予同意，目标计算机 500 的拥有者已得到包拥有者的允许，没有一个人特别拒绝放置特权的事实，或某些其他已知或发明的条件。位于更新服务器的更新任务列表与特定目标计算机 500 相关联，并至少指明能够找到软件更新的一个下载地址。该下载地址可让计算机能理解的任何格式。本发明不依赖于任何指定的协定。当前使用的两个公共寻址格式是“统一资源定位符（Universal Resource Locator）”和“全资格域名（fully qualified domain name”格式。其他的格式是 PURL（持续统一资源定位符（Persistent Uniform Resource Locators））和 URN（统一资源名），及其他命名方案可在将来知道。将首先尝试下载包含在任务识别符内的其他信息，例如的日期。多个下载地址，它们中的每个指明能找到软件更新的一个位置，都可以与特定软件更新相关联。

在启动任务步骤 304 期间，软件更新至少试图从软件包计算机 567 上载到更新服务器 528。在可任意选择的软件包计算机步骤 306 期间，如果不至一个下载地址放置在任务 id 列表 226 上，选择可下载软件更新的位置。该选择可由任何已知的或发明的方法做出，例如用列表上的第一个位置，用能快速回退（P）16-10 , using … return from most rapidly?）测试信息的位置，用首次可用的机器，等等。

一旦已知用于更新的位置，试图从软件包计算机 548 的位置将软件下载到更新服务器 528 的存储器 530。如果下载不成功，那么按一种发明的方法，从任务更新列表内的可能位置列表中选择另一个位置，并再次尝试下载软件更新。在某些实施中，如果因某原因不能完成下载，更新服务器 528 等待一段时间并再次尝试从软件包计算机 567 下载。如果下载成功，那么，更新服务器 528

试图将软件更新下载 312 到目标计算机 500。

一旦该下载位于更新计算机内的高速缓冲存储器或其他存储器内，试图进行第二次下载，将软件包从更新服务器下载到目标计算机。在该方法的某些实施例中，由某些预定准则延迟 310 第二次下载 312。这延迟可从第一次下载起开始，其延迟周期基于将软件更新从软件包计算机下载到更新服务器所需的时间估计。当目标计算机 500 具有较少的使用机会时，第二次下载也可延迟到一天的特定时间，例如交易结束后的那一天，也可以使用其他已知的或发明的延迟准则。

监视器 302 检查安装，执行通常由管理员所起的角色，以确定安装的结果 314。一旦知道该结果，能通知管理员 328。通知可以是通过发送电子邮件 330，通过无线寻呼某人，通过发送预记录电话消息，或通过任何其他已知的或发明的方法和装置。

如果监视步骤检测到故障 316，那么故障的任务被悬挂 318。倘若到更新服务器 528 的第一次下载 308 故障，从更新服务器 528 到目标计算机 500 的第二次下载也将故障。如果有要安装软件更新的多台目标计算机，第 N 次安装也将故障，将等等。较佳地应确定结果，超出了简单地确保软件更新似乎适当地安装，并在本发明的某些实施例中延伸一段超过安装的时间。例如，监视器的一个实施例通过下面步骤来测试补丁应用：使它仅安装在一台目标计算机上，确信：它适当地下载，安装它，并然后观察它某段时间周期，直到设置时间延迟的管理员在该补丁上获得足够信任，以允许它应用于其他目标计算机为止。这个补丁的应用如引起异常动作，如在其软件修改的程序中或在计算机其他地方的令人讨厌行为所察知的，能自动地悬挂该转入，直到解决该问题为止。

此外，在检测出故障的某些情况中，软件更新被禁止或从目标计算机中去除 324，并且那台机器基本上回退到它预更新状态或另一个可接受（工作）的非更新状态。这可意指：将安装的软件从目标机取走 322；或不仅取走该软件，而且将所有辅助文件（.dll, .exe 文件）恢复到它们预更新状态。在其他情况中，它可意指：在安装软件更新之前，备份目标计算机或其某些部分，并且该备份它自己被恢复到该机器上。

如果有多台目标计算机 500，在软件安装在一台或多台机器上后，由监视

器可检测出故障。在这种情况中，软件更新不仅可从发现故障的目标计算机 500 中去除 322，而且也可从先前安装该软件的所有其他目标计算机 500 中去除 326。该去除请求能来自管理员，或在检测出故障 316 后自动执行去除操作。

监视器 302 比简单地等待倾听是否成功地安装软件包能执行更多的任务。例如，在监视器等待安装后的一段时间周期 400 以及如果它未听到其他消息的某些情况中，确信该安装是成功的。

管理员和管理员帮助者能从中心资源库库获得很多益处，它们能进入该中心资源库库并获取有关帮助请求的信息。一种这样的方法是帮助台“记录单”。记录单记录请求者，请求类型，何时请求帮助，何时完成对该请求的响应，及其他有用信息。PatchLink 帮助台服务给管理员提供便利，以经一个中心资源库库管理它们的网络请求和网络资源，人员和计算机资源两者。PatchLink 帮助台软件在互联网络上提供这些便利，不要求在管理员网络上的入侵式应用安装，那还将引入必须管理，备份，及更新的另外的资源---界外管理中心透明地照顾这种情况。

网站， 通过准则网站浏览器或一些其他已知的或发明的网络连接或获得的，提供使用帮助台服务的便利。一种较佳的实施当前是在 PatchLink 网站，在www.patchlink.com可获得。简单的网页表支持请求开始注册过程的数据收集。一旦完成注册过程，管理员能许可在递归登记基（recurring subscription basis？）上的一次或多次服务。

当管理员通过签约并指出参与者的某一预定级启动该过程时，注册过程就开始。本发明的一个较佳实施例有三种不同的用户级：客户机级，正常级，和执行级。允许客户机浏览网站，并能阅读用户论坛，但不能邮寄给论坛。正常成员能执行客户机特性并也能在聊天室内聊天，并能邮寄给该论坛。执行成员具有到该网站的登记。他或她能执行正常成员的特性，并也能使用网站的更先进的特性，例如，界外自动包更新（例如，PatchLink 更新服务），界外监视（例如，PatchLink 监视服务），及界外帮助台特性（例如，PatchLink 帮助台服务）。

该方法的一个实施例使一个电子邮件发送给客户机照顾代理，赋给客户机电话区码。该客户机照顾代理打电话给待解决的用户以完成登记处理。客户机

照顾代理收集必须的身份信息和付款信息，将然后更新待解决的用户该帐号，以允许使用该帐号，使待解决用户变成管理员/用户。管理员/用户能参与或使用的区域是由更新主数据库的许可产品表内的条目控制的。这些条目是在登记处理期间由客户机照顾代理建立的。

回忆起：经浏览器或互联网上的其他网络连接，所有这些服务对管理员都是可用的。当监视器登记一张进入帮助台的票，并在发明的方法的某些实例中启动转入（rollout），那么，该监视器决定故障是否已经发生 316，406。为了决定：监视器可查看最近已经安装了什么软件更新，多久之间进行安装，当前的硬件和软件配置，等等。应当考虑故障可能是哪些事件，没有限制，是由管理员设置；能使用缺省，并且帮助台人员的判断也可考虑到。

在检测成功步骤 408 中，在成功地完成从更新服务器到目标计算机的下载后，目标计算机 500 将一条消息 410 发送给更新服务器。如果某一指定时间周期已经消逝而未注意到或未通知一个故障，监视器能假定成功 404。

用其他方法 316,406 能检测故障。例如，目标计算机能通报监视器已经发生了故障；用户能经过帮助台或经过直接链路通知监视器已经发生了故障；当目标计算机在从第二次下载 312 开始的指定时间内不能使监视器接触目标机时，人工管理员能宣称已经发生了故障；等等。注意：即使在监视器已经宣称下载的结果是成功之后，后面的事件，例如来自帮助台的故障指示，能使监视器宣称下载故障。

在本发明的一个实施例中，更新服务器 528 等待：在下个目标计算机 500 使软件更新放置在它更新列表 222 之前成功安装的确认（由监视器，或由另一个已知或发明的接触方法）。更新服务器检查目标计算机 500，是符合软件更新，但还未接收到它 412。如果已经找到一个 414，能指明目标机，软件更新，和位置的合适的任务标识符被添加到更新服务器 528 的任务更新列表。这样，替代所有符合的计算机使软件全部安装它们中的大量更新，首次展示每次处理一台计算机的转入，直到：一个缺省的或用户定义的成功安装次数后，转入被认为是成功后为止；在那个接合点，每次将软件更新可用于不至一台目标计算机。

通过查看已经安装软件包和补丁的特定目标计算机 500 也不是总是清楚

的。本发明包括一种方法：分析目标计算机 500 以保证在本发明试图安装那个补丁之前，某个给定补丁不能已经安装在该计算机 500 上。下列的讨论包括参考图 8 和 9，并继续参考图 5。

下面将更详细地描述能定义特定软件更新的补丁指纹。通过为一个新补丁指纹 902 监视一个补丁组件数据库位置 900 可定位该补丁指纹 800。这儿，词“新”表示该补丁还未下载到资源库组件 600，或因某些原因待再次下载到资源库组件，即使已经先前下载了。可能有一个或多个补丁组件位置；这些位置可以位于经网络链路连接到系统的一台分立计算机，在更新服务器 528 上，在目标计算机 599 上，在软件包计算机 567 上，在非网络化位置，例如 CD，磁带，软盘等，或某些其他已知的或发明的位置。

一旦补丁指纹 906 被定位了 800，将它放置 802 进资源库组件 600 内。常用的放置方法是将补丁指纹 906 下载 804 进资源库组件，但在某些实施例中，该指纹 906 将在相同的文件系统上，因此，补丁指纹将不用网络复制，例如分区间的复制。

描述的补丁指纹包括一个或多个一般目录安装相关性 912，该相关性能用于进行高级查看：以观看某特定补丁是否能安装在一台机器上。它也包括：签名块 910，能用于从一台目标计算机 500 中请求特定信息；及存在测试 908，能使用签名块信息来确定某一特定补丁是否已经装载在一台机器上。

在本发明的某些版本中，目录安装相关性 912 至少描述了必须安装到目标计算机 500 上的某些必需软件和硬件。这些相关性 912 与先前已经储存在资源库库 918 内的有关目标计算机 806 的信息进行比较。如果安装的信息与资源库库信息不匹配，那么，该补丁不能安装。在本发明某些版本中，将一条消息发送给包括请求安装的组件（例如必需的硬件和软件）列表的至少一个管理员。

如果必需的目录信息是在目标计算机 500，或如果目录信息不被使用，那么，将签名块从资源库计算机 600 发送 810 给目标计算机 500。在签名块中的请求的信息，可包括更多特定安装信息，是由发现代理 548 收集的，并然后发送回资源库组件 818。在本发明的某些版本中，发现代理也收集有关目标计算机的其他信息，例如，使用统计量，安装的硬件和软件，配置，等等。然后，这信息能用于填充目录库 918。

一旦签名信息 910 已经发送给资源库组件 600，评估器 914 利用该存在测试 908，以及某些情况中，利用目录安装信息 912 至少评估由签名块请求的一部分特定安装信息，以确定该补丁是否不在 822 目标计算机 500 上。

作为一个可选步骤，一旦已经确定该补丁是否不存在，一条消息发送 824 给与一个管理员相关联的至少一个地址。这条消息可使用各种方法发送，包括电子邮件，寻呼机，传真，语音邮件，即时消息，SNMP 通知，等等。

补丁指纹

继续参考图 5，8 和 9，该系统的一个实施例检验：一个软件包在试图安装之前能被或应当被安装在一台给定目标计算机 500 上。为了检验，例如通过客户机上的代理使用补丁指纹 906。该补丁指纹定义：怎样确定某一给定软件包/增量补丁是否已先前安装。它也可定义：该补丁安装所需的最小硬件/软件配置。这些补丁指纹 906 储存在指纹库 904 内。指纹库 904 位于资源库组件 600 内。这资源库组件 600 可位于更新服务器 528 上，或可以在更新服务器 528 和目标计算机 500 可访问的一个单独位置。本发明的某些版本也包括包括目标目录的目录库 918。每个目标目录 920 包括有关定义的一组目标计算机 500 的硬件和软件信息。这定义的组可包括小到一台计算机或多到某一给定网络内的所有计算机，或其间的一些计算机。

指纹库 904 能自动地补充。在某些实施例中，至少一个，但可能几个，监视补丁组件数据库位置 900 以发现新补丁 902 的。在本发明的某些实施例中，来自位置 900 的一个信息对资源库组件指出：新补丁 902 是可用的 800。在较佳实施中，指纹库 904 是用新补丁指纹在特定时间间隔更新的。资源库组件 600 知道新指纹后，该补丁指纹放置进资源库组件 802，通常通过使用下载器 924 来下载该新补丁指纹。然而，补丁指纹可以按其他方法放进资源库组件。例如，一个或多个补丁指纹可以由管理员人工地安装进指纹库内。

目录库

资源库组件 600 也包括一个目录库 918。发现代理 548，在某些实施例中最初居留在更新服务器 528 上，是用已知的或发明的方法从更新服务器 528 安装到目标计算机 500。这个发现代理 548，下面将更详细地描述，至少编制一些：目标计算机 500 的软件信息 606；硬件信息 608，包括要安装的特定软

件更新和补丁；使用信息 604；注册信息 612；网站信息 610，配置信息 614，服务 618，文件信息，已经利用的补丁签名等等。

然后在某些实施例中按压缩形式将这信息，或子集或其超集，发送给目录库 918 内的目标计算机目录 920。结果信息的容量是相当大的，并因此，可进行压缩以利有效地上载，并使客户机网络上的带宽使用减少到最小。一种较佳实施是用 XML 数据传送器，经过任何其他已知的或能使用的发明的数据传送方法，来发送数据。目录信息的传送也可在客户机网络内进行加密，以防止系统配置信息的不希望的导线级窃听。

报告发生器

用这种信息，报告产生器 922 能给用户呈送网络内所有计算机的当前补丁状态的详细报告，描述下列几种数量：要求补丁的计算机数；已经用补丁安装的计算机数；不能接收补丁直到硬件或软件更新后的计算机数，等等。另外，报告产生器 922 能提供附加到网络上的计算机的部分或全部目录。在某些实施例中，报告产生器 922 提供目录的图形表示，用于由管理员进行分析，以跟踪硬件位置以及保证软件许可符合。然而，资源库组件 600 也可使用目录库 918 的信息以及检测指纹信息，以将相关签名 910 从补丁指纹 906 分配给发现代理 548，这样，通过消除目标计算机 500 上不要求的扫描工作，极大地优化了补丁发现处理。

发现代理

能决定某一给定软件程序或补丁是否能安装的可选步骤是检验：必需的硬件，如可用，是存在的，和/或必需软件是存在的。例如，某些程序或许要求某一特定操作系统，某些程序或许要求某一确定的处理器。作为一个例子，微软文字处理软件的更新有待安装，微软文字处理软件必需在该机器上。这些高级的依赖，在某些版本是，是储存在补丁指纹内的目录安装块 912 内。目录安装块内的信息级别通常足够高，以使它能被调出储存在目录库 918 内的特定目标计算机 500 的目标目录 920。

在本发明的某些实施中，补丁指纹 906 也包括安装依赖信息 912。如上面解释的，这是有关目标计算机 500 的信息，这些信息期望能在目录库内找到，并因此，能被检查，而不需查询目标计算机 500。这包括应当存在的软件（例

如程序，补丁，数据文件或驱动器的指定版本），应当存在的硬件组件，或不应当存在的特定硬件和/或软件。

如果目录库不包括目标计算机 500 的最近目录，发现代理能用于扫描目标计算机 500，以找出目录信息；它不必要求也同时扫描签名信息。在较佳实施中，发现代理 548 首次在某一给定目标计算机上运行时，它仅扫描目录信息，并然后将那信息装载进目录库 918；它忽略了补丁指纹信息。在其他时间，当发现代理 548 运行时，它可忽略目录信息，并可更正确地，被用于检查特定签名信息 910，以测试某一指定补丁的存在。当查找签名块信息时，可录入例如注册的值，并检查 INI 文件值的存在，或可将实际值回退给资源库组件 600。

每个补丁指纹包括：签名块 910 和存在测试 908。补丁签名块是一组信息请求，该信息本身是由目标计算机 500 收集的，然后被用于确定是否安装了所有必需的故障修复及安全补丁。补丁签名块信息的例子包括但不限制于：文件；硬件；注册和配置信息；特定文件名或目录名，能期望找到一个文件的所有或部分路径；文件的指定版本号；文件的建立日期；文件的指定文件版本；及指定注册值。

在一个实施中，指纹库 904 是 SQL 数据库。补丁签名 910 是从 SQL 指纹库中提取的，并然后发送给能满足操作系统和安装软件的依赖准则（如在目录安装信息 912 内指定的）的所有目标计算机。

一种较佳实施应用 XML 基请求输入文件。发送回更新服务器 528 的结果文件也应用 SML 格式。这结果文件包括目标计算机的签名信息，并也包括软件和硬件目录更新。发送给更新服务器的该目录和签名信息的容量是相当大的，并因此在较佳实施中要进行压缩，也可进行加密。下面是一个样本补丁签名，将收集微软 Outlook 的注册信息以及 EXE 日期和时间，及注册内的信息：

```
<file component id="1" report ID="1">
    <name>lutlook.exe</name>
    <path></path>
    <version>9.0.2416</version>
    <created></created>
    <size><soze>
```

<root>HKEY_LOCAL_MACHINE</root>

<Key>SOFTWARE\Microsoft\Windows\Current Version\App Paths\OUTLLOK.EXE</key>

<value>Path</value>

</file>

一旦目标计算机上的发现代理已经回退该签名的扫描结果，由评估器914使用存在测试908逻辑，推断特定计算机是否实际包括补丁。这算法使必须由评估器进行的测试次数减少到最小；它唯一的责任是发现信息—允许由资源库组件600本身进行数据分析。按这种方式分配工作量为扫描和分析巨大数量的工作站和服务提供一种更好的实施。

每个存在测试是专门对某一给定补丁。一个样本的存在测试或许看来是：如果注册QQ包括值ZFILEVAL或（如果文件_Z123.bat是在2000年12月12日下午11：52修改的，而文件Z的大小为ZFILESIZE），那么，补丁ZPATCH是存在的。补丁指纹库的较佳实施例是SQL数据库，但可使用其他已知的或发明的数据库。

注意：补丁指纹也可包括对其他指纹定义的依赖性：例如，“MS-023 IIS脆弱性修复”补丁或许假设地要求“微软视窗服务包2（Microsoft Windows Service Pack 2）”的存在。这用于进一步优化补丁签名实际发送到何处。这些或许有时用在安装依赖信息412，且其他时间用在签名块910，依据环境而定。

另外，指纹定义906也通常与适合于由系统部署的软件包554相关联。一旦通过扫描网络内一台计算机或所有计算机上的它的签名已经建立了特定补丁的要求，那么它能由管理员通过仅选择日期和时间来快速地部署。

指纹定义906也可包括应被评估的逻辑表达式，以评定：是否应将补丁签名内的其他成分评定为真（TRUE（修补过））或假（未修补过）。该表达式是例如（A与B）|C的简单逻辑句，这儿A，B和C涉及补丁签名内的其他指纹定义。

在某些实施中，下载器924定期地检查补丁组件数据库，是否有新补丁指纹（P）26 -27~28 check ... for ...）。当定位到新补丁指纹时，将它下载进资源库组件。评估器对安装信息912内列出的特定补丁实施所需的依赖性与目录

库内列出的目标计算机 500 说明的每个进行比较。然后建立更新列表，该更新列表能识别：要求补丁的所有目标计算机 500，不要求补丁的所有目标计算机，能接收该补丁的所有目标计算机，因它们包括必需的依赖性；和/或已经接收该补丁的所有目标计算机 500。现在，这更新列表可用于更新目标计算机，和/或由通知器 916 发送给管理员。

在本发明的某些情况中，补丁组件数据库是由除目标计算机 500 的拥有者以外的某人所拥有。只有当这补丁更新主人已经许可目标计算机 500 的拥有者，将允许下载器将新补丁指纹下载进资源库组件。该允许包括：进货协议，租借协议，下载允许签署及评估协议。

如果做出管理员感兴趣的任何修改，通知器 916 将发送包括新补丁更新的一条通知消息，该新补丁更新已变成可用，或补丁相关状态改变，该改变是在它的网络配置中发生的。通知可经电子邮件，寻呼机，电话，SNMP 广播或即时消息来发送。

目标计算机

在一个实施例中，发明的系统包括三个部件：目标计算机 500，更新服务器 528，和软件包计算机 548。目标计算机 500 包括：存储器 502 和网络连接 504，在本发明至少一个实施中的网络连接是 winsock 层。Socketless 协议能被实现，或任何其他已知的或发明的网络连接能被使用。更新服务器 528 包括存储器 530 和网络连接 532，该存储器 530 可包括可选备份存储装置 534。软件包计算机 567 具有存储器 550，和网络连接 552。为了便利，图 5 示出一台目标计算机 500，但在一个给定实施例中可以有更多台计算机。另外，为了便利，示出一台更新服务器 528，及一台软件包计算机 567，本发明可仅要求一台，但也可支持两台或更多台。在一个较佳实施例中，这几个部件都是单独的计算机，但它们可是相同计算机的虚拟件，这样，它们看来似乎是不同的。例如，“软件包计算机”部件可居留在更新服务器的不同分区或相同分区。

目标计算机包括网络连接 544，由防火墙 526 保护免受外部入侵，如上面讨论的。网络内不同的目标计算机可运行在不同平台上；例如，某些可以是 Winodws 机器，某些为 Unix 机器等。相同的更新服务器 528 可用于所有平台，或不同更新服务器 528 能由平台类型来指定，或更新服务器 528 可用不同模式

赋给目标计算机 500。

目标计算机 500 也包括更新代理 508。更新代理是一种软件组件，可用发明的方法及时地安装在多台机器上，或在该系统的某些实施例中，能按传统方式安装在目标计算机 500 上。一旦注册了，更新代理 508 知道怎样执行三个基本任务：1） 怎样接触更新服务器 528，以从它的更新列表 536 中检索它的任务列表，2） 怎样启动接收的任务列表中的任务，及 3） 怎样从能控制轮询间隔，运行小时数等的更新服务器 528 中检索接收的策略信息。

更新代理

目标计算机 500 的更新代理接触更新服务器 528，以确定是否有代理 508 要做的工作。更新服务器 528 通过分析代理的更新列表队列 536 排队来确定这事。这更新列表 536 最少包括软件位置基准 538，但也包括表示能安装软件包 554 的最近日期的日期 540，并且如果相同软件包可从多个位置可得到，也可包括多个软件位置基准。能更新的软件类型 554 包括，没有限制：补丁文件 556，更新在目标计算机上当前安装的软件程序；数据文件 558，脚本文件 562，新应用软件文件 564，可执行文件 560，驱动程序更新，新软件版本，并对更新代理文件本身的更新 566。

当更新代理发现它相关更新列表 536 内的一个条目时，用合适的日期 540，如有的话，安装器 510 最初检验，以查看软件包的副本已存在更新服务器 528 的存储器 530 内。如果找到，那么它从更新服务器直接下载该软件包。当先前目标计算机 500 已经从更新服务器 528 请求了该软件包时，可引起这种情况。

如果未找到该软件包，那么安装器 510 用它的网络连接试图从软件位置基准 538 给出的软件包计算机位置直接将该更新下载到目标计算机存储器 502。如果没有防火墙 526 或如果更新服务器能连接到软件包计算机位置 548，这将是可能的。

当管理员建立了能强制性更新代理 508 从例如软件包计算机 567 的“非信任”源中检索文件的包时，安装器 510 将不能直接检取资源。然而，更新代理能请求更新服务器 528 检取该包。在某些实施中，有多个更新服务器，而更新代理 508 用某些预定准则决定它们中的哪个来存取。例子包括：选择可用的第

一个更新服务器 528，选择最不忙的更新服务器，选择连网术语中“最靠近的“更新服务器，等等。

在本发明的一个实施例中，如果更新服务器 528 能到达界外软件包计算机 567，它对该更新代理 508 报告：它能达到该资源并评估能取回的时间。这评估通知代理：在请求的资源可用之前将等待多长时间。如果计算评估不精确，因为它可能将不会是因为互联网业务量波动和服务器响应变化，然后，如果代理又请求资源，该更新服务器将提供另一等待时间长度，并且该代理将再次等待。将重复该循环，直到更新服务器 528 在存储器内具有可用资源为止，且能依据下个请求将它传递给代理。

因为特定软件包可由不同代理 508 请求多次，在本发明一个实施中，更新服务器 528 将这资源储存在本地高速缓冲存储器 530 内，从这本地高速缓冲存储器 530 中，它能完成附加的检取请求。为了防止更新服务 528 由老的软件包填满所有它的可用存储器，一个实施例储存访问该包的次数，和最近访问所储存的软件包的时间，并评估该资源停留在它高速缓冲存储器的时间：“存活时间（time to live）”。在更新服务 528 内运行的一个单独任务将定期地检查包括“存储过长的”它们有效性的资源，并通过从高速缓冲存储器 530 中去除该储存的软件包更新来恢复更新主机的存储资源。

在一个实施例中，更新服务器将使这些包对代理列表一次可用一个。如果代理 508 或结果搜索器 512 报告补丁应用故障，或如果补丁将代理目标计算机 500 放置在它不再能与更新服务器进行通信的这样一种状态，那么，更新服务器自动地代表管理员悬挂转入。在这点，该结果能通知给管理员，或一些其他指定人员 516。

结果搜索器 512 确定该软件包安装是否成功，并然后将它的发现传送给更新服务器 528。如果结果是不成功的，如上面讨论的，恢复器 514 将目标计算机放置于一种可接受的非更新状态。结果搜索器 512 不要求仅监视实际软件安装；而是，它能设置成：观看经修补的软件，整个目标计算机，和/或能网连到目标计算机的计算机的使用，达某段设计的时间周期。结果搜索器也能包括不同的成功级别。例如，安装本身（文件复制）能看作为一个低成功级，而其后无行为不端达一段时间周期的目标计算机可看作为一个高成功级，依据成功级

来采取不同的动作。那么能按先前描述的来监视成功或故障，并如要求，安装可恢复，悬挂等。

在将软件包安装在目标计算机500之前，某些实施例将储存目标计算机500的备份506，534，或其一部分。有时该备份534存储在更新服务器上，有时储存在正在使它的软件更新的目标计算机506，500，而有时将它储存在资源库站点点600的界外。当结果搜索器512报告软件安装的问题时，恢复器514能使用该备份534，以将目标计算机回退到非更新状态。

在本发明的一个实施例中，在下个目标计算机500具有涉及到放置在更新服务器的它的更新列表536内的软件位置538之前，更新服务器528等待确认成功地安装（通过结果搜索器512，或通过另一个已知的或发明的接触方法）。在一个较佳实施例中，当安装结束时，通过电子邮件 518，寻呼机 520，语音邮件522，SNMP通知568，即时消息570，传真或通过一些其他装置将结果通知给管理员。如果安装故障，能识别安装故障的特定机器。在某些实施例中，在缺省或用户定义成功安装数后，可使该包一次对不至一个用户是可用的。

这些更新列表536方便了预建包，或客户机构建包的管理员的指定，要被传递或转入到管理工作站客户机或服务器，那些称作为目标计算机 500。当这些包变得可用时，由管理员按排更新，以由本发明执行；它可使一个先前任务自动化：请求管理员访问一个客户机，安装补丁或服务包。

更新代理508可了解它在运行的平台，并可进行编程或可手写，以代表管理员执行动作。在一个实施中，经过 Package Builder 向导，使这些特性暴露给管理员。“软件包”可以是文件，服务包，热修复，软件安装和脚本的任何组合。这为远程机器的管理呈现一种机会，因为能在远程机器上执行的几乎任何事件都可经起到管理员作用的代理来完成。

本发明的一个实施允许脚本562在包安装之前（预安装）和在包安装之后（后安装）运行。预安装脚本的一个例子可以是：（按伪码）

检查可用的磁盘空间；

如果可用磁盘空间大于值 X（这儿值 X=安装所需的空间加缓冲区），然后继续安装；

否则警告界外管理：已经发生错误，并终止。

一个后安装脚本的例子（又，按伪码）：

如果安装是成功的，那么通知外部源：安装成功；

如果安装是不成功的，那么通知外部源：安装不成功。

现在参考图 6 和 7，网络 200 可包括许多不同种类的目标计算机，每台目标计算机带有为特定目标平台特别地形成的代理。例如，运行微软视窗 PC，Apple Macintosh 计算机，和 UNIX 计算机的网络可有三种类型的代理。这在下列情况中能提供益处：该代理能调查它目标计算机，并将这台计算机信息 602 报告给更新服务器 528 和/或单独的资源库站点点 600，用于贮存。在该系统的某些情况中，给发现代理 548 提供哪个能执行该扫描，如同另外描述的。在其他情况中，由更新代理 508，或下载脚本文件 562 执行扫描。硬件配置 608，软件配置 606，有关使用各种硬件和软件组件 604 的信息，访问的网站，发送和接收的电子邮件 610 都能发送给界外位置 600。一旦这信息在更新服务器可用，管理员能从一个地方浏览整个管理网络。

当这发明的系统是在现有网络上实行时，发现代理 548 用检测和和储存在资源库点 600 存储器内的现有的软件配置 700，可执行至少在一台目标计算机 500 上存在的软件调查。一些系统可调查整个网络 200。当调用更新时，该系统知道哪一个的确不要求再测量网络机器以检查它们当前状态。

目标计算机 500 的一个推荐配置 704 放置在更新服务器 528，或放置在资源库站点点 600。该推荐的配置可按许多方法决定，既是发明的的或对那些数据库技术熟练人员已知的方法，例如，通过硬件配置，通过软件配置，通过计算机类型，通过最后包更新等等。然后，发现代理 548 对当前配置 700 和推荐配置 704 进行比较，并为目标计算机 500 准备一张提议的更新列表 708。该更新列表可包括：用于安装软件的服务包，先前安装的软件，更新数据文件，及类似的。准备建议列表的过程不仅考虑到当前软件配置，而且考虑到例如硬件配置 608 的信息，和怎样频繁地访问某个特定程序，数据文件等 604，以及对技术熟练人员已知的其他信息。更新列表可自动地通知管理员。

假定：目标计算机当前配置 700 产生一张建议更新列表 706，可自动地通知管理员 708，在这点，可以限制计算机的使用，直到新的目标计算机至少部分更新为止，直到管理员允许为止，或直到满足其他创造的或已知条件。这张

建议的更新列表 706 也可用于定义用于实际更新计算机的一张更新列表 536，如另外解释的。

包由表示文件的模块形成，例如软件文件或数据文件，及脚本，那些是依据包内的文件采取的动作顺序。替代地，在包内容内可包含一个或多个脚本文件，这些文件由代理执行，以安装补丁。在本发明的某些实施例中，管理人员接收新软件补丁可用性的通知。在其他实施例中，通知直接发送给界外更新服务器 528，服务器 528 决定何时将它们转出。该界外更新服务器能配置成，将已经储存在每台目标计算机的包存储在永久存储器内。当一个新包变成可用时，或在安装现有包期间，在界外更新服务器 528 的某些实施例内，及资源库站点 600 的其他情况中，可利用要求安装的软件包的现有证据，以及有关先前安装的信息。

有待更新的包不要求由接受对它访问的目标计算机 500 的用户拥有。在该系统的一个实施例中，该软件包是由将软件转让给用户的第三方拥有。在另一个实施例中，该软件包是由更新服务器拥有的，然后，该更新服务器将对该软件包的访问转让给或提供给目标计算机 500 的用户。

安全和关键补丁的管理，特性

本发明提供用于管理及分布关键补丁的工具和技术，能解决在各种操作系统中已知的安全脆弱性和其他可靠性问题或增强等。合适的操作系统包括，没有限制：所有微软操作系统（例如 95，98，ME，NT，W2K，XP，W2K3），UNIX 操作系统（例如，Linux, Solaris, AIX, HP-UX, SCO, 等），以及 Novel NetWare 操作系统。操作系统的产品名是它们各自拥有者的标记。

在过去，为了管理安全或另外的关键补丁，公司和其他计算机用户频繁地检查销售商网站，例如，通过阅读环球网上邮递的或发送的新闻报告或文本警告或电子邮件的通知，脚本或新闻组等，以查出有关的新补丁。一旦获悉由公司使用软件的销售商已经发表新补丁以修复或增强应用软件，驱动软件，和/或硬件，公司的软件管理人员通常必须人工地下载最近的相应补丁，在各种布局和配置中测试它们与公司机器的兼容性，并然后人工地或使用它们传统的软件分配工具分配该补丁。

相反，本发明能按前摄方式给计算机提供关键更新的通知 824，无论他

们是否有互联网接入。通过执行补丁下载它能提前主动地运行，不需一个特殊管理员强制性来执行每次下载。它也有助于将软件更新，软件包，和其他数据分配和安装到连网的桌上型电脑，服务器，移动和其他计算机。

本发明的一个实施例包括经过更新服务器 528 的内容复制，它从例如软件包计算机 567 的主档案中检取最近的关键更新。为了安全地传送，检索可使用 128 比特的 SSL 或其他常见的协议。因为新更新添加到主档案，更新元数据自动地下载到更新服务器和/或指纹库 904。如果元数据指明一个补丁是关键的，该补丁能被下载到更新服务器并高速缓存在那里，用于快速部署。每个补丁包括一个相关的安装器 912，必须具备的签名 910，及其他指纹标识符 906。

在某些实施例中，信息仅按单方向发送，即，从主档案到更新服务器，由此，增强了主档案的安全性。另外，在某些实施例中，所有传送的信息都要进行加密，CRC（循环冗余校验）检查，压缩，数字签名，及在 128 比特的 SSL 连接上的下载 308。SSL 连接应用安全网协议，该安全网协议确认并确定作为补丁源的主档案的可靠性。其他安全网络协议也可使用，在其他实施例中，省略了这些要点的某些要点，例如，不进行 CRC 检查和/或不使用数字签名等。

更新服务器 528 起着客户机目标计算机 500 的补丁源作用。更新服务器，包括用于管理更新和软件包的复制服务和管理工具，用例如 HTTP，HTTPS 和 XML 的协议，能扫描客户机 500 并安排将补丁传递给它们。在某些实施例中，更新服务器使用微软互联网信息服务。该更新服务器能实现成：自动地资源库它从主档案接收的关键更新。在某些实施例中，管理员能设置复制方案，能人工地触发复制，或能使更新服务器内的复制软件自动地复制和分配软件，以响应期望的或测量的网络不活动性。

在某些实施例中，管理员能建立软件包 554，然后，他们能相似地部署（像任何其他补丁那样）。即，通常理解中的“补丁”不要求预示正在修改的先前安装的密切相关的软件块，但可包括对目标来说是新的软件块。例如，包括微软 Office 2000 的包应当被部署到每台桌上型电脑。客户机应用软件管理员能同样地建立包，以转入客户机应用软件和它们的补丁。某些实施例的管理员也可利用内置的软件分配特性，以将任何软件包分配给任何目标计算机。

在某些实施例中，更新服务器 528 是用软件和/或硬件配置的，能显示企

业的报告矩阵或公司或其他企业内的机器补丁状态的其他摘要。该报告显示给负责维护企业的计算机特性的网络管理员和/或其他人员。管理员影响（并在某种情况下完全控制）：通过设备策略，定义组，响应警报，和/或采取这儿讨论的或已经熟悉的其他步骤，将来自更新服务器的哪些更新或包推到客户机 500。在某些实施例中，管理员已经完全控制补丁的部署，包括重新启动和设置电源或修改客户机机代理策略的控制。

补丁可以最初在它们广泛经过企业部署之前进行测试，因为一个给定补丁在不同企业内的运行可能会不同。PatchLink.com 公司（“PatchLink”），提供商用软件和补丁管理服务，并是这个应用软件和它的最初版）的受让人，在由 PatchLink 发布它们之前继续研究，测试，及改善补丁。例如，当由微软发布微 W2K(视窗 2000)操作系统的热修复时，在由 PatchLink 将它释放给主档案 567 之前，由 PatchLink 在两百种或更多种不同的 W2K 配置上，按各种服务包和其他热修复相组合，进行安装和测试，这些配置例如为：准则 W2K，带有 SQL 服务器的 W2K，带有 Office 的 W2K，和带有交换的 W2K（微软标记），等等，。

在某些实施例中，客户机代理 508 检查 332 内联网主持的更新服务器，以确定在所论的客户机上要求哪些更新。它报告收集的信息，例如当前配置 700，回退给更新服务，为管理员建立矩阵（matrix）。在某些实施例中，管理员用部署向导指定和改善补丁部署。管理员批准的更新和包被在后台下载，由此减少对接收下载的计算机用户的麻烦，并然后依据由管理员设置的方案自动地安装。管理员定义的规则能控制补丁安装过程的运行状态。

本发明的一个实施例提供前摄服务，该前摄服务允许管理员使实施例自动地下载 308，312，并安装 510 软件包和更新，例如关键操作系统修复和安全补丁。

本发明某些实施例的内置安全特性使用数字安全标识符。在将一个下载更新安装 520 在目标 500 之前，这特性检验该数字证书，CRC 校验，压缩，以及每个文件或包上的加密。在更新服务器 528 上，对管理页和其他控制的访问限制在授权的管理员。在某些实施例中，更新的复制（下载）使用 SSL 并且该实施例检查下载到更新服务器的有效性，如果 SSL 证书不能适合地识别一个认

可的源（例如，PatchLink.com），那么，该下载故障，而服务器将一份电子警报发送给管理员。在某些实施例中，所有下载（主档案到更新服务器，更新服务器到目标）中的所有信息都要进行加密，CRC 校验，压缩，数字签名，并且仅在 128 比特的 SSL 连接上发送。在其他实施例中，这些要点被修改（例如，40 比特加密）和/或省略。

补丁签名 910 特性允许一个实施例扫描目标 500 并确定每个补丁的先决条件必要求满足，例如，使代理检查目标上适当的软件版本和适当的硬件驱动器。补丁签名和补丁指纹特性每个可用于做出一个检测报告，该检测报告在企业报告矩阵内是可视的。工作站目录特性使用发现代理 508，以指出目标计算机的所需软件和硬件驱动器。发现代理也可为指纹的必需签名而扫描目标。PatchLink.com 包括一个主档案，该主档案现在主宿世界上最大自动补丁指纹资源库库中的一个。

在某些实施例中的后台下载 312 特性提供一个带有内置带宽节流的安全后台传送服务，由此，网络管理员能决定在大规模部署期间应当怎样利用带宽。某些实施例给管理员提供可配置代理 508 策略，该策略允许他们定义代理通信间隔和运行小时数。例如，管理员可设定该策略，以仅在午夜到上午 2：00 使补丁转出到产品服务器。在某些情况中，在某一给定时间，代理可包括不至一个活动的策略。

链状安装特性允许管理员通过使用微软 Qchain.exe 工具减少反复的重新引导动或使重新引导动的次数减少到最小。如果应当安装 510 能请求多次重新引导动的多个更新，管理员能使用与 Qchain 相连接的本发明性能，以很少几次重新引导动来部署更新，在某些情况中，仅要求单次重新引导动。这种重新引导动次数的减少能增加正在更新的任务关键计算机 560 的正常运行时间。Qchain 将 DLL 再排列成一个次序，将最近的更新置成有效。在部署期间，管理员能选择这选项。

用下载取回特性，例如通过服务输出，一个实施例检测下载的中断 316。如果目标 500 是移动工作站，那么用户能简单地断开它，并且将它重新连接在不是在服务外的不同位置。如果能够访问更新服务器（例如，经 TCP/IP），该实施例可从在或接近在下载中发生中断的那点继续它的下载，而不是又从转发

整个包的起始点开始。

移动用户支持特性允许管理员将补丁和软件更新部署到目标计算机 500，当部署开始时，这些目标计算机 500 不连接到网络。当移动目标随后连接到网络时，该实施例将自动地扫描它并执行必需的操作，以使那目标是最新的。

实施例特性客户机代理 508，为了安全下载 312 与更新服务器 528 进行通信。使用代理也允许增强企业范围实施例内的性能和可量测性，允许单个更新服务器能服务于数千个客户机。该代理能跨防火墙 116，214 工作，并可在带有连接到企业网络的 TCP/IP（或其他）的任何计算机 500 上运行。

某些实施例特性支持多销售商补丁 554，那也可称作为“综合补丁扫描”。更新服务器 528 不限制于来自单个销售商的补丁，但替代地支持来自多个销售商的补丁的发明的管理。例如，更新服务器可与目标代理协调，以扫描目标 500，是否包括来自微软, IBM, Adobe, Corel, Symantec, McAfee, Compag, WinZip, Citrix, Novell, 和许多其他（各个公司的标记）软件内的与补丁相关的安全脆弱性。

某些实施例的分组特性允许管理员将选择的目标计算机 500 划分成例如称作为“容器”或“组”的集合。那么，对单台目标计算机可适用的操作也可应用于包括可能目标计算机的合适子集的容器/组，即，应用于属于特定容器的每台目标计算机 500（或考虑到补丁签名和指纹，应用于每台合适的目标计算机）。这特性便利管理员的管理：部署，指纹报告，目录报告，强制性补丁基线策略，和/或客户机代理策略，这取决于实施例。例如，每个容器可具有以下属性：指明它的成员，它的客户机代理 508 的策略，和它的强制性补丁基线策略。管理员能选择单个客户机 500，先前定义的客户机组，和/或用户定义的部署组。在某些实施例中，可依据它们要求的补丁自动地将计算机分组。

在某些实施例中，管理员能指定组管理员和代表，限制对它们的管理控制。从组管理员的观点，那么将发明的实施例的浏览和控制缩小到仅覆盖已经由管理员赋给管理组的那些计算机 500，所有那些较佳地使用相同的更新服务器 528。管理员还能浏览和另外管理网络内所有计算机，不仅是特定组内的那些计算机。

某些实施例中的强制性补丁基线策略特性允许管理员为一台或多台网络

计算机指定最小（基线）配置。该实施例将操作系统和/或应用软件提前主动地修改到由基线策略定义的组织准则。支持企业内补丁策略允许发明的实施例的管理员为他/她的公司设置补丁策略，由此，在公司内无机器 500，例如，能落在最小补丁级之下。例如，如果 W2K 组的强制性补丁基线策略包括：微软 Office 200, Adobe Acrobat Reader 5.0, 和服务包 2，那么，放置在这个组内的所有计算机（是否最初放置在组定义内）至少包括安装它们上的这些软件块。

用于补丁的基线可与一组计算机 500 相关联，该组计算机 500 是由组定义的（例如，用户定义组或管理员定义组），或与使用特定操作系统（例如，所有 W2K 计算机，不管用户或管理员定义组）的一组计算机 500 相关联，或与使用特定应用软件的一组计算机（例如，使用微软 Office XP 的所有计算机）相关联，或与它们的某些组合相关联。例如，在某些实施例中，管理员可设置陈述是否安装微软 Office XP 的基线策略，那么，该系统应当自动地在 Office XP 服务版本 1 内打补丁。

当使用强制性补丁基线策略时，在代理 508 确定该新配置并且该新配置与由该策略要求的基线进行比较 822（通过客户机代理和/或更新服务器）后，补丁 554 将自动地重新安装，通过从磁带备份，镜相图像，或类似中恢复软件，该补丁 554 是从目标 500 中丢去（去除）的。这样由这些实施例维持基线的完整性。

可依据本发明使用强制性补丁基线策略，以执行不想要软件的自动检测，并从网络内的目标计算机中去除不想要的软件。当检测到不想要的软件时，要被应用的强制性部署补丁应当是卸载（UNINSTALL）该不想要项。例如，一个这样的补丁应当是检测到的“卸载 KaZaA”，并从企业网中去除 KaZaA 文件共享应用软件，由此，减少企业雇员在营业日过程中违反版权法的风险，或减少他们为娱乐目的消耗所有可用网络带宽的风险。用政府代理和其他大规模实体，消除弹出软件和使用户不能专心于他们指定责任的其他事件可以是高优先级。

本发明也提供可以看成强制性补丁的相反逻辑的一种特性，能医治网络内的脆弱性。相反逻辑，可称作为“禁止补丁”特性，用于指示决不能安装的服务包，热修复，或其他软件。正象强制性补丁特性用于自动地修复脆弱性，该

禁止补丁特性用于防止网络管理员安装能破坏运行配置的软件。作为一个例子，假定一台计算机包括不能与视窗 2000 的最近微软服务包一起运行的一个工资单系统。如果该服务包补丁曾经人工或自动地部署该工资单系统，管理员要求立刻知道，否则在周末没有一个员工能取得工资。本发明的某些实施例能扫描搜索和检测“禁止补丁”的存在，并报警给管理员。它们也可提供规则：使得管理员不会不注意地将禁止补丁部署到不应当安装那补丁的机器上，而不管另外所说的可用组补丁策略。

在某些实施例中的补丁依赖确信特性给管理员提供为特定计算机或一组计算机 500 锁定一组补丁 554 的选项。即，某些补丁是要求的，但按比强制性基线特性中较弱的一种方式。如果按违反补丁要求的一种方法尝试改变目标 500 的配置，一条电子邮件报警消息 824 发送给管理员。例如，几台 W2K 计算机可属于“IIS 服务器”的管理员定义组，该管理员定义组服从补丁依赖性。为了安全，该实施例因而锁住所有操作系统补丁和所有互联网信息服务器补丁。如果在某些稍后点上，替换这样的补丁（包括没有限制性 DLL），那么，该实施例将能识别计算机 500 名字和/或对它所做修改的电子邮件报警发送给管理员。能够识别最近非依赖性计算机和非依赖性的原因—它们的配置和锁住配置之间差异的摘要。在某些情况中，这个依赖性特性可由管理员使用，以识别安装新软件或从他们机器中去除现有软件的用户。注意：这依赖性锁住特性连同强制性补丁基线特性可由某些实施例使用，以自动地修改是非依赖性的目标 500。当去除一个锁住补丁或其他软件组件时，那么它能自动地重新安装，并通过电子邮件通知 824 管理员。

某些实施例中的服务改变特性允许管理员锁住在客户机工作站提供的服务（驻留在一个组内或单独地），并且然后如果用户未直接接触管理员就启动或中止一个服务项，就通知管理员。当用户改变和/或试图改变锁住客户机 500 上的服务状态时，一个电子邮件报警 824 发送给管理员，标识计算机和（试图）服务改变。

某些实施例中的硬件改变特性允许管理员锁住在客户机工作站 500（例如在组内）上提供的硬件配置，并如果用户未直接接触管理员就安装硬件项或从这样的工作站中去除硬件项，那么就通知管理员。因为用户改变（或试图改变）

锁定客户机上的硬件配置，一个电子邮件报警 824 发送给管理员，标识计算机和（试图的）硬件改变。

输入/输出特性便利于未连接到互联网络的网络上的计算机的更新，例如，高安全的军事或政府代理计算机。用一种除互联网外的装置将内容从主档案传送到目标网络的更新服务器 528，例如在主档案装载有内容 554 的物理传送带，盘，或其他存储介质，该装置带有在传送期间采用的合适的物理安全措施。一旦该介质可到达安全目标网络的更新服务器 528，能够应用上面讨论的内置安全措施（加密，CRC 等），同时将该内容从传送介质传递给更新服务器的本地存储器。然后，那更新服务器能完成更新 304 该安全网络的目标计算机，如先前讨论的。

某些实施例中的递归分配特性便于重复更新的数据或文档的分配，例如，一个企业雇员目录或防病毒定义/数据文件。依据由管理员指定的递归方案，能将一个或多个这样的数据或文档文件部署到所有目标 500，例如，或部署到管理员指定的组或单个目标。其他步骤，例如递归服务器重新启动，可也在相同情况中指定。

某些实施例的灾难故障恢复特性帮助管理员从系统故障中恢复，系统故障例如为硬盘崩溃或服务器硬件故障。如果更新服务器 528 故障，管理员建立具有如故障服务器相同 DNS 名的另一个服务器，并将相同的更新服务器软件（如果要求，可带有相同的序列号）重新安装在新服务器。由该实施例使用的文档，镜像，或另外储存的数据文件 600 可按要求重新恢复到新的更新服务器。然后，目标代理 508 将自动地与该更新服务器的新实例相连接，并在目标代理提供由服务器故障丢失的信息（如果有的话）后，将恢复正常运行。

某些实施例中的自动高速缓存特性使更新服务器 528 自动地下载和高速缓存在它的本地更新服务器存储器补丁内，这些补丁标记为关键的，高优先级的，和/或安全相关的。该更新服务器通知管理员有关哪些补丁是关键的，及哪些被高速缓存，并扫描要求补丁的目标计算机 500。相反，仅在首次部署后，可将非关键补丁高速缓存在更新服务器内。当补丁请求可压制易受攻击的软件的销售商时，在它们初始部署之前高速缓存该关键和安全补丁给目标计算机提供容易利用的补丁源。例如，在 Code Red 和 Nimda 病毒攻击期间，某些用户必须

等待数小时，才能连接到微软网站以得到补丁，因为对它们的极其繁重的需求。在发明的更新服务器 528 中的前摄高速缓存关键和安全补丁减少目标计算机 500 的运行将被中断或由于缺乏这样的补丁危及安全的风险。

某些实施例具有智能多补丁部署特性，该特性使补丁 554 匹配于操作系统，由此，减少管理员快速和完全识别用在每台目标计算机上的操作系统的要求。例如，假定微软为它的操作系统发布了一个公告，那公告为几个不同操作系统平台指定不同补丁 554。使用这发明的实施例的管理员仅要求选择用于部署的“微软操作系统”；它们能不管操作系统的不同，给目标计算机 500 指定各种指定目标的细节。该实施例为兼容性和补丁的要求对补丁和操作系统需求进行比较，以保证适合的补丁安装在某一给定目标上。这样，微软视窗 98 平台的补丁将安装在运行视窗 98 操作系统的目标计算机上，微软 NT 平台的补丁将安装在运行 NT 操作系统的目标计算机上，等等。这个特性通过使管理员免除要求依据包括的操作系统人工地使补丁匹配于目标而加速了补丁的部署。

另一个特性有助于检测可用补丁 554 和管理补丁的互相依赖，由此，帮助管理员免除人工地分类数十打（或甚至数百打）一般不相关的补丁。替代地，用它们的元数据，指纹，和/或签名数据，依据例如包括的操作系统，其他补丁的存在（或不存在），不同补丁的互相依赖（识别哪些补丁依赖于哪些其他能正常工作的补丁），及强制性补丁基线策略（如果有的话），该实施例识别可用的补丁。然后，给管理员示出哪些补丁是所论的目标 500 可使用的。例如，仅如果 IIS 安装在目标计算机上，一个实施例给管理员示出 IIS 补丁。如果一贯地使用，这个特性帮助保证一个补丁何时向目标部署，目标具有所论的应用软件以及将该补丁安装在那个目标上。

作为补丁互相依赖的例子，在微软 W2K 平台上，一个实施例将向管理员推荐服务包 2，并且一旦安装了服务包 2，然后它推荐 Security Rollup 补丁，该 Sercurity Rollup 补丁依赖于服务包 2。该实施列读取注册和文件信息两者，以正确地进行指纹识别，以使补丁 554 的标识符有效。

某些实施例允许管理员回顾新近操作的历史或日志，并允许卸载补丁 554 或其中的部分，以及反转将补丁部署到新网络的效果。这允许管理员取消已经引起问题的补丁安装。丢失的用户数据将不要求恢复，但用恢复器 514 能采用

由传统的卸载器采用的普通步骤，例如去除 DLL，去除注册条目，重新恢复路径或其他系统可用值，等等。另外，将特别对该实施例的配置状态更新到能反映遇到的问题和/或该补丁的去除，配置状态例如为签名，指纹，报警，和报告。如果在补丁依赖和/或强制性补丁基线上出现该去除的补丁，也能通知管理员。

某些实施例包括“目录中性”的特性，意指：它们是平台中性并且不要求为了运行的目录，例如 Novell 的 NDS 目录或微软的活动目录产品。然而，某些实施例能与特定组织内的这样的目录集成在一起和与它们合作。

某些实施例依据一个可选补丁特性来运行，在该可选补丁特性下，除非请求它们满足强制性补丁基线策略，补丁 554 不能自动地安装。在某些情况中，标记为关键和/或安全补丁的补丁也可自动地安装。在这样的实施例中，其他补丁不能安装，直到管理员选择它们，并明白地批准它们安装为止；这允许管理员在将它们安装在该组织的计算机上之前，内部测试它们组织内的补丁。一旦充分地测试了该补丁，它能被添加到所论目标组 500 的强制性补丁基线，使得当要求时它能被自动地安装。

某些实施例支持能防止应用软件运行在目标机 500 上的安全策略补丁 554。这提供一种策略驱动方法，以钩进目标计算机文件系统并从执行中停止一个特殊文件（或多个文件的执行）。这可由能重新命名所论的可执行/DLL 文件来实现，并适当地替代其没有做什么的代码，或给用户显示出错信息的代码，和/或由电子邮件通知管理员的代码。

通过考虑到下列示范性情景可进一步明白发明的实施例的运行。在一种情景中，当由它们各自销售商发布新补丁 554 时，更新服务器 528 从主档案 567 中下载相关的指纹。然后通过将用于由代理 508 扫描的补丁指纹发送给目标，该实施例检验，以查看任何目标计算机 500 是否满足简档（要求所论补丁）。将网络上新补丁和它潜在影响通知管理员，并一个报告矩阵告知管理员，哪些目标要求补丁，以及哪些目标不要求补丁。管理员选择一台或多台单个目标计算机和/或组，并批准部署。部署按这儿讨论的进行。管理员可设置部署的时间，并决定在安装后是否要重新启动。

在一个管理数据中心情景中，中心的管理员从每群数据服务器中建立一补丁组。管理员能测试从主档案 567 中接收的关键更新，并然后将测试的补丁 554

部署在网络目标上，或者突然，或者分阶段地部署到组。代理策略能帮助管理员指定每组的运行小时数。

在一个实施例的更新情景中，由该实施例使用的软件是通过使用该实施例来更新的。即，当销售商（例如 PatchLink.com）将补丁 554 提供给目标代理 508，更新服务器 528 的软件，和/或其他实施例软件时，那些补丁能按这儿讨论的部署，使用应当更经常使用的发明的工具和技术，以将补丁部署到操作系统或用户应用软件。例如，管理员能选择 PatchLink HotFix 客户机补丁并将它部署到更新客户机代理软件。可通过将它们推给所有目标计算机，可最初部署客户机代理。

实施注意

下面提供有关特殊实施例的附加细节。这些实施细节按出错的次序提供—如果出错—通过包含过分多的信息，而不是包括过分少的信息。不会因如此来临而处罚申请者。特别地，包含细节不应看作为假设或承认：那些细节，或类似的细节，或类似级细节，被实际要求，以支持最后同意的权利要求。不应当通过论及能简单地实现由其他人构思的发明性想法的发明家人员而误解包含特殊实施细节。

代理

* 微软视窗代理

* NetWare 代理

* Linux 代理

* Java 代理

包结构/包维护

管理员使用这个模块建立分配到指定更新代理的包。它个包可以是文件分配或软件包，当更新现有安装软件时，经过指定管理机器，允许更灵活地安装新软件，文件复制等等。

下面是合适包建立的步骤；

1、键入包说明

* 包名 --- 标记，贯穿更新过程的包；

* 包类型 --- 当在软件包例行程序中选择软件包时，在该包的源文件按

它们适合的目标序列放置后，管理员可立刻结束包建立（给其余任选项使用预定缺省值）。文件分配要求管理员完成包建立例程中的所有步骤。

* 操作系统 --- 选择包能被转出到的操作系统。目前，每个包可选择一个操作系统。这些操作系统包括：Linux, NetWare, 视窗 2000/NT， 视窗 NT，视窗 95/98/ME。

* （可任选）输入 --- 输入一个先前输出的包。这任选项有用于为多操作系统建立相同包。

2、添加源

* 添加文件 --- 添加一个来自你本地工作站或网络位置的文件，那是可读的；

* 添加目录 --- 添加一个来自你本地工作站或网络位置的目录，那是可读的；

* 添加 URL --- 经过众所周知的协议将一个远程文件添加到该包。能添加的各种类型的 URL 是：本地文件 --- 文件://，FTP --- ftp://, Secure HTTP --- https://, 另外选择的任何文件，只要代理认可该协议（这文件是可编辑的）。

* 去除 --- 从该包中去除一个文件；

* 属性 --- 显示每个文件怎样储存在更新服务器内的细节。在一个源繁忙或变慢（例如，由于纯延迟）的情况中，允许多个源。代理自动地询问其他源；

* 输入文件 --- 从先前输出的包中输入一张文件指定列表；

3、添加目的地

* 目标计算机 --- 包文件目的地的分层结构树图。所示的各种缺省目录取决于将该包作为目标的操作系统。该包总是显示在相同的目录路径内，最初从该目标路径输入源文件（见步骤 2）。为了移动文件，简单地高亮该目录或文件，并将它拖到它的新位置；

* 属性 --- 如果没有显示文件应当安装的目录，高亮一个文件并点击属性按钮。这显示源文件来自何处的基本信息和目标地的一个输入字段。键入新的位置并点击 OK，示出你的改变（这可能要等一会儿，因为为大规

模包文件数重新连接路径）；

* 输出文件 --- 将一个基础包输入给一个文件（源和目的地信息）以便在后面的输入特性中使用；

4、从属物

* 左栏 --- 已准备转出的现有包的列表（操作系统从属）。例如，如果有必须转出到众多计算机的 Java 基包，应当选择特定 JDK 包作为你的从属物，使得 JDK 要在当前包之前安装；

* 右栏 ---放置在这儿（通过使用箭头按钮）的包是你包的从属物。使用+和-按钮以按重要次序排列从属物（最重要的是第一从属物）。在你的包之前处理从属物；

* 资产--- 如果没有发现从属物，包安装故障。例如，如果要建立微软 Office 2000 SR1 包，它的资产从属物是必须已经安装的微软 Office 2000；

* 安装 --- 如果没有发现从属物，在安装当前包之前安装他们。使用上面的例子，如果未发现 MS Office 2000，在安装 RS1 包之前安装 MS Office 2000；

5、包设置

* 备份 --- 备份任何在目的地机器上找到的任何现有包文件。可编辑的下拉列表包括所论的操作系统的最普通的目录。如果未发现你的目录，仅仅是将它键入该列表内；

* 可信度--- 所有新包的缺省值为新。可信度指出这个包经过测试，且它的性能已经确定了它的可信度；

* 可用性 --- 缺省值是可用，它指出这个包可用于转出。不可用指出这个建立的包不能用于转出。

6、脚本

* 有三种类型可使用的包脚本：强制性行 --- 这脚本的内容可执行为准则强制性行。 在文件复制到它们目的地后可发送该脚本。预脚本 – 这脚本的内容可在文件复制到机器之前执行。后脚本 --- 这脚本的内容可在文件复制到机器之后执行；

7、系统设置

* 语言 --- 选择包可供用于的语言。然后，代理检验该语言是在该机器

上，并在安装该包之前检查该包的匹配；

* 处理器类型 --- 为可利用包选择处理器。然后，代理检验处理器在该机器上，并在安装该包之前检查包的匹配；

8、结束 --- 点击完成（Finish），以上载文件并组装该包。当组装过程结束时，按钮从结束变成做完（Done）。点击做完以完成包建立功能。

定义组/修改组

这个模块让管理员将机器组合在一起，使转出过程更容易，使得转出易适合于一台机器一样如同也易适合于 500 台机器。另外，管理员可依据它们的特性或位置分组机器，以使带宽的利用对它们的网络更有效。

1、组名 --- 该组的标签目的地；

2、机器列表 --- 选择该组将包括的所有机器。一台机器仅在安装更新代理及注册后才显示出；

3、结束（Finish） --- 在将机器放置在组内后，将结束按钮改变为做完（Done）。点击做完，以完成组特性.

安排转出/浏览现有转出

转出方案定义包对目标机器可利用的日期和时间。

1、选择一个包

* 包选择列表 --- 选择一个要安装的包（这次只选择一个）；

2、选择机器

* 添加一个组 --- 这一按钮显示一个对话框，示出可用组列表。高亮希望部署的组，然后，点击 OK 按钮。

* 去除一个组 --- 高亮不想将该包转出到的组，然后，点击去除组按钮；

* 添加一台机器 --- 这个按钮显示一个对话框，示出可用机器的列表（在它们上面带有注册更新代理）。高亮要添加的机器，然后点击 OK 按钮。

* 去除一台机器 --- 高亮不想将该包转出到的机器，然后点击去除一台机器按钮；

* 回退 --- 去除刚安装的包，并回退备份（如果指定了一个）。这

选项仅经 View Existing Rollouts 才可用；

* 再申请 --- 再安装该包。

3、选择转出日期和时间

* 日历 --- 选择发生转出安装的日期。

* 时间 --- 当包要转出时，服务器上的时间。

4、选择带宽和顺序

* 带宽 --- 这一级确定服务器下载该包将利用多少带宽。最小值是30%，而最大值为 100%；

* 顺序 --- 选择 YES（缺省值），在整个转出过程中引起机器到机器的转出，并在最后一台机器做完时结束。如果在转出过程中任何地方出错，停止转出。选择 NO，使转出将包安装在所有机器上。如果一台机器上出错，不会影响到其他机器上的包转出。

5、结束 --- 在点击做完按钮后，转出被建立或更新，并保存。

用 POST 方法，代理请求将是以 HTML 形式。主机响应将是良好格式化的 XML1.0 文档。大多数回退的文档具有这样简单的结构，将不包括 DTD，名字空格，或模式，但它们将在语句形成上和结构上兼容于 XML 规格。所有日期和时间标准化成协调世界时（GMT）。

这描述了在代理，请求者，和主机，更新服务之间的事务处理和数据流。所有更新事务处理将由代理初始化，除了下面情况：主机将打开，发送代理 ID 并然后依据代理 IP 地址的端口和协议关闭同意的，以有效地“Ping”或通知代理：它将不管它的请求方案，从主机中请求一张工作列表。

首次接触：

要求与更新服务器 528 的服务相反的任何代理将总是向指定主站请求/更新子目录。这子目录将配置成：能回退‘302 目标移动了’或它的‘新’位置。

如下面例子中示范的，代理执行www.patchlink.com 站更新子目录上的‘HEAD’请求。

Head 请求：

HEAD/update http/1.1

主机响应：去除该目标，并在由位置：header 提供的地址上可找到新位置。

Install Shield 代理注册：

在‘更新代理’的物理安装期间，管理员将要求在安装代理之前键入一些信息。该管理员（Admin）将被要求键入主机名或 IP 地址，账号标识符，GUID（全球唯一标识符），和用户名及注册时指定的口令。这数据将发送给主机，确认安装代理软件，并为该代理产生 ID 的能力。

代理任务列表

一旦 InstallShield 已经成功地将 BootStrap 代理软件安装在计算机上，这是代理开始工作的时间。在代理解决了更新服务器 528 的主站地址后，它邮寄一个“任务列表”请求。“任务列表”是一张简单的“任务”项列表，是管理员已经为代理安排要执行的任务项。

BootStrap 代理必须能够：

1、请求最初的任务列表；

2、接收该最初任务列表；

3、理解该最初任务列表；

4、下载全部代理的安装文件；

5、运行代理安装；

6、报告任何安装问题，假如这样的话，按指示继续；

7、启动全代理

8、轮询新任务列表；

9、理解 SoftPkg ID 和从属物并下载它们；

10、通过调用外部脚本引擎或通过从代理内调用脚本引擎来初始化“动作脚本”。

做出最初任务列表请求并处理回退响应的该代理完成这工作。例如：

任务列表请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：32

动作=任务列表

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 0.0

&本地时间 = 20000628010100

&状态 = 0

在这请求中，代理版本是 0.0。这给主机指出：这是该代理的新安装以及主机应当为该代理准备‘任务’，下载最近版的合适代理软件。在下列响应中，这被显示为第一‘任务’-任务 ID = “C1D50120-FE13-11d3-95B5-000629526438”。

无论何时存在有对代理策略的修改，主机将包括“任务列表”内的策略数据---因为这是来自代理的最初请求，策略数据包含在这个响应中。

本地时间正好就是本地的时间（不是 GMT）。这允许服务器正确地知道它在代理机器上的时间。格式是：YYYYMMDDHHMMSS。

状态告诉任务列表处理器，如果有任务要执行，仅回退一个简单的 yes 或 no 状态。

状态=0 意指回退一张正常任务列表，状态=1 意指告诉代理：你是否有任务要执行。这允许代理要进入 non-SSL 并做一次快速检验。

代理软件包请求

第一个任务指出：有一个模块要安装。如下面示出的，代理从主机请求详细的安装信息：

软件包请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnnn

动作 = SOFTPKG

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 0.0

&任务 ID = C1D50120-FE13-11d3-95B5-000629526438

&Pkg ID = 12340000-1111-0000-0000-000000000000

&本地时间 = 20000628010100

注意：在这情况中，代理的版本为 0.0。这给主机指出：要更新代理软件的包应当包含在任务列表响应内。这允许主机动态地确定：何时存在可用的代理软件的新版本，并指引代理更新它自己。

主机将“打开软件分配”的文档放在一起，所述文档详述了：代理能完成该任务所需的信息：

本地时间正好就是本地的时间（不是 GMT）。这允许服务器正确地知道一台代理机器上的时间。格式是 YYYYMMDDHHMMSS.

软件包（所有成分）

软件包示出了所有可能的 XML 组件（显示备份）。

<?xml 版本=“1.0”>

<!DOCTYPE SOFTPKG SYSTEM

“http://msdn.microsoft.com/standards/osd/osd.dtd”>

<SOFTPKG xmlns:GX=“http://www.patchlink.com/standards/osd/update.dtd”

GX：任务 ID =“ C1D50120-FE13-11d3-95B5-000629526438”

GX：Pkg ID =“12340000-1111-0000-0000-000000000000”

名字=“12340000-1111-0000-0000-000000000000”

GX：重新安装=“N” GX：回退“N”>

<标题>视窗 NT 更新代理</标题>

<IMPLEMENTATION>

<操作系统值=“win2k” />

<操作系统值=“win98” />

<硬盘大小值=“123456” />

<编码基数>

<GX：DIR 模块 ID=“00000104-0000-0000-0000-000000000000”>

<GX：目标地>

<GX：URI 日期时间=“20000415010100”>

<GX：URL>文件：//%TEM%</GX:URL>

<GX：ACL 属性=“RWXHSMA 名=”$其他”/>

<GX：ACL 属性=“RWXHSMA 名=”$用户”/>

<GX：URI>

<GX：目的地>

<GX：DIR>

<GX：文件扩展=“N” 重写=“Y” 模块 ID=“00000100-0000-0000-0000-000000000000”>

软件包状状态---成功

回退代码 RC 和 SoftPkgRC 是按十进制格式。SoftPkgRC 指示软件包全部完成。某些模块应当已经成功（RC=0），但另外的可能已引起出错。如果转出试图与已经曾经安装的包一起，那么，代理为它安装的所有模块回退（RC=0），并回退（SoftPkgRC=725003）或已安装了的 0x000b100b 软件包。

一旦完成了任务，代理将用该结果更新主机：

请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnn

动作 = Status

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 0.0

&任务 ID = C1D50120-FE13-11d3-95B5-000629526438

&PKG ID = 12340000-1111-0000-0000-000000000000

&安装 ID 日期 = 20000101123456

&软件 PkgRC = 0

&模块 ID = 0000010-0000-0000-0000-000000000000

&RC = 0

&RCMsg = 成功

文件属性和 ACL

这部分描述在 GX：目标地（GX：URI）成分中找到的 GX：ACL 成分。该更新内的属性提供给来自下面定义的超级集合内的代理。

在做基本文件属性的问题是：某些文件系统模糊了属性和 ACL 之间界线。属性是一个文件的基本 ACL，并且这儿定义的是一个小交叉平台超集。例如，视窗 NTFS 包括只读属性标记，但它也包括 Read ACL。因此，如果正在制作普通属性标记，那么必须期望：当用作为 ACL 时稍微要提防的含意。Unix 平台上的那些将看不见差别，除了类似于其他平台外，应当忽略不理解的标记或这儿列出的未定义的行为。

三个缺省 ACL 被定义了并起着类似基本文件属性的作用；$其他, $组, $用户。

在 Unix 文件系统中，将使用所有这三个属性 ACL。

然而，NT，FAT 和 NetWare 将仅使用$其他，作为基本文件属性。在 ACL 的 element.data 中的任何其他名字将形成一个名字。

ACL 和属性标记

字母	简称	定 义
R	读	显示文件数据，属性，拥有者，及许可
W	写	写进文件，附加到文件
X	执行	运行该文件（如果它是程序或包括与它相关的程序，应有必须的许可）
H	高速缓存	高速缓存文件
S	系统	系统文件
M	修改	读，写，修改，执行及改变文件属性
A	文档	文件已经准备好存档

XML 语法：

这给用户指示 ACL

<GX:ACL 属性 = “RWXHSMA” 名 = “用户名” />

对于组的 ACL，注意：$组将总是使用组=

<GX:ACL 属性 = “RWXHSMA” 组 = “组名” />

软件包 - 回退

HTTP/1.1 200 OK

连接：闭合

内容-类型：text/hml

内容-长度：nnn

<?xml 版本=“1.0” >

<!DOCTYPE SOFTPKG SYSTEM

“http://msdn.microsoft.com/standards/osd/osd.dtd” >

<SOFTPKG xmlns:GX=“http://www.patchlink.com/standards/osd/update.dtd”

GX：任务 ID = “ C1D50120-FE13-11d3-95B5-000629526438”

GX：Pkg ID = “12340000-1111-0000-0000-000000000000”

名字=“12340000-1111-0000-0000-000000000000”

GX：重新安装=“N” GX：回退“Y” >

<TITLE>视窗 NT 更新代理</TITLE>

<IMPLEMENTATION>

<硬盘大小值=“432” />

<编码基数>

<GX：文件扩展=“N” 重写=“Y” 模块 ID=“00000100-0000-0000-0000-000000000000” >

<GX：目的地>

<GX：URL>

<GX：URL>FILE://%TEM%/</GX：RL>

<GX：文件名>Hello World.txt</GX:文件名>

</GX：URL>

</GX：目的地>

<GX：备份>

<GX：URL>

<GX：URL>FILE://%TEM%/备份</GX:URL>

<GX：URL>

</GX：备份>

</GX：文件>

</CODEBASE>

</IMPLEMENTATION>

</SOFTTPKG>

这个例子回退带有上面所示备份的简单文件副本。代理指示来自SOFTPKG成分标签内的属性GX:Rollback = “Y”的回退。没有提供GX：Source成分标签。

目标地必须包括以将备份恢复到的一个文件名（注意：如果在回退之前不存在备份文件，这不是出错（当分配包时，目标地可以还未存在）。然而，如果在回退之前目的地存在且不能被去除，这是出错）。

代理服务器获取

有时代理可能安装在防火墙后面，在这样一种配置中，该代理仅允许访问主站点。该代理将检测它试图为位于销售商网站上的包检索一个模块时的情况。当该代理认识到；它不能与准则HTTP获取进行通信时，它能请求主机通过使用‘代理服务器获取’请求来获取代理行为上的文件---如下面描述的：

请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnn

动作 = 代理服务器获取

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 2.0

&URL = http://www.Microsoft.com/hotfix/Q12345.exe

代理服务器获取状态

请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnn

动作 = 代理服务器获取状态

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 2.0

&参考（Fef）ID = 107045CF06E011D28D6D00C04F8EF8E0

获取请求

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnn

动作 = 获取

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 2.0

&参考（Fef）ID = 107045CF06E011D28D6D00C04F8EF8E0

HTTP 获取

请求：

GET/download/Q12345.EXE http/1.1

带宽利用

范围指定获取请求：

HTTP/1.1 允许客户机请求：含在响应内的仅部分（响应实体的范围）响应实体。HTTP/1.1 使用在 Range and Content Range 标头字段的范围单位。一个实体可依据各种结构单位划分成子范围。

范围-单位 = 字节单位|其他范围单位

字节-单位 = “字节”

其他范围-单位 = 记号（token）

只有由 HTTP/1.1 定义的范围单位是“字节”。HTTP/1.1 的实现可忽略用其他单位指定的范围。HTTP/1.1 已经设计成：允许不要求依据范围知识就能实现应用软件。

因为所有 HTTP 实体在 HTTP 消息内表示为字节序列，字节范围的概念对任何 HTTP 实体是有意义的。

HTTP 内的字节范围规范应用于实体主体内的字节序列（不必与信息主体相同）。字节范围的操作可指定单个实体内的单个字节范围，或一组范围。

当管理员已经选择带宽利用特性，通过在代理策略数据内指定它们，该代理将做出“范围”指定的获取请求，而不是简单获取请求。

考虑下面代理简档：

<策略间隔类型=“S” 间隔=“60” 开始=“000000” 结束=“060000”

再试=“3” 后退=“10%” 总是使用代理服务器获取=“Y”

故障动作=“停止” UDP 口=“1234”，TCP 口=“Y”

保持有效期计数=“Y”

下载可恢复=“Y” 下载块大小=“1024”

下载等待方案=“S” 下载等待间隔=“10” />

下面示出 Q12345.Exe 文件的首次 1024 个字节的请求，以及主机的响应：

请求：

GET/download/Q12345.EXE http/1.1

范围：字节=0-1023

代理服务器获取请求：

POST *server_object_returned_in_firstcontact* http/1.1

内容-类型：text/html

内容-长度：nnn

动作 =获取

&帐号 ID = AF011203-7A09-4b67-A38E-1CB8D8702A50

&代理 ID = D7292F2D-CCFE-46dc-B036-3B318C2952E3

&代理版本 = 2.0

&参考 ID = 107045CF06E011D28D6D00C04F8EF8E0

&范围字节=0-1023

响应 XML 成分

成分	策略
属性	间隔类型 --- 时间周期类型； * S=秒 * M=分 * H=小时 间隔 --- 代理应当检查主机任务列表的时间周期数量； 开始 --- 代理应当启动运行并检查要做工作的天的时间（GMT）； 停止 --- 代理应当停止运行并检查要做工作的天的时间（GMT）； 再试 --- 在应用回退量之前再试请求的时间量； 回退 --- 在与主机故障接触后要添加到间隔的间隔类型时间量。通过附加一个百分号%，这可表示为百分数； UDP 口 --- {nnn} 用于唤醒代理的 UDP 端口号； TCP 口 --- {nnn} 用于唤醒代理的 TCP 端口号； 跟踪级 – OFF = 0， INFO = 1， DETAILED = 2，DEBUG = 3 清除间隔类型 --- 时间周期类型（见间隔类型） 清除间隔 --- 时间周期数（清除类型），代理应当扫描备份并清除具有比清除间隔更长时间的那些
依附于	任务列表
根	

源为	

成分	任务
属性	任务 ID --- 唯一任务标识符 PkgID --- 要激活的包标识符
依附于	任务列表
根源为	

发现代理 XML 标签

<名>标签 --- 这是想要搜索的文件名

* <路径>标签 --- 非常通用。这是想搜索文件所在的路径

<版本>标签 --- 这是想要寻找文件的版本

<建立>标签 --- 这是文件建立的日期

例子：<版本> > 5/30/2001 12:01:04PM</版本>

注意：较佳地是这种精确的日期格式。

<大小>标签 --- 这是想要搜索文件的大小；注意：Cannot due <or>

<根>标签 --- 这是搜索注册要进入的根键；

<键>标签 --- 这是想要寻找的注册内的键；

<值>标签 --- 这是想要寻找的键内的值；

<数据>标签 --- 这是期望在该键内找到的数据；

<类>标签 --- 能指定任何有效 WMI 类，使其有意义，例子 win32-services；

<搜索字段> --- 这是能最佳地确定要查看的 wmi 条目的字段；

<搜索值> --- 这是能最佳地确定要查看 wmi 条目的值；

<检查字段> --- 这是看望以获取期望获得值的字段；

<检查值> --- 这是期望找到的值。

输入文件<注册>段的例子。

<注册组件 id>=“” 报告 ID = “”>

<根></根>

<键></键>

<值></值>、

<数据></数据>

</注册>

补丁指纹签名例子

<报告 报告 id=“22”>

<文件组件 id=“1” 报告 ID=“1”>

<名>outlook.exe</名>

<路径></路径>

<版本></版本>

<建立></建立>

<大小>57393</大小>

<根>HKEY_LOCAL_MACHINE</根>

<键>SOFTWARE\Microsoft\Windows\Current\Version\App

路径\OUTLOOK.EXE</键>

<值>路径</值>

</文件>

</报告>

上面的例子将从注册中发现 outllook 路径并然后将更新它的大小。

摘要

本发明提供系统，方法，和配置存储介质，用于保证：软件更新是要求的，并计算机包括必需的软件和硬件组件，然后，用较小人工监督或不要求人工监督就更新网络上的软件，不要求其客户机正在更新的网络上管理机器上软件补丁的复制，并从受影响机器中去除该更新，当在安装期间发现问题或在用安装的补丁进行安装后使它们留在可用状态。

如这儿所用的，例如“一个”和“该”的术语和例如“更新服务器”的项目指定包括一个或多个的指定项目。特别地，在权利要求中，对一个项目的

参考意指至少要求一个这样的项目。当打算真正要一个项目时，这个文档将特别声明该需求。本发明可按其他特定格式来实施，并不背离它的基本特征。描述的实施例在所有方面仅被看作为示范性的而不是限制性的。标题仅为了方便。权利要求是描述本发明的说明书的一部分。因此，本发明的范畴是由附加权利要求指明的，而不是由前面的描述。在权利要求的相等物的意义和范围内的所有改变都包含在它们的范畴内。

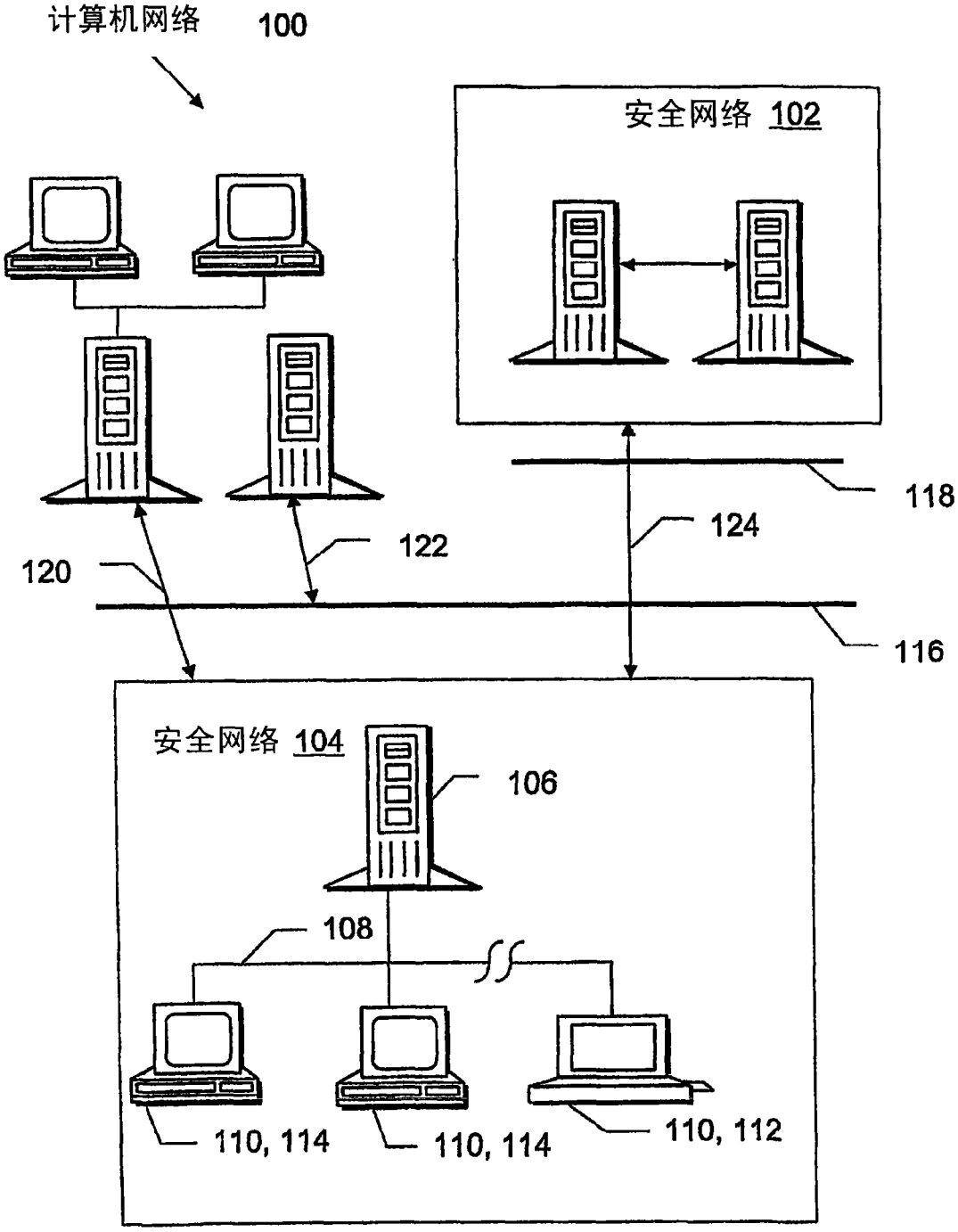

计算机网络 100
安全网络 102
118
124
122
120
116
安全网络 104
106
108
110, 114
110, 114
110, 112

图 1

2/8

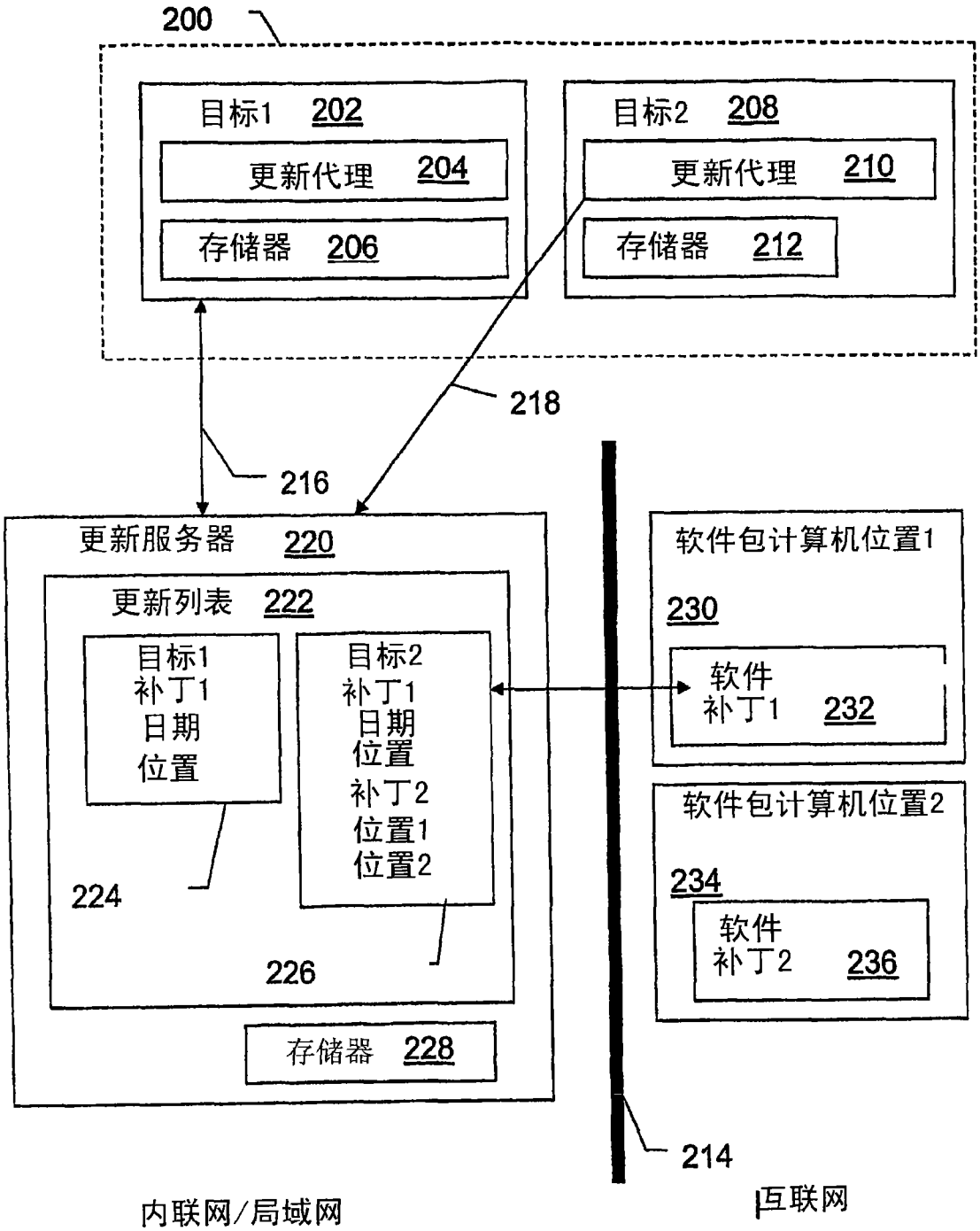

200
目标1 202
更新代理 204
存储器 206
目标2 208
更新代理 210
存储器 212
218
216
更新服务器 220
更新列表 222
目标1
补丁1
日期
位置
目标2
补丁1
日期
位置
补丁2
位置1
位置2
224
226
存储器 228
软件包计算机位置1
230
软件
补丁1 232
软件包计算机位置2
234
软件
补丁2 236
214
内联网/局域网
互联网

图 2

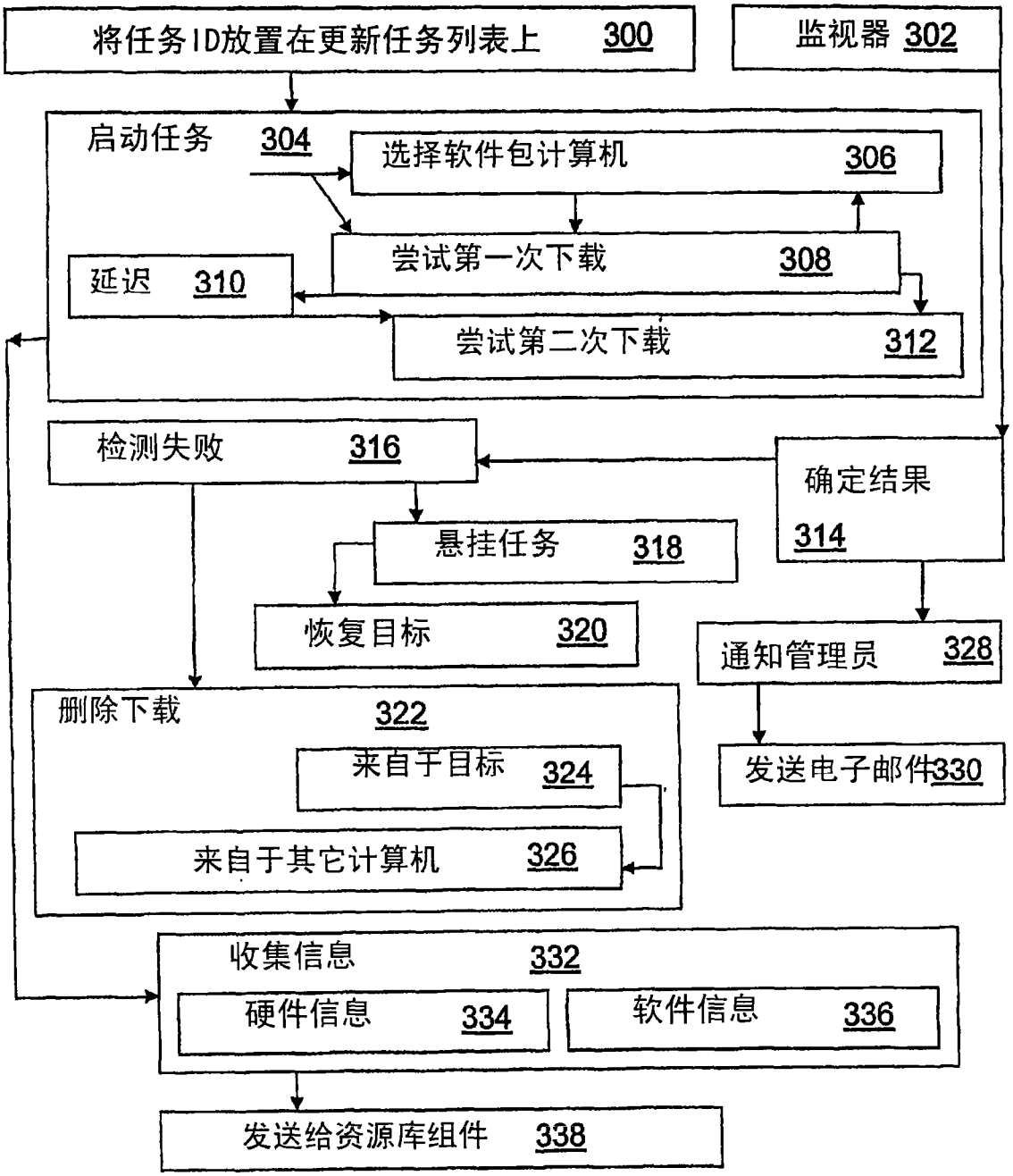

将任务ID放置在更新任务列表上 300
监视器 302
启动任务 304
选择软件包计算机 306
尝试第一次下载 308
延迟 310
尝试第二次下载 312
检测失败 316
确定结果 314
悬挂任务 318
恢复目标 320
通知管理员 328
删除下载 322
来自于目标 324
发送电子邮件330
来自于其它计算机 326
收集信息 332
硬件信息 334
软件信息 336
发送给资源库组件 338

图 3

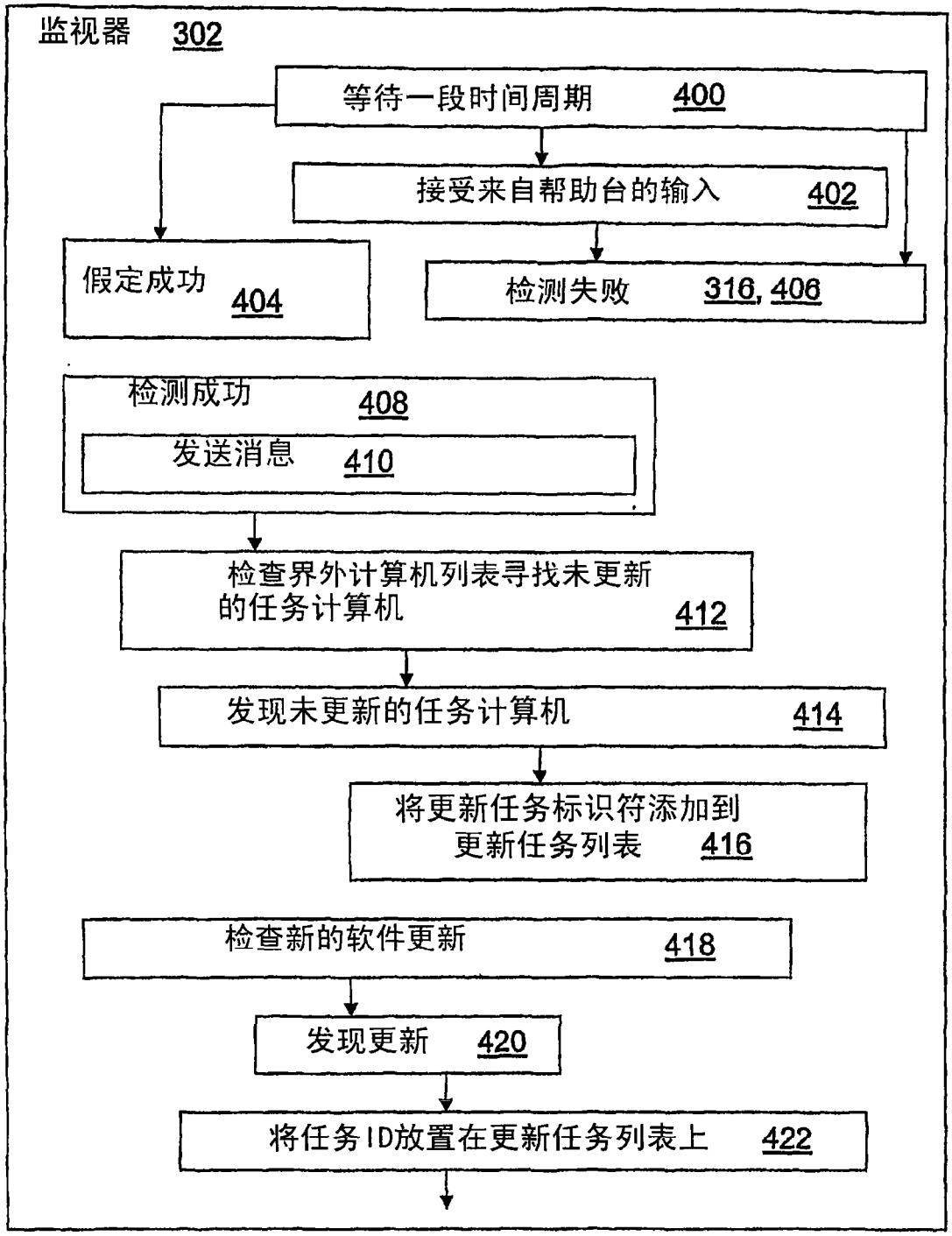

监视器 302
等待一段时间周期 400
接受来自帮助台的输入 402
假定成功 404
检测失败 316, 406
检测成功 408
发送消息 410
检查界外计算机列表寻找未更新的任务计算机 412
发现未更新的任务计算机 414
将更新任务标识符添加到更新任务列表 416
检查新的软件更新 418
发现更新 420
将任务ID放置在更新任务列表上 422

图 4

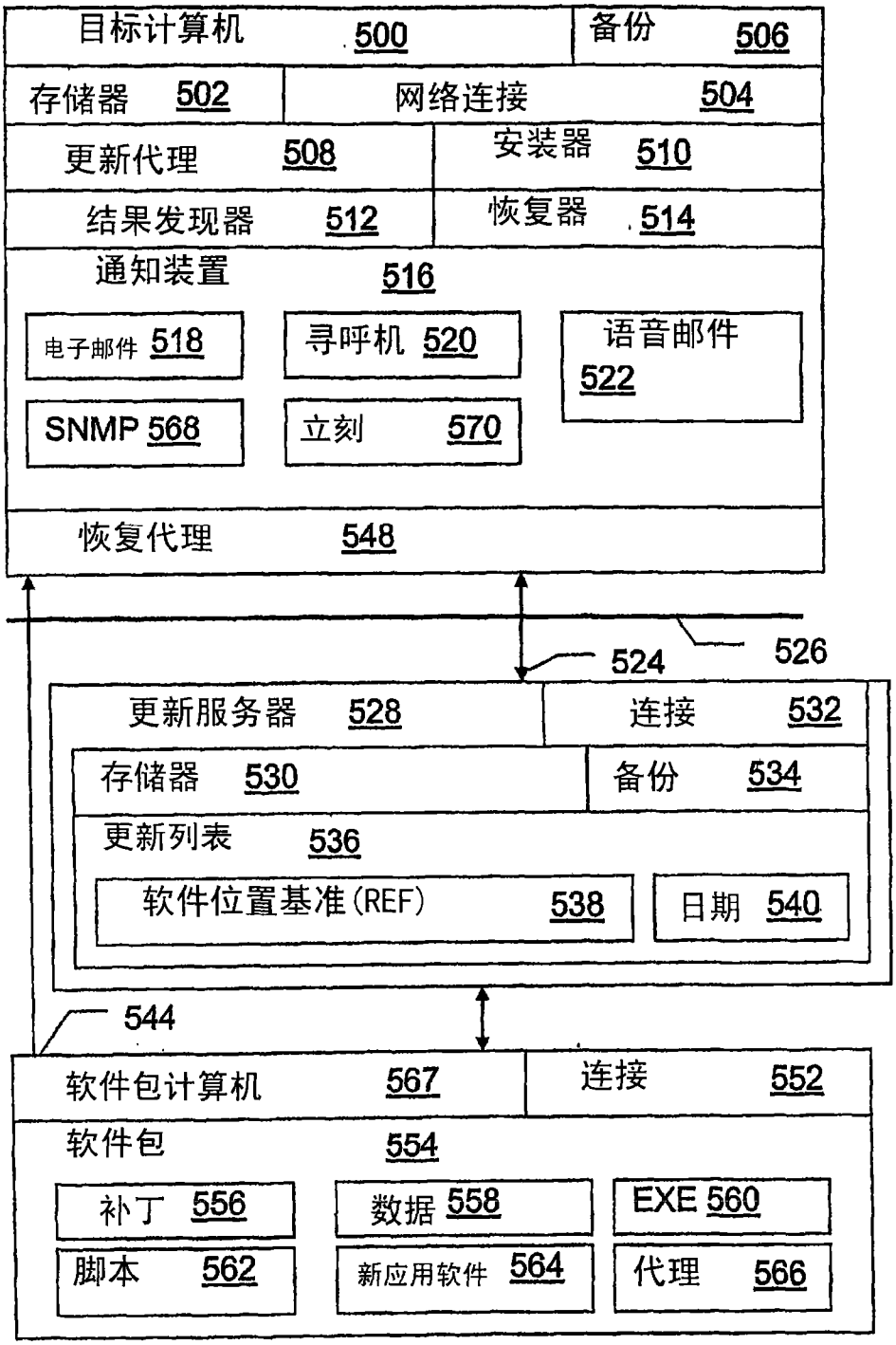

目标计算机 500
备份 506
存储器 502
网络连接 504
更新代理 508
安装器 510
结果发现器 512
恢复器 514
通知装置 516
电子邮件 518
寻呼机 520
语音邮件 522
SNMP 568
立刻 570
恢复代理 548
524
526
更新服务器 528
连接 532
存储器 530
备份 534
更新列表 536
软件位置基准(REF) 538
日期 540
544
软件包计算机 567
连接 552
软件包 554
补丁 556
数据 558
EXE 560
脚本 562
新应用软件 564
代理 566

图 5

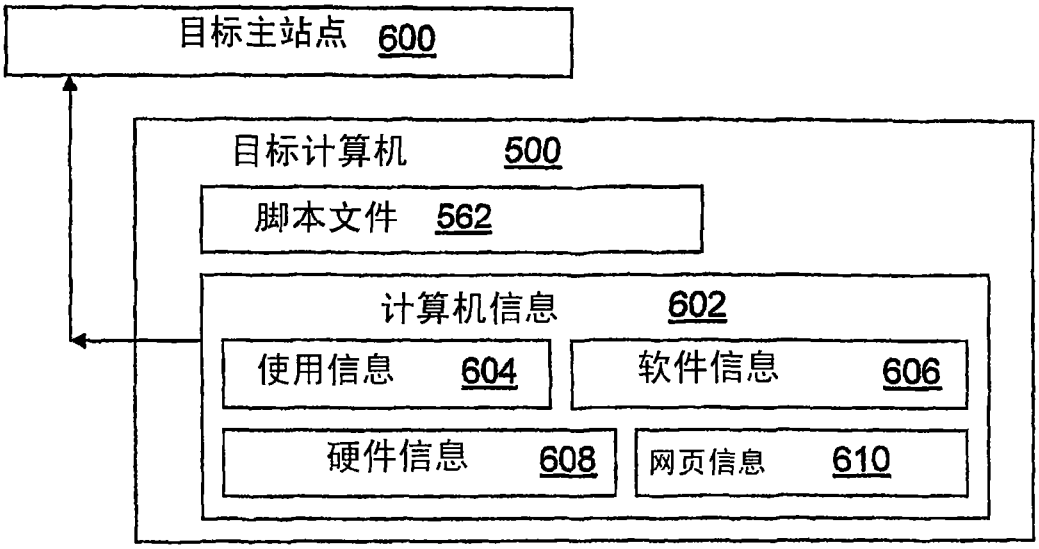

目标主站点 600
目标计算机 500
脚本文件 562
计算机信息 602
使用信息 604
软件信息 606
硬件信息 608
网页信息 610

图 6

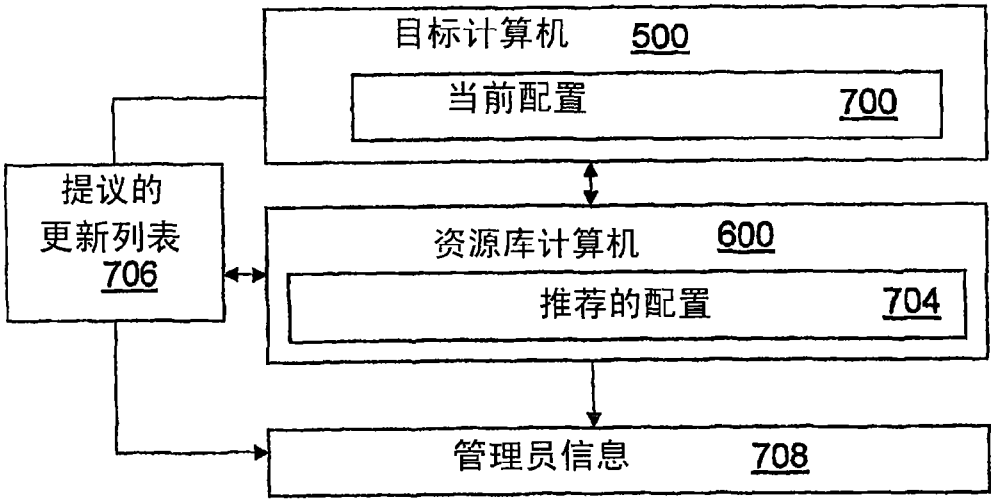

目标计算机 500
当前配置 700
提议的
更新列表
706
资源库计算机 600
推荐的配置 704
管理员信息 708

图 7

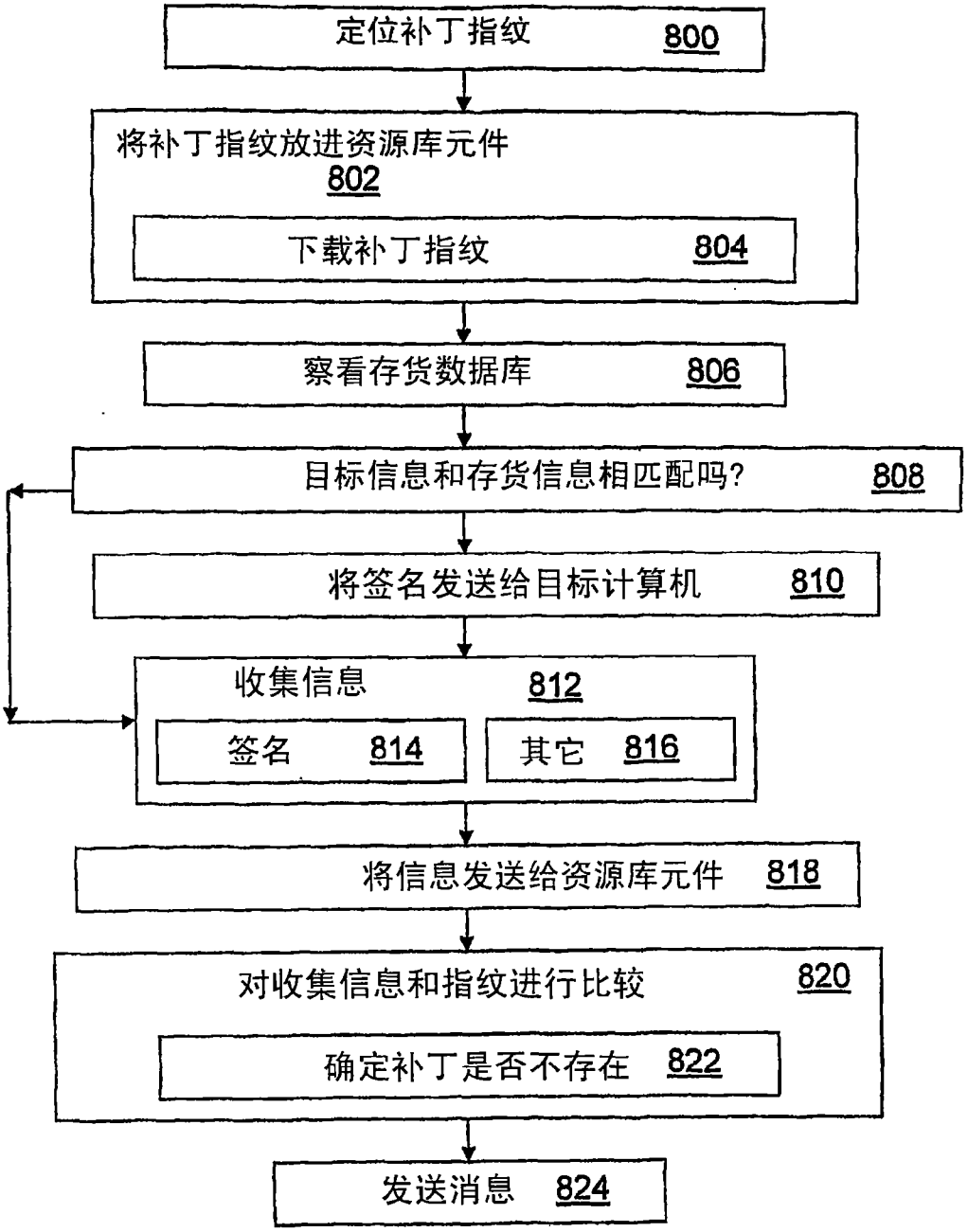

定位补丁指纹 800
将补丁指纹放进资源库元件 802
下载补丁指纹 804
察看存货数据库 806
目标信息和存货信息相匹配吗? 808
将签名发送给目标计算机 810
收集信息 812
签名 814
其它 816
将信息发送给资源库元件 818
对收集信息和指纹进行比较 820
确定补丁是否不存在 822
发送消息 824

图 8

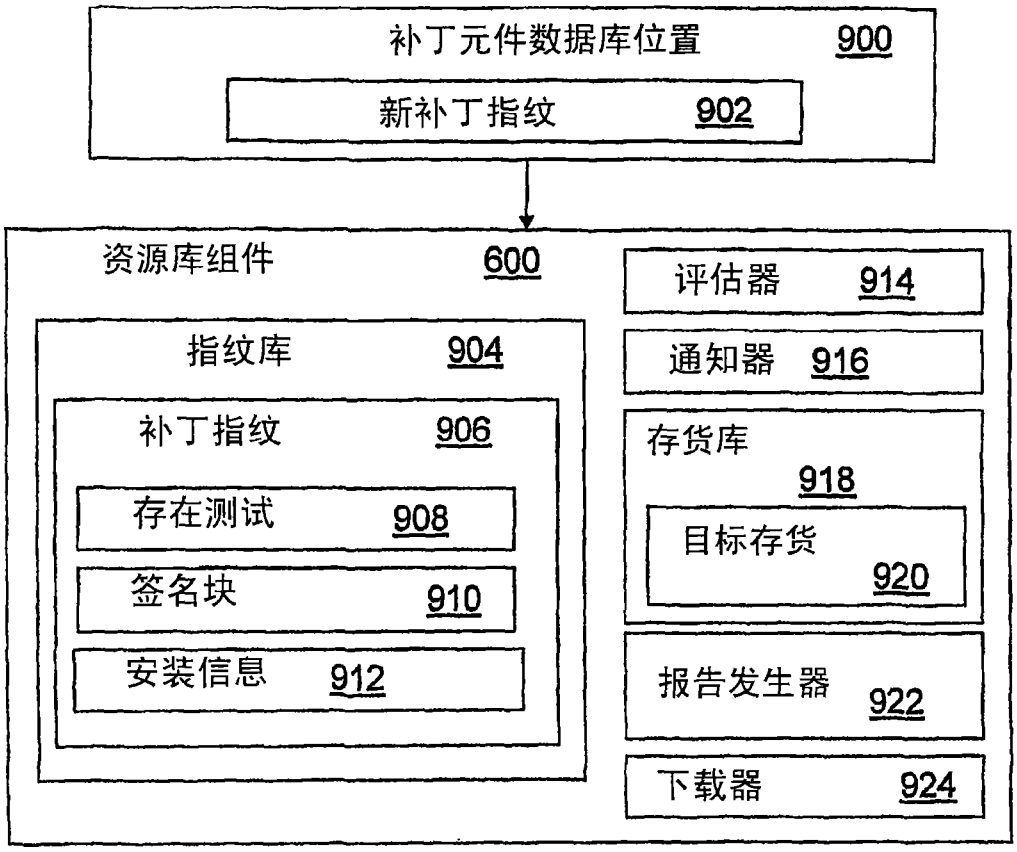

补丁元件数据库位置 900
新补丁指纹 902
资源库组件 600
指纹库 904
补丁指纹 906
存在测试 908
签名块 910
安装信息 912
评估器 914
通知器 916
存货库 918
目标存货 920
报告发生器 922
下载器 924

图 9