



(12) 发明专利

(10) 授权公告号 CN 101523866 B

(45) 授权公告日 2013. 10. 30

(21) 申请号 200780037294. 3

(74) 专利代理机构 北京泛华伟业知识产权代理

(22) 申请日 2007. 08. 02

有限公司 11280

(30) 优先权数据

11/462, 345 2006. 08. 03 US

代理人 王勇 姜华

(85) PCT申请进入国家阶段日

2009. 04. 03

(51) Int. Cl.

H04L 29/08 (2006. 01)

审查员 许洪岩

(86) PCT申请的申请数据

PCT/US2007/075037 2007. 08. 02

(87) PCT申请的公布数据

W02008/017012 EN 2008. 02. 07

(73) 专利权人 思杰系统有限公司

地址 美国佛罗里达

(72) 发明人 A·谢蒂 J·苏甘蒂 S·卡马斯

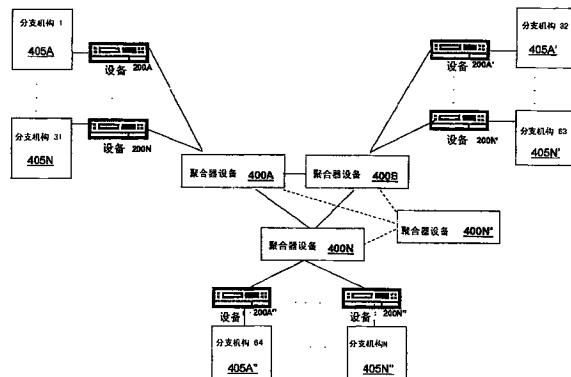
权利要求书3页 说明书28页 附图10页

(54) 发明名称

用于分层全局负载平衡的系统和方法

(57) 摘要

本发明所公开的系统和方法用于提供设备的分层以更加有效地跨越多个分支机构访问资源。方法包括如下步骤：由第一聚合器设备(400A)建立与第一多个分支机构设备(200A, ..., 200N)的连接；由第二聚合器设备(400B)建立与第二多个分支机构设备(200A', ..., 200N')的连接；第一多个分支机构设备不具有识别第二多个分支机构设备的信息；由第一聚合器设备(400A)从第一分支机构设备(200A)接收来自客户端访问资源的请求；由第一聚合器设备(400A)经由第二聚合器设备(400B)从第二多个分支机构设备(200A', ..., 200N')识别一个第二分支机构设备(200A')以服务该请求；由第一聚合器设备(400A)向第一分支机构设备(200A)发送识别第二分支机构设备(200A')的信息；并且由第一分支机构设备(200A)建立与第二分支机构设备(200A')的连接。本发明也描述了对应的系统。



1. 一种提供设备的分层以更加有效地跨越多个分支机构访问资源的方法,该方法包括:

(a) 由第一聚合器设备建立与第一多个分支机构设备的连接,所述第一多个分支机构设备提供服务给多个分支机构;

(b) 由第二聚合器设备建立与第二多个分支机构设备的连接,所述第二多个分支机构设备提供服务给另外多个分支机构,所述第一多个分支机构设备不具有识别所述第二多个分支机构设备的信息;

(c) 建立所述第一聚合器设备和第二聚合器设备之间的连接以交换关于分支机构设备的所聚合的信息,该分支机构设备不知道接收该信息的聚合器设备,所述第一聚合器设备从所述第二聚合器设备接收由所述第二聚合器设备收集的关于所述第二多个分支机构操作的所聚合的信息;

(d) 由所述第一聚合器设备从所述第一多个分支机构的第一分支机构设备接收来自客户装置访问资源的请求;

(e) 由所述第一聚合器设备经由来自所述第二聚合器设备的所聚合的信息从所述第二多个分支机构设备识别一个第二分支机构设备以服务所述请求;

(f) 由所述第一聚合器设备向所述第一分支机构设备发送识别所述第二分支机构设备的信息;和

(g) 由所述客户装置建立与所述第二分支机构设备的连接。

2. 权利要求 1 的方法,其中,步骤(f)还包括由所述第一分支机构设备发送识别所述第二分支机构设备的信息给所述客户装置。

3. 权利要求 1 的方法,包括由所述客户装置经由所述第一分支机构设备与服务器通过所述第二分支机构设备建立第二连接。

4. 权利要求 1 的方法,包括由所述第一聚合器设备建立与所述第二聚合器设备的通信。

5. 权利要求 3 的方法,包括由所述第一聚合器设备将关于所述第一多个分支机构设备的信息通信给所述第二聚合器设备。

6. 权利要求 3 的方法,包括由所述第二聚合器设备将关于所述第二多个分支机构设备的信息通信给所述第一聚合器设备。

7. 权利要求 1 的方法,由所述第一聚合器设备确定关于所述第一多个分支机构设备的每一个的性能或者操作特征的其中之一的信息。

8. 权利要求 1 的方法,由所述第二聚合器设备确定所述第二多个分支机构设备的每一个的性能或者操作特征的其中之一。

9. 权利要求 7 的方法,其中,步骤(e)包括由所述第一聚合器设备基于所述性能或者操作特征的其中之一来选择所述第二分支机构设备。

10. 权利要求 3 的方法,包括由所述第一分支机构设备或者所述第二分支机构设备的其中之一加速所述客户装置和所述服务器之间的通信。

11. 权利要求 10 的方法,其中,加速包括以下一个或者多个技术的使用:

压缩;

TCP 连接池;

TCP 连接多路复用；

TCP 缓冲；和

高速缓存。

12. 权利要求 1 的方法，其中，所述第一聚合器设备或者所述第二聚合器设备的其中之一被布署在数据中心。

13. 权利要求 1 的方法，其中，所述客户装置布署在所述第一分支机构。

14. 一种用于提供设备的分层以更加有效地跨越多个分支机构访问资源的系统，该系统包括：

第一聚合器设备，用于建立与第一多个分支机构设备的连接，所述第一多个分支机构设备提供服务给多个分支机构；

第二聚合器设备，用于建立与第二多个分支机构设备的连接，所述第二多个分支机构设备提供服务给另外多个分支机构，所述第一多个分支机构设备不具有识别所述第二多个分支机构设备的信息；以及

其中在所述第一聚合器设备和第二聚合器设备之间建立连接以交换关于分支机构设备的所聚合的信息，该分支机构设备不知道接收该信息的聚合器设备，所述第一聚合器设备从所述第二聚合器设备接收由所述第二聚合器设备收集的关于所述第二多个分支机构操作的所聚合的信息；

所述第一多个分支机构的第一分支机构设备发送来自客户装置的访问资源的请求给所述第一聚合器设备；

其中，所述第一聚合器设备经由所述第二聚合器设备从所述第二多个分支机构设备识别一个第二分支机构设备以服务所述请求，并且向所述第一分支机构设备发送识别所述第二分支机构设备的信息；并且

所述客户装置建立与所述第二分支机构设备的连接。

15. 权利要求 14 的系统，其中，所述第一分支机构设备发送识别所述第二分支机构设备的信息给所述客户装置。

16. 权利要求 14 的系统，其中，所述客户装置经由所述第一分支机构设备与服务器通过所述第二分支机构设备建立第二连接。

17. 权利要求 14 的系统，其中，所述第一聚合器设备建立与所述第二聚合器设备的通信。

18. 权利要求 17 的系统，其中，所述第一聚合器设备将关于所述第一多个分支机构设备的信息通信给所述第二聚合器设备。

19. 权利要求 14 的系统，其中，所述第二聚合器设备将关于所述第二多个分支机构设备的信息通信给所述第一聚合器设备。

20. 权利要求 14 的系统，其中，所述第一聚合器设备确定关于所述第一多个分支机构设备的每一个的性能或者操作特征的其中之一的信息。

21. 权利要求 14 的系统，其中，所述第二聚合器设备确定所述第二多个分支机构设备的每一个的性能或者操作特征的其中之一。

22. 权利要求 21 的系统，其中，所述第一聚合器设备基于所述性能或者操作特征的其中之一来选择所述第二分支机构设备。

23. 权利要求 14 的系统, 其中, 所述第一分支机构设备或者所述第二分支机构设备的其中之一加速所述客户装置和服务器之间的通信。

24. 权利要求 23 的系统, 其中, 加速包括以下一个或者多个技术的使用 :

压缩 ;

TCP 连接池 ;

TCP 连接多路复用 ;

TCP 缓冲 ; 和

高速缓存。

25. 权利要求 14 的系统, 其中, 所述第一聚合器设备或者所述第二聚合器设备的其中之一被布署在数据中心。

26. 权利要求 14 的系统, 其中, 所述客户装置布署在所述第一分支机构。

用于分层全局负载平衡的系统和方法

技术领域

[0001] 本发明主要涉及数据通信网络,更具体地,本发明涉及提供用于分支机构的全局和分层负载平衡的聚合器设备的系统和方法。

背景技术

[0002] 公司或者企业网络可以服务许多分支机构。每个分支机构可以具有其自己的网络、服务器和资源。可以在分支机构布署设备,用来为位于分支机构的客户端或者服务器本地提供网关服务。在公司范围网络中,可以在每个分支机构布署分支机构设备。可以跨越这些分支机构布署诸如服务器、应用、数据文件的许多资源。此外,分支机构可以具有未充分利用的资源和可用的计算时间。

[0003] 在任一分支机构,可以存在能够由其它分支机构的用户或者计算装置访问的可用的或者有用的资源。例如,第一分支机构的客户端可以想要访问第二分支机构的服务器上的诸如应用的资源。在一些实例中,第一分支机构的客户端不知道第二分支机构的资源的存在或者可用性。在其它实例中,由于分支机构的资源对于跨越公司网络的用户不能容易地使用,而被搁置不用。这将导致公司网络和布署的资源的低效率的使用。为了有利于分支机构的客户端访问另一个分支机构的资源,管理员需要人工并且特定地配置网关或者分支机构设备,以知道网络中其它设备。在资源遍布许多分支机构布署的情况下,每个分支机构设备需要被人工配置,以知道其它分支机构设备。这导致在配置和维持多个分支机构设备或者网关中的大量的时间和成本。

[0004] 因此,期望提供减少分支机构配置而跨越企业和分支机构全局负载平衡资源的系统和方法。

发明内容

[0005] 本发明涉及聚合器设备,以分层的形式和减少分支机构设备配置的方式来提供分支机构设备的聚合和负载平衡。任一分支机构设备可以被配置以知道或者识别单个聚合器设备 400。例如,第一分支机构设备可以被配置以识别和连接到第一聚合器设备。第一分支机构设备可以不被配置为具有任何信息,并且因此可以不知道第二聚合器设备或者连接到第二聚合器设备的任一分支机构设备。以此方式,减少了分支机构设备的配置。虽然配置被减少,但是服务请求的分支机构设备可以访问聚合器设备所知道的任一其它设备。由于聚合器设备共享分支机构设备的信息,第一聚合器设备可以向第一分支机构设备识别标识经任一聚合器设备连接的任一分支机构设备的信息。以此方式,资源请求可以跨越所有的分支机构和分支机构设备被全局负载平衡。

[0006] 在一方面,本发明涉及一种用于提供设备的分层以更加有效地跨越多个分支机构访问资源的方法。该方法包括如下步骤:由第一聚合器设备建立与第一多个分支机构设备的连接,并且由第二聚合器设备建立与第二多个分支机构设备的连接。第一多个分支机构设备可以不具有识别第二多个分支机构设备的信息。第二多个分支机构设备也可以不具有

识别第一多个分支机构设备的信息。该方法包括由第一聚合器设备从第一多个分支机构的第一分支机构设备接收来自客户端访问资源的请求。由第一聚合器设备经由第二聚合器设备从第二多个分支机构设备识别一个第二分支机构设备以服务该请求。第一聚合器设备向第一分支机构设备或者客户端的其中之一发送识别第二分支机构设备的信息。该方法包括客户端建立与第二分支机构设备的连接。

[0007] 在一个实施例中，该方法包括由第一分支机构设备发送识别第二分支机构设备的信息给客户端。在另一个实施例中，该方法包括由客户端经由第一分支机构设备通过第二分支机构设备与服务器建立第二连接。在一些实施例中，该方法包括由第一聚合器设备建立与第二聚合器设备的通信。在一个实施例中，第一聚合器设备将关于第一多个分支机构设备的信息通信给第二聚合器设备。在另一个实施例中，第二聚合器设备将关于第二多个分支机构设备的信息通信给第一聚合器设备。

[0008] 在另一个实施例中，该方法包括由第一聚合器设备确定关于第一多个分支机构设备的每一个的性能或者操作特征的信息。在一些实施例中，该方法包括由第二聚合器设备确定第二多个分支机构设备的每一个的性能或者操作特征。在一个实施例中，该方法包括由第一或者第二聚合器设备基于性能或者操作特征的其中之一来选择第二分支机构设备。

[0009] 在又一个实施例中，该方法包括由第一分支机构设备或者第二分支机构设备加速客户端和服务器之间的通信。该方法可以包括使用以下一个或者多个技术进行加速：1) 压缩，2) TCP 连接池，3) TCP 连接多路复用，4) TCP 缓冲，和 5) 高速缓存。在一些实施例中，第一聚合器设备或者第二聚合器设备被部署在数据中心。在另一个实施例中，客户端部署在第一分支机构。

[0010] 在另一方面，本发明涉及用于提供设备的分层以更加有效地跨越多个分支机构访问资源的系统。该系统包括第一聚合器设备和第二聚合器设备。第一聚合器设备建立与第一多个分支机构设备的连接。第二聚合器设备建立与第二多个分支机构设备的连接。第一多个分支机构设备可以不具有识别第二多个分支机构设备的信息。第二多个分支机构设备也可以不具有识别第一多个分支机构设备的信息。该系统还包括发送来自客户端访问资源的请求给第一聚合器设备的第一多个分支机构的第一分支机构设备。第一聚合器设备经由第二聚合器设备从第二多个分支机构设备识别一个第二分支机构设备以服务该请求，并且向该第一分支机构设备发送识别第二分支机构设备的信息。该系统还包括建立与第二分支机构设备的连接的客户端。

[0011] 在一个实施例中，第一分支机构设备发送识别第二分支机构设备的信息给客户端。在另一个实施例中，客户端经由第一分支机构设备通过第二分支机构设备与服务器建立第二连接。在一些实施例中，第一聚合器设备建立与第二聚合器设备的通信。在一个实施例中，第一聚合器设备将关于第一多个分支机构设备的信息通信给第二聚合器设备。在又一个实施例中，第二聚合器设备将关于第二多个分支机构设备的信息通信给第一聚合器设备。在一些实施例中，第一或者第二聚合器设备确定关于第一多个分支机构设备的每一个的性能或者操作特征的信息。在系统的另一个实施例中，第一聚合器设备基于性能或者操作特征的其中之一来选择第二分支机构设备。

[0012] 在一些实施例中，第一分支机构设备或者第二分支机构设备加速客户端和服务器之间的通信。该加速技术可以包括以下技术中的一个或者多个：1) 压缩，2) TCP 连接池，3)

TCP 连接多路复用, 4) TCP 缓冲, 和 5) 高速缓存。在其它实施例中, 第一聚合器设备或者第二聚合器设备被部署在数据中心。在一个实施例中, 客户端部署在第一分支机构。

[0013] 在以下附图和描述中提出本发明的不同实施例的细节。

附图说明

[0014] 该发明的前述和其它目的、方面、特征和优点, 通过参见下述结合附图的细节描述将会更加明显并更好理解, 其中: 图 1A 是对于客户端通过设备访问服务器的网络环境的实施例的框图; 图 1B 是用于通过设备从服务器传送计算环境到客户端的环境的实施例的框图; 图 1C 和 1D 是计算装置的实施例的框图; 图 2A 是用于处理客户端和服务器之间的通信的设备的实施例的框图; 图 2B 是用于优化、加速、负载平衡和路由客户端和服务器之间的通信的设备的另一个实施例的框图; 图 3 是用于通过设备与服务器通信的客户端的实施例的框图; 图 4A 是跨越分支机构访问资源的聚合器设备的实施例的框图; 图 4B 为负载平衡多个分支机构的聚合器设备的部署的另一个实施例的框图; 和图 5 是描述使用聚合器设备实现分层负载平衡以跨越分支机构访问资源的方法实施例的步骤的流程图。

[0015] 从下面结合附图所提出的详细描述, 本发明的特征和优点将更明显, 其中, 相同的参考标记在全文中表示相应的元件。附图中, 相同的附图标记通常表示相同的、功能类似、和 / 或结构类似的元件。

具体实施方式

A、网络和计算环境

[0016] 在讨论设备和 / 或客户端的系统和方法的实施例的细节之前, 讨论这些实施例所部署的网络和计算环境是有帮助的。现在参见图 1A, 描述了网络环境的实施例。概括来讲, 网络环境包括通过一个或多个网络 104、104' (总的称为网络 104) 与一个或多个服务器 106a-106n (同样总的称为服务器 106, 或远程机器 106) 通信的一个或多个客户端 102a-102n (同样总的称为本地机器 102, 或客户端 102)。在一些实施例中, 客户端 102 通过设备 200 与服务器 106 通信。

[0017] 虽然图 1A 示出了在客户端 102 和服务器 106 间的网络 104 和网络 104', 客户端 102 和服务器 106 可以位于同一个网络 104 上。网络 104 和 104' 可以是相同类型的网络或不同类型的网络。网络 104 和 / 或网络 104' 可为诸如企业内部网的局域网 (LAN), 城域网 (MAN)、或者例如因特网或万维网的广域网 (WAN)。在一个实施例中, 网络 104' 可为专用网络并且网络 104 可为公用网络。在一些实施例中, 网络 104 可为专用网络并且网络 104' 可为公用网络。在另一个实施例中, 网络 104 和 104' 可都为专用网络。在一些实施例中, 客户端 102 可位于公司企业的分支机构中, 通过网络 104 上的 WAN 连接与位于公司数据中心的服务器 106 通信。

[0018] 网络 104 和 / 或 104' 是任何类型和 / 或形式的网络, 并且可包括任一下述网络: 点对点网络, 广播网络, 广域网, 局域网, 电信网络, 数据通信网络, 计算机网络, ATM (异步传输模式) 网络, SONET (同步光纤网络) 网络, SDH (同步数字体系) 网络, 无线网络和有线网络。在一些实施例中, 网络 104 可以包括无线链路, 诸如红外信道或者卫星频带。网络 104

和 / 或 104' 的拓扑可为总线型、星型或环型网络拓扑。网络 104 和 / 或 104' 以及网络拓扑可以是对于本领域普通技术人员所熟知的、可以支持此处描述的操作的任何这样的网络或网络拓扑。

[0019] 如图 1A 所示,设备 200 被示在网络 104 和 104' 之间,设备 200 也可被称为接口单元 200 或者网关 200。在一些实施例中,设备 200 可位于网络 104 上。例如,公司的分支机构可在该分支机构中布署设备 200。在其它实施例中,设备 200 可位于网络 104' 上。例如,设备 200 可位于公司的数据中心。在又另一个实施例中,多个设备 200 可布署在网络 104 上。在一些实施例中,多个设备 200 可布署在网络 104' 上。在一个实施例中,第一设备 200 与第二设备 200' 通信。在其它实施例中,设备 200 作为客户端 102 可以是位于同一或不同的网络 104、104' 上的任一客户端 102 或服务器 106 的一部分。一个或多个设备 200 可位于客户端 102 和服务器 106 之间的网络或网络通信路径中的任一点。

[0020] 在一个实施例中,系统可包括多个逻辑分组的服务器 106。在这些实施例中,服务器的逻辑分组可以被称为服务器群组 38。在其中一些实施例中,服务器 106 可为地理上分散的。在一些情况中,群组 38 可以作为单个实体被管理。在其它实施例中,服务器群组 38 包括多个服务器群组 38。在一个实施例中,服务器群组执行代表一个或者多个客户端 102 的一个或者多个应用。

[0021] 在每个群组 38 中的服务器 106 可为不同种类。一个或多个服务器 106 可根据一种类型的操作系统平台 (例如,由 Washington, Redmond 的 Microsoft 公司制造的 WINDOWS NT) 操作,而一个或多个其它服务器 106 可根据另一类型的操作系统平台 (例如, Unix 或 Linux) 操作。每个群组 38 的服务器 106 不需要与同一群组 38 内的另一个服务器 106 物理上接近。因此,逻辑分组作为群组 38 的服务器 106 的组可使用广域网 (WAN) 连接或中等区域网 (MAN) 连接来互联。例如,群组 38 可包括物理上位于不同大陆或大陆、国家、州、城市、校园或房间的不同区域的服务器 106。如果服务器 106 使用局域网 (LAN) 连接或一些直接连接的形式进行连接,则在群组 38 中的服务器 106 间的数据发送速度将增加。

[0022] 服务器 106 可指文件服务器、应用服务器、web 服务器、代理服务器或者网关服务器。在一些实施例中,服务器 106 可以有作为应用服务器或者作为主应用服务器工作的能力。在一个实施例中,服务器 106 可包括活动目录。客户端 102 也可称为客户端节点或端点。在一些实施例中,客户端 102 有能力作为在服务器上搜索对应用的访问的客户端节点工作,也有能力作为提供对用于其它客户端 102a-102n 所寄载的应用的访问的应用服务器工作。

[0023] 在一些实施例中,客户端 102 与服务器 106 通信。在一个实施例中,客户端 102 可与群组 38 中的服务器 106 之一直接通信。在另一个实施例中,客户端 102 执行程序邻近应用以与群组 38 内的服务器 106 通信。在又另一个实施例中,服务器 106 提供主节点的功能。在一些实施例中,客户端 102 通过网络 104 与群组 38 中的服务器 106 通信。通过网络 104,客户端 102 例如可以请求执行在群组 38 中的服务器 106a-106n 寄载的各种应用,并接收应用执行结果的输出用于显示。在一些实施例中,只有主节点提供要求识别和提供地址信息的功能,其中的地址信息与寄载所请求的应用的服务器 106' 相关。

[0024] 在一个实施例中,服务器 106 提供网络 (Web) 服务器的功能。在另一个实施例中,服务器 106a 接收来自客户端 102 的请求,将该请求转发到第二服务器 106b 并以来自服务

器 106b 对该请求的响应通过客户端 102 来响应该请求。在又另一个实施例中，服务器 106 获得客户端 102 可用的应用的列举以及地址信息，该地址信息与服务器 106 相关，该服务器 106 寄载由该应用的列举所识别的应用。在又一个实施例中，服务器 106 使用网络接口呈现对客户端 102 的请求的响应。在一个实施例中，客户端 102 直接与服务器 106 通信以访问所识别的应用。在另一个实施例中，客户端 102 接收应用输出数据，诸如显示数据，该应用输出数据通过对在服务器 106 上所识别的应用的执行而产生。

[0025] 现在看图 1B，示出了在客户端 102 上用于传送和 / 或操作计算环境的网络环境。在一些实施例中，服务器 106 包括用于向一个或多个客户端 102 传送计算环境或应用和 / 或数据文件的应用传送系统 190。总的来说，客户端 10 通过网络 104、104' 和设备 200 与服务器 106 通信。例如，客户端 102 可驻留在公司的远程办公室里，例如分支机构，并且服务器 106 可驻留在公司数据中心。客户端 102 包括客户端代理 120 以及计算环境 15。计算环境 15 可执行或操作用于访问、处理或使用数据文件的应用。计算环境 15、应用和 / 或数据文件可通过设备 200 和 / 或服务器 106 被传送。

[0026] 在一些实施例中，设备 200 加速计算环境 15 或者其任一部分到客户端 102 的传送。在一个实施例中，设备 200 通过应用传送系统 190 加速计算环境 15 的传送。例如，可使用此处描述的实施例来加速从中央公司数据中心到远程用户位置（例如公司的分支机构）的应用可处理的流应用和数据文件的传送。在另一个实施例中，设备 200 加速客户端 102 和服务器 106 之间的传输层通信量。设备 200 可以提供加速技术用于加速从服务器 106 到客户端 102 的任一传输层有效载荷，诸如：1) 传输层连接池，2) 传输层连接多路复用，3) 传输控制协议缓冲，4) 压缩，以及 5) 高速缓存。在一些实施例中，设备 200 响应来自客户端 102 的请求提供服务器 106 的负载平衡。在其它实施例中，设备 200 充当代理或者访问服务器来提供对一个或者多个服务器 106 的访问。在另一个实施例中，设备 200 提供从客户端 102 的第一网络 104 到服务器 106 的第二网络 104' 的安全虚拟专用网络连接，诸如 SSL VPN 连接。在又一些实施例中，设备 200 提供客户端 102 和服务器 106 之间的连接和通信的应用防火墙安全、控制和管理。

[0027] 在一些实施例中，基于多个执行方法并且基于通过策略引擎 195 所应用的任一验证和授权策略，应用传送管理系统 190 提供应用传送技术来传送计算环境到用户的桌面（远程的或者其它的）。使用这些技术，远程用户可以从任一网络连接装置 100 获取计算环境并且访问服务器所存储的应用和数据文件。在一个实施例中，应用传送系统 190 可驻留在服务器 106 上或在其上执行。在另一个实施例中，应用传送系统 190 可驻留在多个服务器 106a-106n 上或在其上执行。在一些实施例中，应用传送系统 190 可在服务器群组 38 内执行。在一个实施例中，执行应用传送系统 190 的服务器 106 也可存储或提供应用和数据文件。在另一个实施例中，一个或多个服务器 106 的第一组可执行应用传送系统 190，并且不同的服务器 106n 可存储或提供应用和数据文件。在一些实施例中，应用传送系统 190、应用和数据文件中的每个可驻留或位于不同的服务器上。在又一个实施例中，应用传送系统 190 的任何部分可驻留、执行、或被存储于或分发到设备 200 或多个设备。

[0028] 客户端 102 可以包括计算环境 15，用于执行使用或者处理数据文件的应用。客户端 102 通过网络 104、104' 和设备 200 可以请求来自服务器 106 的应用和数据文件。在一个实施例中，设备 200 可以转发来自客户端 102 的请求到服务器 106。例如，客户端 102 可

以不具有本地存储或者本地可访问的应用和数据文件。响应请求,应用传送系统 190 和 / 或服务器 106 可以传送应用和数据文件到客户端 102。例如,在一个实施例中,服务器 106 可以按照应用流来发送应用以在客户端 102 上的计算环境 15 中操作。

[0029] 一些实施例中,应用传送系统 190 包括 Citrix Systems, Inc. 的 CitrixAccess Suite™的任何部分,诸如MetaFrame或者Citrix Presentation Server™和/或Microsoft 公司制造的任一的Microsoft® Windows Terminal Services。在一个实施例中,应用传送系统 190 可以通过远程显示协议或者通过基于远程或者基于服务器计算的其它方式来传送一个或者多个应用到客户端 102 或者用户。在另一个实施例中,应用传送系统 190 可以通过应用流来传送一个或者多个应用到客户端或者用户。

[0030] 在一个实施例中,应用传送系统 190 包括策略引擎 195,用于控制和管理对应用执行方法和应用的传送的访问、选择。在一些实施例中,策略引擎 195 确定用户或者客户端 102 可以访问的一个或者多个应用。在另一个实施例中,策略引擎 195 确定应用应该如何被传送到用户或者客户端 102,例如执行方法。在一些实施例中,应用传送系统 190 提供多个传送技术,从中来选择应用执行的方法,诸如基于服务器的计算、流式传输或者本地传送应用到客户端 120 用于本地执行。

[0031] 在一个实施例中,客户端 102 请求应用程序的执行并且包括服务器 106 的应用传送系统 190 选择执行应用程序的方法。在一些实施例中,服务器 106 从客户端 102 接收证书。在另一个实施例中,服务器 106 从客户端 102 接收对于可用应用的列举的请求。在一个实施例中,响应该请求或者证书的接收,应用传送系统 190 列举对于客户端 102 可用的多个应用程序。应用传送系统 190 接收请求来执行所列举的应用。应用传送系统 190 例如响应策略引擎的策略,选择预定数量的方法之一来执行所列举的应用。应用传送系统 190 可以选择执行应用的方法,使得客户端 102 接收通过执行服务器 106 上的应用程序所产生的应用输出数据。应用传送系统 190 可以选择执行应用的方法,使得本地机器 10 在检索包括应用的多个应用文件之后本地执行应用程序。在又一个实施例中,应用传送系统 190 可以选择执行应用的方法,以通过网络 104 流式传输应用到客户端 102。

[0032] 客户端 102 可以执行、操作或者以其它方式提供应用,应用可为任何类型和 / 或形式的软件、程序或者可执行指令,例如任何类型和 / 或形式的 web 浏览器、基于 web 的客户端、客户端 - 服务器应用、瘦客户端计算客户端、ActiveX 控件、或者 Java 程序、或者可以在客户端 102 上执行的任一其它类型和 / 或形式的可执行指令。在一些实施例中,应用可以是代表客户端 102 在服务器 106 上执行的基于服务器或者基于远程的应用。在一个实施例中,服务器 106 可以使用任一瘦客户端或者远程显示协议来显示输出到客户端 102,诸如由 Florida, Ft. Lauderdale 的 CitrixSystemsInc. 制造的独立计算架构 (ICA) 协议,或者由 Washington, Redmond 的 Microsoft 公司制造的远程桌面协议 (RDP)。应用可使用任何类型的协议,并且它可为,例如, HTTP 客户端、FTP 客户端、Oscar 客户端或 Telnet 客户端。在其它实施例中,应用包括涉及到 VoIP 通信的任何类型的软件,例如软 IP 电话。在进一步的实施例中,应用包括涉及到实时数据通信的任何应用,例如用于流式传输视频和 / 或音频的应用。

[0033] 在一些实施例中,服务器 106 或服务器群组 38 可运行一个或多个应用,例如提供瘦客户端计算或远程显示表示应用的应用。在一个实施例中,服务器 106 或服务器群组 38

作为一个应用来执行 Citrix Systems Inc. 的 Citrix Access Suite™ 的任一部分（例如 MetaFrame 或 CitrixPresentation Server™），和 / 或 Microsoft 公司制造的 Microsoft® Windows Terminal Services 中的任意一个。在一个实施例中，该应用是位于 Florida, Fort Lauderdale 的 Citrix Systems Inc. 开发的 ICA 客户端。在其它实施例中，该应用包括由位于 Washington, Redmond 的 Microsoft 公司开发的远程桌面 (RDP) 客户端。另外，服务器 106 可以运行一个应用，它例如可以是提供电子邮件服务的应用服务器，例如由位于 Washington, Redmond 的 Microsoft 公司制造的 Microsoft Exchange, web 或 Internet 服务器，或者桌面共享服务器，或者协作服务器。在一些实施例中，任一应用可以包括任一类型的所寄载的服务或产品，例如位于 California, Santa Barbara 的 Citrix Online Division 提供的 GoToMeeting™，位于 California, Santa Clara 的 WebEx Inc. 提供的 WebEx™，或者位于 Washington, Redmond 的 Microsoft 公司提供的 Microsoft Office Live Meeting。

[0034] 客户端 102、服务器 106 和设备 200 可以部署为和 / 或执行在任一类型和形式的计算装置上，诸如能够在任一类型和形式的网络上通信并执行此处描述的操作的计算机、网络装置或者设备。图 1C 和 1D 描述用于实现客户端 102、服务器 106 或者设备 200 的实施例的计算装置 100 的框图。如图 1C 和 1D 所示，每个计算装置 100 包括中央处理单元 101，以及主存储单元 122。如图 1C 所示，计算装置 100 可以包括虚拟显示装置 124、键盘 126 和 / 或诸如鼠标的定点设备 127。每个计算装置 100 也可包括其它可选择的部件，例如一个或多个输入 / 输出装置 130a-130b（总的使用标号 130 表示），以及与中央处理单元 101 通信的高速缓存存储器 140。

[0035] 中央处理单元 101 是响应并处理从主存储单元 122 取得的指令的任何逻辑电路。在许多实施例中，中央处理单元由微处理器单元提供，例如：由 California, Mountain View 的 Intel 公司制造的；由 Illinois, Schaumburg 的 Motorola 公司制造的；由 California, Santa Clara 的 Transmeta 公司制造的；由 New York, White Plains 的 International Business Machines 公司制造的、RS/6000 处理器；或者由 California, Sunnyvale 的 Advanced Micro Devices 公司制造的。计算装置 100 可以基于任一这些处理器或者能够进行如此处描述操作的任一其它处理器。

[0036] 主存储单元 122 可以是一个或多个存储芯片，这些存储芯片可以存储数据并允许微处理器 101 直接访问任何存储位置，例如静态随机存取存储器 (SRAM)、突发 (Burst) SRAM 或同步突发 (SynchBurst) SRAM (BSRAM)，动态随机存取存储器 (DRAM)、快页模式 (Fast Page Mode) DRAM (FPM DRAM)、增强型 DRAM (EDRAM)、扩展数据输出 (Extended Data Output) RAM (EDO RAM)、扩展数据输出 (Extended Data Output) DRAM (EDO DRAM)、突发扩展数据输出 DRAM (BEDO DRAM)、增强型 DRAM (EDRAM)、同步 DRAM (SDRAM)、JEDEC SRAM、PC100 SDRAM、双数据率 SDRAM (DDR SDRAM)、增强型 SDRAM (ESDRAM)、同步链接 DRAM (SLDRAM)、直接 Rambus DRAM (DRDRAM) 或者铁电 RAM (FRAM)。主存储器 122 可以基于任一上述的存储器芯片或者能够进行如此处描述的操作的任一其它可用的存储器芯片。在图 1C 所示的实施例中，处理器 101 通过系统总线 150（下面将更详细的介绍）与主存储器 122 通信。图 1C 描述计算装置 100 的实施例，其中处理器通过存储器端口 103 直接与主存储器 122 通信。例如，在图 1D 中，主存储器 122 可为 DRDRAM。

[0037] 图 1D 描述的实施例中，主处理器 101 通过次级总线，有时称为“背端”总线，直接与

高速缓存存储器 140 通信。在其它实施例中，主处理器 101 使用系统总线 150 与高速缓存存储器 140 通信。高速缓存存储器 140 通常具有比主存储器 122 更快的响应时间，并通常通过 SRAM、BSRAM、或 EDRAM 来提供。在图 1C 所示的实施例中，处理器 101 通过本地系统总线 150 与各种 I/O 装置 130 通信。各种总线可以被用于连接中央处理单元 101 到任一 I/O 装置 130，包括 VESA VL 总线、ISA 总线、EISA 总线、微通道结构 (MCA) 总线、PCI 总线、PCI-X 总线、PCI-Express 总线、或者 NuBus。对于这样的实施例，其中 I/O 装置是视频显示器 124，处理器 101 可使用高级图形端口 (AGP) 与显示器 124 通信。图 1D 描述了计算机 100 的实施例，其中主处理器 101 通过 HyperTransport、RapidI/O 或者 InfiniBand 与 I/O 装置 130 直接通信。图 1D 也描述了一个实施例，其中本地总线和直接通信是混合的：处理器 101 使用本地互联总线与 I/O 装置 130 通信，而与 I/O 设备 130 直接通信。

[0038] 计算装置 100 可以支持任何适合的安装装置 116，例如用于接收诸如 3.5 英寸、5.25 英寸软盘或 ZIP 盘的软盘驱动器、CD-ROM 驱动器、CD-R/RW 驱动器、DVD-ROM 驱动器、各种格式的磁带驱动器、USB 装置、硬盘驱动器、或者适用于安装软件、程序（例如任一客户端代理 120 或其中一部分）的任一其它装置。计算装置 100 还可以包括存储装置 128，诸如一个或者多个硬盘驱动器或者独立磁盘的随机阵列，用于存储操作系统和其它相关软件，以及用于存储诸如涉及客户端代理 120 的任一程序的应用软件。可选地，任一安装装置 116 也可以被用作存储装置 128。此外，操作系统和软件可从可引导介质运行，诸如 KNOPPIX®，一种用于 GNU/Linux 的可引导 CD，该可引导 CD 可自 knoppix.net 作为 GNU/Linux 分发获得。

[0039] 此外，计算装置 100 可以包括通过多个连接来对接到局域网 (LAN)、广域网 (WAN) 或者因特网的网络接口 118，该多个连接包括但不限于标准电话线、LAN 或 WAN 链路（如 802.11、T1、T3、56kb、X.25）、宽带连接（例如，ISDN、帧中继、ATM）、无线连接或它们的任一或者全部的一些组合。网络接口 118 可以包含内置网络适配器、网络接口卡、PCMCIA 网卡、卡总线网络适配器、无线网络适配器、USB 网络适配器、调制解调器或适合将计算装置 100 对接到能够通信并执行此处所描述的操作的任一类型网络的任一其它装置。在计算装置 100 中可提供多个种类的 I/O 装置 130a-130n 的多个种类。输入装置包括键盘、鼠标、轨迹板、轨迹球、麦克风、以及绘画板。输出装置包括视频显示器、扬声器、喷墨打印机、激光打印机、及染料升华 (dye-sublimation) 打印机。如图 1C 所示，I/O 装置 130 可以由 I/O 控制器 123 控制。I/O 控制器可以控制诸如键盘 126 和定点设备 127（例如鼠标或者光学笔）的一个或者多个 I/O 装置。此外，I/O 装置也可为计算装置 100 提供存储器 128 和 / 或安装介质 116。在另其它实施例中，计算装置 100 可以提供 USB 连接用来接收手持 USB 存储装置，例如由 California, LosAlamitos 的 Twintech Industry Inc. 制造的 USB 闪烁驱动器系列装置。

[0040] 在一些实施例中，计算装置 100 可以包括多个显示装置 124a-124n 或与其相连，这些显示装置可以是相同或不同的类型和 / 或形式。同样的，I/O 装置 130a-130n 中的任意一个和 / 或 I/O 控制器 123 可以包括任一类型和 / 或形式的适当硬件、软件或软硬件组合以支持、启用或提供计算装置 100 对多个显示装置 124a-124n 的连接和使用。例如，计算装置 100 可以包括任一类型和 / 或形式的视频适配器、视频卡、驱动器和 / 或库，以与显示装置 124a-124n 对接、通信、连接或使用显示装置。在一个实施例中，视频适配器可以包括多

一个连接器以与多个显示装置 124a-124n 对接。在其它实施例中，计算装置 100 可以包括多个视频适配器，每个视频适配器与显示装置 124a-124n 中的一个或多个连接。在一些实施例中，计算装置 100 的操作系统的任一部分都可以被配置用于使用多个显示器 124a-124n。在其它实施例中，显示装置 124a-124n 中的一个或多个可以由一个或多个其它计算装置提供，诸如（例如通过网络）与计算装置 100 连接的计算装置 100a 和 100b。这些实施例可以包括被设计和构造的任一类型的软件，以使用另一个计算机的显示装置作为计算装置 100 的第二显示装置 124a。本领域的普通技术人员认识和意识到可以将计算装置 100 配置成拥有多个显示装置 124a-124n 的各种方式和实施例。

[0041] 在进一步的实施例中，I/O 装置 130 可为在系统总线 150 和外部通信总线间的桥 170，外部通信总线例如 USB 总线、Apple Desktop 总线、RS-232 串行连接、SCSI 总线、FireWire 总线、FireWire800 总线、Ethernet 总线、AppleTalk 总线、Gigabit Ethernet 总线、异步传输模式总线、HIPPI 总线、Super HIPPI 总线、SerialPlus 总线、SCI/LAMP 总线、FibreChannel 总线、或者串行连接 (Serial Attached) 小型计算机系统接口总线。

[0042] 图 1C 和图 1D 中描述的种类的计算装置 100 通常在操作系统的控制下操作，该操作系统控制任务的调度和对系统资源的访问。计算装置 100 可运行任何操作系统，例如任何版本的 Microsoft® Windows 操作系统，不同版本的 Unix 和 Linux 操作系统，用于 Macintosh 计算机的任何版本的 Mac OS®, 任何嵌入式操作系统，任何实时操作系统，任何开放源操作系统，任何专有操作系统，用于移动计算装置的任何操作系统，或者可以在计算装置上运行并执行此处所述操作的任何其它操作系统。典型的操作系统包括：由 Washington, Redmond 的 Microsoft 公司制造的 WINDOWS 3.x、WINDOWS 95、WINDOWS 98、WINDOWS 2000、WINDOWSNT 3.51、WINDOWS NT 4.0、WINDOWS CE 和 WINDOWS XP；由 California, Cupertino 的 Apple 计算机公司制造的 MacOS；由 New York, Armonk 的 International Business Machines 制造的 OS/2；以及由 Utah, Salt Lake City 的 Caldera 公司发布的可自由获得的操作系统 Linux，以及除此之外的任一类型和 / 或形式的 Unix 操作系统。

[0043] 在其它实施例中，计算装置 100 可以具有与该装置相容的不同的处理器、操作系统和输入装置。例如，在一个实施例中，计算机 100 是 palm Inc. 制造的 Treo180、270、1060、600 或者 650 的智能电话。在此实施例中，Treo 智能电话在 PalmOS 操作系统的控制下运行并且包括触针输入装置以及五向导向装置。此外，计算装置 100 可以是任一工作站、桌面计算机、膝上型或笔记本计算机、服务器、手持计算机、移动电话、任一其它计算机、或能够通信并有足够的处理器能力和存储容量以执行此处所述的操作的其它形式的计算或者电信装置。

B、设备架构

[0044] 图 2A 示出设备 200 的一个示例实施例。图 2A 中的设备 200 的架构只是通过示意的方式提供，并不意于要限制本发明。如图 2 所示的，设备 200 包括硬件层 206 和分为用户空间 202 和内核空间 204 的软件层。

[0045] 硬件层 206 提供硬件元件，在内核空间 204 和用户空间 202 内的程序和服务在该硬件元件上被执行。硬件层 206 也提供结构和元件，使得内核空间 204 和用户空间 202 内的

程序和服务对于设备 200 既在内又向外进行数据通信。如图 2 所示，硬件层 206 包括用于执行软件程序和服务的处理单元 262、用于存储软件和数据的存储器 264、用于在网络上发送和接收数据的网络端口 266 以及用于执行涉及在网络上被发送和接收的数据的加密套接字协议层处理的功能的加密处理器 260。在一些实施例中，中央处理单元 262 可在单一的处理器中执行加密处理器 260 的功能。另外，硬件层 206 可包括用于每个处理单元 262 和加密处理器 260 的多个处理器。处理器 262 可以包括以上结合图 1C 和 1D 所述的任一处理器 101。在一些实施例中，中央处理单元 262 可在单一的处理器中执行加密处理器 260 的功能。另外，硬件层 206 可包括用于每个处理单元 262 和加密处理器 260 的多个处理器。例如，在一个实施例中，设备 200 包括第一处理器 262 和第二处理器 262'。在其它实施例中，处理器 262 或者 262' 包括多核处理器。

[0046] 虽然设备 200 的硬件层 206 通常被示出带有加密处理器 260，但是处理器 260 可为执行涉及任何加密协议的功能的处理器，例如加密套接字协议层 (SSL) 或者传输层安全 (TLS) 协议。在一些实施例中，处理器 260 可为通用处理器 (GPP)，并且在进一步的实施例中，可为具有用于执行任何安全相关协议的处理的可执行指令。

[0047] 虽然在图 2 中设备 200 的硬件层 206 被示出具有一些元件，但是设备 200 的硬件部分或部件可包括计算装置的任何类型和形式的元件、硬件或软件，例如此处结合图 1C 和 1D 示出和讨论的计算装置 100。在一些实施例中，设备 200 可包括服务器、网关、路由器、交换机、桥接器或其它类型的计算或网络装置，并且具有与此相关的任何硬件和 / 或软件元件。

[0048] 设备 200 的操作系统分配、管理或另外分离可用的系统存储器到内核空间 204 和用户空间 204。在示例的软件架构 200 中，操作系统可为任何类型和 / 或形式的 Unix 操作系统，虽然本发明并未如此限制。同样的，设备 200 可运行任何操作系统，例如任何版本的 Microsoft® Windows 操作系统，不同版本的 Unix 和 Linux 操作系统，用于 Macintosh 计算机的任何版本的 Mac OS®，任何嵌入式操作系统，任何网络操作系统，任何实时操作系统，任何开源操作系统，任何专有操作系统，用于移动计算装置或网络装置的任何操作系统，或者可以在设备 200 上运行并执行此处所述操作的任何其它操作系统。

[0049] 内核空间 204 被保留用于运行内核 230，包括任一设备驱动器、内核扩展或其它内核相关软件。就像本领域技术人员所知的，内核 230 是操作系统的根本，并提供对设备 104 的资源和硬件相关元件的访问、控制和管理。根据设备 200 的实施例，内核空间 204 也包括与高速缓存管理器 232 协同工作的多个网络服务或进程，有时也称为集成的高速缓存，其益处此处将进一步详细描述。另外，内核 230 的实施例将依赖于通过设备 200 安装、配置或其它使用的操作系统的实施例。

[0050] 在一个实施例中，设备 200 包括一个网络堆栈 267，例如基于 TCP/IP 的堆栈，用于与客户端 102 和 / 或服务器 106 通信。在一个实施例中，使用网络堆栈 267 与诸如网络 108 的第一网络以及第二网络 110 通信。在一些实施例中，设备 200 终止第一传输层连接，例如客户端 102 的 TCP 连接，并建立到服务器 106 的第二传输层连接，用于由客户端 102 使用，例如，在设备 200 和服务器 106 处终止第二传输层连接。可通过单一的网络堆栈 267 建立第一和第二传输层连接。在其它实施例中，设备 200 可包括多个网络堆栈，例如 267 或 267'，并且可在单一的网络堆栈 267 建立或终止第一传输层连接，在第二网络堆栈 267' 可建立或者终止第二传输层连接。例如，一个网络堆栈可用于在第一网络上接收和发送网络包，并且另

一个网络堆栈用于在第二网络上接收和发送网络包。在一个实施例中，网络堆栈 267 包括用于排队一个或多个网络包的缓冲器 243，其中网络包由设备 200 发送。

[0051] 如图 2 所示，内核空间 204 包括高速缓存管理器 232、高速层 2-7 集成包引擎 240、加密引擎 234、策略引擎 236 以及多协议压缩逻辑 238。在内核空间 204 或内核模式而不是用户空间 202 中运行这些组件或进程 232、240、234、236 和 238 提高这些组件中的每个的单独的和结合的性能。内核操作意味着这些组件或进程 232、240、234、236 和 238 在设备 200 的操作系统的核地址空间中运行。例如，在内核模式中运行加密引擎 234 通过移动加密和解密操作到内核来提高加密性能，从而减少在内核模式中的存储空间或内核线程与在用户模式中的存储空间或线程之间的转换的数量。例如，在内核模式中获得的数据可以不需要传输或拷贝到运行在用户模式的进程或线程，例如从内核级数据结构到用户级数据结构。在另一个方面，也可减少内核模式和用户模式之间的上下文切换的数量。另外，任何组件或进程 232、240、234、236 和 238 的同步和其之间的通信在内核空间 204 中可被更有效地执行。

[0052] 在一些实施例中，组件 232、240、234、236 和 238 的任何部分可在内核空间 204 中运行或操作，而这些组件 232、240、234、236 和 238 的其它部分可在用户空间 202 中运行或操作。在一个实施例中，设备 200 使用内核级数据结构来提供对一个或多个网络包的任何部分的访问，例如，包括来自客户端 102 的请求或者来自服务器 106 的响应的网络包。在一些实施例中，可以由包引擎 240 通过到网络堆栈 267 的传输层驱动器接口或过滤器获得内核级数据结构。内核级数据结构可包括通过与网络堆栈 267 相关的内核空间 204 可访问的任何接口和 / 或数据、由网络堆栈 267 接收或发送的网络业务或包。在其它实施例中，任何组件或进程 232、240、234、236 和 238 可使用内核级数据结构来执行组件或进程的期望的操作。在一个实施例中，当使用内核级数据结构时，组件 232、240、234、236 和 238 在内核模式 204 中运行，而在另一个实施例中，当使用内核级数据结构时，组件 232、240、234、236 和 238 在用户模式中运行。在一些实施例中，内核级数据结构可被拷贝或传输给第二内核级数据结构，或任何期望的用户级数据结构。

[0053] 高速缓存管理器 232 可包括软件、硬件或软件和硬件的任一组合，以提供对任何类型和形式的内容的高速缓存访问、控制和管理，例如对象或由源服务器 106 服务的动态产生的对象。由高速缓存管理器 232 处理和存储的数据、对象或内容可包括任何格式的数据，例如标记语言，或通过任何协议通信。在一些实施例中，高速缓存管理器 232 复制存储在其它地方的原始数据或先前被计算、产生或发送的数据，其中相对于读高速缓存存储元件，原始数据可能需要更长的访问时间以便取得、计算或获得。一旦数据被存储在高速缓存存储元件中，将来的使用可通过访问高速缓存的副本而非再取回或再计算原始数据而实现，因而减少了访问时间。在一些实施例中，高速缓存存储元件 nat 包括设备 200 的存储器 264 中的数据对象。在其它实施例中，高速缓存存储元件可包括具有比存储器 264 更快的存取时间的存储器。在另一个实施例中，高速缓存存储元件可以包括设备 200 的任何类型和形式的存储元件，诸如硬盘的部分。在一些实施例中，处理单元 262 可提供被高速缓存管理器 232 使用的高速缓存存储器。在又一个实施例中，高速缓存管理器 232 可使用存储器、存储设备或处理单元的任何部分和组合来高速缓存数据、对象或其它内容。

[0054] 另外，高速缓存管理器 232 包括用于执行此处描述的设备 200 的技术的任一实施

例的任何逻辑、功能、规则或操作。例如，高速缓存管理器 232 包括基于无效时间周期的终止，或者从容户端 102 或服务器 106 接收无效命令，无效对象的逻辑或功能。在一些实施例中，高速缓存管理器 232 可作为在内核空间 204 中执行的程序、服务、进程或任务来操作，并且在其它实施例中在用户空间 202 中执行。在一个实施例中，高速缓存管理器 232 的第一部分在用户空间 202 内执行，而第二部分在内核空间 204 内执行。在一些实施例中，高速缓存管理器 232 可包括任何类型的通用处理器 (GPP)，或者任何其它类型的集成电路，例如现场可编程门阵列 (FPGA)、可编程逻辑器件 (PLD) 或者专用集成电路 (ASIC)。

[0055] 策略引擎 236 可包括，例如，智能统计引擎或其它可编程应用。在一个实施例中，策略引擎 236 提供配置机制以允许用户识别、指定、定义或配置高速缓存策略。在一些实施例中，策略引擎 236 也访问存储器以支持数据结构，例如查找表或哈希 (hash) 表，以启用用户选择的高速缓存策略决定。在其它实施例中，策略引擎 236 可包括任何逻辑、规则、功能或操作以决定和提供除了对安全、网络业务、网络访问、压缩或其它任何由设备 200 执行的功能或操作的访问、控制和管理之外的对设备 200 所高速缓存的对象、数据、或内容的访问、控制和管理。特定高速缓存策略的其它实施例在此处进一步进行了描述。

[0056] 加密引擎 234 包括用于控制任何安全相关协议处理，例如 SSL 或 TLS，或其相关的任何功能的任何逻辑、商业规则、功能或操作。例如，加密引擎 234 加密并解密通过设备 200 通信的网络包，或其任何部分。加密引擎 234 也可代表客户端 102a-102n、服务器 106a-106n 或设备 200 来安装或建立 SSL 或 TLS 连接。同样的，加密引擎 234 提供 SSL 处理的卸载和加速。在一个实施例中，加密引擎 234 使用隧道协议来提供在客户端 102a-102n 和服务器 106a-106n 间的虚拟专用网络。在一些实施例中，加密引擎 234 与加密处理器 260 通信。在其它实施例中，加密引擎 234 包括运行在加密处理器 260 上的可执行指令。

[0057] 多协议压缩引擎 238 包括用于压缩一个或多个网络包协议（例如被设备 200 的网络堆栈 267 使用的任何协议）的任何逻辑、商业规则、功能或操作。在一个实施例中，多协议压缩引擎 238 双向压缩在客户端 102a-102n 和服务器 106a-106n 间任何基于 TCP/IP 的协议，包括消息应用编程接口 (MAPI)（电子邮件 email）、文件传输协议 (FTP)、超文本传输协议 (HTTP)、通用 Internet 文件系统 (CIFS) 协议（文件传输）、独立计算架构 (ICA) 协议、远程桌面协议 (RDP)、无线应用协议 (WAP)、移动 IP 协议以及 IP 语音 (VoIP) 协议。在其它实施例中，多协议压缩引擎 238 提供基于超文本标记语言 (HTML) 的协议的压缩，并且在一些实施例中，提供任何标记语言的压缩，例如可扩展标记语言 (XML)。在一个实施例中，多协议压缩引擎 238 提供任何高性能协议的压缩，例如为设备 200 设计的用于设备 200 通信的任何协议。在另一个实施例中，多协议压缩引擎 238 使用修改的传输控制协议（例如事务 TCP (T/TCP)、带有选择确认的 TCP (TCP-SACK)、带有大窗口的 TCP (TCP-LW)、例如 TCP-Vegas 协议的拥塞预报协议以及 TCP 电子欺骗协议）来压缩任何通信或其任何有效载荷。

[0058] 同样的，多协议压缩引擎 238 通过桌面客户端，例如 Microsoft Outlook 和非 web 瘦客户端，诸如由通用企业应用像 Oracle、SAP 和 Siebel 启动的任何客户端，甚至移动客户端，例如便携式个人计算机，来加速用户访问应用的执行。在一些实施例中，多协议压缩引擎 238 通过在内核模式 204 内部执行并与访问网络堆栈 267 的包处理引擎 240 集成，可以压缩 TCP/IP 协议承载的任何协议，例如任何应用层协议。

[0059] 集成高速层 2-7 的包引擎 240，通常也称为包处理引擎，或包引擎，通过网络端口

266 负责设备 200 接收和发送的包的内核级处理的管理。集成高速层 2-7 的包引擎 240 可包括在处理期间用于排队一个或多个网络包的缓冲器,例如用于网络包的接收或者网络包的发送。另外,集成高速层 2-7 的包引擎 240 通过网络端口 266 与一个或多个网络堆栈 267 通信以发出和接收网络包。集成高速层 2-7 的包引擎 240 与加密引擎 234、高速缓存管理器 232、策略引擎 236 和多协议压缩逻辑 238 协同工作。更具体地,配置加密引擎 234 以执行包的 SSL 处理,配置策略引擎 236 以执行涉及业务管理的功能,例如请求级内容切换以及请求级高速缓存重定向,并配置多协议压缩逻辑 238 以执行涉及数据压缩和解压缩的功能。

[0060] 集成高速层 2-7 的包引擎 240 包括包处理定时器 242。在一个实施例中,包处理定时器 242 提供一个或多个时间间隔以触发输入的(即接收的,或者输出的(即发送的))网络包的处理。在一些实施例中,集成高速层 2-7 的包引擎 240 响应于定时器 242 处理网络包。包处理定时器 242 向包引擎 240 提供任一类型和形式的信号以通知、触发或传送时间相关的事件、间隔或发生。在许多实施例中,包处理定时器 242 以毫秒级运行,例如 100ms、50ms、或 25ms。例如,在一些实施例中,包处理定时器 242 提供时间间隔或者使由集成高速层 2-7 的包引擎 240 以 10ms 时间间隔处理网络包,而在其它实施例中,以 5ms 时间间隔,并且在又进一步的实施例中,短到 3、2 或 1ms 时间间隔。集成高速层 2-7 的包引擎 240 在操作期间可与加密引擎 234、高速缓存管理器 232、策略引擎 236 以及多协议压缩引擎 238 对接、集成或通信。同样的,响应于包处理定时器 242 和 / 或包引擎 240,可执行加密引擎 234、高速缓存管理器 232、策略引擎 236 以及多协议压缩逻辑 238 的任何逻辑、功能或操作。因此,可在由包处理定时器 242 提供的时间间隔粒度(例如小于或等于 10ms 的时间间隔)执行加密引擎 234、高速缓存管理器 232、策略引擎 236 以及多协议压缩逻辑 238 的任何逻辑、功能或操作。例如,在一个实施例中,响应于集成高速层 2-7 的包引擎 240 和 / 或包处理定时器 242,高速缓存管理器 232 可执行任何高速缓存对象的无效。在另一个实施例中,高速缓存对象的终止或无效时间被设定为与包处理定时器 242 的时间间隔相同的粒度级,例如每 10ms。

[0061] 与内核空间 204 形成对比,用户空间 202 是操作系统的存储区域或部分,被用户模式应用或在用户模式中以其它方式运行的程序所使用。用户模式应用不能直接访问内核空间 204 并且为了访问内核服务而使用服务调用。如图 2 所示,设备 200 的用户空间 202 包括图形用户界面 (GUI) 210、命令行接口 (CLI) 212、壳服务 (shell service) 214、健康监控程序 216 以及守护 (daemon) 服务 218。GUI 210 和 CLI 212 提供一种方法,通过该方法系统管理员或其它用户可与设备 200 的操作相互作用并控制该设备 200 的操作,例如通过设备 200 的操作系统,并且或者是用户空间 202 或者内核空间 204。GUI 210 可为任何类型和形式的图形用户界面,并且可通过文本、图形或其它任一类型的程序或应用来呈现,例如浏览器。CLI 212 可为任何类型和形式的命令行或基于文本的接口,例如通过操作系统提供的命令行。例如,CLI 212 可包括壳 (shell),该壳是使得用户能够与操作系统交互的工具。在一些实施例中,可通过 bash、csh、tcsh 或者 ksh 类型的壳提供 CLI 212。壳服务 214 包括程序、服务、任务、进程或可执行指令以支持由用户通过 GUI 210 和 / 或 CLI 212 的与设备 200 或者操作系统的交互作用。

[0062] 使用健康监控程序 216 来监控、检查、报告并确保网络系统正常地运行以及用户通过网络接收所请求的内容。健康监控程序 216 包括一个或多个程序、服务、任务、进程或

可执行指令,为监控设备 200 的任何行为而提供逻辑、规则、功能或操作。在一些实施例中,健康监控程序 216 拦截并检查通过设备 200 传递的任何网络业务。在其它实施例中,健康监控程序 216 通过任何合适的方法和 / 或机制与一个或多个下述设备对接:加密引擎 234、高速缓存管理器 232、策略引擎 236、多协议压缩逻辑 238、包引擎 240、守护服务 218 以及壳服务 214。同样的,健康监控程序 216 可调用任何应用编程接口 (API) 以确定设备 200 的任何部分的状态、情况或健康。例如,健康监控程序 216 可基于周期性地查验或发送状态查询以检查程序、进程、服务或任务是否被激活并当前正在运行。在另一个示例中,健康监控程序 216 可检查由任何程序、进程、服务或任务提供的任何状态、错误或历史日志以确定设备 200 任何部分的任何条件、情况或错误。

[0063] 守护服务 218 是连续地或在后台中运行的程序,并且处理由设备 200 接收的周期性服务请求。在一些实施例中,守护服务向其它程序或进程转发请求,例如向合适的另一个守护服务 218。如本领域技术人员所公知,守护服务 218 可无人监护的运行,以执行连续的或周期性的系统范围功能,例如网络控制,或者执行任何期望的任务。在一些实施例中,一个或多个守护服务 218 运行在用户空间 202 中,而在其它实施例中,一个或多个守护服务 218 运行在内核空间。

[0064] 现在参见图 2B,描述了设备 200 的另一个实施例。总的来说,设备 200 提供以下服务、功能性或者操作的一个或者多个:用于一个或者多个客户端 102 和一个或者多个服务器 106 之间的通信的 SSL VPN 连接性 280、转换 / 负载平衡 284、域名服务解析 286、加速 288 和应用防火墙 290。在一个实施例中,设备 200 包括由 Florida, Ft. Lauderdale 的 Citrix Systems Inc. 制造的任一网络装置,称为 Citrix NetScaler 装置。服务器 106 的每一个可以提供一个或者多个网络相关服务 270a-270n(称为服务 270)。例如,服务器 106 可以提供 http 服务 270。设备 200 包括一个或者多个虚拟服务器或者虚拟互联网协议服务器,称为 vServer、VIP 服务器或者仅是 VIP275a-275n(此处也称为 vServer 275)。vServer275 根据设备 200 的配置和操作来接收、拦截或者以其它方式处理客户端 102 和服务器 106 之间的通信。

[0065] vServer 275 可以包括软件、硬件或者软件和硬件的任一组合。vServer275 可包括在设备 200 中的用户模式 202、内核模式 204 或者其任一组合中运行的任一类型和形式的程序、服务、任务、进程或者可执行指令。vServer 275 包括任一逻辑、功能、规则或者操作,以执行此处所述技术的任一实施例,诸如 SSL VPN 280、转换 / 负载平衡 284、域名服务解析 286、加速 288 和应用防火墙 290。在一些实施例中, vServer 275 建立到服务器 106 的服务 270 的连接。服务 275 可以包括能够连接到设备 200、客户端 102 或者 vServer 275 并与之通信的任一程序、应用、进程、任务或者可执行指令集。例如,服务 275 可以包括 web 服务器、http 服务器、ftp、电子邮件或者数据库服务器。在一些实施例中,服务 270 是守护进程或者网络驱动器,用于监听、接收和 / 或发送用于应用的通信,诸如电子邮件、数据库或者企业应用。在一些实施例中,服务 270 可以在特定的 IP 地址、或者 IP 地址和端口上通信。

[0066] 在一些实施例中, vServer 275 应用策略引擎 236 的一个或者多个策略到客户端 102 和服务器 106 之间的网络通信。在一个实施例中,该策略与 vServer275 相关。在另一个实施例中,该策略基于用户或者用户组。在又一个实施例中,策略为通用的并且应用到一个或者多个 vServer 275a-275n 和通过设备 100 通信的任一用户或者用户组。在一些实

施例中，策略引擎的策略具有基于通信的任一内容应用该策略的条件，通信的内容诸如互联网协议地址、端口、协议类型、包中的首部或者域、或者通信的上下文，诸如用户、用户组、vServer 275、传输层连接、和 / 或客户端 102 或者服务器 106 的标识或者属性。

[0067] 在其它实施例中，设备 200 和策略引擎 236 通信或者对接，以确定远程用户或者远程客户端 102 访问计算环境 15、应用、和 / 或来自服务器 106 的数据文件的验证和 / 或授权。在另一个实施例中，设备 200 和策略引擎 236 通信或者对接，以确定远程用户或者远程客户端 102 的验证和 / 或授权来使得应用传送系统 190 传送一个或者多个计算环境 15、应用、和 / 或数据文件。在又一个实施例中，设备 200 基于对远程用户或者远程客户端 103 的策略引擎 236 的验证和 / 或授权来建立 VPN 或者 SSLVPN 连接。在一个实施例中，设备 102 基于策略引擎 236 的策略来控制网络业务和通信会话的流。例如，设备 200 可以基于策略引擎 236 来控制对计算环境 15、应用或者数据文件的访问。

[0068] 在一些实施例中，vServer 275 与客户端 102 经客户端代理 120 建立传输层连接，诸如 TCP 或者 UDP 连接。在一个实施例中，vServer 275 监听和接收来自客户端 102 的通信。在其它实施例中，vServer 275 与客户端服务器 106 建立传输层连接，诸如 TCP 或者 UDP 连接。在一个实施例中，vServer 275 建立到运行在服务器 106 上的服务器 270 的互联网协议地址和端口的传输层连接。在另一个实施例中，vServer 275 将到客户端 102 的第一传输层连接与到服务器 106 的第二传输层连接相关联。在一些实施例中，vServer 275 建立到服务器 106 的传输层连接池并且经由池化的传输层连接多路复用客户端请求。

[0069] 在一些实施例中，设备 200 提供客户端 102 和服务器 106 之间的 SSL VPN 连接 280。例如，第一网络 102 上的客户端 102 请求建立到第二网络 104' 上的服务器 106 的连接。在一些实施例中，第二网络 104' 是不能从第一网络 104 路由的。在其它实施例中，客户端 102 位于公用网络 104 上，并且服务器 106 位于专用网络 104' 上，例如企业网。在一个实施例中，客户端代理 120 拦截第一网络 104 上的客户端 102 的通信，加密该通信，并且经第一传输层连接发送该通信到设备 200。设备 200 将第一网络 104 上的第一传输层连接与到第二网络 104 上的服务器 106 的第二传输层连接相关联。设备 200 接收来自客户端代理 102 的所拦截的通信，加密该通信，并且经第二传输层连接发送该通信到第二网络 104 上的服务器 106。第二传输层连接可以是池化的传输层连接。同样的，设备 200 提供用于两个网络 104、104' 之间的客户端 102 的端到端安全传输层连接。

[0070] 在一个实施例中，设备 200 寄载虚拟专用网络 104 上的客户端 102 的内部网内部网协议或者 intranetIP 282 地址。客户端 102 具有本地网络识别符，诸如互联网协议 (IP) 地址和 / 或第一网络 104 上的主机名称。当经设备 200 连接到第二网络 104'，对于第二网络 104' 上的客户端 102，设备 200 建立、分配或者以其它方式提供 IntranetIP，其是网络识别符，诸如 IP 地址和 / 或主机名称。设备 200 在第二或者专用网络 104' 上监听和接收使用客户端建立的 IntranetIP 282 的指向客户端 102 的任一通信。在一个实施例中，设备 200 用作或者代表第二专用网络 104 上的客户端 102。例如，在另一个实施例中，vServer 275 监听和响应到客户端 102 的 IntranetIP 282 的通信。在一些实施例中，如果第二网络 104' 上的计算装置 100 发送请求，设备 200 如同客户端 102 一样来处理该请求。例如，设备 200 可以响应对客户端 IntranetIP 282 的查验。在另一个实施例中，设备可以与请求和客户端 IntranetIP 282 连接的第二网络 104 上的计算装置 100 建立连接，诸如 TCP 或者 UDP 连接。

[0071] 在一些实施例中，设备 200 提供一个或者多个以下加速技术 288 以在客户端 102 和服务器 106 之间通信：1) 压缩；2) 解压缩；3) 传输控制协议池；4) 传输控制协议多路复用；5) 传输控制协议缓冲；和 6) 高速缓存。在一个实施例中，设备 200 通过开启与每一服务器 106 的一个或者多个传输层连接并且维持这些连接以允许由客户端经因特网的重复数据访问，来为服务器 106 缓解由重复开启和关闭到客户端 102 的传输层连接所带来的许多处理负载。该技术在此处被称为“连接池”。

[0072] 在一些实施例中，为了无缝拼接从客户端 102 经池化的传输层连接到服务器 106 的通信，设备 200 通过在传输层协议级修改序列号和确认号来翻译或多路复用通信。这被称为“连接多路复用”。在一些实施例中，不需要应用层协议交互作用。例如，在入站包（即，从客户端 102 接收的包）的例子中，包的源网络地址被改变到设备 200 的输出端口的地址，并且目的网络地址被改变到指定的服务器的地址。在出站包（即，从服务器 106 接收的包）的例子中，源网络地址从服务器 106 的地址被改变为设备 200 的输出端口的地址，并且目的地址从设备 200 的地址被改变到请求客户端 102 的地址。包的序列号和确认号也被翻译为到客户端 102 的设备 200 的传输层连接上的客户端 102 所期待的序列号和确认。在一些实施例中，传输层协议的包校验和被重新计算以计及这些翻译。

[0073] 在另一个实施例中，设备 200 提供转换或者负载平衡功能性 284 用于客户端 102 和服务器 106 之间的通信。在一些实施例中，基于层 4 或者应用层请求数据，设备 200 分发业务并且将客户端请求指向服务器 106。在一个实施例中，尽管网络层或者网络包的层 2 识别目的服务器 106，但设备 200 确定服务器 106 利用传输层包的有效载荷所承载的应用信息和数据来分发网络包。在一个实施例中，设备 200 的健康监控程序 216 监控服务器的健康来确定分发客户端请求用于哪个服务器 106。在一些实施例中，如果设备 200 探测到服务器 106 不可用或者具有超过预定阈值的负载，设备 200 可以将客户端请求指向或者分发到另一个服务器 106。

[0074] 在一些实施例中，设备 200 用作域名服务 (DNS) 解析器或者以其它方式提供来自客户端 102 的 DNS 请求的解析。在一些实施例中，设备拦截由客户端 102 发送的 DNS 请求。在一个实施例中，设备 200 以设备 200 所寄载的或其 IP 地址来响应客户端的 DNS 请求。在此实施例中，客户端 102 发送用于域名的网络通信到设备 200。在另一个实施例中，设备 200 以第二设备 200' 所寄载的或其 IP 地址来响应客户端的 DNS 请求。在一些实施例中，设备 200 使用由设备 200 确定的服务器 106 的 IP 地址来响应客户端的 DNS 请求。

[0075] 在又一个实施例中，设备 200 提供用于客户端 102 和服务器 106 之间通信的应用防火墙功能性 290。在一个实施例中，策略引擎 236 提供用于探测和阻断非法请求的规则。在一些实施例中，应用防火墙 290 防御拒绝服务 (DoS) 攻击。在其它实施例中，设备检查所拦截的请求的内容，以识别和阻断基于应用的攻击。在一些实施例中，规则 / 策略引擎 236 包括一个或者多个应用防火墙或者安全控制策略，用于提供保护各种类别和类型的基于 web 或者因特网的漏洞，诸如以下一个或者多个：1) 缓冲溢出，2) CGI-BIN 参数操纵，3) 表格 / 隐藏域操纵，4) 强迫浏览，5) cookie 或者会话中毒，6) 中断的访问控制列表 (ACL) 或者弱的口令，7) 跨站脚本攻击 (XSS)，8) 命令注入，9) SQL 注入，10) 错误独发敏感信息漏，11) 密码学的不安全使用，12) 服务器误配置，13) 后门和调试选项，14) web 站点毁损，15) 平台或者操作系统漏洞，和 16) 零天攻击。在实施例中，应用防火墙 290 为以下一个或者多个以检

查或者分析网络通信的形式来提供 HTML 格式域保护 :1) 返回所需要的域,2) 不允许增加的域,3) 只读和隐藏域施行,4) 下拉列表和单选按钮域一致,5) 表域最大长度施行。在一些实施例中,应用防火墙 290 确保没有修改 cookie。在其它实施例中,应用防火墙 290 通过执行合法的 URL 来防御强迫浏览。

[0076] 在又另一些实施例中,应用防火墙 290 保护包括在网络通信中的任一机密信息。应用防火墙 290 可以根据引擎 236 的规则或者策略来检查或者分析任一网络通信,以识别网络包的任一域中的任一机密信息。在一些实施例中,应用防火墙 290 识别网络通信中的信用卡号、口令、社会安全号码、名称、患者号码、接触信息和年龄的一个或者多个的出现。网络通信的编码部分可以包括这些出现或者机密信息。基于这些出现,在一个实施例中,应用防火墙 290 可以采取作用于网络通信上的策略,诸如阻止网络通信的发送。在另一个实施例中,应用防火墙 290 可以重写、移动或者以其它方式掩蔽该所识别的出现或者机密信息。

C、客户端代理

[0077] 现在看图 3,描述客户端代理 120 的实施例。客户端 102 包括客户端代理 120,用于经网络 104 与设备 200 和 / 或服务器 106 来建立和交换通信。总的来说,客户端 102 在计算装置 100 上操作,该计算装置 100 拥有带有内核模式 302 以及用户模式 303 的操作系统,以及带有一个或多个层 310a-310b 的网络堆栈 310。客户端 102 可以已经安装和 / 或执行一个或多个应用。在一些实施例中,一个或多个应用可通过网络堆栈 310 与网络 104 通信。诸如 web 浏览器的应用之一也可包括第一程序 322。例如,可在一些实施例中使用第一程序 322 来安装和 / 或执行客户端代理 120,或其中任一部分。客户端代理 120 包括拦截机制或者拦截器 350,用于拦截经由网络堆栈 310 来自一个或者多个应用的网络通信。

[0078] 客户端 102 的网络堆栈 310 可包括任何类型和形式的软件、或硬件或其组合,用于提供与网络的连接和通信。在一个实施例中,网络堆栈 310 包括用于网络协议组的软件实现。网络堆栈 310 可包括一个或多个网络层,例如为本领域技术人员所公认和了解的开放式系统互联 (OSI) 通信模型的任何网络层。同样的,网络堆栈 310 可包括任一类型和形式的协议,这些协议用于 OSI 模型的任何以下层 :1) 物理链路层,2) 数据链路层,3) 网络层,4) 传输层,5) 会话层,6) 表示层,以及 7) 应用层。在一个实施例中,网络堆栈 310 可包括在互联网协议 (IP) 的网络层协议上的传输控制协议 (TCP),通常称为 TCP/IP。在一些实施例中,可在 Ethernet 协议上承载 TCP/IP 协议,Ethernet 协议可包括 IEEE 广域网 (WAN) 或局域网 (LAN) 协议的任何族,例如被 IEEE 802.3 覆盖的那些协议。在一些实施例中,网络堆栈 310 包括任何类型和形式的无线协议,例如 IEEE 802.11 和 / 或移动互联网协议。

[0079] 考虑基于 TCP/IP 的网络,可使用任何基于 TCP/IP 的协议,包括消息应用编程接口 (MAPI) (电子邮件)、文件传输协议 (FTP)、超文本传输协议 (HTTP)、通用因特网文件系统 (CIFS) 协议 (文件传输)、独立计算框架 (ICA) 协议、远程桌面协议 (RDP)、无线应用协议 (WAP)、移动 IP 协议,以及 IP 语音 (VoIP) 协议。在另一个实施例中,网络堆栈 310 包括任何类型和形式的传输控制协议,诸如修改的传输控制协议,例如事务 TCP (T/TCP),带有选择确认的 TCP (TCP-SACK),带有大窗口的 TCP (TCP-LW),拥塞预测协议,例如 TCP-Vegas 协议,以及 TCP 电子欺骗协议。在其它实施例中,任何类型和形式的用户数据报协议 (UDP),例如 IP 上 UDP,可被网络堆栈 310 使用,诸如用于语音通信或实时数据通信。

[0080] 另外,网络堆栈 310 可包括支持一个或多个层的一个或多个网络驱动器,例如 TCP 驱动器或网络层驱动器。网络驱动器可被包括作为计算装置 100 的操作系统的一部分或者作为计算装置 100 的任何网络接口卡或其它网络访问组件的一部分。在一些实施例中,网络堆栈 310 的任何网络驱动器可被定制、修改或调整以提供网络堆栈 310 的定制或修改部分,用来支持此处描述的任何技术。在其它实施例中,设计并构建加速程序 120 以与网络堆栈 310 协同操作或工作,上述网络堆栈 310 由客户端 102 的操作系统安装或以其它方式提供。

[0081] 网络堆栈 310 包括任何类型和形式的接口,用于接收、获得、提供或以其它方式访问涉及客户端 102 的网络通信的任何信息和数据。在一个实施例中,网络堆栈 310 的接口包括应用编程接口 (API)。接口也可包括任何函数调用、钩子或过滤机制、事件或回调机制、或任何类型的接口技术。网络堆栈 310 通过接口可接收或提供与网络堆栈 310 的功能或操作相关的任何类型和形式的数据结构,例如对象。例如,数据结构可包括涉及到网络包的信息和数据,或一个或多个网络包。在一些实施例中,数据结构包括在网络堆栈 310 的协议层处理的网络包的一部分,例如传输层的网络包。在一些实施例中,数据结构 325 包括内核级数据结构,而在其它实施例中,数据结构 325 包括用户模式数据结构。内核级数据结构可包括在内核模式 302 中操作的网络堆栈 310 的部分获得的或涉及的数据结构,或者运行在内核模式 302 中的网络驱动器或其它软件,或者通过在操作系统的内核模式中运行或操作的服务、进程、任务、线程或其它可执行指令获得或接收的任何数据结构。

[0082] 此外,网络堆栈 310 的一些部分可在内核模式 302 中执行或操作,例如,数据链路或网络层,而其它部分在用户模式 303 中执行或操作,例如网络堆栈 310 的应用层。例如,网络堆栈的第一部分 310a 可为应用提供对网络堆栈 310 的用户模式的访问,而网络堆栈 310 的第二部分 310b 提供对网络的访问。在一些实施例中,网络堆栈的第一部分 310a 可包括网络堆栈 310 的一个或多个更上层,例如层 5-7 的任一层。在其它实施例中,网络堆栈 310 的第二部分 310b 包括一个或多个较低的层,例如层 1-4 的任一层。网络堆栈 310 的每个第一部分 310a 和第二部分 310b 可包括网络堆栈 310 的任何部分,在任意一个或多个网络层,在用户模式 203、内核模式 202,或其组合,或在网络层的任何部分或者指向网络层的接口点,或用户模式 303 和内核模式 302 的任何部分或指向用户模式 303 和内核模式 302 的接口点。

[0083] 拦截器 350 可以包括软件、硬件、或者软件和硬件的任一组合。在一个实施例中,拦截器 350 在网络堆栈 310 的任一点拦截网络通信,并且重定向或者发送网络通信到由拦截器 350 或者客户端代理 120 所期望的、管理的或者控制的目的地。例如,拦截器 350 可以拦截第一网络的网络堆栈 310 的网络通信并且发送该网络通信到设备 200,用于在第二网络 104 上发送。在一些实施例中,拦截器 350 包括含有诸如被构建和设计来与网络堆栈 310 对接并一同工作的网络驱动器的驱动器的任一类型的拦截器 350。在一些实施例中,客户端代理 120 和 / 或拦截器 350 操作在网络堆栈 310 的一个或者多个层,诸如在传输层。在一个实施例中,拦截器 350 包括过滤器驱动器、钩子机制、或者对接到网络堆栈的传输层的任一形式和类型的合适网络驱动器接口,诸如通过传输驱动器接口 (TDI)。在一些实施例中,拦截器 350 对接到诸如传输层的第一协议层和诸如传输协议层之上的任一层的另一个协议层,例如,应用协议层。在一个实施例中,拦截器 350 可以包括遵守网络驱动器接口规范

(NDIS) 的驱动器,或者 NDIS 驱动器。在另一个实施例中,拦截器 350 可以包括微型过滤器或者迷你端口驱动器。在一个实施例中,拦截器 350 或其部分在内核模式 202 中操作。在另一个实施例中,拦截器 350 或其部分在用户模式 203 中操作。在一些实施例中,拦截器 350 的一部分在内核模式 202 中操作,而拦截器 350 的另一部分在用户模式 203 中操作。在其它实施例中,客户端代理 120 在用户模式 203 中操作,但通过拦截器 350 对接到内核模式驱动器、进程、服务、任务或者操作系统的部分,诸如以获取内核级数据结构 225。在其它实施例中,拦截器 350 为用户模式应用或者程序,诸如应用。

[0084] 在一个实施例中,拦截器 350 拦截任一传输层连接请求。在这些实施例中,拦截器 350 执行传输层应用编程接口 (API) 调用以设置目的信息,诸如到期望位置的目的 IP 地址和 / 或端口用于定位。在此方式中,拦截器 350 拦截并且重定向传输层连接到由拦截器 350 或者客户端代理 120 控制或者管理的 IP 地址和端口。在一个实施例中,拦截器 350 设置用于到客户端 102 的本地 IP 地址和端口的连接的目的信息,其中客户端代理 120 正在监听该客户端 102 的本地 IP 地址和端口。例如,客户端代理 120 可以包括为重定向的传输层通信监听本地 IP 地址和端口的代理服务。在一些实施例中,客户端代理 120 随后将重定向的传输层通信传送到设备 200。

[0085] 在一些实施例中,拦截器 350 拦截域名服务 (DNS) 请求。在一个实施例中,客户端代理 120 和 / 或拦截器 350 解析 DNS 请求。在另一个实施例中,拦截器发送所拦截的 DNS 请求到设备 200 用于 DNS 解析。在一个实施例中,设备 200 解析 DNS 请求并且将 DNS 响应通信到客户端代理 120。在一些实施例中,设备 200 经另一个设备 200' 或者 DNS 服务器 106 来解析 DNS 请求。

[0086] 在又一个实施例中,客户端代理 120 可以包括两个代理 120 和 120'。在一个实施例中,第一代理 120 可以包括在网络堆栈 310 的网络层操作的拦截器 350。在一些实施例中,第一代理 120 拦截诸如因特网控制消息协议 (ICMP) 请求 (例如,查验和跟踪路由) 的网络层请求。在其它实施例中,第二代理 120' 可以在传输层操作并且拦截传输层通信。在一些实施例中,第一代理 120 在网络堆栈 210 的一层拦截通信并且与第二代理 120' 对接或者将所拦截的通信传送到第二代理 120'。

[0087] 客户端代理 120 和 / 或拦截器 350 可以以对网络堆栈 310 的任一其它协议层透明的方式在协议层操作或与之对接。例如,在一个实施例中,拦截器 350 可以以对诸如网络层的传输层之下的任一协议层和诸如会话、表示或应用层协议的传输层之上的任一协议层透明的方式在网络堆栈 310 的传输层操作或与之对接。这允许网络堆栈 310 的其它协议层如所期望的进行操作并无需修改以使用拦截器 350。同样的,客户端代理 120 和 / 或拦截器 350 可以与传输层对接以安全、优化、加速、路由或者负载平衡通过由传输层承载的任一协议所提供的任一通信,诸如 TCP/IP 上的应用层协议。

[0088] 此外,客户端代理 120 和 / 或拦截器可以以对任一应用、客户端 102 的用户和与客户端 102 通信的诸如服务器的任一其它计算装置透明的方式在网络堆栈 310 上操作或与之对接。客户端代理 120 和 / 或拦截器 350 可以以无需修改应用的方式被安装和 / 或执行在客户端 102 上。在一些实施例中,客户端 102 的用户或者与客户端 102 通信的计算装置未意识到客户端代理 120 和 / 或拦截器 350 的存在、执行或者操作。同样的,在一些实施例中,客户端代理 120 和 / 或拦截器 350 以对应用、客户端 102 的用户、诸如服务器的另一个计算

装置、或者由拦截器 350 对接到的协议层之上和 / 或之下的任一协议层透明的方式被安装、执行、和 / 或操作。

[0089] 客户端代理 120 包括加速程序 302、流客户端 306 和 / 或收集代理 304。在一个实施例中，客户端代理 120 包括由 Florida, Fort Lauderdale 的 Citrix Systems Inc. 开发的独立计算架构 (ICA) 客户端或其任一部分，并且也指 ICA 客户端。在一些实施例中，客户端 120 包括应用流客户端 306，用于从服务器 106 流式传输应用到客户端 102。在一些实施例中，客户端代理 120 包括加速程序 302，用于加速客户端 102 和服务器 106 之间的通信。在另一个实施例中，客户端代理 120 包括收集代理 304，用于执行端点检测 / 扫描并且收集用于设备 200 和 / 或服务器 106 的端点信息。

[0090] 在一些实施例中，加速程序 302 包括客户端侧加速程序，用于执行一个或多个加速技术以加速、增强或以其它方法改进客户端与服务器 106 的通信和 / 或对服务器 106 的访问，例如访问由服务器 106 提供的应用。加速程序 302 的可执行指令的逻辑、功能和 / 或操作可以执行一个或多个以下的加速技术：1) 多协议压缩，2) 传输控制协议池，3) 传输控制协议多路复用，4) 传输控制协议缓冲，以及 5) 通过高速缓存管理器的高速缓冲。另外，加速程序 302 可执行由客户端 102 接收和 / 或发送的任何通信的加密和 / 或解密。在一些实施例中，加速程序 302 以集成的方式或者格式执行一个或者多个加速技术。另外，加速程序 302 可以在作为传输层协议的网络包的有效载荷所承载的任一协议或者多协议上执行压缩。

[0091] 流客户端 306 包括用于接收和执行从服务器 106 所流式传输的应用的应用、程序、进程、服务、任务或者可执行指令。服务器 106 可以流式传输一个或者多个应用数据文件到流客户端 306，用于播放、执行或者以其它方式引起客户端 102 上的应用被执行。在一些实施例中，服务器 106 发送一组压缩或者打包的应用数据文件到流客户端 306。在一些实施例中，多个应用文件被压缩并存储在文件服务器上档案文件中，例如 CAB、ZIP、SIT、TAR、JAR 或其它档案文件。在一个实施例中，服务器 106 解压缩、解包或者解档应用文件并且将该文件发送到客户端 102。在另一个实施例中，客户端 102 解压缩、解包或者解档应用文件。流客户端 306 动态安装应用或其部分，并且执行该应用。在一个实施例中，流客户端 306 可以为可执行程序。在一些实施例中，流客户端 306 可以能够启动另一个可执行程序。

[0092] 收集代理 304 包括应用、程序、进程、服务、任务或者可执行指令，用于识别、获取和 / 或收集关于客户端 102 的信息。在一些实施例中，设备 200 发送收集代理 304 到客户端 102 或者客户端代理 120。收集代理 304 可以根据设备的策略引擎 236 的一个或者多个策略被配置。在其它实施例中，收集代理 304 发送在客户端 102 上所收集的信息到设备 200。在一个实施例中，设备 200 的策略引擎 236 使用所收集的信息来确定和提供客户端到网络 104 的连接的访问、验证和授权控制。

[0093] 在一个实施例中，收集代理 304 包括端点检测和扫描机制，其识别并且确定客户端的一个或者多个属性或者特征。例如，收集代理 304 可以识别和确定以下任意一个或者多个客户端侧属性：1) 操作系统和 / 或操作系统的版本，2) 操作系统的服务包，3) 运行的服务，4) 运行的进程，和 5) 文件。收集代理 304 也可以识别和确定客户端上以下任意一个或者多个的存在或者版本：1) 防病毒软件，2) 个人防火墙软件，3) 防蠕虫软件，和 4) 互联网安全软件。策略引擎 236 可以具有基于客户端或者客户端侧属性的任意一个或者多个属

性或者特征的一个或者多个策略。

[0094] 在一些实施例中，仍旧参见图 3，第一程序 322 可以被用于自动地、静默地、透明地或者以其它方式安装和 / 或执行客户端代理 120 或其部分，诸如拦截器 350。在一个实施例中，第一程序 322 包括插件组件，例如 ActiveX 控件或 Java 控件或脚本，其加载到应用并由应用执行。例如，第一程序包括被 web 浏览器应用载入和运行的 ActiveX 控件，例如在存储器空间或应用的上下文中。在另一个实施例中，第一程序 322 包括可执行指令组，该可执行指令组被例如浏览器的应用载入并执行。在一个实施例中，第一程序 322 包括被设计和构造的程序以安装客户端代理 120。在一些实施例中，第一程序 322 通过网络从另一个计算装置获得、下载、或接收客户端代理 120。在另一个实施例中，第一程序 322 是用于在客户端 102 的操作系统上安装例如网络驱动器的程序的安装程序或即插即用管理器。

D. 分层全局负载平衡

[0095] 现在参见图 4A，描述了跨越分支机构对资源进行负载平衡的聚合器设备 400A-400B（此处也称为聚合器设备 400）的分层的实施例。总的来说，第一聚合器设备 400A 被连接到提供服务给分支机构 405A-405N 的第一组分支机构设备 200A-200N（也称为分支机构设备 200）。第二聚合器设备 400B 被连接到提供服务给分支机构 405A'-405N' 的第二组分支机构设备 200A'-200N'。第一聚合器设备 405A 和第二聚合器设备 400B 互相建立连接以通信关于各自分支机构设备的性能和操作特征的信息 410A、410A' 和 410B、410B'。使用该信息 410、420，聚合器设备 400A-400N 中的任一个能够执行负载平衡 / 转换 284，以从第一组分支机构设备 200A-200N 或者第二组分支机构设备 200A'-200N' 中选择分支机构设备 200，来服务来自客户端 102 的访问资源的请求。

[0096] 任一分支机构设备 200A-200N 或者 200A'-200N' 可以被配置为知道或者识别单个聚合器设备 400。例如，第一分支机构设备 200A 可以被配置以识别和连接到第一聚合器设备 400A。第一分支机构设备 200A 可以不被配置为具有任何信息，并且因此可以不知道第二聚合器设备 400B 或者连接到第二聚合器设备 400B 的任一分支机构设备 200A'-200N'。以此方式，减少了分支机构设备 200 的配置。虽然该配置被减少，但是服务请求的分支机构设备可以访问聚合器设备 400 所知道的任一其它设备 200A-200N'。由于聚合器设备 400A-400B 共享关于分支机构设备 200A-200N' 的信息，第一聚合器设备 200 能够向第一分支机构设备 200 识别通过任一聚合器设备 400A-400B 连接的任一分支机构设备 200A-200N' 的信息。

[0097] 在一些实施例中，分支机构设备 200 提供结合图 2A 和 2B 所述的设备 200 的任何功能、操作和服务。分支机构设备 200A'-200N' 为其各自分支机构 405A'-405N' 的任一计算装置和用户提供加速 288、负载平衡 / 转换 284、SSL VPN 280 和 / 或应用防火墙服务 290。分支机构设备 200A-200N 为其各自分支机构 405A-405N 的任一计算装置和用户提供加速 288、负载平衡 284、转换、SSL VPN 280 和 / 或应用防火墙服务 290。在一个实施例中，分支机构设备 200A'-200N' 的每一个提供同样的功能、操作和服务。在其它实施例中，分支机构设备 200 的每一个可以提供与另一个分支机构设备不同的功能、操作或者服务。例如，第一分支机构设备 200A 可以提供 SSL VPN 280 和加速 288，而第二分支机构设备 200A' 可以向负载平衡 / 转换 284 提供 SSL VPN 280。第三分支机构设备 200N 可以仅提供 SSL VPN 280，而第四分支机构设备 200N 提供加速 288。进一步的例子中，第五分支机构设备 200B 可

以提供加速 288, 而第六分支机构设备 200C 提供应用防火墙 290 功能。

[0098] 虽然分支机构设备 200 总的被描述为分支机构 405 中的设备 200, 但是分支机构设备 200 可以为被部署在网络 104、105' 中的任一位置的设备 200。例如, 分支机构设备 200 可以被部署在数据中心。在另一个例子中, 分支机构设备 200 可以被部署在公司 LAN 104 的子网或者网络段上。在另一个实施例中, 分支机构设备 200A 可以被部署在第一公司 LAN 上, 而第二分支机构设备 200B' 布署在第二公司 LAN 上。在一些例子中, 分支机构设备 200 可以被部署在同一网络 104、104' 上, 作为聚合器设备 400。所以, 尽管设备 200 在图 4A 中被描述为分支机构设备 200, 但是其不限于仅在分支机构 405 的操作。

[0099] 聚合器设备 400 包括软件、硬件或者软件和硬件的任一组合。在一个实施例中, 聚合器设备 400 包括逻辑、功能或者操作 (诸如通过聚合器 450) 来确定、收集和聚合关于一个或者多个分支机构设备 200 的信息 410。例如, 信息 410 可以包括关于分支机构设备 200 的状态、负载或者性能的信息。在一个实施例中, 聚合器 450 包括应用、进程、服务、任务或可执行指令集。聚合器 450 包括用于接收和存储关于任一分支机构设备 200 的信息 410 的任一类型、形式和组合的数据结构、对象、文件和 / 或数据库。在一些实施例中, 聚合器 450 可以被组织或者被整理的方式来存储与分支机构设备 200 的名称或者识别符相关的或者由其识别的信息 410。例如, 可以通过设备 200 的识别符来索引信息 410。在一些实施例中, 聚合器 450 存储时间数据或者将其与信息 410 关联, 诸如记录的时间或者涉及事件的时间。

[0100] 在一个实施例中, 聚合器设备 400 和 / 或聚合器 450 从分支机构设备经由连接来接收信息 410。在一些实施例中, 聚合器设备 400 和分支机构设备 200 建立传输层连接或者通过传输层连接通信, 诸如 TCP 或者 UDP 连接。在其它实施例中, 聚合器设备 400 和分支机构设备 200 保持连接。在其它实施例中, 聚合器设备 400 和分支机构设备 200 基于需要建立连接, 例如当其需要通信时连接和重连。

[0101] 在一些实施例中, 聚合器设备 400 与预定数量的分支机构设备 200 建立连接或者通信。在其它实施例中, 聚合器设备 400 收集和聚合关于预定数量分支机构设备 200 的信息。在一个实施例中, 分支机构的预定数量为 31。在另一个实施例中, 分支机构的预定数量为 32。在又一个实施例中, 分支机构的预定数量为 16、48、60、96、128 或者 256。在进一步的实施例中, 分支机构的预定数量为 10、20、30、40、50、60、70、80、90、100、150、200 或者 250。聚合器设备 400 可以连接的或者从其收集信息的分支机构的数量可以依赖于网络 104、104'、设备 200、分支机构 405、分支机构网络 104 的操作或者性能特征以及跨越分支机构的应用、数据和用户的资源使用。在一些实施例中, 分支机构设备 200 的预定数量可以不设置或者配置, 或者以其它方式仅由聚合器设备 400 的存储器、容量和性能限制。

[0102] 在另一个实施例中, 聚合器设备 400 从其所连接的每一个分支机构设备 200 请求信息 410。在一些实施例中, 聚合器设备 400 依据到分支机构设备 200 的连接的建立来请求信息。在其它实施例中, 聚合器设备 400 从分支机构设备 200 以预定的频率请求信息 410, 诸如每隔 1 秒或者 1 毫秒。例如, 聚合器设备 400 可以每隔 1 秒为了信息 410 而轮询其每个分支机构设备 200A-200N。在一些实施例中, 聚合器设备 400 在预定的时间周期上从分支机构设备 200 请求信息 410, 诸如 1 个小时每隔 1 秒。在又一个实施例中, 聚合器设备 400 依据事件从分支机构设备 200 请求信息 410, 诸如接收来自客户端 102 的请求, 或者接收 DNS 请求。

[0103] 信息 410 可以包括涉及或者相关分支机构设备 200、分支机构设备 200 的网络 104、和 / 或诸如通过客户端 102、服务器 106 或者聚合器设备 400 的到分支机构设备 200 的任一连接的操作和 / 或性能特征的任一类型和形式的数据、统计、状态或者信息。在一些实施例中，信息 410 包括关于连接到分支机构设备 200 的任一客户端 102 和 / 或服务器 106 的操作和 / 或性能的数据。在一个实施例中，分支机构设备 200 确定关于其连接到的或者服务的任一客户端 102 和 / 或服务器 106 的操作和 / 或性能信息，并且在这些客户端 102 和 / 或服务器 106 上建立信息 410。在此实施例中，分支机构设备 200 可以提供该信息 410 到聚合器设备 400。

[0104] 在一些实施例中，操作和 / 或性能特征信息 410 包括关于任一以下对于分支机构设备 200、客户端 102 或者服务器的信息：1) 负载；2) 连接的数量和类型；3) 资源使用；4) 资源可用性；5) 未完成请求的数量；6) 所发送的请求的数量；7) 服务的客户端的数量；8) 响应时间信息，包括平均和历史响应时间；9) 连接的错误、状态、性能或者带宽；和 10) 会话的数量、和其状况或状态。在另一个实施例中，信息 410 包括与设备 200 的任一 IP 或者网络层信息、或者设备 200 的或者设备 200 服务的客户端和 / 或服务器的连接有关的信息。例如，信息 410 可以包括设备 200 的路由表，用于执行网络地址翻译，诸如用于 SSL VPN 连接。

[0105] 聚合器设备 400A-400B 的每一个可以共享或者以其它方式与其它聚合器设备对所聚合的信息 410 进行通信。第一聚合器设备 400A 与第二聚合器设备 400B 建立诸如 TCP 或者 UDP 传输层连接的连接。在一个实施例中，第二聚合器设备 400B 使用此连接。在另一个实施例中，第二聚合器设备 400B 与第一聚合器设备 400A 建立诸如 TCP 或者 UDP 传输层连接的连接。在一个实施例中，聚合器设备 400A-400B 可以依据引导或者启动来建立互相之间的连接或者通信信道。在其它实施例中，聚合器设备 400A-400B 可以依据配置改变或者事件来建立连接。在另一个实施例中，聚合器设备 400A-400B 可以在网络 104 上发布广播以确定另一个聚合器设备 400 的存在或者可用性。

[0106] 在一个实施例中，第一聚合器设备 400A 发送其信息 410A 到第二聚合器设备 400B。第二聚合器设备 400B 存储所接收的信息 410A 为信息 410A'，如图 4A 所示。在一些实施例中，信息 410A' 与信息 410A 被聚合或者组合。在其它实施例中，信息 410A' 与信息 410A 关联。在另一个实施例中，第二聚合器设备 400B 发送其信息 410B 到第一聚合器设备 400A。第一聚合器设备 400A 存储所接收的信息 410B 作为信息 410B'，如图 4A 所示。在一些实施例中，信息 410B' 与信息 410B 被聚合或者组合。在其它实施例中，信息 410B' 与信息 410B 相关联。第一和第二聚合器设备 400A-400B 可以交换或者提供信息 410A 和 410B 一次，或者以诸如每隔 1 毫秒或者 1 秒的预定频率。在一些实施例中，第一和第二聚合器设备 400A-400B 使用请求 / 回复消息机制或者协议来互相发送信息 410A-410B。在其它实施例中，第一和第二聚合器设备 400A-400B 具有定制或者专用交换协议，用于交换关于分支机构设备 200A-200N' 的信息 410A-410B。

[0107] 通过交换信息 410A-410B，第一聚合器设备 400A 和第二聚合器设备 400B 的每一个具有第一组一个或者多个分支机构设备 200A-200N 和第二组一个或者多个分支设备 200A'-200N' 上的信息 410A 和 410B。虽然第一聚合器设备 400A 正收集、聚合和监控关于分支机构设备 200A-200N 的信息 410A，但是第一聚合器设备 400A 得到关于分支机构设备 200A'-200N' 的、由第二聚合器设备 400B 收集、聚合和监控的信息 410B。同样，虽然第二聚

合器设备 400B 正收集、聚合和监控关于分支机构设备 200A' -200N' 的信息 410B,但是第二聚合器设备 400B 得到关于分支机构设备 200A-200N 的、由第一聚合器设备 400A 收集、聚合和监控的信息 410A。

[0108] 使用聚合器设备 400A-400B,在一个实施例中,第一分支机构设备 200A 仅需要知道第一聚合器设备 400A 的标识或者互联网协议信息,但通过聚合器设备 400A 获取其它分支机构设备 200A' -200N' 的标识。例如,依据从客户端接收对资源的请求,第一分支机构设备 200A 可以转发请求到聚合器设备 400a。相应地,聚合器设备 400A 可以发送聚合器设备 400B 所监控的分支机构设备 200A' -200N' 的标识以服务该请求。在一些实施例中,这简化了每个或者任一分支机构设备 200 的配置,而同时允许任一分支机构设备 200A-200N 以通过另一个分支机构设备 200A' -200N' 访问资源服务或者连接到资源。以此方式,客户端可以经由任一分支机构设备 200A-200N' 使用通过聚合器设备 400A-400B 收集的信息 410A-410B 来跨越任一分支机构 405A-405N 访问资源。在其它实施例中,客户端 102 能够直接连接到任一聚合器 400A-400N,并且得到对任一分支机构设备 200 的负载平衡。

[0109] 聚合器设备 400A-400B 包括负载平衡 / 转换 284 功能性、操作和 / 或逻辑,用于确定和提供对于任一分支机构设备 200、分支机构 405 的客户端 102、或者经由分支机构 405 或者分支机构设备 200 访问的服务器 106 的负载平衡服务。在一个实施例中,使用信息 410A 和 410B',第一聚合器设备 400A 能够确定来自任一分支机构设备 200A-200N' 的分支机构设备 200,以服务来自客户端 102 的请求。在另一个实施例中,使用信息 410A' 和 410B,第二聚合器设备 400B 能够确定来自任一分支机构设备 200A-200N' 的分支机构设备 200,以服务来自客户端 102 的请求。此外,聚合器设备 400A-400N 能够使用信息 410A、410N 来确定经由分支机构设备 200 访问的资源,诸如服务器 106,以服务请求。以此方式并且在一些实施例中,对于跨越所有分支机构 405A-405N' 的分支机构设备 200A-200N 和所有资源的聚合,聚合器设备 400A-440N 提供负载平衡和转换信息。

[0110] 在一些实施例中,聚合器设备 400 包括分支机构设备 200 的任一功能性、操作或者服务。例如,除了此处所述的聚合器设备 400 的负载平衡 284 和聚合操作,聚合器设备可以执行加速、SSL VPN 或者应用防火墙功能性。第一聚合器设备 400A 和第二聚合器设备 400B 可以被布署在同一网络 104 和 / 或不同网络 104、104' 上。在一些实施例中,可以布署附加的聚合器设备 400 以按比例扩大来服务多个分支机构 405 和分支机构设备 200。

[0111] 现在参见图 4B,描述布署多个聚合器设备的另一个实施例。总的来说,布署多个聚合器设备 400A、400B 和 400N 以提供对以下多个分支机构的聚合和 / 或负载平衡服务:分支机构 1-31 405A-405N、分支机构 32-63 405A' -405N'、和分支机构 64-N405A" -405N"。第一聚合器设备 400A 连接到第一组一个或者多个分支机构设备 405A-405N 并且获取该第一组一个或者多个分支机构设备 405A-405N 上的信息 410。第二聚合器设备 400B 连接到第二组一个或者多个分支机构设备 405A' -405N' 并且获取该第二组一个或者多个分支机构设备 405A' -405N' 上的信息 410。第三聚合器设备 400N 连接到第三组一个或者多个分支机构设备 405A" -405N" 并且获取该第三组一个或者多个分支机构设备 405A" -405N" 上的信息 410。

[0112] 每个聚合器设备 400A-400N 可以互相交换信息 410,以识别、了解和获取其它分支机构设备 200A-200N、200A' -200N'、200A" -200N" 上的信息 410。在一个实施例中,第一聚

合器设备 400A 与第二聚合器设备 400B 以及第三聚合器设备 400N 建立连接。在另一个实施例中，第二聚合器设备 400B 与第一聚合器设备 400A 以及第三聚合器设备 400N 建立连接。在又一个实施例中，第三聚合器设备 400N 与第二聚合器设备 400B 以及第一聚合器设备 400A 建立连接。通过任一这些连接，聚合器设备 400 可以询问、接收、发送或者以其它方式得到其当前可以不连接的一组一个或者多个分支机构设备 200 上的信息 410。

[0113] 在一些实施例中，每个聚合器设备 400 可以连接到不同于另一个聚合器设备 400 的多个分支机构设备 200 并且获取和监控该多个分支机构设备 200 上的信息 410。例如，第一聚合器设备 400A 可以监控和获取 2、3、4、5 或者 10 个设备 200 上的信息 410，而第二聚合器设备 200 监控和获取 20、30 或者 31 个设备 200 上的信息 410。在进一步的例子中，第三聚合器设备 400C 可以监控和获取单个分支机构设备 200 或者任一数量分支机构设备 200 上的信息 410。虽然图 4B 中所示的布署描述服务三组多个分支机构的三个聚合器设备 400A-400N，但是可以布署任意个聚合器设备 400 来服务任意个分支机构 405。

[0114] 在一个实施例中，在图 4B 中以虚线连接描述的诸如聚合器设备 400N' 的聚合器设备可以被用作主聚合器节点或者设备 400。例如，在一些实施例中，主聚合器设备 400N' 可以不直接收集来自分支机构设备 200 的信息 410，而聚合器设备 400N' 收集这些信息的其它聚合器设备 400A-400N 的信息 410。在一些实施例中，主聚合器设备 400N 对于任一其它聚合器设备 400 用作备份服务。例如，在一个例子中，如果聚合器设备 400A 曾被关机或者被重启，启动聚合器设备 400A 可以获取来自主聚合器设备 400N' 的最近存储的信息 410。在其它实施例中，聚合器设备 400A-400N 的每一个建立与主聚合器设备 400N' 的连接，以提供或者更新主聚合器设备 400N' 上的信息 410 和 / 或也从其它设备 400 获取其还不具有的信息 410。

[0115] 使用图 4B 中所示的布署架构，在一些实施例中，可以布署任意数量的聚合器设备 400 以对任意数量的分支机构 405 进行规模负载平衡和聚合服务。当分支机构 405 和 / 或分支机构设备 200 的数量增加时，由于仅需要被配置以知道存在的聚合器设备 400A 或者新布署的聚合器设备 400N，所以分支机构设备 200 的配置保持相对简单。通过在聚合设备 200 之间的信息 410 的聚合和交换，任一客户端或者分支机构设备 200 可以跨越任一分支机构 405 访问资源。

[0116] 参见图 5，描述用于通过聚合设备 400 实现聚合和负载平衡的方法 500 的实施例的步骤。总的来说，在步骤 505，第一聚合器设备 405A 建立与第一多个分支机构设备 200A-200N 的连接并且获取该第一多个分支机构设备 200A-200N 上的信息 410A。在步骤 510，第二聚合器设备 410A 建立与第二多个分支机构设备 200A'-200N' 的连接并获取该第二多个分支机构设备 200A'-200N' 上的信息 410B。一个或者多个第一组分支机构设备 200A-200N 可以不具有任何信息或者被配置以识别任一第二组分支机构设备 200A'-200N'。在步骤 515，第一和第二聚合器设备 400A-400B 互相之间建立连接或者通信。在步骤 520，第一和第二聚合器设备 400A-400N 交换关于第一和第二组分支机构设备 200 的标识、操作和性能信息 410。在步骤 525，第一聚合器设备 400A 接收来自客户端 102 访问资源的请求。例如，第一分支机构设备 200A 可以发送该请求到第一聚合器设备 400A，诸如为图 4A 中描述的客户端 102A。在另一个例子中，客户端 102 可以发送该请求到的聚合器设备 400A，诸如图 4A 中所示的客户端 102b 和 102n。在步骤 530，第一聚合器设备通过从第二聚合器设备 400B 接收的信息 410，从第二组分支机构设备 200A'-200N' 选择第二分支机构设

备 200A' 以服务该请求。在步骤 540, 第一聚合器设备 200 直接地或经由服务于客户端 102 的第一分支机构设备 200A 为客户端 102 发送所选择的第二分支机构设备 200A' 上的信息。在步骤 545, 客户端 102 直接地或者经由第一分支机构设备 200A 建立与第二分支机构设备 200A' 的连接。

[0117] 在进一步的细节中, 在步骤 505, 第一聚合器设备 200A 建立与一个或者多个分支机构设备 200A-200N 的任一类型和形式的连接。在一个实施例中, 第一聚合器设备 200A 建立诸如 TCP 或者 UDP 的传输层连接到分支机构设备 200A-200N。在一个实施例中, 任一分支机构设备 200A-200N 请求与聚合器设备 400A 的连接。在另一个实施例中, 聚合器设备 400A 请求与任一分支机构设备 200A-200N 的连接。在一些实施例中, 任一分支机构设备 200A-200N 可以具有传输层连接到诸如客户端代理 120 的一个或者多个客户端 102。在另一个实施例中, 任一分支机构设备 200A-200N 可以具有传输层连接到诸如服务 270 的一个或者多个服务器 106。

[0118] 第一聚合器设备 400A 可以通过任一的其到任一的第一组分支机构设备 200A-200N 的连接来获取关于这些设备的信息 410。在一个实施例中, 第一聚合器设备 400A 依据连接的建立来获取来自分支机构设备 200 的信息 410。在另一个实施例中, 第一聚合器设备 400A 依据预定的频率从分支机构设备 200 获取信息 410, 诸如每隔 1 毫秒或者 1 秒的轮询。在一些实施例中, 第一聚合器设备 400A 通过请求 / 回复机制从分支机构设备 200 获得信息 410。在又一个实施例中, 分支机构设备 200 在启动时或者以预定频率发送信息 410 到聚合器设备 400A, 诸如将信息每隔 1 毫秒或者 1 秒推进到聚合器 400 中。

[0119] 与步骤 505 类似地, 在步骤 510, 第二聚合器设备 400B 建立诸如传输层连接的连接到第二组一个或者多个分支机构设备 200A'-200N'。第二组分支机构设备 200A'-200N' 可以具有传输层连接到一个或者多个客户端 102 和 / 或服务器 106。第二聚合器设备 400B 可以通过任一的其到任一的第二组分支机构设备 200A'-200N' 的连接来获取关于这些设备的信息 410。第二聚合器设备 400B 可以在任一时间或者以任一频率来接收、请求或者获取信息 410。

[0120] 虽然第一聚合器设备 400A 具有第一组分支机构设备 200A-200N 上的信息 410A 并且第二聚合器设备 400B 具有第二组分支机构设备 200A'-200N' 上的信息 410B, 但是第一聚合器设备 400A 可以不知道任一第二组分支机构设备 200A'-200N' 的标识或者不具有该任一第二组分支机构设备 200A'-200N' 上的信息。类似地, 第二聚合器设备 400B 可以不知道任一第一组分支机构设备 200A-200N 的标识或者不具有该任一第一组分支机构设备 200A-200N 上的信息。在一些实施例中, 第一组分支机构设备 200A-200N 的第一分支机构设备 200A 不知道任一第二组分支机构设备 200A'-200N' 的标识或者不具有该任一第二组分支机构设备 200A'-200N' 上的信息。在其它实施例中, 第二组分支机构设备 200A'-200N' 的第二分支机构设备 200A' 不知道任一第二组分支机构设备 200A-200N 的标识或者不具有该任一第二组分支机构设备 200A-200N 上的信息。

[0121] 在步骤 515, 第一聚合器设备 400A 和第二聚合器设备 400B 通过诸如传输层连接建立通信, 例如 TCP 或者 UDP。在一些实施例中, 第一聚合器设备 400A 和第二聚合器设备 400B 在互相之间建立一个用于通信的连接。在其它实施例中, 第一聚合器设备 400A 建立与第二聚合器设备 400B 的连接, 而第二聚合器设备 400B 建立与第一聚合器设备 400A 的连接。

[0122] 在步骤 520,聚合器设备 400A 和 400B 可以以周期为基础交换信息 410,诸如每隔 1 秒或者 1 毫秒的频率。在一些实施例中,聚合器设备 400A 依据来自分支机构设备 200 的信息 410 的接收来发送该信息 410 到另一个聚合器设备 400B。在一个实施例中,聚合器设备 400A 和 400B 交换或者接收来自主聚合器设备 400N' 的信息 410。通过信息 410 的交换或者接收,每个聚合器设备 400A-400B 具有每组分支机构设备上的信息 410A、410B。虽然第一聚合器设备 400A 连接到第一组分支机构设备 200A-200N,但是第一聚合器设备 400A 也获取了第二组分支机构设备 200A'-200N' 上的信息 410B'。类似地,虽然第二聚合器设备 400B 连接到第二组分支机构设备 200A'-200N',但是第二聚合器设备 400B 也获取了第一组分支机构设备 200'-200N 上的信息 410A'。使用两组信息 410A、410B,聚合器设备 400 能够做出转换和负载平衡的决定,以跨越所有的分支机构设备 200 和分支机构 405 访问资源。

[0123] 在步骤 525,聚合器设备 400 的其中之一接收来自客户端的访问资源的请求。在一个实施例中,客户端 102 发送该请求到聚合器设备 400。在另一个例子中,分支机构设备 200 代表该客户端 102 发送请求到聚合器设备 400。在又一个实施例中,另一个聚合器设备 400B 可以发送该请求到聚合器设备 400A。在一些实施例中,请求包括连接请求,诸如 TCP 或者 UDP 连接请求,或者 VPN 请求。在其它实施例中,请求包括会话请求,诸如 SSL 或者 TLS 会话,或者诸如到所寄载的服务的应用会话。在另一个实施例中,请求包括域名服务 (DNS) 请求,诸如解析域名。在一个实施例中,请求包括执行应用的请求,诸如经由应用传送系统 500。在其它实施例中,请求包括验证或者授权请求。在又一个实施例中,请求包括接收计算环境 15 的一部分的请求,诸如应用或者其中一部分,或者数据文件。

[0124] 在步骤 535,响应于请求的接收,聚合器设备 400 确定、识别和选择分支机构设备 200,以服务该请求。聚合器设备 400 使用任一的信息 410A、410B 来确定适合于服务请求的分支机构设备 200。在一个实施例中,聚合器设备 400 使用信息 410 来确定、识别和选择由分支机构设备 200 访问或者服务的服务器 106。在一些实施例中,聚合器设备 400 分析或者处理信息 410 的任一的操作和 / 或性能特征来确定适合用于请求的设备 200。在其它实施例中,聚合器设备 400 可以保持客户端 102 和分支机构设备 200 之间的持续性。例如,聚合器设备 400 可以为当前服务客户端 102、最近服务过该客户端 102 或者之前已经服务过该客户端 102 的分支机构设备 200 指定客户端 102。

[0125] 在一些实施例中,第一聚合器设备 400A 从第二组分支机构设备 200A'-200N' 中识别和选择第二分支机构设备 200A'。在一个实施例中,第一聚合器设备 400A 从第一组分支机构设备 200A-200N 中识别和选择第一分支机构设备 200A。在其它实施例中,第二聚合器设备 400B 从第一组分支机构设备 200A-200N 中识别和选择第一分支机构设备 200A。在又一个实施例中,第二聚合器设备 400B 从第二组分支机构设备 200A'-200N' 中识别和选择第二分支机构设备 200A'。

[0126] 在步骤 540,响应于客户端请求,聚合器设备 400 为客户端 102 或者服务该客户端 102 的设备 200 发送关于所选择的分支机构设备 200 的信息。在一个实施例中,聚合器设备 400 直接发送设备 200 的标识或者选择到客户端 102,诸如到客户端代理 120。在另一个实施例中,聚合器设备 400 发送设备 200 的标识或者选择到分支机构设备 200。在一些实施例中,聚合器设备 400 识别所选择的分支机构设备 200 的 IP 地址或者域名或者其它 IP 层信息到客户端 102 或者分支机构设备。在其它实施例中,聚合器设备 400 识别连接到所选择

分支机构设备 200 的信息到客户端 102 或者分支机构设备 200。

[0127] 在步骤 545, 客户端 102 建立与聚合器设备 400 所选择或者识别的分支机构设备 200 的连接。在一些实施例中, 客户端 102 诸如经由客户端代理 120 建立与所选择分支机构设备 200 的传输层连接, 例如 TCP 或者 UDP。在其它实施例中, 连接到客户端 102 的分支机构设备 200 例如代表客户端 102 建立传输层连接到所选择分支机构设备。在一些实施例中, 客户端 102 与所选择的分支机构设备 200 建立 SSL VPN 连接。在一些实施例中, 所选择的分支机构设备 200 提供或者建立到一个或者多个服务器 106 的连接。例如, 分支机构设备 200 可以具有到服务器 106 上的客户端请求被多路复用的池化的传输层连接。在又一些实施例中, 所选择的分支机构设备 200 可以为客户端 102 提供附加的负载平衡 / 转换功能性 284。在另一个实施例中, 所选择的分支机构设备 200 提供加速或者应用防火墙服务到客户端 102。

[0128] 虽然方法 500 的实施例以上通常结合访问来自分支机构 405 和 / 或分支机构设备 200 的资源的客户端 102 被描述, 但是方法 500 可以通过访问来自任一位置的聚合器设备 400 的任一客户端 102 来实现。例如, 如图 4A 所示, 客户端 102b 和 102n 可以访问聚合器设备 400, 而无需首先访问分支机构设备 200。在一个实施例中, 客户端 102b 或者 102n 可以位于因特网上并且连接到聚合器设备 200。在其它实施例中, 客户端 102a 或者 102n 可以位于同一网络 104 上, 诸如 LAN, 作为聚合器设备 400A-400N。聚合器设备 400 能够负载平衡客户端请求, 并且将客户端 102b-102n 指向所选择的分支机构设备 200。

[0129] 考虑到此处所描述的聚合器设备的结构、功能和操作, 聚合器设备提供简化了的分支机构设备的配置, 同时提供分支机构设备的可扩展的、分层的布署。通过在以分层方式布署的聚合器设备中交换分支机构设备信息, 任一的聚合器设备能够做出负载平衡和转换决定来访问任一分支机构设备、或者通过分支机构设备提供的任一资源。虽然分支机构设备可以被配置为与聚合器设备通信或者被聚合器设备可知, 但是分支机构设备通过此处讨论的聚合和负载平衡技术可以获悉或者获取其它分支机构资源的信息。该聚合器设备全局负载平衡来自跨越所有分支机构和分支机构设备的任一位置的任一客户端的资源请求。

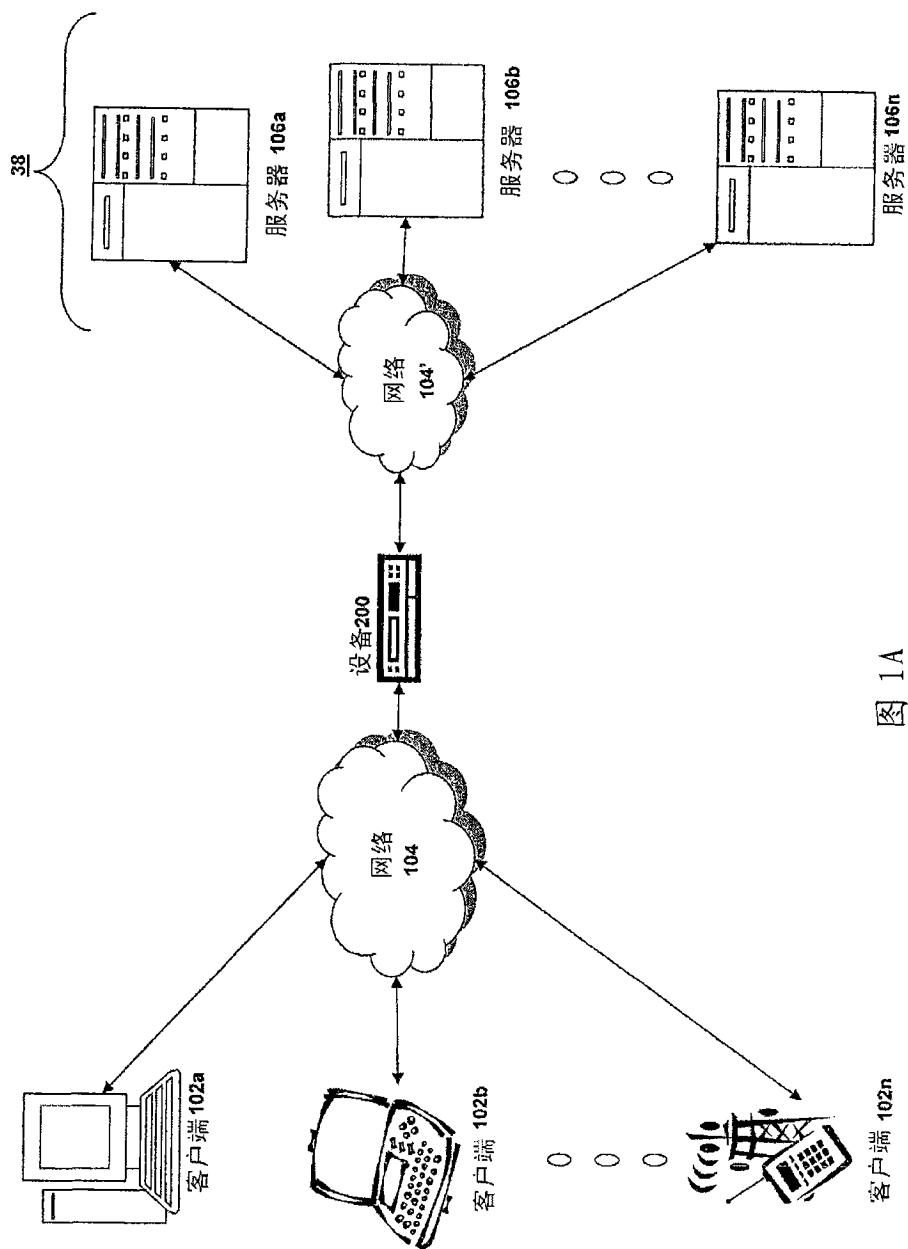


图 1A

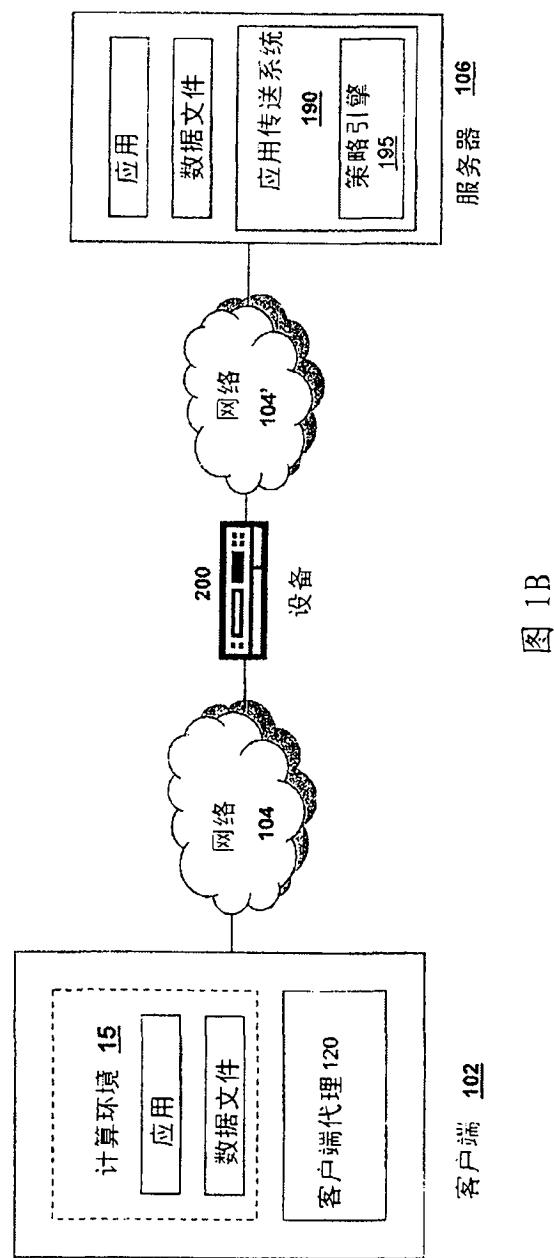


图 1B

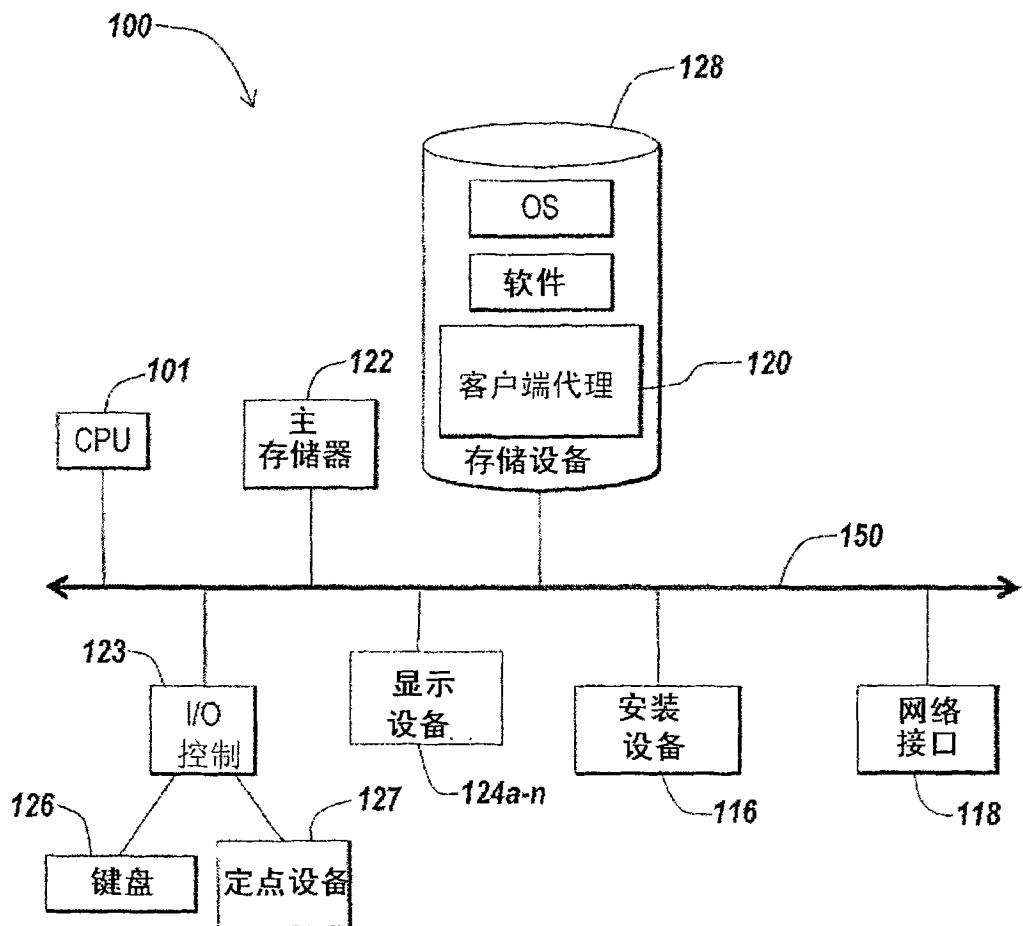


图 1C

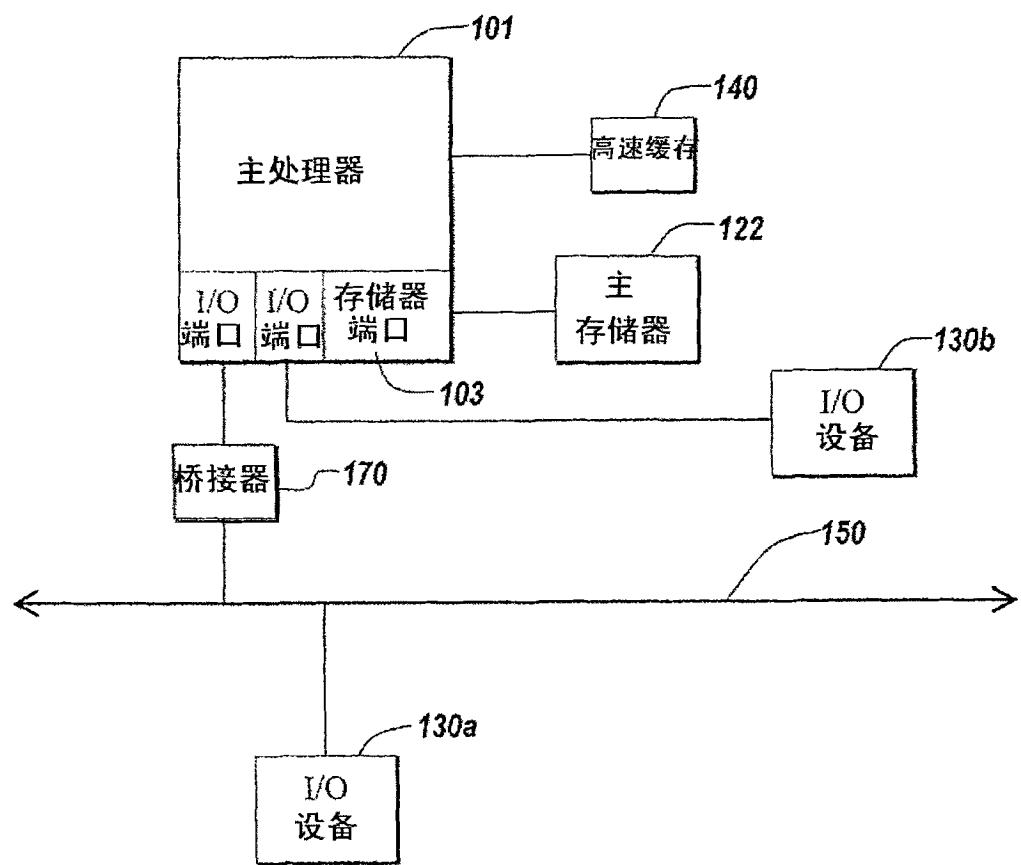


图 1D

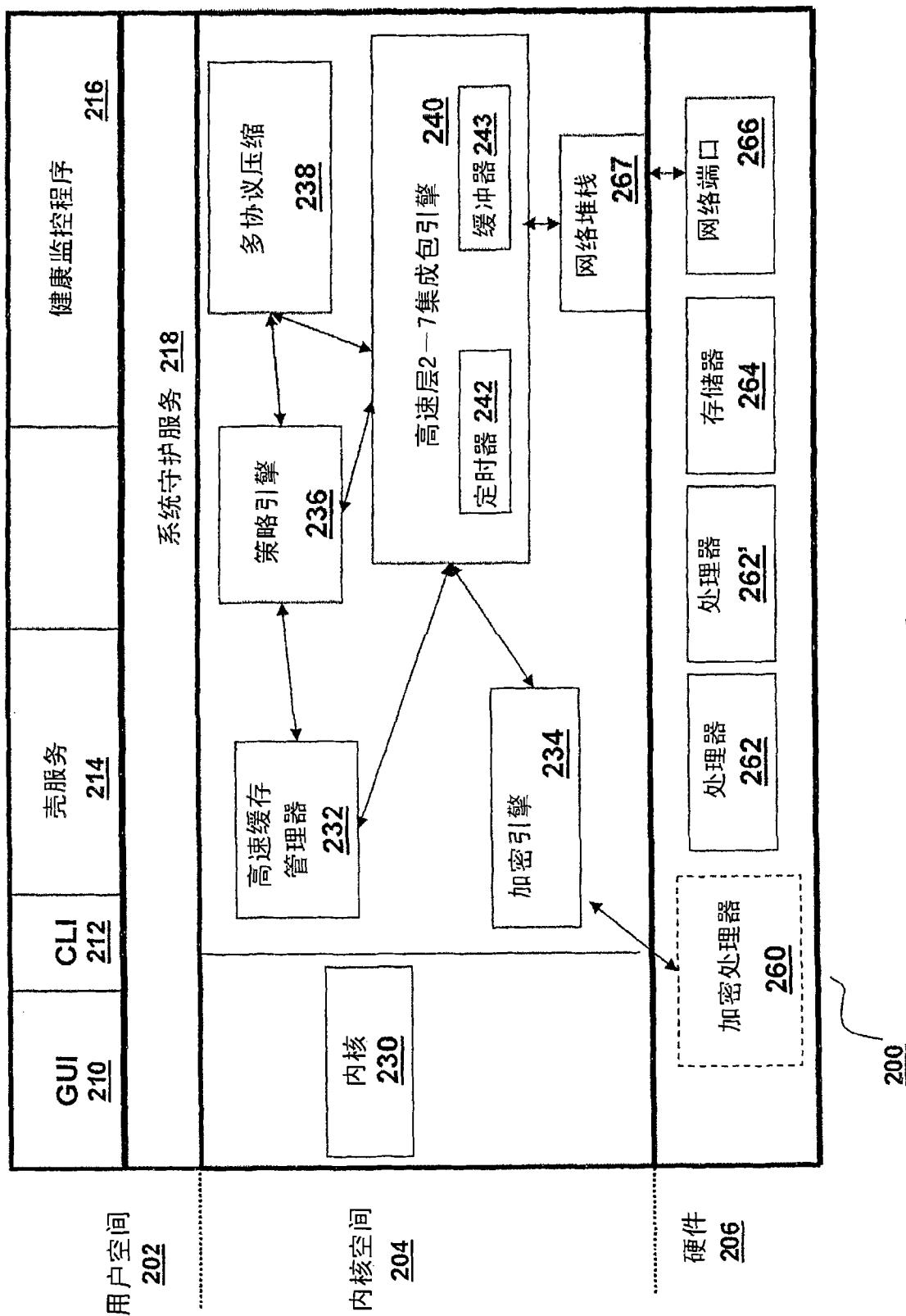


图 2A

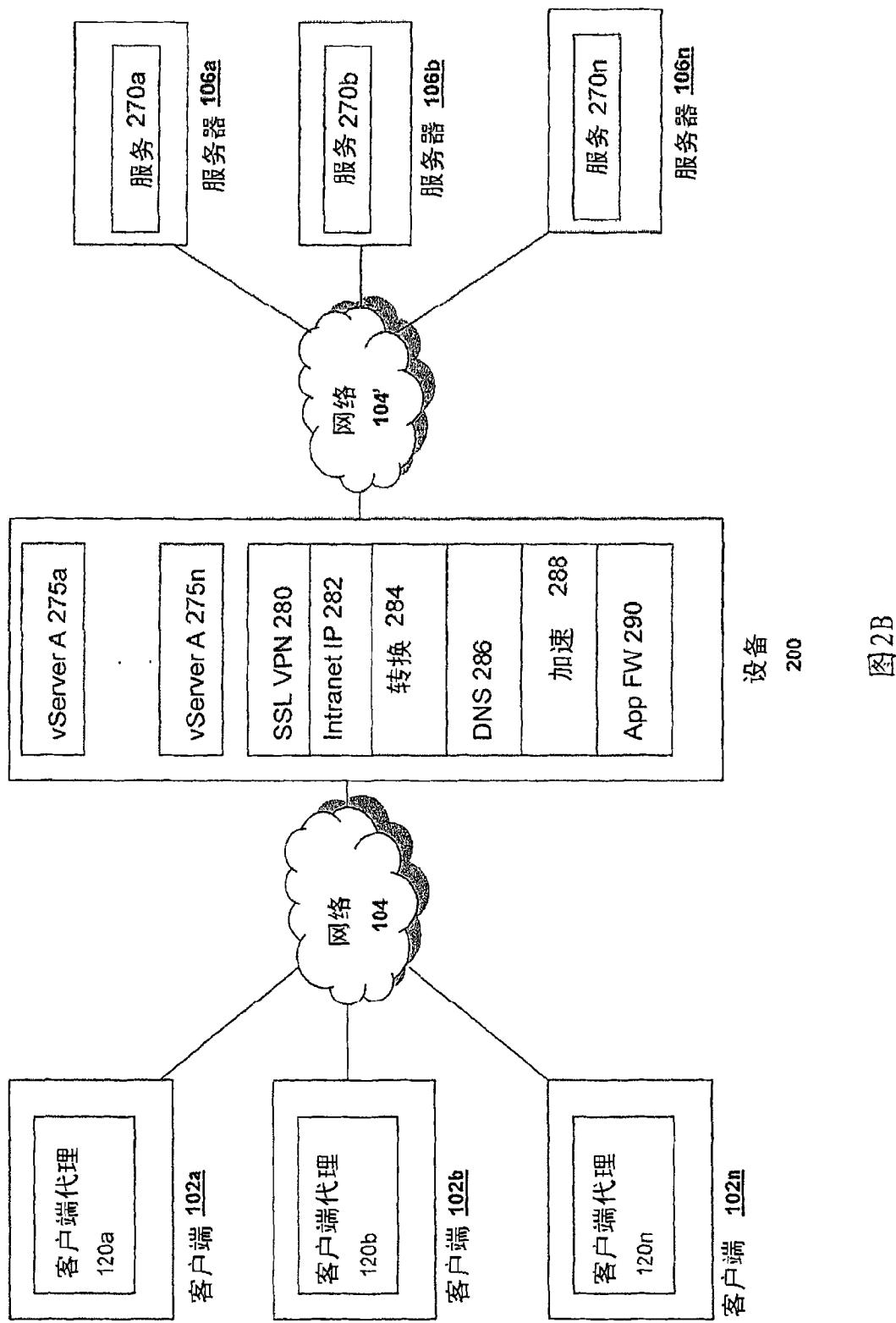
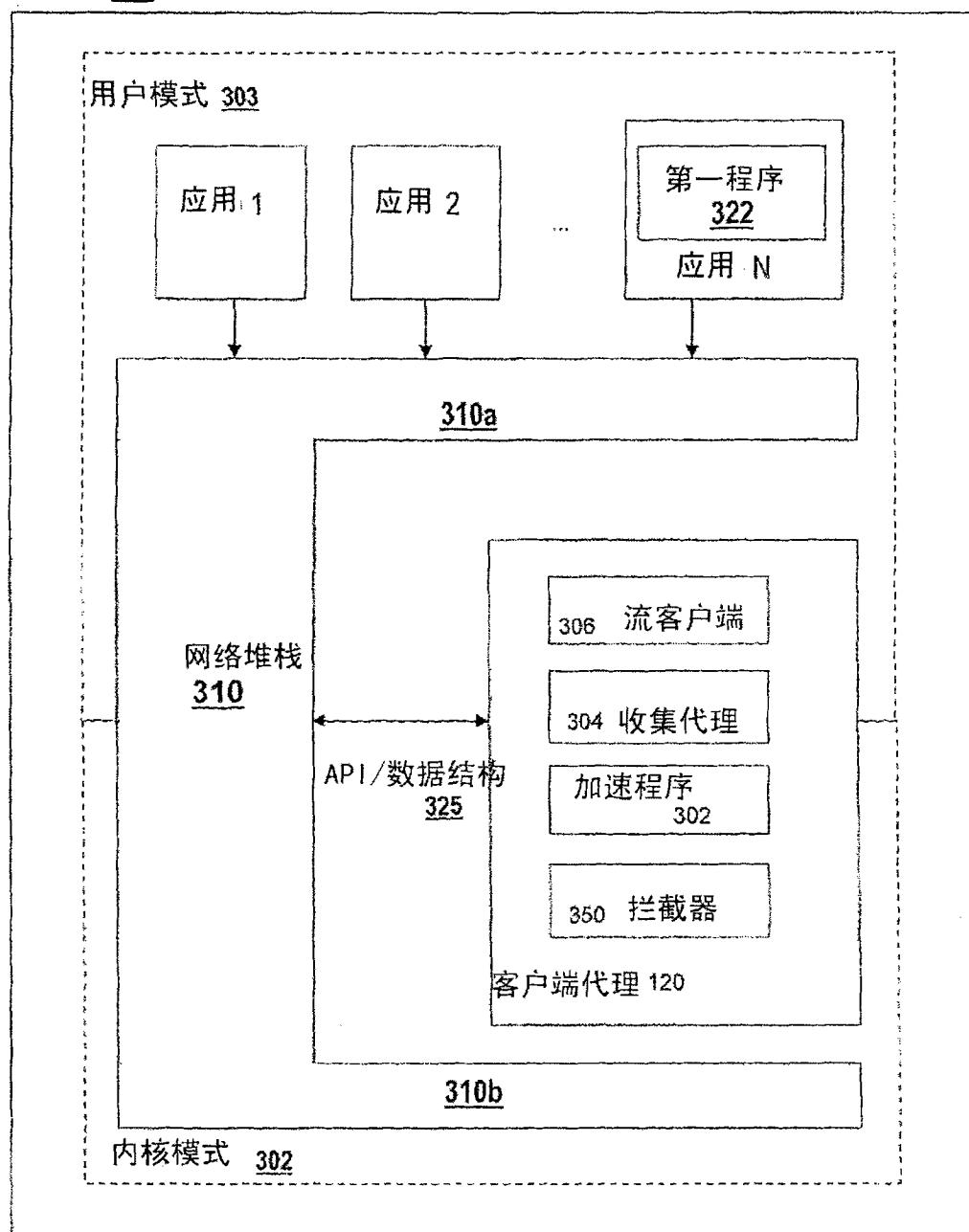


图 2B

客户端 102



100

图 3

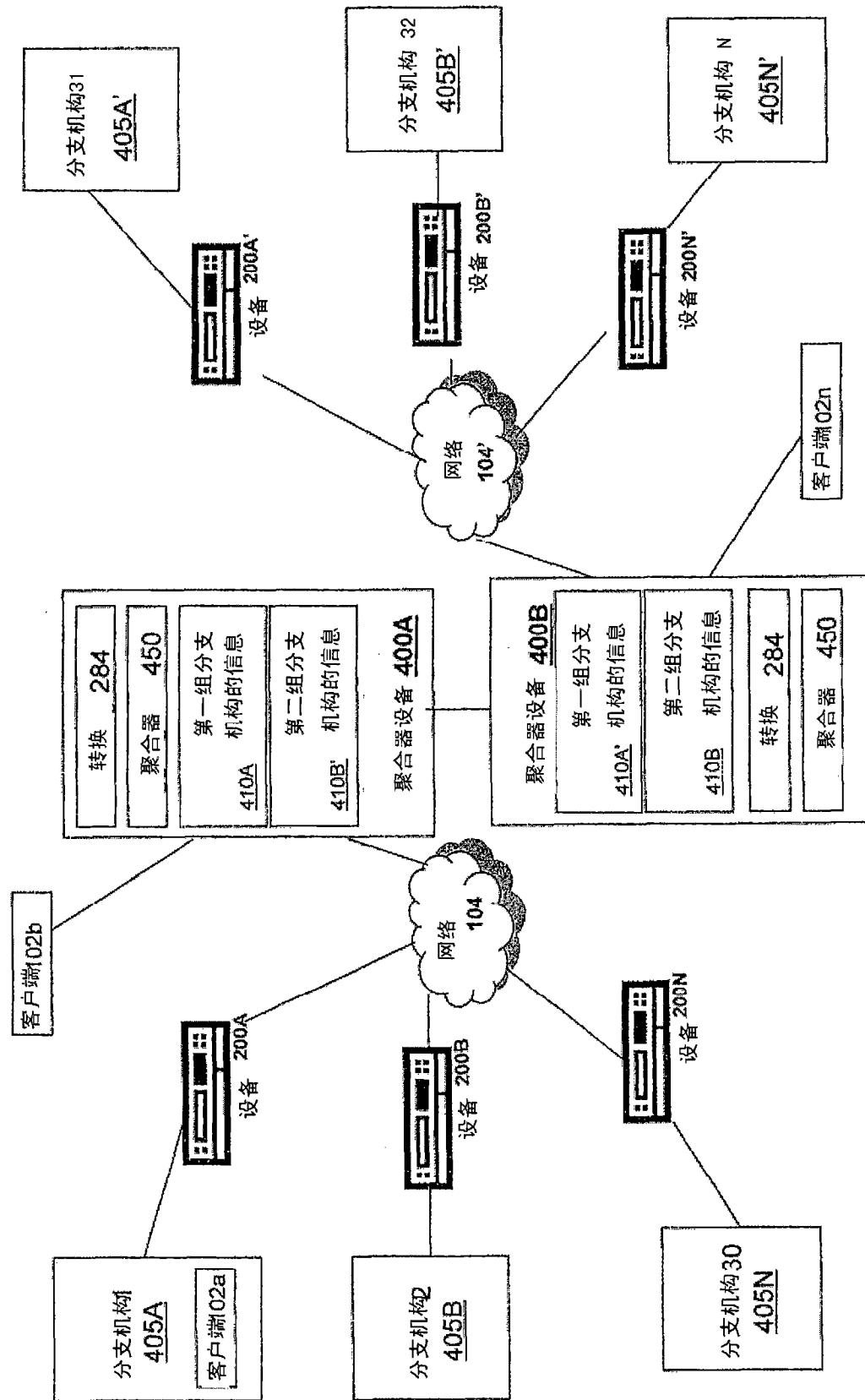


图 4A

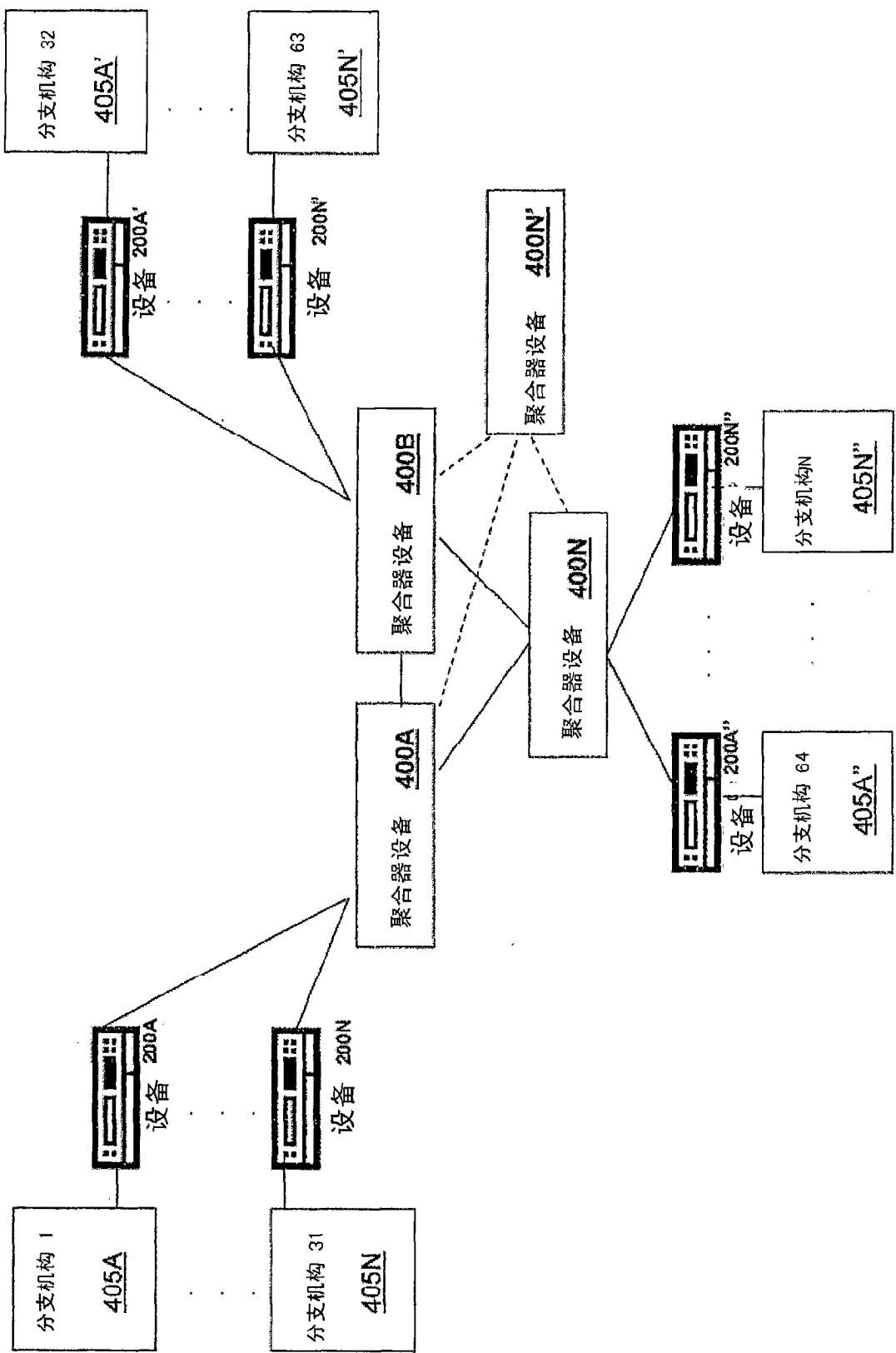
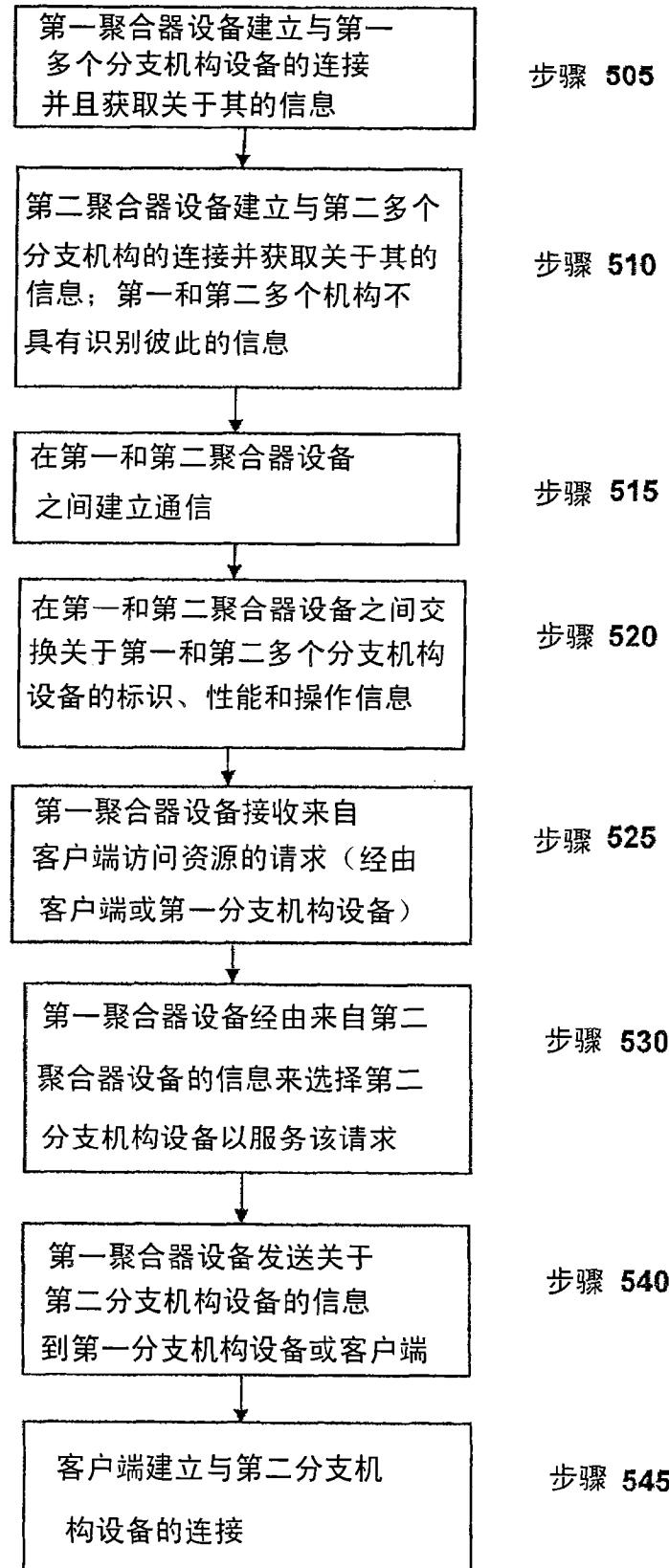


图4B



500

图5