

[19] 中华人民共和国国家知识产权局

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



[12] 发明专利申请公布说明书

[21] 申请号 200580007173.5

[43] 公开日 2007 年 3 月 14 日

[11] 公开号 CN 1930817A

[22] 申请日 2005.3.1

[74] 专利代理机构 北京东方亿思知识产权代理有限公司

[21] 申请号 200580007173.5

代理人 王 怡

[30] 优先权

[32] 2004.3.9 [33] US [31] 10/797,773

[86] 国际申请 PCT/US2005/006738 2005.3.1

[87] 国际公布 WO2005/093991 英 2005.10.6

[85] 进入国家阶段日期 2006.9.5

[71] 申请人 思科技术公司

地址 美国加利福尼亚州

[72] 发明人 马克·阿马尔·拉耶斯 迈克尔·张
拉尔夫·多莫斯 彼得·迪尼

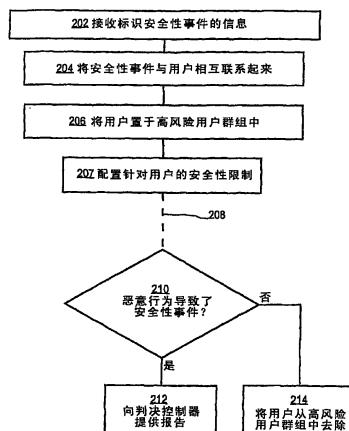
权利要求书 4 页 说明书 13 页 附图 6 页

[54] 发明名称

针对与高风险相关联的网络用户的隔离手段

[57] 摘要

一种提供与高网络风险相关联的计算机网络主机(110A)的隔离的计算机系统，其中所述网络包括一个或多个客户端(122A)、一个或多个交换机(108A)、一个或多个服务器资源(130)、网络管理站(102)以及管理正常地址池(124A)的地址服务器(124)，该系统的特征在于：高警戒地址池(124B)，其与可疑恶意网络用户相关联，并由地址服务器所管理；以及判决控制器(105)，其被配置用于：确定与导致网络中的安全性事件的网络设备相关联的用户标识符；使网络设备接收从高警戒地址池内的地址子集中选择出来的网络地址；以及针对选定的网络地址配置一个或多个安全性限制。



1. 一种提供与高网络风险相关联的计算机网络主机的隔离的计算机系统，其中所述网络包括一个或多个客户端、一个或多个交换机、一个或多个服务器资源、网络管理站以及管理正常地址池的地址服务器，所述系统的特征在于：

与所述正常地址池相分离的高警戒地址池，其与可疑恶意网络用户相关联，并由所述地址服务器所管理；

耦合在所述网络中并包括一个或多个计算机程序指令序列的判决控制器，所述指令在被一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

确定与导致网络中的安全性事件的网络设备相关联的用户标识符；

使所述网络设备接收从所述高警戒地址池内的地址子集中选择出来的网络地址；以及

针对选定的网络地址配置一个或多个安全性限制。

2. 如权利要求 1 所述的计算机系统，其中所述判决控制器接收标识所述网络中的安全性事件的信息，并且将所述安全性事件信息与网络用户信息相互联系起来，以便确定与所述网络设备相关联的用户标识符。

3. 如权利要求 1 所述的计算机系统，其中所述网络设备使用动态主机控制协议（DHCP）来获得所述网络地址，并且其中使所述网络设备接收网络地址的步骤包括重置耦合到所述网络设备的端口以提示用户命令所述网络设备利用 DHCP 请求新的网络地址。

4. 如权利要求 1 所述的计算机系统，其中所述网络设备使用动态主机控制协议（DHCP）来获得所述网络地址，并且其中使所述网络设备接收网络地址的步骤包括向所述网络设备发出 DHCP FORCE_RENEW 消息。

5. 如权利要求 1 所述的计算机系统，其中所述网络设备使用动态主机控制协议（DHCP）来获得所述网络地址，并且其中使所述网络设备接收网络地址的步骤包括提示所述网络设备利用 DHCP 请求新的网络地址。

6. 如权利要求 1 所述的计算机系统，其中所述网络设备使用动态主机控制协议（DHCP）来获得所述网络地址，并且其中使所述网络设备接收网络地址的步骤包括等待所述网络设备对当前网络地址的租期期满。

7. 如权利要求 1 所述的计算机系统，其中使所述网络设备接收网络地址的步骤包括以下步骤：向所述网络设备提供从特殊 IP 子网内的多个 IP 地址中选择出来的 IP 地址。

8. 如权利要求 7 所述的计算机系统，其中所述判决控制器向网络服务提供商公布描述所述特殊 IP 子网的特性的信息。

9. 如权利要求 1 所述的计算机系统，其中配置安全性限制的步骤包括以下步骤：修改与耦合到所述网络设备的端口相关联的互联网协议（IP）访问控制列表（ACL）以只许可来自选定网络地址的 IP 流量进入。

10. 如权利要求 1 所述的计算机系统，其中配置安全性限制的步骤包括以下步骤：修改与耦合到所述网络设备的端口相关联的媒体访问控制（MAC）ACL，以只许可针对绑定到选定网络地址的 MAC 地址的流量进入。

11. 如权利要求 1 所述的计算机系统，其中所述判决控制器确定是否恶意行为导致了所述安全性事件，如果是，则向安全性判决控制器提供关于所述安全性事件或恶意行为的信息。

12. 如权利要求 1 所述的计算机系统，其中所述判决控制器确定是否恶意行为导致了所述安全性事件，如果不是，则将所述用户从所述高风险群组中去除。

13. 如权利要求 1 所述的计算机系统，其中所述判决控制器确定是否恶意行为导致了所述安全性事件，其中如果所述用户与网络服务提供商的可信顾客相关联，则所述网络中的合法用户动作不被确定为是恶意行为。

14. 一种提供与高网络风险相关联的计算机网络主机的隔离的计算机系统，其中所述网络包括一个或多个客户端、一个或多个交换机、一个或多个服务器资源、网络管理站以及管理正常地址池的地址服务器，所述系统的特征在于：

与所述正常地址池相分离的高风险安全性群组，其与可疑恶意网络用

户相关联，并由所述地址服务器所管理；

耦合在所述网络中并包括一个或多个计算机程序指令序列的判决控制器，所述指令在被一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

接收标识网络中的安全性事件的信息；

将所述安全性事件信息与网络用户信息相互联系起来以便确定与所述网络设备相关联的网络用户；

将所述用户置于所述高风险安全性群组中；

针对选定的网络地址配置一个或多个安全性限制；

确定是否恶意行为导致了所述安全性事件；

如果恶意行为导致了所述安全性事件，则将关于所述安全性事件或恶意行为的信息提供给安全性判决控制器；

如果恶意行为未曾导致所述安全性事件，则将所述用户从所述高风险群组中去除。

15. 如权利要求 14 所述的计算机系统，其中将所述用户标识符置于高风险安全性群组中还包括以下步骤：强迫所述用户获取来自与高用户风险相关联的用户预留的指定网络地址群组的新网络地址。

16. 如权利要求 15 所述的计算机系统，其中所述判决控制器通过重新配置动态主机控制协议（DHCP）服务器以要求所述服务器只从与高用户风险相关联的用户预留的指定网络地址群组向所述网络设备发出新网络地址并且执行以下步骤中的任何一个来强迫所述用户获取新网络地址：重置耦合到所述网络设备的端口以触发所述网络设备利用 DHCP 请求新网络地址；向所述网络设备发出 DHCP FORCE_RENEW 消息；提示所述网络设备利用 DHCP 请求新网络地址；等待所述网络设备对当前网络地址的租期期满。

17. 如权利要求 14 所述的计算机系统，其中所述判决控制器通过以下操作来配置一个或多个安全性限制：修改与耦合到所述网络设备的端口相关联的互联网协议（IP）访问控制列表（ACL）以只许可来自选定网络地址的 IP 流量进入；并且修改与所述端口相关联的媒体访问控制（MAC）

ACL 以只许可针对绑定到所述选定网络地址的 MAC 地址的流量进入。

18. 一种提供与高网络风险相关联的计算机网络主机的隔离的计算机系统，其中所述网络包括一个或多个客户端、一个或多个交换机、一个或多个服务器资源、网络管理站以及管理正常地址池的地址服务器，所述系统的特征在于：

与所述正常地址池相分离的高警戒地址池，其与可疑恶意网络用户相关联，并由所述地址服务器所管理；

耦合在所述网络中并包括一个或多个计算机程序指令序列的判决控制器；

用于确定与导致网络中的安全性事件的网络设备相关联的用户标识符的装置；

用于使所述网络设备接收从与可疑恶意网络用户相关联的指定池的地址子集中选择出来的网络地址的装置；以及

用于针对选定的网络地址配置一个或多个安全性限制的装置。

针对与高风险相关联的网络用户的隔离手段

技术领域

本发明总地涉及计算机网络。本发明更具体而言涉及用于提高网络安全性的手段。

背景技术

这一部分中描述的手段可以实现，但是并不一定是先前已察觉或已实现的手段。因此，除非这里另有指明，否则这一部分中描述的手段并不是本申请中权利要求的现有技术，也不应当因为被包括在这一部分中而被当作现有技术。

2003年10月16日递交的Mark Ammar Rayes等人(Rayes等人的申请)的题为“Policy-based network security management”的美国专利申请10/688,051描述了一种基于策略的安全性管理控制器，其利用网络警戒状态、风险级别和网络健康状态信息来确定响应于网络安全性攻击应当采取什么动作。在一个实施例中，控制器利用历史警报或事件识别潜在的入侵者。

控制器还允许服务提供商针对可能的入侵者采取动作。为了防止恶意用户通过诸如IP地址欺骗、在动态主机控制协议(DHCP)下对网络地址的外来请求以及MAC地址欺骗来实现拒绝服务(DoS)，可能需要采取动作，在网络警戒级别较高时尤其如此。为了保持网络的完整性和稳定性，在网络性能降低之前防止攻击者造成进一步损害是很重要的。

安全性控制器是捕捉可能的入侵者并采取服务提供商所定义的适当动作的第一应用。但是，可能希望对潜在恶意用户采取比起完全禁止用户的网络访问来不那么严厉的动作。例如，在设置期间过多次地改变设备的IP地址的不熟练用户可能被不适当地区分为发起DoS攻击的恶意用户。由于安全性控制器不适当地区分这类无辜用户分类为恶意用户而对该用户拒绝服

务可能会导致用户选择另一个服务提供商。

另一方面，控制器负责防止灾害性巨大网络故障，尤其是在网络性能较坏期间。在服务提供商能够确定可疑用户是否真的是恶意用户之前需要对可疑用户行为进行详细分析，而这种分析是花时间的。控制器可能在不等待这种分析的情况下判决禁止用户访问以确保不能造成进一步的损害，尽管这种判决可能是错误的。

因此，需要这样一种方式，这种方式允许服务提供商在不完成阻止网络访问的情况下防止对网络的损害，同时允许有时间来对可疑用户的流量行为应用进一步的诊断和分析，而不会使非恶意用户那部分感到受挫。

附图说明

在附图中以示例方式而非以限制方式图示了本发明，在附图中，相似的标号指代类似的元件，在附图中：

图 1A 是可用于实现实施例的示例性网络上下文的框图；

图 1B 是可使用的替换网络上下文的框图；

图 2 是示出针对与高风险相关联的网络用户的隔离手段的一个实施例的高级别概况的流程图；

图 3A 是配置安全性限制的过程的流程图；

图 3B 是将用户置于高风险用户群组中的过程的流程图；

图 4 是将用户从高风险用户群组中去除的过程的流程图；以及

图 5 是示出可以用来实现实施例的计算机系统的框图。

具体实施方式

描述了提供针对与高风险相关联的网络用户的隔离手段的方法和装置。在下面的描述中，出于说明目的，给出了大量具体细节以便完全理解本发明。但是，本领域技术人员将会清楚，没有这些具体细节也可以实施本发明。在其他实例中，公知的结构和设备以框图形式示出，以避免不必要的模糊本发明。

这里根据下面的大纲描述实施例：

1.0 概述

2.0 针对与高风险相关联的网络用户的隔离手段

2.1 将用户置于高风险用户群组中

2.2 配置安全性限制

2.3 将用户从高风险用户群组中去除

2.4 与安全性控制器交互

2.5 其他实施例

3.0 实现机构—硬件概述

4.0 扩展和替换

1.0 概述

在本发明中实现了在前述背景技术部分中提出的需要、以及将从下面的描述中变清楚的其他需要和目的，本发明包括一种针对与高风险相关联的网络用户的隔离手段。根据一种手段，一种方法包括以下用计算机实现的步骤：确定与导致网络中的安全性事件的网络设备相关联的用户标识符；使所述网络设备接收从与可疑恶意网络用户相关联的指定池内的地址子集中选择出来的网络地址；以及针对选定的网络地址配置一个或多个安全性限制。

在第二方面中，一种方法包括以下用计算机实现的步骤：接收标识网络中的安全性事件的信息；将所述安全性事件信息与网络用户信息相互联起来以便确定与所述网络设备相关联的网络用户；将所述用户置于高风险安全性群组中；针对选定的网络地址配置一个或多个安全性限制；确定是否恶意行为导致了所述安全性事件；如果恶意行为导致了所述安全性事件，则将关于所述安全性事件或恶意行为的信息提供给安全性判决控制器；并且如果恶意行为未曾导致所述安全性事件，则将所述用户从所述高风险群组中去除。

前述的方面可能包括许多其他特征、替换和变化，这些特征、替换和变化将从下面的描述和权利要求中显现出来。此外，在其他方面中，本发明包括被配置为执行前述步骤的计算机装置和计算机可读介质。

这里的公开引入了“高警戒”网络用户群组。被怀疑对网络执行诸如任何类型的欺骗攻击、拒绝服务攻击等恶意行为的网络用户被强制进入高警戒用户群组。高警戒用户群组中的用户的流量被路由经过监视服务器，在该监视服务器处执行详细的流量分析，以确定用户是否确实在执行恶意行为，以便采取适当的动作。关于适当动作的判决可以在安全性控制器的帮助下作出。在安全性控制器作出判决之前，在执行监视的同时，高警戒用户群组中的用户继续接收受限的网络服务。结果，用户服务并未被完全中断。在某些情况下，这确保了用户和服务提供商之间的任何服务协议不会遭到破坏。

在一个特定实施例中，检测安全性事件并使之与用户相互联系起来。通过改变用户所使用的末端站的网络地址，将用户置于高警戒用户群组中。通过将可疑恶意用户的所有流量路由经过监视服务器，来密切监视可疑用户在网络中的动作。可疑用户的网络访问受到限定或限制，以便用户不能损害网络。例如，高警戒用户群组中的可疑用户不能改变网络针对用户末端站所识别的 MAC 地址，用户需要接收来自为高警戒用户群组预留的特殊地址池的网络地址，等等。只有在管理员确定用户确实在进行安全性侵害之后才执行更重大的动作，例如终止用户的网络访问或将用户放回不受限用户群组中。此外，在一个实施例中，可以向高警戒用户群组中的所有可疑用户应用单个动作。例如，在紧急情况下，这种集体动作可能是适当的。集体动作的示例是临时暂停对高警戒用户群组的所有成员的服务并提供说明性消息。

在特定实施例中，应用 DHCP 动态地址分布、IP 地址子网、交换机 ARP 表和网络管理技术来将可疑用户放到高警戒群组中，用户的流量在其下被网络密切监视，同时服务合同中指定的用户服务不受影响或者只是部分受影响。

2.0 针对与高风险相关联的网络用户的隔离手段

图 1A 是可以用于实现实施例的示例性网络上下文的框图。图 1A 意图是示出一个示例性上下文；但是，这里描述的手段可以在任何网络上下文

中实现。在图 1A 中，网络操作中心 100 由管理被管理网络 106 的网络服务提供商所拥有或操作。一般来说，私有企业使用被管理网络 106，并且是网络服务提供商的顾客。

一个或多个经授权的用户 110A、110B 利用网络元件 108 来发送或接收数据或多媒体通信，以与服务器资源 130 交互。网络元件 108 可以包括路由器、交换机或其他基础设施元件，而被管理网络 106 可以包括以任何有用或合乎需要的拓扑耦合的任何数目的网络元件。此外，除服务器资源 130 之外，被管理网络 106 还可以包括任何数目的末端站或资源，例如其他服务器、工作站，或者个人计算机、打印机、存储装置和其他外围设备。

恶意用户 120 也可能尝试利用被管理网络 106 发送或接收未经授权的数据或命令。恶意用户 120 可以是尝试危害被管理网络 106 或致使服务器资源 130 或网络元件 108 对他人不可用的用户，或者未经授权的用户可以是无意地执行未经授权的行为或者多次尝试执行根据指定访问策略被视为过度的动作的无辜个体。

如图 1A 所示的经授权的用户 110A、110B 和恶意用户 120 广泛地代表诸如个人计算机、工作站等任何末端站设备，单独或共同使用诸如路由器、集线器等网络基础设施元件，以及单独或共同具有使用、拥有或操作这种设备的相关用户。

网络操作中心包括网络管理站（NMS）102、监视服务器 104 和判决控制器 105。网络管理站 102 包括容宿着提供诸如网络元件 108 的配置这样的功能的网络管理软件的工作站或计算机。监视服务器 104 可以针对网络元件 108 执行流量分析或详细监视功能。判决控制器 105 可以接收来自 NMS 102 和监视服务器 104 的输入，并且可以确定在被管理网络 106 中应当采取什么动作来防止被管理网络遭到未经授权的用户的攻击或危害。

图 1B 是可以使用的替换网络上下文的框图。图 1B 具体指示 NOC 100 可以包括用于动态地向经授权的用户 110A、110B 和恶意用户 120 提供网络地址的 DHCP 服务器 124。如下文进一步描述的，DHCP 服务器 124 可以在适当的判决逻辑的控制下选择来自正常地址池 124A 或来自高警戒地

址池 124B 的地址。经授权的用户 110A、110B 和恶意用户 120 分别容宿着 DHCP 客户端 122A、122B、122C，这些 DHCP 客户端利用 DHCP 消息来与 DHCP 服务器 124 交互，如这里进一步描述的。

经授权的用户 110A、110B 和恶意用户 120 可通信地耦合到交换机 108A，该交换机维护着地址解析协议（ARP）表 126。在一个实施例中，ARP 表 126 除了其他信息以外还维护着经授权的用户 110A、110B 和恶意用户 120 的 MAC 地址与已由 DHCP 服务器 124 分配给经授权的用户 110A、110B 和恶意用户 120 的 IP 地址的关联。ARP 表 126 与 DHCP 服务器 124 的交互在下文进一步描述。

图 2 是示出针对与高风险相关联的网络用户的隔离手段的一个实施例的高级别概况的流程图。在步骤 202 中，接收标识安全性事件的信息。在步骤 204 中，将安全性事件信息相互联系起来，从而识别导致安全性事件或与安全性事件相关联的用户。相关可以包括诸如在用户信息数据库中查找安全性事件信息中携带的网络地址这样的动作。

在步骤 206 中，将用户置于高风险用户群组中。用于将用户置于高风险用户群组中的特定手段在后面的部分中描述。

在步骤 207 中，为用户配置一个或多个安全性限制。安全性限制限定用户在被管理网络中能够执行的动作。一般来说，配置安全性限制的目的是隔离网络中的恶意用户，以便检疫可疑恶意用户，从而避免对网络造成进一步损害。用于将用户置于高风险用户群组中的特定手段在后面的部分中描述。

在步骤 207 之后的不确定长的时间之后，如虚线 208 所示，在步骤 210 处执行测试，以确定是否恶意行为导致了在步骤 202 中接收到其有关信息的安全性事件。步骤 210 例如可以包括网络管理人员详细审查安全性事件，针对识别出的用户或用户使用的网络元件执行流量分析，等等。在一个实施例中，如果发觉用户在执行可疑的网络动作，就将用户分类为恶意用户，所述可疑的网络动作例如是污染交换机 108A 的 ARP 表 126（图 1B）、IP 欺骗等等。这种动作可由执行指定的软件应用的网络硬件检测到，例如来自 Cisco System, Inc. 的 Cisco Catalyst 6500 系列交换机中的

ARP 检查特征或动态 ARP 检查特征。这种动作也可以由 Rayes 等人的申请中描述的安全性控制器来确定。

在步骤 212 中，如果步骤 210 的测试为真，则向判决控制器提供报告。在步骤 214 中，如果步骤 210 的测试为假，则将用户从高风险用户群组中去除。用于将用户从高风险用户群组中去除的特定手段在后面的部分中描述。

利用前述手段，在对用户、安全性事件或其他信息进行详细审查的同时，有效地限制或检疫与安全性事件相关联的用户。并不完全切断用户对被管理网络的访问，而是限制用户的动作。结果，可在评估恶意用户的动作的同时检疫恶意用户，而无辜用户不会遭受连接断开或与缺乏网络访问相关联的受挫感。

2.1 将用户置于高风险用户群组中

图 3B 示出将用户置于高风险用户群组中的过程的流程图。为了示出清楚的示例，图 3B 和下文随后描述的剩余附图是在图 1B 的示例性上下文中描述的。但是，这里描述的技术也适用于其他上下文中。

图 2 和图 3B 都假定已经创建了高风险用户群组。在被管理网络 106 是基于 IP 分组的网络的一个实施例中，创建高风险用户群组包括特别为被管理网络的可疑订户或用户创建新的 IP 地址子网。该子网可被称为“高警戒 IP 地址池”。从而，高警戒地址池 124B（图 1B）可以包括新 IP 子网中的地址。

创建高警戒 IP 地址池可通过请求 IP 地址分配机构（例如因特网分配名称和号码组织（ICANN））创建特别用于可疑恶意用户的全局可识别 IP 范围来执行。例如，可以使用子网 34.34.x.x。该手段在 IPv6 的上下文中尤其有用，其提供了可用来创建高警戒地址范围的额外地址空间。或者，可以在 ISP 网络内创建高警戒 IP 地址池；不需要针对整个互联网全局地定义池。

或者，服务提供商可以创建为可疑恶意用户预留的特殊 IP 地址范围，并且可以向其他服务提供商公开定义特殊范围的参数。例如，具有范围

xxx.xxx.xxx.240-250 内的主机 IP 地址的地址可被指定为处于高警戒地址池 124B 内。接收从高警戒地址池 124B 选择出来的网络地址以用于高风险用户设备的用户被称为处于高警戒用户群组内。

为了将可疑用户置于高警戒群组中，用户的设备需要接收处于高警戒地址范围内的新网络地址。在一个实施例中，在步骤 206A 中，DHCP 服务器 124 被用指令重新配置，以使 DHCP 服务器仅将来自高警戒地址池 124B 的地址提供给用户设备。例如，在一个实施例中，操作支持系统（OSS）、订户管理系统或网络管理站 102 配置 DHCP 服务器 124 或网络元件 108 中的 DHCP 服务器，以向恶意设备分配来自高警戒地址池 124B 的网络地址。

在步骤 206B 中，用户末端站被强迫获取来自高警戒地址池的新网络地址。在 DHCP 实施例中，OSS 使恶意设备发送 DHCPREQUEST。如图 3B 所示，可以使用若干个不同的技术来使设备请求新地址。例如，如方框 302 所示，OSS 使交换机或访问设备，例如交换机 108A，执行端口重置。在一个实施例中，方框 302 包括执行 2003 年 11 月 24 日递交的 Ralph Droms 的题为“Methods and apparatus supporting configuration in a network”、代理案卷号为 No. CIS03-51 (7908)的共同待决的申请中描述的技术，这里通过引用将该申请的全部内容结合进来，就好像在这里完全阐述了一样。

或者，如方框 304 所示，OSS 等待恶意用户 120 为其当前网络地址保持的租期（lease）期满。恶意用户 120 的末端站设备在期满时或期满之前不久将会自动请求来自 DHCP 服务器 124 的新地址。又或者，在方框 306 中，OSS 或 NMS 102 提示恶意用户 120 执行 ipconfig/release 和 ipconfig/renew 操作。又或者，在方框 308 中，OSS 或 NMS 102 使交换机 108A 或其他访问设备发送 DHCP FORCE_RENEW 消息，如果交换机 108A 或访问设备支持这种功能的话。作为响应，恶意用户 120 的末端站设备自动请求来自 DHCP 服务器 124 的新地址。

在执行前述替换方案中的任何一种之后，在步骤 206C 中，DHCP 服务器 124 向与恶意用户 120 相关联的客户端设备分配来自高警戒地址池

124B 的地址。在步骤 206D 中，可疑恶意用户所使用的网络访问设备处的 ARP 表被用新地址更新。例如，恶意用户 120 所使用的交换机 108A 的 ARP 表 126 被更新。

例如，作为交换机 108A 中的 ARP 过程的正常操作的一部分，ARP 过程检测恶意用户 120 的新地址，因为该新地址与当前存储在 ARP 表 126 中的在先地址不同。因此，在恶意用户 120 接收或发送第一个数据报之后，ARP 过程自动更新 ARP 表 126。或者，如果在访问设备中 DHCP 偷听（snooping）或安全 ARP 特征是活动的，则响应于交换机 108A 检测到 DHCP 服务器 124 和恶意用户 120 之间的 DHCP 事务，ARP 表 126 被自动更新。

2.2 配置安全性限制

图 3A 是配置安全性限制的过程的流程图。在一个实施例中，图 3A 的过程被用于实现图 2 的步骤 207。

在一个实施例中，为了确保可疑用户不能对网络造成损害，使用了访问控制列表（ACL）和 DHCP 流量标记。例如，在步骤 207A 中，MAC 访问控制列表条目被设置，在步骤 207B 中，IP 访问控制列表条目被设置。

例如，在图 1A 的网络元件 108 或图 1B 的交换机 108A 是在 Cisco 命令行接口（CLI）语言的控制下工作的 Cisco 交换机或路由器的实现方式中，可以使用下面的 CLI 命令。作为步骤 207A 的一部分，耦合到恶意用户 120 的网络元件 108 或交换机 108A 处的端口的 MAC ACL 被用命令“`permit mac <user's MAC address> any`”修改。前述命令的作用是在相关联的端口上只许可带有指定用户的 MAC 地址的流量。

类似地，用户端口处的 IP ACL 可被用命令“`permit ip <special IP> any`”修改。前述命令的作用是只允许带有新分配的特殊 IP 的流量进入网络元件 108 或交换机 108A 的相关联端口。

IP ACL 和 MAC ACL 的配置只是步骤 207 中可以应用的安全性措施的一个示例。也可以应用其他安全性措施。例如，来自可疑用户的所有流量都可被强迫经过监视服务器 104。在一种实现方式中，交换机 108A 处的

策略路由选择可被用来在将所有来自具有高警戒地址池中的地址的用户的流量转发到实际目的地之前，先将它们路由到监视服务器 104。

通过在受到密切监视的高警戒子网中实施这种严格的安全性措施，可疑恶意用户被检疫。这种用户还被置于密切监视之下，并且被防止对网络造成进一步的危害。

2.3 将用户从高风险用户群组中去除

图 4 是用于将用户从高风险用户群组中去除的过程的流程图。在一个实施例中，图 4 的过程被用于实现图 2 的步骤 214。一般来说，图 4 代表图 3A、图 3B 的逆转。从而，在步骤 214A 中，用户末端站被强迫获取来自常规网络地址的指定群组的新网络地址。可以使用图 3B 的步骤 206A、302、304、306、308 和 206D 的技术。但是，在图 4 的情况下，分配给用户末端站的新网络地址是从常规网络地址池中选择出来的。例如，这些技术导致 DHCP 服务器 124（图 1B）将来自正常地址池 124A 的地址分配给恶意用户 120。

在步骤 214B 中，MAC 访问控制列表条目被重置。在步骤 214C 中，IP 访问控制列表条目被重置。步骤 214B、214C 可以包括将恶意用户 120 在其上与网络元件 108 或交换机 108A 通信的端口的 MAC ACL 和 IP ACL 的状态恢复到用户被置于高警戒用户群组之前的状态。或者，步骤 214B、214C 可以包括发出去除先前设置的安全性限制的命令。例如，在 Cisco 实施例中，可以发出命令“permit mac any any”和“permit ip any any”。

结果，恶意用户 120 被从高警戒用户群组去除并被置于正常用户群组中。与高警戒用户群组相关联的安全性限制被去除，并且用户接收不受限制的网络访问。在监视服务器 104 进行监视或判决控制器 105 进行判决期间，用户接收受限制的网络访问，但并未与被管理网络 106 完全切断。

3.0 实现机构—硬件概述

图 5 是示出可以实现本发明的实施例的计算机系统 500 的框图。计算机系统 500 包括用于传输信息的总线 502 或其他通信机构和与总线 502 相耦合用于处理信息的处理器 504。计算机系统 500 还包括诸如随机存取存储器 (RAM) 或其他动态存储设备之类的主存储器 506，其耦合到总线 502，用于存储信息和处理器 504 要执行的指令。主存储器 506 还可用于存储在处理器 504 执行指令期间的临时变量或其他中间信息。计算机系统 500 还包括只读存储器 (ROM) 508 或其他静态存储设备，其耦合到总线 502，用于存储静态信息和处理器 504 的指令。提供了诸如磁盘或光盘之类的存储设备 510，其耦合到总线 502，用于存储信息和指令。

计算机系统 500 可以经由总线 502 耦合到显示器 512，例如阴极射线管 (“CRT”)，用于向计算机用户显示信息。包括字母数字和其他键的输入设备 514 被耦合到总线 502，用于向处理器 504 传输信息和命令选择。另一类用户输入设备是光标控制装置 516，例如鼠标、跟踪球、触笔或光标方向键，用于向处理器 504 传输方向信息和命令选择，并用于控制显示器 512 上的光标移动。该输入设备一般具有两个轴（第一轴（例如 x）和第二轴（例如 y））上的两个自由度，其允许设备指定平面中的位置。

本发明涉及使用计算机系统 500 来实现针对与高风险相关联的网络用户的隔离手段。根据本发明的一个实施例，针对与高风险相关联的网络用户的隔离手段由计算机系统 500 响应于处理器 504 执行包含在主存储器 506 中的一条或多条指令的一个或多个序列而提供。这种指令可以被从另一计算机可读介质（如存储设备 510）读取到主存储器 506 中。包含在主存储器 506 中的指令序列的执行使得处理器 504 执行这里描述的过程步骤。在替换实施例中，可以使用硬线电路来替代软件指令或与软件指令相组合以实现本发明。从而，本发明的实施例并不限于硬件电路和软件的任何特定组合。

这里所用的术语“计算机可读介质”指参与向处理器 504 提供指令以供执行的任何介质。这种介质可以采取许多形式，包括但不限于：非易失性介质、易失性介质和传输介质。非易失性介质例如包括光盘或磁盘，如

存储设备 510。易失性介质包括动态存储器，如主存储器 506。传输介质包括同轴电缆、铜线和光纤，包括含总线 502 的线路。传输介质也可以采取声波或光波的形式，例如在无线电波和红外数据通信期间生成的声波或光波。

计算机可读介质的常见形式例如包括软盘、柔性盘、硬盘、磁带或任何其他磁介质，CD-ROM、任何其他光介质，穿孔卡、纸带、任何其他具有孔图案的物理介质，RAM、PROM 和 EPROM、FLASH-EPROM、任何其他存储器芯片或磁带盒（cartridge），下文中描述的载波，或者计算机可以读取的任何其他介质。

计算机可读介质的各种形式可用于将一条或多条指令的一个或多个序列传输到处理器 504 以供执行。例如，指令可以首先承载在远程计算机的磁盘上。远程计算机可以将指令加载到其动态存储器中，并利用调制解调器经由电话线发送指令。计算机系统 500 本地的调制解调器可以接收电话线上的数据，并使用红外发送器来将数据转换为红外信号。红外检测器可以接收在红外信号中携带的数据，并且适当的电路可以将数据置于总线 502 上。总线 502 将数据传输到主存储器 506，处理器 504 从主存储器 506 取得指令并执行指令。主存储器 506 接收的指令可以可选地在处理器 504 执行之前或之后存储到存储设备 510 上。

计算机系统 500 还包括耦合到总线 502 的通信接口 518。通信接口 518 提供到连接到本地网络 522 的网络链路 520 的双向数据通信耦合。例如，通信接口 518 可以是综合业务数字网络（ISDN）卡或调制解调器，以提供到相应类型电话线的数字通信连接。又例如，通信接口 518 可以是局域网（LAN）卡，以提供到兼容 LAN 的数据通信连接。也可以实现无线链路。在任何这种实现方式中，通信接口 518 发送并接收电的、电磁的或光信号，这些信号携带了代表各种类型信息的数字数据流。

网络链路 520 一般经过一个或多个网络提供到其他数据设备的数据通信。例如，网络链路 520 可以经过本地网络 522 提供到主机计算机 524 或由因特网服务供应商（ISP）526 操作的数据设备的连接。ISP 526 又经过全球分组数据通信网络（现在通常称为“因特网”528）提供数据通信服

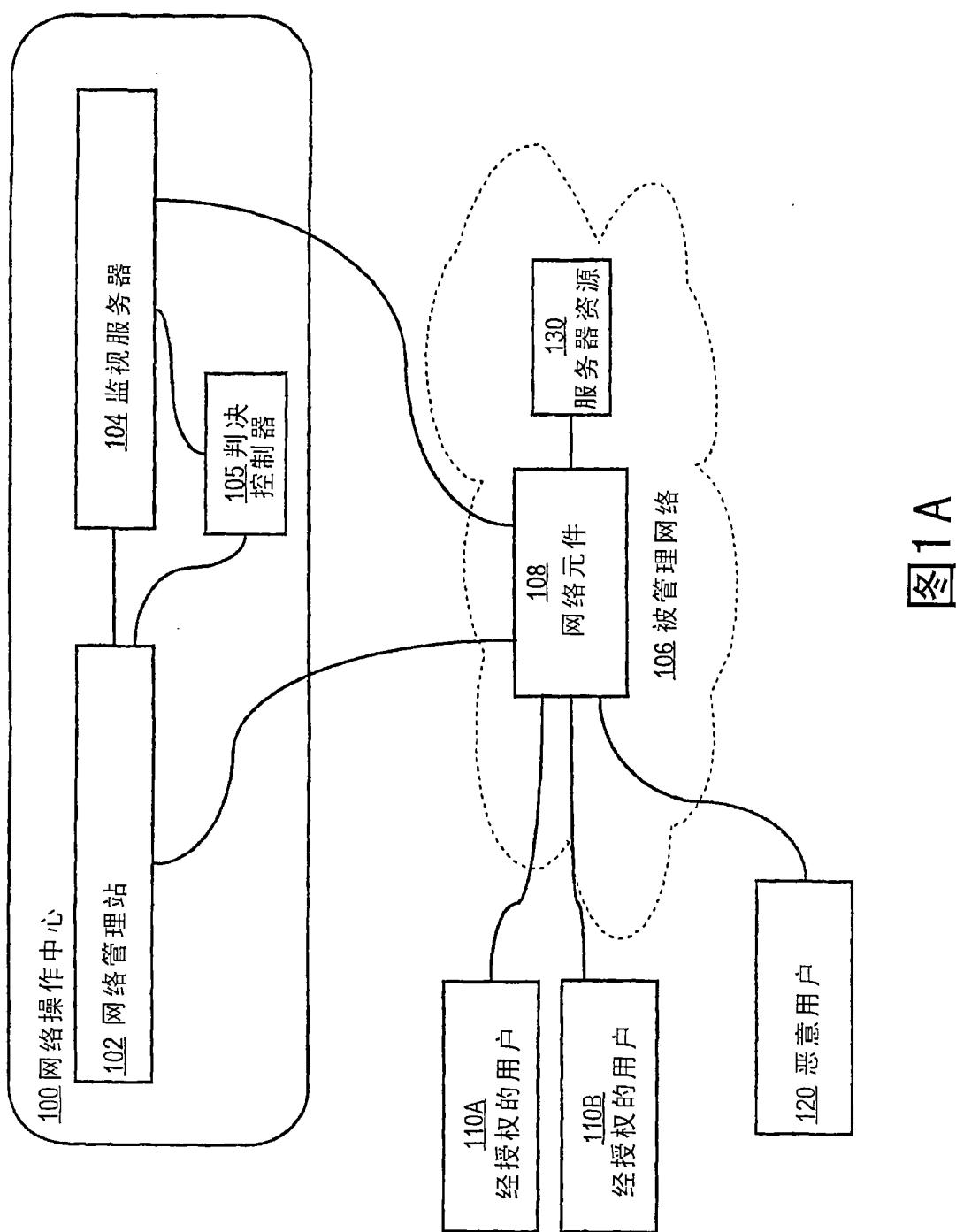
务。本地网络 522 和因特网 528 都使用携带数字数据流的电的、电磁的或光信号。经过各种网络的信号和在网络链路 520 上并经过通信接口 518 的信号（这些信号携带去往和来自计算机系统 500 的数字数据）是传输信息的载波的示例性形式。

计算机系统 500 可以经过网络、网络链路 520 和通信接口 518 发送消息并接收数据，包括程序代码。在因特网示例中，服务器 530 可以经过因特网 528、ISP 526、本地网络 522 和通信接口 518 发送针对应用程序的请求代码。根据本发明，一个这种下载的应用程序提供了如这里所述的针对与高风险相关联的网络用户的隔离手段。

接收到的代码可以在接收时被处理器 504 执行，和/或被存储在存储设备 510 或其他非易失性存储介质中以供后续执行。以这种方式，计算机系统 500 可以获得载波形式的应用代码。

4.0 扩展和替换

在前述说明书中，已参考特定实施例描述了本发明。但是，应当清楚，在不脱离本发明更宽广的精神和范围的前提下，可以进行各种修改和改变。因此，说明书和附图都应当认为是示例性的，而非限制性的。



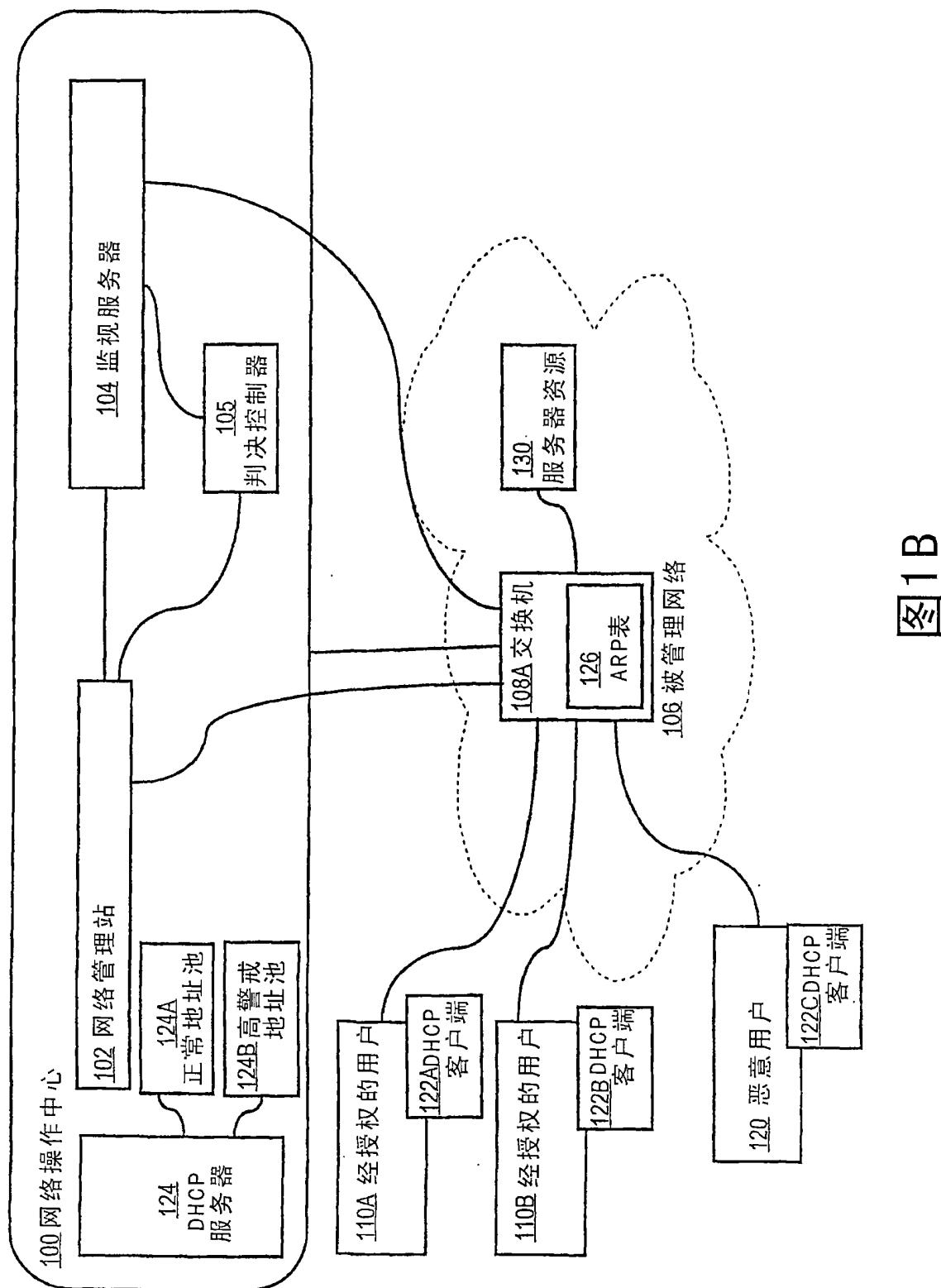


图 1 B

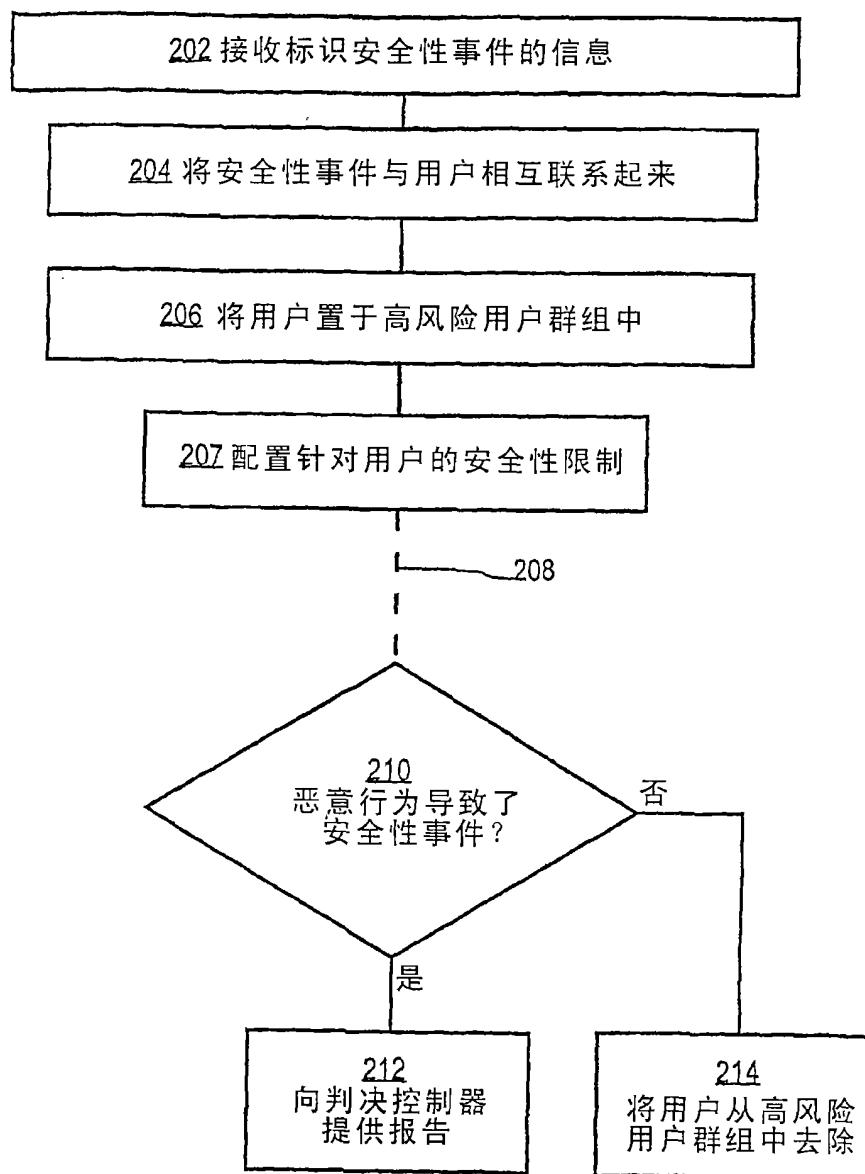


图2

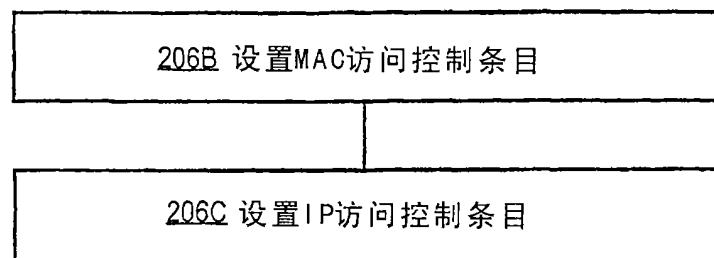


图3 A

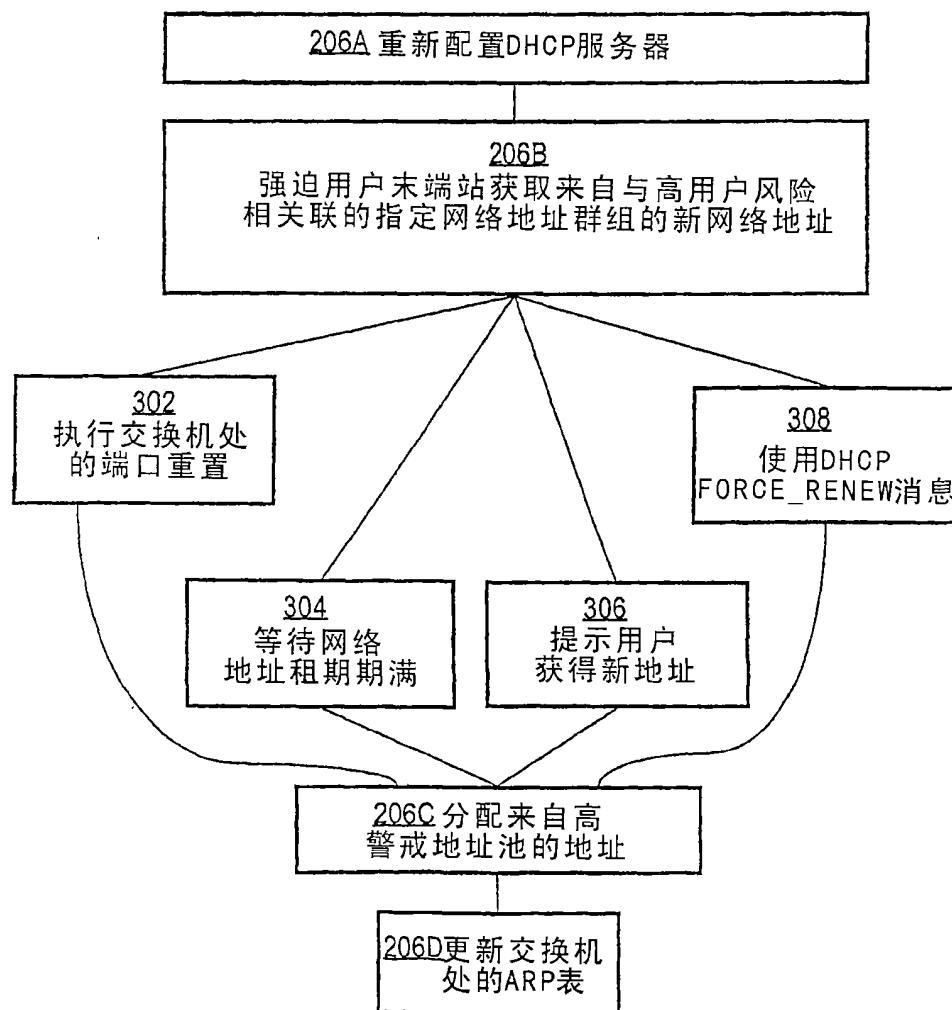


图3 B

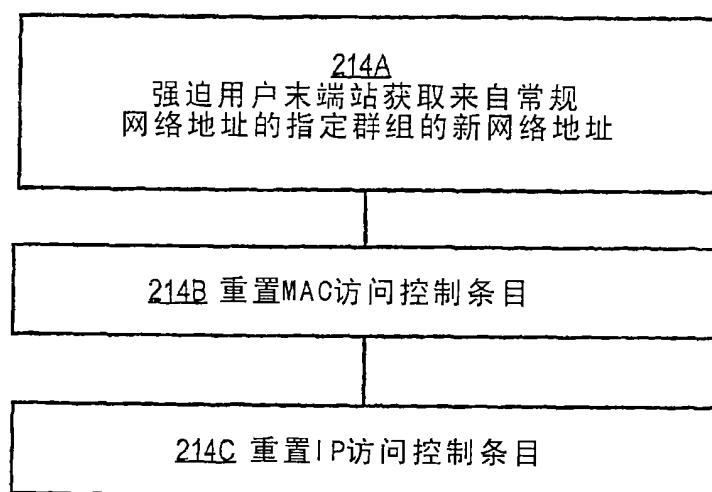


图4

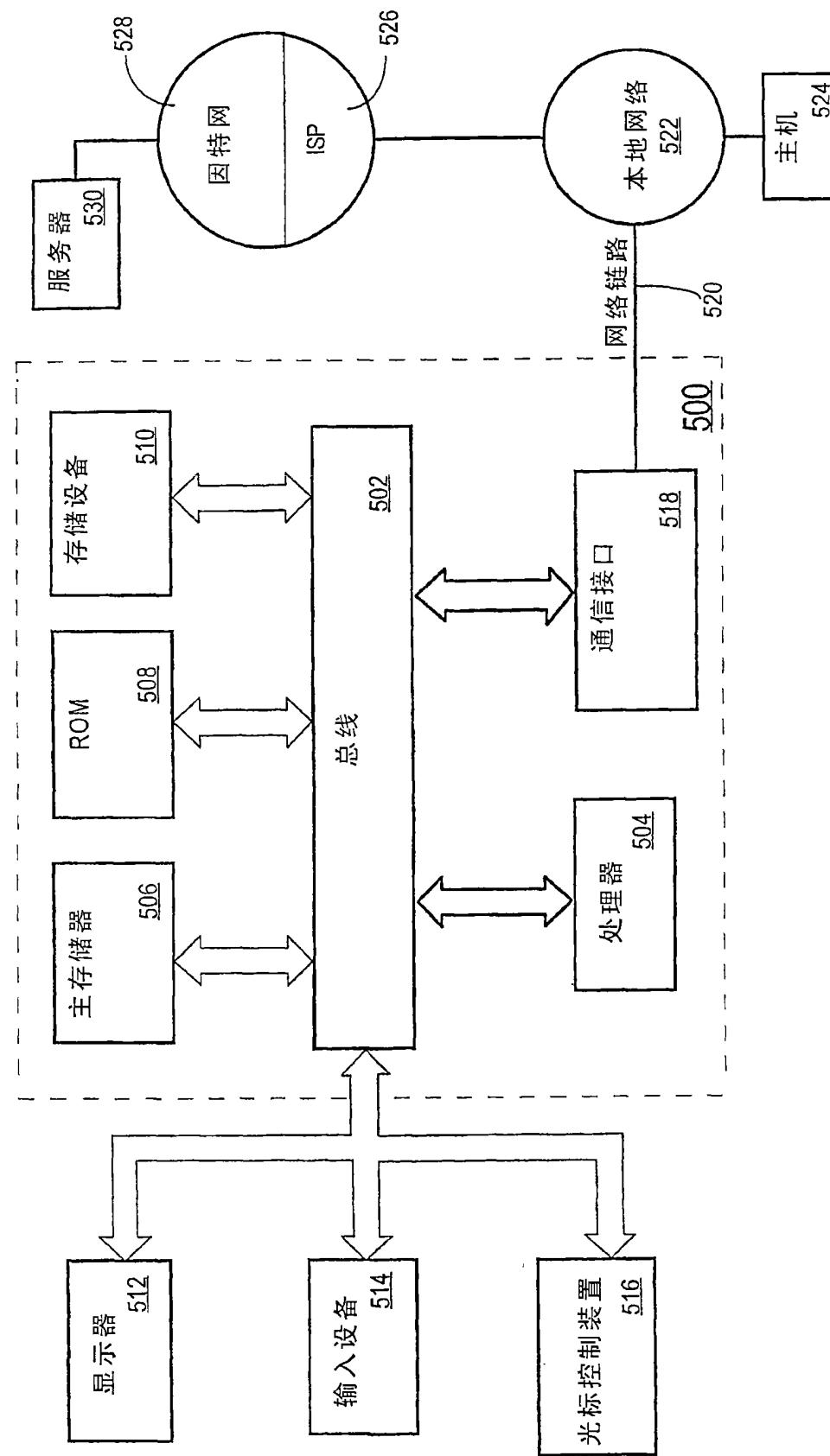


图5