



(12) 发明专利申请

(10) 申请公布号 CN 102132255 A

(43) 申请公布日 2011.07.20

(21) 申请号 200980130117.9

(74) 专利代理机构 北京泛华伟业知识产权代理

(22) 申请日 2009.05.27

有限公司 11280

(30) 优先权数据

12/128978 2008.05.29 US

代理人 王勇

(85) PCT申请进入国家阶段日

(51) Int. Cl.

2011.01.30

G06F 9/50 (2006.01)

H04L 29/08 (2006.01)

(86) PCT申请的申请数据

PCT/US2009/045247 2009.05.27

(87) PCT申请的公布数据

W02009/146311 EN 2009.12.03

(71) 申请人 思杰系统有限公司

地址 美国佛罗里达

(72) 发明人 S·卡马斯 J·苏甘蒂

S·维朱诺夫 M·拉加 A·谢蒂

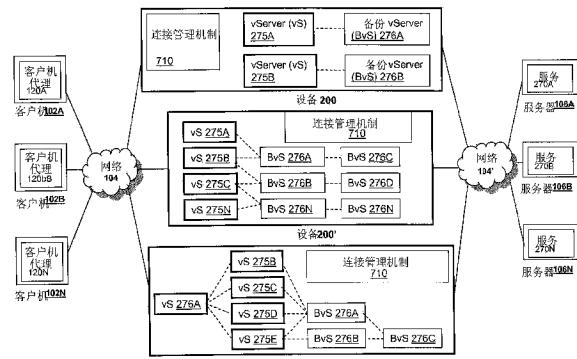
权利要求书 2 页 说明书 42 页 附图 14 页

(54) 发明名称

故障切换时使用备份虚拟服务器的指标通过
多个虚拟服务器负载平衡的系统和方法

(57) 摘要

本发明提供用于故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行负载平衡的方法和系统。此处描述的方法和系统提供如下系统和用于设备的方法：检测用设备进行负载平衡的多个虚拟服务器中的第一虚拟服务器不可用，第一虚拟服务器具有一个或多个备份虚拟服务器；识别到第一虚拟服务器的一个或多个备份虚拟服务器中的至少一个备份虚拟服务器可用；响应于所述识别保持第一虚拟服务器的状态为可用；从一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标；以及使用从与第一虚拟服务器相关联的第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载。



1. 一种故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的方法,所述方法包括如下步骤:

(a) 由设备检测用设备进行负载平衡的多个虚拟服务器中的第一虚拟服务器不可用,第一虚拟服务器具有一个或多个备份虚拟服务器;

(b) 由设备识别第一虚拟服务器的一个或多个备份虚拟服务器中的至少第一备份虚拟服务器可用;

(c) 由设备响应于所述识别保持第一虚拟服务器的状态为可用;

(d) 由设备从一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标;以及

(e) 由设备使用从和第一虚拟服务器相关联的第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载。

2. 根据权利要求 1 所述的方法,包括由设备识别第一虚拟备份服务器不可用,并由设备从第二备份虚拟服务器获得指标。

3. 根据权利要求 2 所述的方法,包括由设备使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器和多个虚拟服务器的负载。

4. 根据权利要求 2 所述的方法,包括由设备使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器的负载或者多个虚拟服务器的负载中的一个。

5. 根据权利要求 1 所述的方法,包括由设备识别第一虚拟服务器可用。

6. 根据权利要求 5 所述的方法,包括由设备使用从第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载。

7. 根据权利要求 5 所述的方法,包括由设备继续把指向第一虚拟服务器的请求发送到第一备份虚拟服务器或第一虚拟服务器之一。

8. 根据权利要求 1 所述的方法,其中步骤 (e) 包括由设备使用从多个备份虚拟服务器中的一个或多个获得的指标确定多个虚拟服务器的负载。

9. 根据权利要求 1 所述的方法,其中步骤 (f) 包括由设备的全局负载平衡虚拟服务器确定多个虚拟服务器的负载。

10. 根据权利要求 1 所述的方法,包括由设备或第二设备中的一个执行第一虚拟服务器。

11. 根据权利要求 1 所述的方法,其中步骤 (d) 包括由设备通过指标交换协议或简单网络管理协议 (SNMP) 获得指标之一。

12. 根据权利要求 1 所述的方法,其中一个或多个指标包括下列之一:连接数量、发往虚拟服务器的分组的数量或由虚拟服务器发送的分组的数量、由虚拟服务器负载平衡的服务的响应时间以及服务使用的网络带宽。

13. 根据权利要求 1 所述的方法,包括由用户识别要收集进行负载平衡的第一虚拟备份服务器或虚拟服务器之一的一个或多个指标。

14. 根据权利要求 19 所述的方法,包括由用户标识要分配给每个用户选择的指标的权重或阈值之一。

15. 一种故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的系统,所述系统包括:

设备,其对多个虚拟服务器进行负载平衡,多个虚拟服务器中的第一虚拟服务器据具有一个或多个备份虚拟服务器;

设备的监控代理,其检测第一虚拟服务器不可用、识别一个或多个备份虚拟服务器中的第一备份虚拟服务器可用并响应于所述识别保持第一虚拟服务器的状态为可用;

设备的负载监控器,其从多个一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标并使用从第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载,以确定第一虚拟服务器的负载。

17. 根据权利要求 15 所述的系统,其中监控代理还识别第一虚拟备份服务器不可用,并且负载监控器从第二备份虚拟服务器获得指标。

18. 根据权利要求 16 所述的系统,其中负载监控器还使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器和多个虚拟服务器的负载。

19. 根据权利要求 16 所述的系统,其中负载监控器还使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器的负载或多个虚拟服务器的负载之一。

20. 根据权利要求 15 所述的系统,其中监控代理还识别第一虚拟服务器可用。

21. 根据权利要求 19 所述的系统,其中负载监控器还使用从第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载。

22. 根据权利要求 19 所述的系统,其中负载监控器还继续把指向第一虚拟服务器的请求发送到第一备份虚拟服务器或第一虚拟服务器之一。

23. 根据权利要求 15 所述的系统,其中负载监控器使用从多个备份虚拟服务器中的一个或多个获得的指标确定多个虚拟服务器的负载。

24. 根据权利要求 15 所述的系统,其中设备的全局负载平衡虚拟服务器确定多个虚拟服务器的负载。

25. 根据权利要求 15 所述的系统,其中设备或第二设备之一执行第一虚拟服务器。

26. 根据权利要求 16 所述的系统,其中负载监控器通过指标交换协议或者简单网络管理协议 (SNMP) 获得指标之一。

27. 根据权利要求 16 所述的系统,其中一个或多个指标包括下列之一:连接数量、发往虚拟服务器的分组的数量或由虚拟服务器发送的分组的数量、由虚拟服务器负载平衡的服务的响应时间以及服务使用的网络带宽。

28. 一种故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的设备,所述设备包括:

用于由设备检测经负载平衡的多个虚拟服务器中的第一虚拟服务器不可用的装置,第一虚拟服务器具有一个或多个备份虚拟服务器;

用于识别第一虚拟服务器的一个或多个备份虚拟服务器中的第一备份虚拟服务器可用的装置;

用于响应于所述识别保持第一虚拟服务器的状态为可用的装置;

用于从一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标的装置;以及

用于使用从和第一虚拟服务器相关联的第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载的装置。

故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器负载平衡的系统和方法

[0001] 相关申请

[0002] 本申请要求 2008 年 5 月 29 日提交的题为“Systems And Methods For Load Balancing Via A Plurality Of Virtual Servers Upon Failover Using Metrics From A Backup Virtual Server”的美国专利申请号 12/128978 的优先权，在此通过引用将该申请并入。

背景技术

[0003] 企业或者公司可以跨越网络布置多种服务来为许多用户提供服务。例如，客户机上的用户可以请求访问诸如 web 服务器的服务。该企业可以布置多个服务器来提供该服务，用来满足访问该服务的大量用户的需求和负载。例如，服务器群可以提供能够处理客户机请求的一组服务器。此外，企业可以布置负载平衡器来管理对多个服务器的访问并且基于负载将客户机请求引导到适合的服务器。负载平衡器通过基于诸如轮询法的调度或者负载分布算法选择下一个服务器来服务所接收的请求，以将负载分布在多个服务器或者服务器上。负载平衡器可以监控客户机和服务器之间的请求和响应来确定服务器的负载或状态。

[0004] 负载平衡器可以包括任意多个用于为请求提供服务的虚拟服务器，诸如负载平衡请求。为请求提供服务的一个虚拟服务器出现故障时，由负载平衡器提供的服务会出现中断或延迟。其他虚拟服务器可以接管出故障的虚拟服务器所服务的业务。

发明内容

[0005] 本发明涉及对进行负载平衡的系统和方法的改进。本发明还涉及故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的解决方案。此处所述的系统和方法提供了一种负载平衡技术，其中，虽然检测到一个或多个虚拟服务器不可用，仍可保持负载平衡。一些方面中，本发明结合虚拟服务器和备份虚拟服务器的功能，从而即便任意多个虚拟服务器或备份虚拟服务器出现故障也可以保持所提供的负载平衡服务。这样，包括多个虚拟服务器和多个备份虚拟服务器的设备可以被配置成把多个虚拟服务器中的第一虚拟服务器以及与第一虚拟服务器相关的备份虚拟服务器视为逻辑单元，其中，和第一虚拟服务器相关联的每个备份虚拟服务器可以执行第

[0006] 一虚拟服务器的任何功能或者提供其提供第一服务器提供的任何服务。

[0007] 一些方面中，本发明涉及一种故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的方法。一些实施例中，该方法包括由设备检测用设备进行负载平衡的多个虚拟服务器中的第一虚拟服务器不可用的步骤。一些实施例中，第一虚拟服务器具有一个或多个备份虚拟服务器。该方法还可以包括由设备识别到第一虚拟服务器的一个或多个备份虚拟服务器中的至少第一备份虚拟服务器可用的步骤。许多实施例中，该方法包括由设备响应于所述识别保持第一虚拟服务器的状态为可用并且从一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标的步骤。多个实施例中，该方法包

括设备使用从与第一虚拟服务器相关联的第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载。

[0008] 多个实施例中,该方法包括由设备识别到第一虚拟备份服务器不可用,并由设备从第二备份虚拟服务器获得指标的步骤。一些实施例中,该方法包括由设备使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器和多个虚拟服务器的负载的步骤。多个实施例中,该方法包括由设备使用从第二备份虚拟服务器获得的指标确定第二备份虚拟服务器的负载或者多个虚拟服务器的负载中的一个的步骤。

[0009] 一些实施例中,该方法包括由设备识别到第一虚拟服务器可用的步骤。某些实施例中,该方法包括由设备使用从第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载的步骤。一些方面中,本方法还可以包括由设备继续把指向第一虚拟服务器的请求发送到第一备份虚拟服务器或第一虚拟服务器之一的步骤。

[0010] 多个实施例中,该方法包括由设备使用从多个备份虚拟服务器中的一个或多个获得的指标确定多个虚拟服务器的负载的步骤。一些实施例中,该方法包括由设备的全局负载平衡虚拟服务器确定多个虚拟服务器的负载的步骤。多个实施例中,该方法包括由设备或第二设备中的一个执行第一虚拟服务器的步骤。某些实施例中,该方法包括由设备通过指标交换协议或简单网络管理协议 (SNMP) 获得指标之一的步骤。

[0011] 一些实施例中,该方法中引入的一个或多个指标可包括:连接的数量、发往虚拟服务器的分组的数量或由虚拟服务器发送的分组的数量、由虚拟服务器负载平衡的服务的响应时间以及服务使用的网络带宽。多个实施例中,该方法包括由用户识别要收集进行负载平衡的第一虚拟备份服务器或虚拟服务器之一的一个或多个指标的步骤。多个实施例中,该方法包括由用户识别要分配给每个用户选择的指标的权重或阈值之一的步骤。

[0012] 某些方面中,本发明涉及一种故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的系统。一些实施例中,该系统包括对多个虚拟服务器进行负载平衡的设备,多个虚拟服务器中的第一虚拟服务器具有一个或多个备份虚拟服务器。该系统还包括设备的监控代理,其检测第一虚拟服务器不可用、识别到一个或多个备份虚拟服务器中的第一备份虚拟服务器可用并响应于所述识别保持第一虚拟服务器的状态为可用。该系统还包括设备的负载监控器,其从多个一个或多个备份虚拟服务器中的第一备份虚拟服务器获得一个或多个指标并使用从一个或多个备份虚拟服务器中的第一备份虚拟服务器获得的这些指标确定多个虚拟服务器的负载,以及使用从与第一虚拟服务器关联的第一备份虚拟服务器获得的指标确定多个虚拟服务器的负载的装置。

附图说明

[0013] 该发明的前述和其它目的、方面、特征和优点通过参考下述结合附图的描述将会更加明显并更易于理解,其中:

[0014] 图 1A 是客户机通过设备访问服务器的网络环境的实施例的框图;

[0015] 图 1B 是通过设备从服务器传送计算环境到客户机的环境的实施例的框图;

[0016] 图 1C 是通过网络从服务器传送计算环境到客户机的环境的实施例的框图;

[0017] 图 1D 是通过网络从服务器传送计算环境到客户机的环境的另一个实施例的框图;

- [0018] 图 1E 和 1F 是计算装置的实施例的框图；
- [0019] 图 2A 是用于处理客户机和服务器之间的通信的设备的实施例的框图；
- [0020] 图 2B 是用于优化、加速、负载平衡和路由客户机和服务器之间的通信的设备的另一个实施例的框图；
- [0021] 图 3 是用于通过设备与服务器通信的客户机的实施例的框图；
- [0022] 图 4 是用于经由网络管理协议收集指标并且用于基于用户选择的指标确定服务的负载的设备的实施例的框图；
- [0023] 图 5A 是用于在异类装置之间执行全局服务器负载平衡的网络环境的实施例的框图；
- [0024] 图 5B 是在异类装置之间执行服务器负载平衡的设备的实施例的框图；
- [0025] 图 6A 是故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行负载平衡的系统的实施例的框图；
- [0026] 图 6B 是故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行负载平衡的方法的步骤实施例的流程图。
- [0027] 从下面所阐述的详细说明并结合附图将明了本发明的特性和优势，其中自始至终同样的附图标记标示相应的单元。在附图中，同样的附图标记通常表示相同的、功能上相似的和 / 或结构上相似的单元。

具体实施方式

- [0028] 为了阅读下面的本发明的多个实施例的描述，说明下面的说明书的各部分以及它们相应的内容是有帮助的：
- [0029] A 部分描述有益于实施本发明实施例的网络环境和计算环境；
- [0030] B 部分描述用于将计算环境加速递送到远程用户的系统和设备架构的实施例；
- [0031] C 部分描述用于加速在客户机和服务器之间的通信的客户机代理的实施例；
- [0032] D 部分描述用于基于用户从设备确定的指标选择的指标和 / 或经由简单网络管理协议从装置收集的指标执行负载平衡的系统和方法的实施例；和
- [0033] E 部分描述用于在异类装置之间进行全局服务器负载平衡的系统和方法的实施例。

[0034] F 部分描述故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡的系统和方法的实施例。

A、网络和计算环境

[0036] 在讨论设备和 / 或客户机的系统和方法的实施例的细节之前，讨论这些实施例所布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，网络环境包括一个或多个客户机 102a-102n（同样总的称为本地机器 102，或客户机 102）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。在一些实施例中，客户机 102 通过设备 200 与服务器 106 通信。

[0037] 虽然图 1A 示出了在客户机 102 和服务器 106 之间的网络 104 和网络 104'，客户机 102 和服务器 106 可以位于相同的网络 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 104' 可为局域网 (LAN), 例如公司内网、城域网 (MAN)、或者广域网 (WAN), 例如因特网或万维网。在一个实施例中, 网络 104' 可为专用网并且网络 104 可为公网。在一些实施例中, 网络 104' 可为专用网并且网络 104' 可为公网。在另一个实施例中, 网络 104 和 104' 可都为专用网。在一些实施例中, 客户机 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。

[0038] 网络 104 和 / 或 104' 可以是任何类型和 / 或形式的网络, 并且可包括任意下述网络: 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。

[0039] 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分支机构中部署设备 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。在另一个实施例中, 多个设备 200 可在网络 104 上部署。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 作为客户机 102 可为位于同一或不同网络 104、104' 的任一客户机 102 或服务器 106 的一部分。一个或多个设备 200 可位于客户机 102 和服务器 106 之间的网络或网络通信路径中的任一点。

[0040] 在一些实施例中, 设备 200 包括由位于 Ft. Lauderdale Florida 的 Citrix Systems 公司制造的被称为 Citrix NetScaler 设备的任意网络设备。在其它实施例中, 设备 200 包括由位于 Seattle, Washington 的 F5 Networks 公司制造的被称为 WebAccelerator 和 BigIP 的任意一个产品实施例。在另一个实施例中, 设备 205 包括由位于 Sunnyvale, California 的 Juniper Networks 公司制造的 DX 加速设备平台和 / 或诸如 SA700、SA2000、SA4000 和 SA6000 的 SSL VPN 系列设备中的任意一个。在又一个实施例中, 设备 200 包括由位于 San Jose, California 的 Cisco Systems 公司制造的任意应用加速和 / 或安全相关的设备和 / 或软件, 例如 Cisco ACE 应用控制引擎模块业务 (Application Control Engine Module service) 软件和网络模块以及 Cisco AVS 系列应用速度系统 (Application Velocity System)。

[0041] 在一个实施例中, 系统可包括多个逻辑分组服务器 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 38。在其中一些实施例中, 服务器 106 可为地理上分散的。在一些情况下, 群 38 可以作为单个实体被管理。在其它实施例中, 服务器群 38 包括多个服务器群 38。在一个实施例中, 服务器群代表一个或多个客户机 102 执行一个或多个应用程序。

[0042] 在每个群 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 38 的服务器 106 不需要与相同群 38 内的另一个服务器 106 物理上接

近。因此，逻辑分组为群 38 的服务器 106 组可使用广域网 (WAN) 连接或中等区域网 (MAN) 连接互联。例如，群 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) 连接或一些直连形式进行连接，则群 38 中的服务器 106 间的数据传送速度可增加。

[0043] 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。客户机 102 也可称为客户机节点或端点。在一些实施例中，客户机 102 可以有作为寻求访问服务器上的应用的客户机节点，以及作为为其它客户机 102a-102n 提供对寄载的应用的访问的应用服务器的能力。

[0044] 在一些实施例中，客户机 102 与服务器 106 通信。在一个实施例中，客户机 102 可与群 38 中的服务器 106 之一直接通信。在另一个实施例中，客户机 102 执行程序邻近应用以与群 38 内的服务器 106 通信。在另一个实施例中，服务器 106 提供主节点的功能。在一些实施例中，客户机 102 通过网络 104 与群 38 中的服务器 106 通信。通过网络 104，客户机 102 例如可以请求执行群 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进行显示。在一些实施例中，只有主节点提供识别和提供与寄载所请求的应用的服务器 106' 相关的地址信息所需的功能。

[0045] 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 从客户机 102 接收请求，将请求转发到第二服务器 106b，并使用服务器 106b 对该请求的响应来对客户机 102 的请求进行响应。在又另一个实施例中，服务器 106 获得客户机 102 可用的应用的列举以及与由该应用的列举所识别的应用的服务器 106 相关的地址信息。在又一个实施例中，服务器 106 使用 web 接口呈现对客户机 102 的请求的响应。在一个实施例中，客户机 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，客户机 102 接收诸如显示数据的应用输出数据，该应用输出数据由服务器 106 上所识别的应用的执行而产生。

[0046] 现在参考图 1B，描述了部署多个设备 200 的网络环境的实施例。第一设备 200 可以部署在第一网络 104 上，而第二设备 200' 部署在第二网络 104' 上。例如，公司可以在分支机构部署第一设备 200，而在数据中心部署第二设备 200'。在另一个实施例中，第一设备 200 和第二设备 200' 被部署在同一个网络 104 或网络 104' 上。例如，第一设备 200 可以被部署用于第一服务器群 38，而第二设备 200 可以被部署用于第二服务器群 38'。在另一个实例中，第一设备 200 可以被部署在第一分支机构，而第二设备 200' 被部署在第二分支机构'。在一些实施例中，第一设备 200 和第二设备 200' 彼此协同或联合工作，以加速客户机和服务器之间的网络业务量或应用和数据的递送。

[0047] 现在参考图 1C，描述了使用一个或多个其它类型的设备（例如在一个或多个 WAN 优化设备 205, 205' 之间的设备），来部署设备 200 的网络环境的另一个实施例。例如，第一 WAN 优化设备 205 显示在网络 104 和 104' 之间，而第二 WAN 优化设备 205' 可以部署在设备 200 和一个或多个服务器 106 之间。例如，公司可以在分支机构部署第一 WAN 优化设备 205，而在数据中心部署第二 WAN 优化设备 205'。在一些实施例中，设备 205 可以位于网络 104' 上。在其它实施例中，设备 205' 可以位于网络 104 上。在一些实施例中，设备 205' 可以位于网络 104' 或网络 104'' 上。在一个实施例中，设备 205 和 205' 在同一个网

络上。在另一个实施例中，设备 205 和 205' 在不同的网络上。在另一个实例中，第一 WAN 优化设备 205 可以被部署用于第一服务器群 38，而第二 WAN 优化设备 205' 可以被部署用于第二服务器群 38'。

[0048] 在一个实施例中，设备 205 是用于加速、优化或者以其他方式改善诸如往和 / 或来自 WAN 连接的业务量的任意类型和形式的网络业务量的性能、操作或服务质量的装置。在一些实施例中，设备 205 是一个性能提高的代理。在其它实施例中，设备 205 是任意类型和形式的 WAN 优化或加速装置，有时也被称为 WAN 优化控制器。在一个实施例中，设备 205 是由位于 Ft. Lauderdale Florida 的 Citrix Systems 公司出品的被称为 WANScaler 的产品实施例中的任意一种。在其它实施例中，设备 205 包括由位于 Seattle, Washington 的 F5 Networks 公司出品的被称为 BIG-IP 链路控制器和 WANjet 的产品实施例中的任意一种。在另一个实施例中，设备 205 包括由位于 Sunnyvale, California 的 Juniper Networks 公司出品的 WX 和 WXC WAN 加速装置平台中的任意一种。在一些实施例中，设备 205 包括由 San Francisco, California 的 Riverbed Technology 公司出品的虹鳟 (steelhead) 系列 WAN 优化设备中的任意一种。在其它实施例中，设备 205 包括由位于 Roseland, New Jersey 的 Expand Networks 公司出品的 WAN 相关装置中的任意一种。在一个实施例中，设备 205 包括由位于 Cupertino, California 的 Packeteer 公司出品的任意一种 WAN 相关设备，例如由 Packeteer 提供的 PacketShaper、iShared 和 SkyX 产品实施例。在又一个实施例中，设备 205 包括由位于 San Jose, California 的 Cisco Systems 公司出品的任意 WAN 相关设备和 / 或软件，例如 Cisco 广域网应用服务软件和网络模块以及广域网引擎设备。

[0049] 在一个实施例中，设备 205 提供为分支机构或远程办公室提供应用和数据加速业务。在一个实施例中，设备 205 包括广域文件服务 (WAFS) 的优化。在另一个实施例中，设备 205 加速文件的递送，例如经由通用 Internet 文件系统 (CIFS) 协议。在其它实施例中，设备 205 在存储器和 / 或存储设备中提供高速缓存来加速应用和数据的递送。在一个实施例中，设备 205 在任意级别的网络堆栈或在任意的协议或网络层中提供网络业务量的压缩。在另一个实施例中，设备 205 提供传输层协议优化、流量控制、性能增强或修改和 / 或管理，以加速 WAN 连接上的应用和数据的递送。例如，在一个实施例中，设备 205 提供传输控制协议 (TCP) 优化。在其它实施例中，设备 205 提供对于任意会话或应用层协议的优化、流量控制、性能增强或修改和 / 或管理。

[0050] 在另一个实施例中，设备 205 将任意类型和形式的数据或信息编码成网络分组的定制或标准的 TCP 和 / 或 IP 报头字段或可选字段，以将存在、功能或能力通告给另一个设备 205'。在另一个实施例中，设备 205' 可以使用在 TCP 和 / 或 IP 报头字段或选项中编码的数据来与另一个设备 205' 进行通信。例如，设备可以使用 TCP 选项或 IP 报头字段或选项来传达在执行诸如 WAN 加速的功能时或者为了彼此联合工作而由设备 205, 205' 所使用的一个或多个参数。

[0051] 在一些实施例中，设备 200 保存在设备 205 和 205' 之间传达的 TCP 和 / 或 IP 报头和 / 或可选字段中编码的任意信息。例如，设备 200 可以终止经过设备 200 的传输层连接，例如经过设备 205 和 205' 的客户机和服务器之间的一个传输层连接。在一个实施例中，设备 200 识别并保存在由第一设备 205 通过第一传输层连接发送的传输层分组中的任意编码信息，并经由第二传输层连接来将具有编码信息的传输层分组传达到第二设备 205'。

[0052] 现在参考图 1D, 描述了用于递送和 / 或操作客户机 102 上的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机 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, 客户机 10 通过网络 104、104' 和设备 200 与服务器 106 通信。例如, 客户机 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。客户机 102 包括客户机代理 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 传送。

[0053] 在一些实施例中, 设备 200 加速计算环境 15 或者其任意部分到客户机 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总公司中央数据中心到远程用户位置 (例如公司的分支机构) 的应用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 加速客户机 102 和服务器 106 之间的传输层业务量。设备 200 可以提供用于加速从服务器 106 到客户机 102 的任意传输层有效载荷的加速技术, 例如 :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) 压缩和 5) 高速缓存。在一些实施例中, 设备 200 响应来自客户机 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 提供从客户机 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 提供客户机 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。

[0054] 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, 远程用户可以从任意网络连接装置 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 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一个可驻留或位于不同的服务器。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。

[0055] 客户机 102 可包括用于执行应用的计算环境 15, 该应用使用或处理数据文件。客户机 102 可通过网络 104、104' 和设备 200 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 可以转发来自客户机 102 的请求到服务器 106。例如, 客户机 102 可能不具有本地存储或者本地可访问的应用和数据文件。响应于请求, 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机 102。例如, 在一个实施例中, 服务器 106 可以应用流传递应用, 以在客户机 102 上的计算环境 15 操作。

[0056] 在一些实施例中, 应用传送系统 190 包括 Citrix Systems, Inc. 的 Citrix Access SuiteTM 的任何部分, 诸如 MetaFrame 或者 Citrix Presentation ServerTM 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机 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机或者用户。

[0057] 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的访问，应用执行方法的选择以及应用的传送。在一些实施例中，策略引擎 195 确定用户或者客户机 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机 102，例如执行方法。在一些实施例中，应用递送系统 190 提供多个递送技术，从中选择应用执行的方法，例如基于服务器的计算、本地流式传输或递送应用给客户机 120 以用于本地执行。

[0058] 在一个实施例中，客户机 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 从客户机 102 接收证书。在另一个实施例中，服务器 106 从客户机 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 列举对于客户机 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，使得客户机 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机 102。

[0059] 客户机 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 的客户机、客户机 - 服务器应用、瘦客户机计算客户机、ActiveX 控件、或者 Java 程序、或者可以在客户机 102 上执行的任意其它类型和 / 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机 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 可以使用任意瘦 - 客户机或远程显示协议来显示输出到客户机 102，所述远程显示协议例如由位于 Ft. Lauderdale, Florida 的 Citrix Systems 公司出品的独立计算架构 (ICA) 协议或由位于 Redmond, Washington 的微软公司出品的远程桌面协议 (RDP)。应用可使用任何类型的协议，并且它可为，例如，HTTP 客户机、FTP 客户机、Oscar 客户机或 Telnet 客户机。在其它实施例中，应用包括和 VoIP 通信相关的任何类型的软件，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一应用，例如用于流式传输视频和 / 或音频的应用。

[0060] 在一些实施例中，服务器 106 或服务器群 38 可运行一个或多个应用，例如提供瘦客户机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 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 Citrix Presentation Server™），和 / 或微软公司开发的 Microsoft® Windows 终端服务中的任意一个。在一个实施例中，该应用是位于 Florida, Fort Lauderdale 的 Citrix Systems Inc. 开发的 ICA 客户机。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) 客户机。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。

[0061] 仍然参看图 1D, 网络环境的一个实施例可以包括监控服务器 106A。监控服务器 106A 可以包括任何类型和形式的性能监控服务 198。性能监控服务 198 可以包括监控、测量和 / 或管理软件和 / 或硬件, 包括数据收集、集合、分析、管理和报告。在一个实施例中, 性能监控服务 198 包括一个或多个监控代理 197。监控代理 197 包括用于在诸如客户机 102、服务器 106 或设备 200 和 205 的装置上执行监控、测量和数据收集活动的任意软件、硬件或其组合。在一些实施例中, 监控代理 197 包括诸如 Visual Basic 脚本或 Javascript 任意类型和形式的脚本。在一个实施例中, 监控代理 197 相对于装置的任意应用和 / 或用户透明地执行。在一些实施例中, 监控代理 197 相对于应用或客户机不引人注目地被安装和操作。在又一个实施例中, 监控代理 197 被安装和操作而不需要用于该应用或装置的任何设备 (instrumentation)。

[0062] 在一些实施例中, 监控代理 197 以预定频率监控、测量和收集数据。在其它实施例中, 监控代理 197 基于检测到任意类型和形式的事件来监控、测量和收集数据。例如, 监控代理 197 可以在检测到对 web 页面的请求或收到 HTTP 响应时收集数据。在另一个实例中, 监控代理 197 可以在检测到诸如鼠标点击的任一用户输入事件时收集数据。监控代理 197 可以报告或提供任何所监控、测量或收集的数据给监控服务 198。在一个实施例中, 监控代理 197 根据时间安排或预定频率来发送信息给监控服务 198。在另一个实施例中, 监控代理 197 在检测到事件时发送信息给监控服务 198。

[0063] 在一些实施例中, 监控服务 198 和 / 或监控代理 197 对诸如客户机、服务器、服务器群、设备 200、设备 205 或网络连接的任意网络资源或网络基础结构元件的进行监控和性能测量。在一个实施例中, 监控服务 198 和 / 或监控代理 197 执行诸如 TCP 或 UDP 连接的任意传输层连接的监控和性能测量。在另一个实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量网络等待时间。在又一个实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量带宽利用。

[0064] 在其它实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量终端用户响应时间。在一些实施例中, 监控服务 198 执行应用的监控和性能测量。在另一个实施例中, 监控服务 198 和 / 或监控代理 197 执行到应用的任意会话或连接的监控和性能测量。在一个实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量浏览器的性能。在另一个实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量基于 HTTP 的事务的性能。在一些实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量 IP 电话 (VoIP) 应用或会话的性能。在其它实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量诸如 ICA 客户机或 RDP 客户机的远程显示协议应用的性能。在又一个实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量任意类型和形式的流媒体的性能。在进一步的实施例中, 监控服务 198 和 / 或监控代理 197 监控和测量寄载应用或软件即服务 (Software-As-A-Service, SaaS) 递送模型的性能。

[0065] 在一些实施例中,监控服务 198 和 / 或监控代理 197 执行与应用相关的一个或多个事务、请求或响应的监控和性能测量。在其它实施例中,监控服务 198 和 / 或监控代理 197 监控和测量应用层堆栈的任意部分,例如任意 .NET 或 J2EE 调用。在一个实施例中,监控服务 198 和 / 或监控代理 197 监控和测量数据库或 SQL 事务。在又一个实施例中,监控服务 198 和 / 或监控代理 197 监控和测量任意方法、函数或应用编程接口 (API) 调用。

[0066] 在一个实施例中,监控服务 198 和 / 或监控代理 197 对经由诸如设备 200 和 / 或设备 205 的一个或多个设备从服务器到客户机的应用和 / 或数据的递送进行监控和性能测量。在一些实施例中,监控服务 198 和 / 或监控代理 197 监控和测量虚拟化应用的递送的性能。在其它实施例中,监控服务 198 和 / 或监控代理 197 监控和测量流式应用的递送的性能。在另一个实施例中,监控服务 198 和 / 或监控代理 197 监控和测量递送桌面应用到客户机和 / 或在客户机上执行桌面应用的性能。在另一个实施例中,监控服务 198 和 / 或监控代理 197 监控和测量客户机 / 服务器应用的性能。

[0067] 在一个实施例中,监控服务 198 和 / 或监控代理 197 被设计和构建为应用递送系统 190 提供应用性能管理。例如,监控服务 198 和 / 或监控代理 197 可以监控、测量和管理经由 Citrix 表示服务器递送应用的性能。在该实例中,监控服务 198 和 / 或监控代理 197 监控单独的 ICA 会话。监控服务 198 和 / 或监控代理 197 可以测量总的资源使用以及每个会话系统资源使用,以及应用和连网性能。监控服务 198 和 / 或监控代理 197 可以识别给定用户和 / 或用户会话的有效服务器。在一些实施例中,监控服务 198 和 / 或监控代理 197 监控在应用递送系统 190 和应用和 / 或数据库服务器之间的后端连接。监控服务 198 和 / 或监控代理 197 可以测量每个用户会话或 ICA 会话的网络等待时间、延迟和容量。

[0068] 在一些实施例中,监控服务 198 和 / 或监控代理 197 测量和监控应用递送系统 190 的内存使用,诸如总的内存使用、每个用户会话和 / 或每个进程的内存使用。在其它实施例中,监控服务 198 和 / 或监控代理 197 测量和监控应用递送系统 190 的 CPU 使用,诸如总的 CPU 使用,每个用户会话和 / 或每个进程的 CPU 使用。在另一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控登录到诸如 Citrix 表示服务器的应用、服务器或应用递送系统所需的时间。在一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控用户登录应用、服务器或应用递送系统 190 的持续时间。在一些实施例中,监控服务 198 和 / 或监控代理 197 测量和监控应用、服务器或应用递送系统会话的有效和无效的会话计数。在又一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控用户会话等待时间。

[0069] 在又一个进一步的实施例中,监控服务 198 和 / 或监控代理 197 测量和监控任意类型和形式的服务器指标。在一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控与系统内存、CPU 使用和磁盘存储器有关的指标。在另一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控与页错误有关的指标,诸如每秒页错误。在其它实施例中,监控服务 198 和 / 或监控代理 197 测量和监控往返时间的指标。在又一个实施例中,监控服务 198 和 / 或监控代理 197 测量和监控与应用崩溃、错误和 / 或挂起相关的指标。

[0070] 在一些实施例中,监控服务 198 和监控代理 198 包括由位于 Ft. Lauderdale, Florida 的 Citrix Systems 公司出品的被称为 EdgeSight 的任意一种产品实施例。在另一个实施例中,性能监控服务 198 和 / 或监控代理 198 包括由位于 Palo Alto, California 的 Symphoniq 公司出品的被称为 TrueView 产品套件的产品实施例的任一部分。在一个实

施例中,性能监控服务 198 和 / 或监控代理 198 包括由位于 San Francisco, California 的 TeaLeaf 技术公司出品的被称为 TeaLeafCX 产品套件的产品实施例的任意部分。在其它实施例中,性能监控服务 198 和 / 或监控代理 198 包括由位于 Houston, Texas 的 BMC 软件公司出品的诸如 BMC 性能管理器和巡逻产品 (BMC Performance Manager and Patrol products) 的商业业务管理产品的任意部分。

[0071] 客户机 102、服务器 106 和设备 200 可以布署为和 / 或执行在任意类型和形式的计算装置上,诸如能够在任意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 1E 和 1F 描述了可用于实施客户机 102、服务器 106 或设备 200 的实施例的计算装置 100 的框图。如图 1E 和 1F 所示,每个计算装置 100 包括中央处理单元 101 和主存储器单元 122。如图 1E 所示,计算装置 100 可以包括可视显示装置 124、键盘 126 和 / 或诸如鼠标的指示装置 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。

[0072] 中央处理单元 101 是响应并处理从主存储器单元 122 取出的指令的任意逻辑电路。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 公司制造的微处理器单元;由 Illinois, Schaumburg 的 Motorola 公司制造的微处理器单元;由 California, Santa Clara 的 Transmeta 公司制造的微处理器单元;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 公司制造的微处理器单元。计算设备 100 可以基于这些处理器中的任意一种,或者能够按照这里所说明的那样运行的任意其它处理器。

[0073] 主存储器单元 122 可以是能够存储数据并允许微处理器 101 直接访问任意存储位置的一个或多个存储器芯片,例如静态随机访问存储器 (SRAM)、Burst (脉冲串) SRAM 或 SynchBurst SRAM (BSRAM)、动态随机访问存储器 DRAM、快速页模式 DRAM (FPM DRAM)、增强 DRAM (EDRAM)、扩展数据输出 RAM (EDO RAM)、扩展数据输出 DRAM (EDO DRAM)、脉冲串扩展数据输出 DRAM (BEDO DRAM)、增强型 DRAM (EDRAM)、同步 DRAM (SDRAM)、JEDEC SRAM、PC100 SDRAM、双数据传输率 SDRAM (DDR SDRAM)、增强 SRAM (ESDRAM)、同步链路 DRAM (SLDRAM)、直接 Rambus DRAM (DRDRAM) 或铁电 RAM (FRAM)。主存储器 122 可以基于上述存储芯片的任意一种,或者能够像这里所说明的那样运行的任意其它可用存储芯片。在图 1E 中所示的实施例中,处理器 101 通过系统总线 150 (在下面进行更详细的描述) 与主存储器 122 进行通信。图 1E 描述了在其中处理器通过存储器端口 103 直接与主存储器 122 通信的计算装置 100 的实施例。例如,在图 1F 中,主存储器 122 可以是 DRDRAM。

[0074] 图 1F 示出主处理器 101 通过第二总线与高速缓冲存储器 140 通信的实施例,第二总线有时也称为背侧总线。其他实施例中,主处理器 101 使用系统总线 150 与高速缓冲存储器 140 通信。高速缓冲存储器 140 通常有比主存储器 122 更快的响应时间,并且通常由 SRAM、BSRAM 或 EDRAM 提供。在图 1E 中所示的实施例中,处理器 101 通过本地系统总线 150 与多个 I/O 装置 130 进行通信。可以使用各种不同的总线将中央处理单元 101 连接到任意 I/O 设备 130,包括 VESA VL 总线、ISA 总线、EISA 总线、微通道体系结构 (MCA) 总线、PCI 总线、PCI-X 总线、PCI-Express 总线或 NuBus。对于 I/O 设备是视频显示器 124 的实施例,处

理器 101 可以使用加速图形接口 (AGP) 与显示器 124 通信。图 1F 说明了主处理器 101 通过超传输 (HyperTransport)、快速 I/O 或者 InfiniBand 直接与 I/O 设备 130b 通信的计算机 100 的一个实施例。图 1F 还示出了混合本地总线和直接通信的实施例：处理器 101 使用本地互连总线与 I/O 装置 130 进行通信，同时直接与 I/O 装置 130 进行通信。

[0075] 计算装置 100 可以支持任意适当的安装装置 116，例如用于接收像 3.5 英寸、5.25 英寸磁盘或 ZIP 磁盘这样的软盘的软盘驱动器、CD-ROM 驱动器、CD-R/RW 驱动器、DVD-ROM 驱动器、多种格式的磁带驱动器、USB 装置、硬盘驱动器或适于安装像任意客户机代理 120 或其部分的软件和程序的任意其它装置。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冗余阵列，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机代理 120 的任意程序的应用软件。或者，可以使用安装设备 116 的任意一种作为存储设备 128。此外，操作系统和软件可从例如可引导 CD 的可引导介质运行，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。

[0076] 此外，计算设备 100 可以包括网络接口 118 以通过多种连接（包括但不限于标准电话线路、LAN 或 WAN 链路（例如 802.11, T1, T3, 56kb, X.25）、宽带连接（如 ISDN、帧中继、ATM）、无线连接、或上述任意或全部的一些组合）连接到局域网 (LAN)、广域网 (WAN) 或因特网。网络接口 118 可以包括内置网络适配器、网络接口卡、PCMCIA 网络卡、卡总线网络适配器、无线网络适配器、USB 网络适配器、调制解调器或适用于将计算设备 100 连接到能够通信并执行这里所说明的操作的任意类型的网络的任意其它设备。各式各样的 I/O 装置 130a-130n 可以存在于计算装置 100 中。输入设备包括键盘、鼠标、触控板、轨迹球、话筒和绘图板。输出设备包括视频显示器、扬声器、喷墨打印机、激光打印机和热升华打印机。如图 1E 所示，I/O 装置 130 可以由 I/O 控制器 123 控制。I/O 控制器可以控制一个或多个 I/O 设备，例如键盘 126 和定位设备 127（如鼠标或光笔）。此外，I/O 设备还可以为计算设备 100 提供存储设备 128 和 / 或安装介质 116。在其它实施例中，计算设备 100 可以提供 USB 连接以接收手持 USB 存储设备，例如由位于 Los Alamitos, California 的 Twintech Industry 公司生产的设备的 USB 闪存驱动器线。

[0077] 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。因而，任意一种 I/O 装置 130a-130n 和 / 或 I/O 控制器 123 可以包括任一类型和 / 或形式的适当的硬件、软件或硬件和软件的组合，以支持、允许或提供通过计算装置 100 连接和使用多个显示装置 124a-124n。例如，计算装置 100 可以包括任意类型和 / 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。

[0078] 在进一步的实施例中, I/O 设备 130 可以是系统总线 150 和外部通信总线 (如 USB 总线、Apple 桌面总线、RS-232 串行连接、SCSI 总线、FireWire 总线、FireWire800 总线、以太网总线、AppleTalk 总线、千兆位以太网总线、异步传输模式总线、HIPPI 总线、超级 HIPPI 总线、SerialPlus 总线、SCI/LAMP 总线、光纤信道总线或串行 SCSI 总线) 之间的桥 170.

[0079] 图 1E 和 1F 中描述的计算装置 100 类型典型地在操作系统的控制下运行, 操作系统控制任务的调度和对系统资源的访问。装置 100 可以运行任意操作系统, 例如任意版本的 Microsoft ® Windows 操作系统, 不同发行版本的 Unix 和 Linux 操作系统, 用于 Macintosh 计算机的任意版本的 MAC OS ®, 任意嵌入式操作系统, 任意实时操作系统, 任意开源操作系统, 任意专有操作系统, 任意用于移动计算装置的操作系统, 或者任意其它能够在计算装置上运行并完成这里所述操作的操作系统。典型的操作系统包括: WINDOWS 3. x、WINDOWS 95、WINDOWS 98、WINDOWS 2000、WINDOWS NT 3. 51、WINDOWS NT 4. 0、WINDOWS CE 和 WINDOWS XP, 所有这些均由位于 Redmond, Washington 的微软公司出品; 由位于 Cupertino, California 的苹果计算机出品的 MacOS; 由位于 Armonk, New York 的国际商业机器公司出品的 OS/2; 以及由位于 Salt Lake City, Utah 的 Caldera 公司发布的可免费使用的 Linux 操作系统或者任意类型和 / 或形式的 Unix 操作系统, 以及其它。

[0080] 在其它实施例中, 计算设备 100 可以有不同的处理器、操作系统以及与其一致的输入设备。例如, 在一个实施例中, 计算机 100 是由 Palm 公司出品的 Treo180、270、1060、600 或 650 智能电话。在该实施例中, Treo 智能电话在 PalmOS 操作系统的控制下操作, 并包括指示笔输入装置以及五向导航装置。此外, 计算装置 100 可以是任意工作站、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、任意其它计算机、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。

[0081] B、设备架构

[0082] 图 2A 示出设备 200 的一个示例实施例。提供图 2A 的设备 200 架构仅用于示例, 并不意于作为限制性的架构。如图 2 所示, 设备 200 包括硬件层 206 和被分为用户空间 202 和内核空间 204 的软件层。

[0083] 硬件层 206 提供硬件元件, 在内核空间 204 和用户空间 202 中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, 这些结构和元件允许在内核空间 204 和用户空间 202 内的程序和服务既在内部又在外部与设备 200 通信数据。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, 用于通过网络传输和接收数据的网络端口 266, 以及用于执行与安全套接字协议层相关功能的处理单元 260 通过网络传输和接收的数据的加密处理器 260。在一些实施例中, 中央处理单元 262 可在单独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 的多处理器。处理单元 262 可以包括以上结合图 1E 和 1F 所述的任一处理单元 101。在一些实施例中, 中央处理单元 262 可在单独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 的多处理器。例如, 在一个实施例中, 设备 200 包括第一处理单元 262 和第二处理单元 262'。在其它实施例中, 处理单元 262 或者 262' 包括多核处理器。

[0084] 虽然示出的设备 200 的硬件层 206 通常带有加密处理器 260, 但是处理单元 262 可

为执行涉及任何加密协议的功能的处理器,例如安全套接字协议层(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,可为用于执行任何安全相关协议处理的可执行指令。

[0085] 虽然在图2中设备200的硬件层206示为具有一些元件,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1E和1F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、开关、桥接器或其它类型的计算或网络设备,并且拥有与此相关的任何硬件和/或软件元件。

[0086] 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202。在示例的软件架构200中,操作系统可以是任意类型和/或形式的Unix操作系统,尽管本发明并未这样限制。因而,设备200能够运行任意操作系统,例如任意一种版本的Microsoft® Windows操作系统、不同版本的Unix和Linux操作系统、用于Macintosh计算机的任意版本的Mac OS®、任意的嵌入式操作系统、任意的网络操作系统、任意的实时操作系统、任意的开放源操作系统、任意的专用操作系统、用于移动计算装置或网络装置的任意操作系统、或者能够运行在设备200上并执行此处所描述的操作的任意其它操作系统。

[0087] 预定内核空间204用于运行内核230,内核230包括任何设备驱动器,内核扩展或其他内核相关软件。就像本领域技术人员所知的,内核230是操作系统的根本,并提供对资源以及设备104的相关硬件元件的访问、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、配置或其他使用的操作系统的实施例。

[0088] 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,用于与客户机102和/或服务器106通信。在一个实施例中,使用网络堆栈267与例如网络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,例如客户机102的TCP连接,并建立到服务器106的第二传输层连接,客户机102使用该第二传输层连接,例如,在设备200和服务器106终止第二传输层连接。可通过单独的网络堆栈267建立第一和第二传输层连接。在其他实施例中,设备200可包括多个网络堆栈,例如267或267',并且在一个网络堆栈267可建立或终止第一传输层连接,在第二网络堆栈267'上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传输网络分组,并且另一个网络堆栈用于在第二网络上接收和传输网络分组。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分组的缓冲器243,其中网络分组由设备200传输。

[0089] 如图2A所示,内核空间204包括高速缓存管理器232、高速层2-7集成分组引擎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中运行这些部件或进程232、240、234、236和238提高这些部件中的每个单独的和结合的性能。内核操作意味着这些部件或进程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可改进加密性能,从而可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传输的数量。例如,在内核模式获得的数据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，在任何部件或进程 232、240、235、236 和 238 间的同步和通信在内核空间 204 中可被执行的更有效率。

[0090] 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分组的任何部分的访问，例如，包括来自客户机 102 的请求或者来自服务器 106 的响应的网络分组。在一些实施例中，可以由分组引擎 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分组。在其他实施例中，任何部件或进程 232、240、234、236 和 238 可使用内核级数据结构来执行部件或进程的需要的操作。在一个实例中，当使用内核级数据结构时，部件 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，部件 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递到第二内核级数据结构，或任何期望的用户级数据结构。

[0091] 高速缓存管理器 232 可包括软件、硬件或软件和硬件的任意组合，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 提供服务的动态产生的对象。被高速缓存管理器 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，或通过任何协议的通信。在一些实施例中，高速缓存管理器 232 复制存储在其他地方的原始数据或先前计算、产生或传输的数据，其中相对于读高速缓冲存储器元件，需要更长的访问时间以取得、计算或以其他方式得到原始数据。一旦数据被存储在高速缓冲存储器元件中，通过访问高速缓存的副本而不是重新获得或重新计算原始数据而可做出未来的使用，因此而减少了访问时间。在一些实施例中，高速缓存元件可以包括设备 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有比存储器 264 更快的存储时间的存储器。在另一个实施例中，高速缓存元件可以包括诸如硬盘的一部分的设备 200 的任一类型和形式的存储元件。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、存储区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。

[0092] 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，或者从客户机 102 或服务器 106 接收无效命令使对象无效的逻辑或功能。在一些实施例中，高速缓存管理器 232 可作为程序、服务、进程或任务操作执行在内核空间 204 中，并且在其他实施例中，在用户空间 202 中。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 中执行，而第二部分在内核空间 204 中执行。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)，或任何其他类型的集成电路，例如现场可编程门阵列 (FPGA)，可编程逻辑设备 (PLD)，或者专用集成电路 (ASIC)。

[0093] 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 提供配置功能以允许用户识别、指定、定义或配置高速缓存策略。策略引擎 236，在一些实施例中，也访问存储器以支持数据结构，例如备份表或 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，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,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此处进一步描述。

[0094] 在一些实施例中,策略引擎 236 可以提供配置机制以允许用户标识、指定、定义或配置指导包括但不限于图 2B 中描述的诸如 vServers 275、VPN 功能 280、内联网 IP 功能 282、交换功能 284、DNS 功能 286、加速功能 288、应用防火墙功能 290 和监控代理 197 的部件的设备的任意其它部件或功能的行为的策略。在其它实施例中,策略引擎 236 可以响应于任一配置的策略来进行检查、评价、实现或者以其他方式产生作用,并且还可以响应于策略来指导一个或多个设备功能的操作。

[0095] 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 通信的网络分组,或其任何部分。加密引擎 234 也可代表客户机 102a-102n、服务器 106a-106n 或设备 200 来安装或建立 SSL 或 TLS 连接。因此,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机 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。

[0096] 多协议压缩引擎 238 包括用于压缩一个或多个网络分组协议(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 双向压缩在客户机 102a-102n 和服务器 106a-106n 间任一基于 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 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 上语音(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来压缩任何载荷或任何通信,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 欺骗协议。

[0097] 同样的,多协议压缩引擎 238 通过桌面客户机,例如 Microsoft Outlook 和非 web 瘦客户机,诸如由通用企业应用像 Oracle、SAP 和 Siebel 启动的任何客户机,甚至移动客户机,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 的分组处理引擎 240 集成,可以压缩 TCP/IP 协议携带的任何协议,例如任何应用层协议。

[0098] 集成高速层 2-7 的分组引擎 240,通常也称为分组处理引擎,或分组引擎,通过网络端口 266 负责设备 200 接收和发送的分组的内核级处理的管理。集成高速层 2-7 的分组引擎 240 可包括在处理期间用于排队一个或多个网络分组的缓冲器,例如用于网络分组的接收或者网络分组的传输。另外,集成高速层 2-7 的分组引擎 240 通过网络端口 266 与一个或多个网络堆栈 267 通信以发送和接收网络分组。集成高速层 2-7 的分组引擎 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 以执行分组的 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冲重定向, 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。

[0099] 集成高速层 2-7 的分组引擎 240 包括分组处理定时器 242。在一个实施例中, 分组处理定时器 242 提供一个或多个时间间隔以触发输入处理, 例如, 接收或者输出 (即传输) 网络分组。在一些实施例中, 集成高速层 2-7 的分组引擎 240 响应于定时器 242 处理网络分组。分组处理定时器 242 向分组引擎 240 提供任何类型和形式的信号以通知、触发或传输时间相关事件、间隔或发生。在许多实施例中, 分组处理定时器 242 以毫秒级操作, 例如 100ms、50ms、或 25ms。例如, 在一些实例中, 分组处理定时器 242 提供时间间隔或者其它使得由集成高速层 2-7 的分组引擎 240 以 10ms 时间间隔处理网络分组, 而在其它实施例中, 以 5ms 时间间隔, 并且在进一步的实施例中, 短到 3、2 或 1ms 时间间隔。集成高速层 2-7 的分组引擎 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 连接、集成或通信。因此, 响应于分组处理定时器 242 和 / 或分组引擎 240, 可执行加密引擎 234、高速缓存管理器 232、策略引擎 236 以及多协议压缩引擎 238 的任何逻辑、功能或操作。因此, 在由分组处理定时器 242 提供的时间间隔粒度, 可执行加密引擎 234、高速缓存管理器 232、策略引擎 236 以及多协议压缩引擎 238 的任何逻辑、功能或操作, 例如, 时间间隔少于或等于 10ms。例如, 在一个实施例中, 响应于集成高速层 2-7 的分组引擎 240 和 / 或分组处理定时器 242, 高速缓存管理器 232 可执行任何高速缓存的对象的无效。在另一个实施例中, 高速缓存的对象的终止或无效时间被设定为与分组处理定时器 242 的时间间隔相同的粒度级, 例如每 10ms。

[0100] 与内核空间 204 不同, 用户空间 202 是操作系统的存储区域或部分, 被用户模式应用或用户模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 和为了访问内核服务而使用用户服务调用。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 提供方法, 通过该方法系统管理员或其他用户可与设备 200 交互并控制该设备 200 的操作, 例如通过设备 200 的操作系统, 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、图形或通过任意类型的程序或应用的其他形式呈现, 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界面, 例如通过操作系统提供的命令行。例如, CLI 212 可包括壳, 该壳是使用户与操作系统相互作用的工具。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。

[0101] 使用健康监控程序 216 监控、检查、报告并确保网络系统运行正常, 用户正通过网络接收请求的内容。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。在其他实施例中, 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连接: 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, 分组引擎 240, 守护服务 218 以及壳服务 214。因此, 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、服务或任务是否活动并当前正在运行。在另一个实施例中，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 任何部分的任何状况、状态或错误。

[0102] 守护服务 218 是连续运行或在后台运行的程序，并且处理设备 200 接收的周期性服务请求。在一些实施例中，守护服务可向其他程序或进程（例如合适的另一个守护服务 218）转发请求。如本领域技术人员所公知的，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，或者执行任何需要的任务。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。

[0103] 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 提供下列服务、功能或操作中的一个或多个：用于一个或多个客户机 102 以及一个或多个服务器 106 之间的通信的 SSL VPN 连通性 280、交换 / 负载平衡 284、域名服务解析 286、加速 288 和应用防火墙 290。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 275、vS 275、VIP 服务器或者仅是 VIP 275a-275n（此处也称为 vServer 275）。vServer 275 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机 102 和服务器 106 之间的通信。

[0104] vServer 275 可以包括软件、硬件或者软件和硬件的任意组合。vServer 275 可包括在设备 200 中的用户模式 202、内核模式 204 或者其任意组合中运行的任意类型和形式的程序、服务、任务、进程或者可执行指令。vServer 275 包括任意逻辑、功能、规则或者操作，以执行此处所述技术的任意实施例，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 或 vS 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、客户机 102 或者 vServer 275 并与之通信的任意程序、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。

[0105] 在一些实施例中，vS 275 应用策略引擎 236 的一个或者多个策略到客户机 102 和服务器 106 之间的网络通信。在一个实施例中，该策略与 vServer 275 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 200 通信的任意用户或者用户组，其中 n 可以为任意数字或符号。在一些实施例中，策略引擎的策略具有基于通信的任意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、分组中的首部或者字段、或者通信的上下文，诸如用户、用户组、vServer 275、传输层连接、和 / 或客户机 102 或者服务器 106 的标识或者属性。

[0106] 在其他实施例中，设备 200 与策略引擎 236 通信或交互，以便确定远程用户或远程客户机 102 的验证和 / 或授权，以访问来自服务器 106 的计算环境 15、应用和 / 或数据文件。在另一个实施例中，设备 200 与策略引擎 236 通信或交互，以便确定远程用户或远程客

户机 102 的验证和 / 或授权,使得应用传送系统 190 传送一个或多个计算环境 15、应用和 / 或数据文件。在另一个实施例中,设备 200 基于策略引擎 236 对远程用户或远程客户机 103 的验证和 / 或授权建立 VPN 或 SSL VPN 连接。一个实施例中,设备 102 基于策略引擎 236 的策略控制网络业务流量以及通信会话。例如,基于策略引擎 236,设备 200 可控制对计算环境 15、应用或数据文件的访问。

[0107] 在一些实施例中,vServer 275 与客户机 102 经客户机代理 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机 102 的通信。在其它实施例中,vServer 275 与客户机服务器 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 将到客户机 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 的传输层连接池并经由所述池化的传输层连接多路复用客户机的请求。

[0108] 在一些实施例中,设备 200 提供客户机 102 和服务器 106 之间的 SSL VPN 连接 280。例如,第一网络 102 上的客户机 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,客户机 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,客户机代理 120 拦截第一网络 104 上的客户机 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 接收来自客户机代理 102 的所拦截的通信,解密该通信,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 为两个网络 104、104' 之间的客户机 102 提供端到端安全传输层连接。

[0109] 在一个实施例中,设备 200 寄载虚拟专用网络 104 上的客户机 102 的内部网内部互联网协议或者 IntranetIP 282 地址。客户机 102 具有本地网络识别符,诸如第一网络 104 上的互联网协议 (IP) 地址和 / 或主机名称。当经设备 200 连接到第二网络 104' 时,设备 200 为第二网络 104' 上的客户机 102 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。使用为客户机的所建立的 IntranetIP 282,设备 200 在第二或专用网 104' 上监听并接收指向该客户机 102 的任意通信。在一个实施例中,设备 200 用作或者代表第二专用网络 104 上的客户机 102。例如,在另一个实施例中, vServer 275 监听和响应到客户机 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 如同客户机 102 一样来处理该请求。例如,设备 200 可以响应对客户机 IntranetIP 282 的查验。在另一个实施例中,设备可以与请求和客户机 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。

[0110] 在一些实施例中,设备 200 为客户提供机 102 和服务器 106 之间的通信提供下列一个或多个加速技术 288 :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 ;以及 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机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机 102 的传输层连接所带来的许多

处理负载。该技术此处称为“连接池”。

[0111] 在一些实施例中,为了经池化的传输层连接无缝拼接从客户机 102 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,在到来分组(即,自客户机 102 接收的分组)的情况下,所述分组的源网络地址被改变为设备 200 的输出端口的网络地址,而目的网络地址被改为目的服务器的网络地址。在发出分组(即,自服务器 106 接收的一个分组)的情况下,源网络地址被从服务器 106 的网络地址改变为设备 200 的输出端口的网络地址,而目的地址被从设备 200 的地址改变为请求的客户机 102 的地址。分组的序列号和确认号也被翻译为到客户机 102 的设备 200 的传输层连接上的客户机 102 所期待的序列号和确认。在一些实施例中,传输层协议的分组校验和被重新计算以考虑这些翻译。

[0112] 在另一个实施例中,设备 200 为客户机 102 和服务器 106 之间的通信提供交换或负载平衡功能 284。在一些实施例中,设备 200 根据层 4 或应用层请求数据来分配业务量并将客户机请求指向服务器 106。在一个实施例中,尽管网络层或者网络分组的层 2 识别目的服务器 106,但设备 200 确定服务器 106,从而利用承载为传输层分组的有效载荷的应用信息和数据来分发网络分组。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机请求到哪个服务器 106。在一些实施例中,如果设备 200 探测到某个服务器 106 不可用或者具有超过预定阈值的负载,设备 200 可以将客户机请求指向或者分发到另一个服务器 106。

[0113] 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为来自客户机 102 的 DNS 请求提供解析。在一些实施例中,设备拦截由客户机 102 发送的 DNS 请求。在一个实施例中,设备 200 以设备 200 的 IP 地址或其所寄载的 IP 地址来响应客户机的 DNS 请求。在此实施例中,客户机 102 把给域名的网络通信发送到设备 200。在另一个实施例中,设备 200 以第二设备 200' 的或其所寄载的 IP 地址来响应客户机的 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 地址来响应客户机的 DNS 请求。

[0114] 在又一个实施例中,设备 200 为客户机 102 和服务器 106 之间的通信提供应用防火墙功能 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 包括用于提供对多个种类和类型的基于 web 或因特网的脆弱点的保护的一个或多个应用防火墙或安全控制策略,例如下列的一个或多个脆弱点 :1) 缓冲区泄出,2) CGI-BIN 参数操纵,3) 表单 / 隐藏字段操纵,4) 强制浏览,5) cookie 或会话中毒,6) 被破坏的访问控制列表 (ACLs) 或弱密码,7) 跨站脚本处理 (XSS),8) 命令注入,9) SQL 注入,10) 错误触发敏感信息泄露,11) 对加密的不安全使用,12) 服务器错误配置,13) 后门和调试选项,14) 网站涂改,15) 平台或操作系统弱点,和 16) 零天攻击。在一个实施例中,对下列情况的一种或多种,应用防火墙 290 以检查或分析网络通信的形式来提供 HTML 格式字段的保护 :1) 返回所需的字段,2) 不允许附加字段,3) 只读和隐藏字段强制,4) 下拉列表和单选按钮字段的一致,以及 5) 格式字段最大长度强制。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。

[0115] 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意机密信息。应用防火墙 290 可以根据引擎 236 的规则或策略来检查或分析任一网络通信以识别在网络分组的任一字段中的任一机密信息。在一些实施例中，应用防火墙 290 在网络通信中识别信用卡号、口令、社会保险号、姓名、病人代码、联系信息和年龄的一次或多次出现。网络通信的编码部分可以包括这些出现或机密信息。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，诸如阻止发送网络通信。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。

[0116] 仍然参考图 2B，设备 200 可以包括如上面结合图 1D 所讨论的性能监控代理 197。在一个实施例中，设备 200 从如图 1D 中所描述的监控服务 1908 或监控服务器 106 中接收监控代理 197。在一些实施例中，设备 200 在诸如磁盘的存储装置中保存监控代理 197，以用于递送给与设备 200 通信的任意客户机或服务器。例如，在一个实施例中，设备 200 在接收到建立传输层连接的请求时发送监控代理 197 给客户机。在其它实施例中，设备 200 在建立与客户机 102 的传输层连接时发送监控代理 197。在另一个实施例中，设备 200 在拦截或检测对 web 页面的请求时发送监控代理 197 给客户机。在又一个实施例中，设备 200 响应于监控服务器 198 的请求来发送监控代理 197 到客户机或服务器。在一个实施例中，设备 200 发送监控代理 197 到第二设备 200' 或设备 205。

[0117] 在其它实施例中，设备 200 执行监控代理 197。在一个实施例中，监控代理 197 测量和监控在设备 200 上执行的任意应用、程序、进程、服务、任务或线程的性能。例如，监控代理 197 可以监控和测量 vServers 275A-275N 的性能与操作。在另一个实施例中，监控代理 197 测量和监控设备 200 的任意传输层连接的性能。在一些实施例中，监控代理 197 测量和监控通过设备 200 的任意用户会话的性能。在一个实施例中，监控代理 197 测量和监控通过设备 200 的诸如 SSL VPN 会话的任意虚拟专用网连接和 / 或会话的性能。在进一步的实施例中，监控代理 197 测量和监控设备 200 的内存、CPU 和磁盘使用以及性能。在又一个实施例中，监控代理 197 测量和监控诸如 SSL 卸载、连接池和多路复用、高速缓存以及压缩的由设备 200 执行的任意加速技术 288 的性能。在一些实施例中，监控代理 197 测量和监控由设备 200 执行的任一负载平衡和 / 或内容交换 284 的性能。在其它实施例中，监控代理 197 测量和监控由设备 200 执行的应用防火墙 290 保护和处理的性能。

[0118] C、客户机代理

[0119] 现在看图 3，描述客户机代理 120 的实施例。客户机 102 包括客户机代理 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，客户机 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。客户机 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 / 或执行客户机代理 120，或其中任意部分。客户机代理 120 包括拦截机制或者拦截器 350，用于从网络堆栈 310 拦截来自一个或者多个应用的网络通信。

[0120] 客户机 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。这样, 网络堆栈 310 可包括用于任何以下 OSI 模型层的任何类型和形式的协议 :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 可包括在因特网协议 (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, 可在以太网协议上实施 TCP/IP 协议, 以太网协议可包括 IEEE 广域网 (WAN) 或局域网 (LAN) 协议的任何族, 例如被 IEEE802.3 覆盖的这些协议。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 / 或移动因特网协议。

[0121] 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) (email)、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。在其他实施例中, 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。

[0122] 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。网络层驱动器可被包括作为计算设备 100 的操作系统的一部分或者计算设备 100 的任何网络接口卡或其它网络访问部件的一部分。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 由客户机 102 的操作系统安装或以其它方式提供。

[0123] 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机 102 的网络通信的任何信息和数据。在一个实施例中, 与网络堆栈 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, 数据结构可以包括与网络分组相关的信息和数据或者一个或多个网络分组。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分组的一部分, 例如传输层的网络分组。在一些实施例中, 数据结构 325 包括内核级别数据结构, 而在其它实施例中, 数据结构 325 包括用户模式数据结构。内核级数据结构可以包括获得的或与在内核模式 302 中操作的网络堆栈 310 的一部分相关的数据结构、或者运行在内核模式 302 中的网络驱动程序或其它软件、或者由运行或操作在操作系统的内核模式的服务、进程、任务、线程或其它可执行指令获得或收到的任意数据结构。

[0124] 此外, 网络堆栈 310 的一些部分可在内核模式 302 执行或操作, 例如, 数据链路或网络层, 而其他部分在用户模式 303 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 可以给应用提供对网络堆栈 310 的用户模式访问, 而网络堆栈 310 的第二部分 310a 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 的任意层。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 的任意层。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,位于任意一个或多个网络层,处于用户模式 203、内核模式 202,或其组合,或在网络层的任何部分或者到网络层的接口点,或用户模式 203 和内核模式 202 的任何部分或到用户模式 203 和内核模式 202 的接口点。

[0125] 拦截器 350 可以包括软件、硬件、或者软件和硬件的任意组合。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 或者客户机代理 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,客户机代理 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、或者连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 连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意层的另一个协议层,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微端口驱动器。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,客户机代理 120 在用户模式 203 操作,但通过拦截器 350 连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。

[0126] 在一个实施例中,拦截器 350 拦截任意的传输层连接请求。在这些实施例中,拦截器 350 执行传输层应用编程接口 (API) 调用以设置目的地信息,诸如到期望位置的目的地 IP 地址和 / 或端口用于定位。以此方式,拦截器 350 拦截并重定向传输层连接到由拦截器 350 或客户机代理 120 控制或管理的 IP 地址和端口。在一个实施例中,拦截器 350 把连接的目的地信息设置为客户机代理 120 监听的客户机 102 的本地 IP 地址和端口。例如,客户机代理 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,客户机代理 120 随后将重定向的传输层通信传送到设备 200。

[0127] 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,客户机代理 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 以进行 DNS 解析。在一个实施例中,设备 200 解析 DNS 请求并且将 DNS 响应传送到客户机代理 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。

[0128] 在又一个实施例中,客户机代理 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' 连接或者将所拦截的通信传送到第二代理 120'。

[0129] 客户机代理 120 和 / 或拦截器 350 可以以对网络堆栈 310 的任意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意协议层和诸如会话、表示或应用层协议的传输层之上的任意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。这样，客户机代理 120 和 / 或拦截器 350 可以与传输层连接以安全、优化、加速、路由或者负载平衡经由传输层承载的任一协议提供的任一通信，诸如 TCP/IP 上的任一应用层协议。

[0130] 此外，客户机代理 120 和 / 或拦截器可以以对任意应用、客户机 102 的用户和与客户机 102 通信的诸如服务器的任意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。客户机代理 120 和 / 或拦截器 350 可以以无需修改应用的方式被安装和 / 或执行在客户机 102 上。在一些实施例中，客户机 102 的用户或者与客户机 102 通信的计算装置未意识到客户机代理 120 和 / 或拦截器 350 的存在、执行或者操作。同样，在一些实施例中，相对于应用、客户机 102 的用户、诸如服务器的另一个计算装置、或者在由拦截器 350 连接的协议层之上和 / 或之下的任意协议层透明地来安装、执行和 / 或操作客户机代理 120 和 / 或拦截器 350。

[0131] 客户机代理 120 包括加速程序 302、流客户机 306、收集代理 304 和 / 或监控代理 197。在一个实施例中，客户机代理 120 包括由 Florida, Fort Lauderdale 的 Citrix Systems Inc. 开发的独立计算架构 (ICA) 客户机或其任一部分，并且也指 ICA 客户机。在一些实施例中，客户机代理 120 包括应用流客户机 306，用于从服务器 106 流式传输应用到客户机 102。在一些实施例中，客户机代理 120 包括加速程序 302，用于加速客户机 102 和服务器 106 之间的通信。在另一个实施例中，客户机代理 120 包括收集代理 304，用于执行端点检测 / 扫描并且用于为设备 200 和 / 或服务器 106 收集端点信息。

[0132] 在一些实施例中，加速程序 302 包括用于执行一个或多个加速技术的客户机侧加速程序，以加速、增强或者以其他方式改善客户机与服务器 106 的通信和 / 或对服务器 106 的访问，诸如访问由服务器 106 提供的应用。加速程序 302 的可执行指令的逻辑、函数和 / 或操作可以执行一个或多个下列加速技术：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 可执行由客户机 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 可以对作为传输层协议的网络分组的有效载荷所承载的任一协议或者多协议执行压缩。

[0133] 流客户机 306 包括用于接收和执行从服务器 106 所流式传输的应用、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机 306，用于播放、执行或者以其它方式引起客户机 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机 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机 102。在另一个实施例中，客户机 102 解压缩、解包或者解档应用文件。流客户机 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，流客户机 306 可以为可

执行程序。在一些实施例中，流客户机 306 可以能够启动另一个可执行程序。

[0134] 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 / 或收集关于客户机 102 的信息。在一些实施例中，设备 200 发送收集代理 304 到客户机 102 或者客户机代理 120。可以根据设备的策略引擎 236 的一个或多个策略来配置收集代理 304。在其它实施例中，收集代理 304 发送收集的客户机 102 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机到网络 104 的连接的访问、验证和授权控制。

[0135] 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机的一个或者多个属性或者特征。例如，收集代理 304 可以识别和确定任意一个或多个以下的客户机侧属性：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 还可以识别并确定客户机上任意一个或多个以下软件的存在或版本：1) 防病毒软件；2) 个人防火墙软件；3) 防垃圾邮件软件，和 4) 互联网安全软件。策略引擎 236 可以具有根据客户机或客户机侧属性的任意一个或多个属性或特性的一个或多个策略。

[0136] 在一些实施例中，客户机代理 120 包括如结合图 1D 和 2B 所讨论的监控代理 197。监控代理 197 可以是诸如 Visual Basic 或 Java 脚本的任意类型和形式的脚本。在一个实施例中，监控代理 129 监控和测量客户机代理 120 的任意部分的性能。例如，在一些实施例中，监控代理 129 监控和测量加速程序 302 的性能。在另一个实施例中，监控代理 129 监控和测量流客户机 306 的性能。在其它实施例中，监控代理 129 监控和测量收集代理 304 的性能。在又一个实施例中，监控代理 129 监控和测量拦截器 350 的性能。在一些实施例中，监控代理 129 监控和测量客户机 102 的诸如存储器、CPU 和磁盘的任意资源。

[0137] 监控代理 197 可以监控和测量客户机的任意应用的性能。在一个实施例中，监控代理 129 监控和测量客户机 102 上的浏览器的性能。在一些实施例中，监控代理 197 监控和测量经由客户机代理 120 递送的任意应用的性能。在其它实施例中，监控代理 197 测量和监控诸如基于 web 或 HTTP 响应时间的应用的最终用户响应时间。监控代理 197 可以监控和测量 ICA 或 RDP 客户机的性能。在另一个实施例中，监控代理 197 测量和监控用户会话或应用会话的指标。在一些实施例中，监控代理 197 测量和监控 ICA 或 RDP 会话。在一个实施例中，监控代理 197 测量和监控设备 200 在加速递送应用和 / 或数据到客户机 102 的过程中的性能。

[0138] 在一些实施例中，仍旧参见图 3，第一程序 322 可以用于自动地、静默地、透明地或者以其它方式安装和 / 或执行客户机代理 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，第一程序包括由 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机代理 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、或接收客户机代理 120。在另一个实施例中，第一程序 322 是用于在客户机 102 的操作系统上安装如网络驱动的程序的安装程序或即插即用管理器。

[0139] D. 使用由用户从设备确定的指标选择的指标和 / 或经由网络管理协议从装置收

集的指标执行负载平衡

[0140] 现在参看图 4, 描述用于负载平衡的系统的多个实施例的各个特征。可基于由设备 200 确定的指标和 / 或由设备经由诸如简单网络管理协议 (SNMP) 的网络管理协议从装置或者服务收集的指标进行负载平衡。该设备提供负载监控器来监控一个或者多个服务 270A-270N 的负载。在一个实施例中, 用户可以基于从自定义指标表选择的指标来配置一个或者多个负载监控器, 该自定义指标表包括经由网络管理协议查询获得的指标或者对象。在另一个实施例中, 用户可以基于由设备收集的指标或者参数来配置一个或者多个负载监控器。在一些实施例中, 用户基于从自定义指标表选择的指标和设备收集的指标来配置一个或者多个负载监控器。响应于用户的选择, 设备确定一个或者多个服务的负载并且使用任一类型的负载平衡技术来负载平衡客户机请求到服务。

[0141] 进一步参考图 4, 描述用于负载平衡一个或者多个服务的设备的实施例。总的来说, 设备 200 具有一个或者多个虚拟服务器, 也称之为 vServer, 其配置用于为布置在一个或者多个服务器 106a-106b 上的或者由一个或者多个服务器 106a-106b 提供的一个或者多个服务 270a-270n 提供负载平衡 284。vServer 275A 和服务 270A 或者一组服务 270A-270N 相关联, 被配置为服务 270A 或者一组服务 270A-270N 或者受其限制。设备 200 具有一个或者多个负载监控器 405A-405N 来监控服务 270A-270N 的状态、操作和 / 或性能。负载监控器和服务 270A 或者一组服务 270A-270N 相关联, 被配置为服务 270A 或者一组服务 270A-270N 或者受其限制。负载监控器 405A-405B 为 vServer 275A-275N 提供信息来确定服务 270A-270N 中的哪一个应该接收由 vServer 275 接收的请求。负载监控器 405 和 / 或 vServer 275 可以使用设备收集的指标 410 和 / 或装置提供的指标 420 来确定跨越多个服务 270A-270N 的负载并且来负载平衡输入的客户机请求。设备 200 还包括配置接口 435 来接收识别由负载监控器 405 和 / 或 vServer 275 所使用的用户选择的或者用户限定的指标 430 的信息用于负载平衡多个服务 270A-270N。

[0142] 设备 200 可以包括任一类型和形式的负载监控器 405A-405N, 还可以称之为监控代理, 用于监控服务 270、服务器 106 或者装置 100 的任一操作或者性能特征或者指标。负载监控器 405 可以包括软件、硬件或者软件和硬件的任一组合。负载监控器 405 可以包括任一应用、程序、脚本、服务、守护进程、过程、任务、线程或者可执行指令集。在一个实施例中, 负载监控器 405 在设备 200 的内核空间中操作或者执行。在另一个实施例中, 负载监控器 405 在设备 200 的用户或者应用空间中操作或者执行。在一些实施例中, 负载监控器 405 的第一部分在内核空间中操作而负载监控器 405 的第二部分在设备 200 的应用层或者空间操作。

[0143] 在一个实施例中, 负载监控器 405 和服务 270 通信一次。在一些实施例中, 负载监控器 405 以诸如每一毫秒或者每一秒的预定频率监控服务 270 或者与之通信。用户可以经由配置接口 425 配置或者指定预定的频率。在其他情况中, 另一个设备或者系统可以经由配置接口 425 来配置或者指定预定的频率。在又一个实施例中, 负载监控器 405 响应于诸如接收请求、响应或者网络分组的一个或者多个事件来监控服务 270 或者与之通信。在一个实施例中, 负载监控器 405 响应于策略引擎的一个或者多个策略来监控服务 270 或者与之通信。

[0144] 在一些实施例中, 负载监控器 405 可以与服务 270 或者服务器 106 使用请求 / 应

答消息机制或者协议。在其他实施例中，负载监控器 405 可以具有自定义或者专用交换协议用于和服务、服务器或者装置通信。在一个实施例中，负载监控器 405 可以使用服务 270 的协议来监控服务 270 或者与之通信。由此，在一些实施例中，负载监控器 405 使用 HTTP 协议来监控 web 服务 270A 或者与之通信，或者使用 FTP 协议用于 FTP 服务器 270B。在又一些实施例中，负载监控器 405 使用 TCP 或者 ICMP 协议用于监控服务 270。在一些实施例中，负载监控器 405 使用网络管理协议来监控或者查询服务、服务器或者装置的状态或者指标。在一个实施例中，负载监控器 405 使用简单网络管理协议 (SNMP)。在另一个实施例中，负载监控器 405 使用通用管理信息协议 (CIMP)。

[0145] 在一些实施例中，单个负载监控器 405 监控多个服务 270A-270N 或者服务器 106A-106B。在其他实施例中，多个负载监控器 405A-405N 监控单个服务 270A 或者服务器 106A。在又一些实施例中，多个负载监控器 405 可以每一个监控多个服务 270A-270N 或者服务器 106A-106N。在一个实施例中，多个负载监控器 405 可以每一个监控服务 270。在又一个实施例中，负载监控器 405A 可以监控一个或者多个其它负载监控器 405B-405N。

[0146] 在一些实施例中，一个或者多个负载监控器 405 和一个或者多个服务 270 相关联。在一个实施例中，用户经由配置接口 425 来指定或者配置负载监控器 405 用于一个或者多个服务 270。例如，用户经由配置接口 435 可以发布命令来绑定监控器 405 到服务 270。在其他实施例中，负载监控器 405 和 vServer 275 相关联（也称为 vS 275）。在一个实施例中，用户经由配置接口 425 指定或者配置负载监控器 405 用于 vServer 275。在又一个实施例中，用户经由配置接口 425 指定或者配置 vServer 275 用于一个或者多个服务 270A-270N。例如，用户可以将 vServer 275 绑定到服务 270。

[0147] 在一些实施例中，一个或者多个负载监控器 405 可以监控设备 200、vServer 275、网络服务 270、客户机 102、服务器 106、装置 100 或者任意其它网络资源。在一个实施例中，用户指定一类网络服务来与一个或者多个监控代理 405 相关联。在另一个实施例中，用户定制监控代理。例如，用户可以实现或者以其他方式提供脚本用于监控服务。在又一个实施例中，使用通用监控代理 405。在一些实施例中，监控器代理 405 可配置地基于一类协议或者一类服务来使用预定的监控器、脚本或者状态消息。

[0148] 在又一个实施例中，一个或者多个监控代理 405 确定一个或者多个网络服务 270 的响应时间，用于响应以下类型的其中一个的请求：查验、传输控制协议 (tcp)、tcp 扩展内容验证、超文本传输协议 (http)、http 扩展内容验证、超文本传输协议安全 (https)、https 扩展内容验证、用户数据报协议、域名服务以及文件传输协议。在一些实施例中，监控代理 405 响应于服务 270 检查预定的状态码。在其他实施例中，监控代理 405 响应于服务 270 检查预定的串模式。

[0149] 在一些实施例中，一个或者多个负载监控器或者监控代理 405 是协议专用的代理。例如，代理 405 可以确定用于特定协议类型的网络服务的可用性。在一些实施例中，监控代理 405 确定对于 TCP 请求的服务器 106 或者网络服务 270 的响应时间。在其中一个这样的实施例中，代理使用“TCP/ICMP 回应请求”命令来发送数据报到网络服务 270，相应地接收来自网络服务 270 的数据报，并且基于数据报的往返时间确定响应时间。在另一个这样的实施例中，监控代理 405 验证来自网络服务 270 的响应包括期望内容。在一个实施例中，监控代理 405 验证响应不包括错误。

[0150] 在其他实施例中，监控代理 405 确定网络服务 270 对于 UDP 请求的可用性。在其中一个这样的实施例中，代理使用“UDP 回应”命令来发送数据报到网络服务 270，相应地接收来自网络服务 270 的数据报，并且基于数据报的往返时间确定响应时间。在另一个这样的实施例中，监控代理 405 验证来自网络服务 270 的响应包括期望内容并且不包括错误。

[0151] 在又一些实施例中，监控代理 405 确定网络服务 270 对于 FTP 请求的可用性。在其中一个这样的实施例中，监控代理 405 发送诸如“get”命令或者“put”命令的 FTP 命令到网络服务 270 并且确定网络服务 270 响应该命令所需要的时间。在另一个这样的实施例中，监控代理 405 验证来自网络服务 270 的响应包括所期望的内容，诸如“get”命令所请求的文件的内容，并且不包含错误。

[0152] 在又一些实施例中，监控代理 405 确定网络服务 270 对于 HTTP 请求的可用性。在其中一个这样的实施例中，监控代理 405 发送诸如用于统一资源定位符 (URL) 或者文件的“get”请求的 HTTP 命令到网络服务 270 并且确定网络服务 270 响应该请求所需要的时间。在另一个这样的实施例中，监控代理 405 验证来自网络服务 270 的响应包括所期望的内容，诸如 URL 识别的 web 页面的内容。在一些实施例中，监控代理 405 检查预定的状态码。在其他实施例中，监控代理 405 检查 HTTP 响应中的预定的串模式。

[0153] 在进一步的实施例中，监控代理 405 确定网络服务 270 对于 DNS 请求的可用性。在其中一个这样的实施例中，监控代理 405 发送诸如对于已知网络地址的 dnsquery 或者 nslookup 的 DNS 请求到服务器 106 或者网络服务 270，并且确定服务器 106 或者网络服务 270 响应该请求所需要的时间。在另一个这样的实施例中，监控代理 405 验证来自网络服务 270 的响应包括所期望的内容，诸如和已知网络地址相关联的计算装置 100 的域名。在一个实施例中，监控代理 405 验证响应不包含错误。

[0154] 在一些实施例中，设备 200 经由监控代理 405 基于通过设备的网络话务量和信息识别并且收集指标 410，或者称之为设备收集的参数或者指标。设备 200 或者代理 405 可以以任一类型或者形式的数据存储机制将设备收集的指标 410 保存在存储器和 / 或磁盘存储装置中。在一个实施例中，设备将指标 410 保存在表中。在另一个实施例中，设备将指标 410 保存在数据库中。在又一个实施例中，设备将指标 410 保存在对象或者数据结构中。仍然在其它实施例中，设备 200 在多个表中和 / 或数据存储机制中保存设备收集的指标 410。在一个实施例中，设备收集的指标 410 可以以任一方式布置在或者组织在多个表中。

[0155] 在一些实施例中，监控代理 405 从由设备所接收和发送的网络分组确定一个或者多个指标 410。在一个实施例中，监控代理 405 确定与一个或者多个服务 270 或者服务器 106 的连接的数量和类型。在另一个实施例中，监控代理 405 确定发送到服务 270 或者服务器 106 的分组的数量。在其他实施例中，监控代理 405 确定从服务 270 或者服务器 106 接收的或者由服务 270 或者服务器 106 发送的分组的数量。在一些实施例中，监控代理 405 确定来自服务 270 或者服务的响应时间。在一个实施例中，监控代理 405 确定平均响应时间。在另一个实施例中，监控代理 405 确定丢失分组的数量或百分比。在其他实施例中，监控代理 405 确定从服务或者服务器接收的错误的数量。

[0156] 在一些实施例中，监控代理 405 确定到服务 270 或者服务器 106 的连接的带宽。在一个实施例中，监控代理 405 基于响应时间和 / 或分组丢失来确定连接的带宽。在另一个实施例中，监控代理 405 基于从服务 270 或者服务器 106 发送或者通信的和 / 或发送或者

通信到其的多个字节来确定连接的带宽。在一个实施例中，监控代理 405 基于通过诸如每秒的预定时间周期上从服务或者服务器接收的字节数量来确定带宽。在另一个实施例中，监控代理 405 基于在预定时间周期发送到服务或者服务器的字节数量来确定带宽。在一些实施例中，监控代理 405 基于在预定时间周期发送到服务或者服务器或者从其接收的字节数量来确定带宽。

[0157] 在一些实施例中，设备 200 经由监控代理 405 识别和收集服务、服务器或者装置提供的指标 430。这些指标 430 也可以称为自定义指标或者自定义指标表。设备 200 或者代理 405 可以以任意类型和形式的数据存储机制将服务或者装置收集的指标 430 保存在存储器和 / 或磁盘存储装置中。在一个实施例中，设备将指标 430 保存在表中。在另一个实施例中，设备将指标 430 保存在数据库中。在又一个实施例中，设备将指标 430 保存在对象或者数据结构中。在一些实施例中，设备将指标 430 以与设备收集的指标 410 相同的数据存储机制保存。在其他实施例中，设备将指标 430 以与设备收集的指标 410 不同的数据存储机制保存。仍然在其它实施例中，设备 200 以多个表和 / 或数据存储机制保存装置提供的指标 420。在一个实施例中，装置收集的指标 420 可以以任一方式布置在或者组织在多个表中。例如，设备 200 可以有每一个服务、装置或者应用的指标表 420。

[0158] 在一个实施例中，负载监控器 405 使用诸如 SNMP 的网络管理协议来向服务器或者装置查询一个或者多个对象标识符和用于对象标识符的对象的数据。仅通过示例并且不以任一方式限制，负载监控器 405 使用 SNMP 架构来提供管理信息库 (MIB) 417，其对于所管理的对象使用包含对象标识符 422A-422N 的分层命名空间来指定诸如服务 270 的装置或者装置子系统的管理数据。在一些实施例中，MIB 417 是分层组织的信息的集合。MIB 417 可以使用诸如 SNMP 的网络管理协议来访问。MIB 417 包括由对象标识符 422A-422N 识别的所管理的对象。在一个实施例中，所管理的对象（有时称为 MIB 对象、对象或者 MIB）是所管理的装置、设备或者系统的任意个特征或者指标的其中一个。在一些实施例中所管理的对象包括一个或者多个对象实例，其对应于或者称为变量。

[0159] 在一个实施例中，MIB 417 分层可以被描述为具有无名根的树，其每一层级由不同的组织分配。在一些实施例中，顶层级 MIB 对象 ID 可以属于不同标准的组织，而较低层级对象 ID 由相关的组织分配。MIB 417 和 / 或对象 422A-422N 可以被布置、构建和组织用于跨越 OSI 参考模型的任意层的管理。在一些实施例中，MIB 417 和 / 或对象 422A-422N 在诸如数据库、电子邮件和 web 服务的应用上提供所管理的数据和信息。此外，MIB 417 和 / 或对象 422A-422N 可以限定任意区域专用或者设备指定信息和操作，诸如对于由设备 200 负载平衡的或者管理的任意类型的服务 270、服务器 106 或者装置 100。

[0160] 在 SNMP 的示例实施例中，SNMP 通信模型基于具有管理信息 417 和管理对象 422A-422N 的数据的管理器 415 和代理 416。在一个实施例中，管理器 415 提供设备和所管理的系统之间的接口。代理 416 提供管理器 415 和所管理的装置、系统、应用、部件、元件或者资源之间的接口。如图 4 中所示，设备 200 可以包括管理器 415，该管理器从诸如服务器 106 上的代理 416 请求和获取来自代理 416 的对象标识符和值。在 SNMP 的例子中，管理器 415 传达 GET 或者 GET-NEXT 消息来请求指定对象的信息。代理 416 响应于管理器的请求，发出具有所请求的信息或者错误消息的 GET-RESPONSE 消息到管理器 415。管理器 415 可以发送 SET 消息来请求对指定变量或者对象 422 的值的改变。代理 416 可以发出 TRAP 消息

来通知事件的管理器 415, 诸如服务 270 上的警告或者错误。

[0161] 尽管总的在 SNMP 网络管理协议的实施例中进行了描述, 但设备 200 和 / 或负载监控器 405 可使用任意类型和形式的网络管理协议和通信模型来从对于所管理的系统、子系统或者服务 270 的另一个装置获取信息的标识符和值, 诸如对象或者变量。例如, 设备 200 可以使用任意一个以下协议和 / 或通信模型: 远程监控 (RMON)、AgentX、简单网关监控协议 (SGMP)、公共管理信息协议 (CMIP)、公共管理信息服务 (CMIS) 或者 TCP/IP 上 CMIP (CMOT)。

[0162] 此外, 尽管 MIB 417 总的参考诸如 SNMP 的示例网络管理协议的管理器 / 代理通信模型来描述, 但是 MIB 417 可以包括对象标识符、变量、参数或者指标的其他标识符的任意类型和形式的数据存储装置。MIB 417 可以是依赖协议或者独立协议。例如, MIB 417 可以包括用于可以经由任意类型和形式的 API 查询的装置或者服务的指标的表。

[0163] 经由网络管理协议提供的所管理的对象或者变量可以提供由设备用于负载平衡或者设备 200 的任意其它功能所使用的服务、服务器或者装置的任意类型和形式的指标或者操作特征。在一个实施例中, 装置提供的指标 420 可以包括如上描述设备所收集的任一指标 410。在另一个实施例中, 装置提供的指标 420 可以包括所管理的装置、服务或者系统的任一资源使用的任一类型和形式的信息。在一个实施例中, 指标 410 包括装置和 / 或服务 270 的 CPU、存储器和 / 或磁盘使用。在其他实施例中, 指标 420 可以包括服务 270 的连接、会话或者客户机的数量的信息。在一些实施例中, 指标 420 包括服务 270 或者服务器 106 的任意阈值的任意信息, 诸如识别最大数量的会话或者客户机的阈值。在又一个实施例中, 指标 420 包括服务 270 的一类协议的任一信息。在其他实施例中, 指标 420 包括服务 270 的任意警告或者错误的任一信息。

[0164] 在一些实施例中, 每一个负载监控器 405 包括设备收集的指标 410。例如, 指标表 410 可以被明确地默认绑定到每一个监控器 405。在其他实施例中, 用户将自定义指标表 420 关联或者绑定到监控器 405。在又一个实施例中, 用户将自定义指标表 420 和设备收集的表 410 关联或者绑定到监控器 405。在又一些实施例中, 用户可以将一个或者多个设备收集的指标表 410 和自定义指标表 420 的任一组合关联或者绑定到一个或者多个负载监控器 405。

[0165] 在一些实施例中, 用户经由配置接口 425 可以对于负载监控器 405 配置或者指定一个或者多个对象标识符 422A-422N 来获取用于并保存在指标 420 中的值。例如, 用户可以指定用户限定的指标 430。在其他实施例中, 设备 200 或者负载监控器 405 从诸如服务器 106 或者服务 270 的装置 100 获得一个或者多个对象标识符 422A-422N 的列表。在又一个实施例中, 设备 200 包括具有已知装置的预定的 OIDS 422A-422N 的一个或者多个指标表 420。例如, 设备 200 可以包括用于任意一个或者多个以下设备或者装置的指标表 420: 1) Florida ft. Lauderdale 的 Citrix Systems 公司出品的任意版本的 NatScaler 装置; 2) 诸如由 Washington Seattle 的 F5 Networks 公司出品的 BIGIP 或者 WebAccelerator 的任一设备; 3) New Jersey Mahwah 的 Radware 公司出品的任意的 AppDirector 或者 AppXcel 装置; 4) California San Jose 的 Cisco Systems 公司出品的和任意应用加速和 / 或安全相关的设备和 / 或软件。

[0166] 设备 200、vServer 275 和 / 或负载监控器 405 基于来自设备收集的指标 410 和 / 或装置提供的指标 420 的任意一个指标来估计、计算或者以其他方式确定对于每个

服务 270 的负载 440。设备 200 对于负载 440 的确定中使用的每一个指标可以使用权重 435A-435N 和阈值 437A-437N。在一个实施例中，设备 200 建立权重 435 和 / 或阈值 437。在其他实施例中，用户建立权重 435 和 / 或阈值 437。例如，在一些情况下，若用户未指定对于多个指标的权重，则设备同等地为每个指标加权。在一个示例实施例中，设备 200 如下确定对于每一个服务的负载 440：

[0167] $\text{Sum}(\text{指标权重} / \text{所建立的指标上限值}) * (\text{所获得的指标值} / \text{所建立的指标上限值}) / \text{Sum}(\text{权重})$

[0168] 在一些实施例中，指标值可以基于 0-100 的范围，或者绝对范围。在其他实施例中，指标值可以不基于 0-100 的范围或者以其他方式与指标的类型和值的可能范围相关。例如，识别连接数量的指标可以具有 10000 的上限或者预定的最大值。在其中一个这样的实施例中，设备建立对于指标值的上限值或者预定上限。在另一个这样的实施例中，用户经由配置接口 425 建立对于指标值的上限值或者预定的上限。在进一步的实施例中，所建立的上限值可以包括低于指标的实际最大值或者范围值的上限的值。例如，用户可以基于指标的期望的操作或者性能范围来指定或者配置相对的范围值。

[0169] 在一些实施例中，如果服务的指标超过用户或者设备提供的阈值，则服务可以从负载确定或者以其他方式从负载平衡决策中排除。在其他实施例中，如果服务的所有指标超过它们对应的阈值，则服务可以从负载确定或者以其他方式从负载平衡决策中排除。在又一个实施例中，即便当服务超过一个或者多个指标的阈值时，在负载确定中或者负载选择时仍可以考虑该服务。在一些情况下，客户机会话可以被识别为对于 vServer 275 或者服务 270 是持续或者稳定的。在这些情况下，如果设备接收到客户机会话的请求，尽管 vServer 或者服务的指标已经超过，设备还可以提供该请求给 vServer 275 或者服务 270。

[0170] 其他实施例中，如果服务或者虚拟服务器的指标的阈值已经超过，则设备可以响应于所超过的阈值将作出请求的客户机重定向到另一个资源。在一个实施例中，设备可以将包含服务器 106 或者服务 270 的地址的 URL 发送到客户机，使得客户机可以绕过该设备 200 并直接访问服务器 106 或者服务 270。在一个实施例中，设备可以发送包含第二设备 200 或者另一个装置的地址的 URL 到客户机。仍在另一个实施例中，设备 200 可以代表客户机将客户机请求重定向到第二设备、装置、服务或者服务器。

[0171] 在一些实施例中，如果服务或者虚拟服务器的指标的阈值已经超过，则设备可以响应于所超过的阈值将客户机请求引导到第二虚拟服务器或者服务。在一个实施例中，第二虚拟服务器可以是主虚拟服务器的备份。当检测到超过阈值时，设备可以泄出请求和连接到第二虚拟服务器。

[0172] 尽管负载 440 总的考虑到上述公式进行讨论，但是设备可以使用任意类型和形式的负载计算、加权或者不加权。在一些实施例中，设备 200 使用指标值的平均值确定负载。在其他实施例中，设备 200 使用指标的派生值来确定负载 440。在另一个实施例中，设备 200 使用指标的任意统计测量来确定负载 440。仍在另一个实施例中，设备 200 使用指标的任意函数或者计算来确定负载 440。在又一些实施例中，设备 200 可以针对每个指标确定负载 440。在这些实施例中，设备 200 可以基于指标对服务负载的贡献的任意类型和形式的集合来聚集、比较或者其他方式计算负载 440。

[0173] 在一些实施例中，用户配置用于服务 270 的多个监控器 405。在这些实施例中，服

务 270 上的负载 440 是所有监控器的负载的和。在一个实施例中，多个监控器 440 的负载的和被加权。设备可以为监控器 405 分配权重。权重可以包括整数、小数或者任意其它数字指示。在一些实施例中，用户可以经由配置接口 425 配置对应于监控器 405 的权重。在一些实施例中，所有的监控器 405 可以被分配相同的权重。在其他实施例中，多个监控器 405 可以每一个分配不同的权重。权重可以基于指示相对重要性的任意标准来分配给监控器，包括但不限于设备或用户根据服务、监控机制的可靠性和监控频率确定监控器的相对重要性或相对值。

[0174] 在一个实施例中，监控代理 405 可以基于通过设备监控的服务的相对重要性来分配权重。例如，如果环境中的大部分用户请求是 HTTP 请求，则监控服务器 106 的 HTTP 可用性的监控代理可以被分配 10 的权重，而监控服务器 106 的 FTP 可用性的监控代理可以被分配 3 的权重。或者，例如，如果管理员为 UDP 应用设置了高的优先级，可为监控服务器的 UDP 可用性的监控代理可分配 20 的权重，而为 DNS 监控代理分配 5 的权重。

[0175] 在一些实施例中，设备 200 可以计算当前报告网络服务 270 在操作中的监控代理的权重的总和。例如，如果五个监控代理监控网络服务 270，为其中每一个监控代理分配 30 的权重，并且五个监控代理的三个报告网络服务 270 可用，则设备可以确定当前报告网络服务 270 在操作中的监控代理的总和是 90。或者例如，如果仅有两个监控代理报告服务器 106 可用，其中一个具有 20 的权重，另一个具有 40 的权重，则设备可以计算当前报告服务器 106 在操作中的监控代理的总和是 60。

[0176] 设备 200 还包括为用户、应用或者系统提供和设备 200 通信的任意类型和形式的接口机制的配置接口 425。在一个实施例中，配置接口 425 包括命令行界面 425B。在另一个实施例中，配置接口 425 包括图形用户界面 425A。在一些实施例中，配置接口 425 包括用于应用、程序或者脚本以与设备 200 通信的应用编程接口 (API) 或者开发工具包。

[0177] 在一些实施例中，设备 200 经由设备的显示器显示配置接口 425。其他实施例中，配置终端或设备 100 连接到设备 200 或和设备 200 通信，并显示配置接口 425。例如，配置设备 100 或终端可通过设备 200 的端口和 IP 地址连接到设备 200。设备 200 可提供对端口和 IP 地址的 web 服务监听以为用户提供页面。所提供的页面可以提供用于配置设备 200 的用户界面。在其他实施例中，配置终端 100 可以经由任意类型和形式的连接来连接到设备 200 并与之通信，包括监控器端口、串行端口或者 USB 连接。

[0178] 经由配置接口 425，设备 200 可以接收识别用户选择的指标 430 的信息来用于确定一个或者多个服务的负载 440。在一个实施例中，用户从多个设备收集的指标 410 中识别或者选择指标。在另一个实施例中，用户从多个装置提供的指标 420 识别或者选择指标。在一些实施例中，用户从设备收集的指标 510 选择一个或者多个指标并且从装置提供的指标 410 选择一个或者多个指标。设备 200 还可以经由配置接口 425 接收识别用户为指标选择或者指定的权重 435 的信息。例如，用户可以提供指标的权重 435 的值。在一些实施例中，设备 200 接收识别阈值 437 的用户提供的值的信息。

[0179] 在操作中，设备 200 可以使用用户选择的指标 430 和用户提供的权重 435 和阈值 437 用于确定负载 440。在另一个实施例中，设备可以使用来自设备收集的指标 410 的任意设备建立的指标用于确定负载。在一个实施例中，用户确定设备提供的指标的权重和 / 或阈值。这样，尽管在一些实施例中指标可以不是用户选择的，但用户可以控制或者配置指标

410 的权重 435 和 / 或阈值 437。在其他实施例中，设备可以使用用户选择的指标 430 和设备建立的指标 410 的任一组合用于确定负载。在另一个实施例中，设备 200 可以使用任意指标的用户提供的权重 435 和 / 或阈值 437 以及设备提供的权重 435 和 / 或阈值 437 的任一组合来确定负载 440。

[0180] E、异类装置间的全局服务器负载平衡

[0181] 现在参考图 5A 和 5B，描述用于负载平衡多个异类装置的系统和方法。此处描述的设备 200 可以被布置来负载平衡多个服务并且负载平衡多个装置。第一设备 200 可以经由预定的指标交换协议 (MEP) 和同类型的第二设备 200A 进行通信。第一设备 200 经由 MEP 协议获取用于确定第二设备 200A 负载的指标。与第一设备不同类型的其它装置可以被布置在网络中来执行本地负载平衡，诸如用于服务器群。一些实施例中，这些装置可以不经由第一设备 200 的 MEP 协议进行通信。一些实施例中，作为替代，这些其他装置可以经由诸如简单网络管理协议 (SNMP) 的网络管理协议来提供指标。使用结合图 4 描述的技术，第一设备 200 从这些异类装置经由网络管理协议来获取指标。使用经由 MEP 协议从同类型的装置获取的指标和经由网络管理协议从不同类型的装置获取的指标，设备 200 可以使用这些组合的指标来确定跨越这些异类装置的负载并基于该负载将请求引导到其中一个装置。

[0182] 现在参考图 5A，描述用于负载平衡包括服务器和本地或者其他负载平衡装置的异类装置的网络环境的实施例的例子。总的来说，网络环境包括多个不同类型的负载平衡装置和服务器。设备 200 被配置为全局负载平衡装置来负载平衡多个负载平衡装置和服务器。负载平衡装置的每一个可以执行对于一个或者多个服务 270A-270N 的本地负载平衡。例如，同样类型的第一组负载平衡设备 200A-200N 可以执行第一网络 104 上服务或者服务器的本地负载平衡。这些设备 200A-200B 可以是同样类型的全局负载平衡设备 200。或者在一些情况下，本地负载平衡设备 200A-200N 被设计和构建为经由指标交换协议 540 传递指标和其他信息。第二类型的负载平衡设备 500A-500N 可以执行对于第二网络 104' 上一个或者多个服务 270A'-270N' 的本地负载平衡。这些负载平衡设备 500A-500N 可以与第一类型的设备 200A-200N 和 / 或全局负载平衡设备 200 类型不同。设备 500A-500N 可以操作或者执行一个或者多个虚拟服务器或者 vServer 275A-275N。设备 500A-500N 可以不被设计为经由设备 200A-200N 的 MEP 协议 540 通信。而是这些设备 500A-500N 可以经由诸如 SNMP 的网络管理协议提供指标。全局负载平衡设备 200 还可以对于诸如服务器群 38 的一个或者多个服务或者服务器执行负载平衡。服务器或者服务的每一个可以是不同类型的，诸如 HTTP 服务和 FTP 服务。

[0183] 考虑图 5A，多个设备、服务器和服务可以以分层方式布置。第一设备 200 可以是处于分层顶部的全局负载平衡设备，来管理多个其他设备 200A-200N、500A-500N 和服务器。在一个情况中，设备 200 直接管理一个或者多个服务器 106 或者服务 270A-270N。在另一个情况中，设备 200 管理一个或者多个设备 200A-200N、500A-500N，其又依次管理一个或者多个服务器 106 或者服务 270A-270N。由第一设备 200 管理的设备可以管理第二设备，其又依次管理一个或者多个服务或者服务器。

[0184] 通过参考不同负载平衡产品的例子，全局负载平衡设备 200 可以是称为 NetScaler 的 Citrix System 公司出品的任意一种产品实施例。设备 200A-200N 也可以是被配置为执行一个或者多个服务 270A-270N 的本地负载平衡的 NetScaler 装置。当设

备 200A-200N 与全局负载平衡设备 200 为相同类型时,这些设备被设计和构建为经由称之为指标交换协议的预定的协议和 / 或通信模型进行通信。设备 200A-200N 可以被配置为以预定频率提供指标信息给设备 200。一个或者多个设备 500A-500N 可以包括另一类型的负载平衡装置,诸如 F5 Networks 公司出品的 BigIP 负载平衡装置。另一个或者多个设备 500A-500N 可以包括不同类型的负载平衡装置,诸如 Radware 有限公司出品的 AppDirector 设备。在一些情况中,一个或者多个设备 500A-500N 可以包括 Cisco 负载平衡装置。在其他情况中,一个或者多个设备 500A-500N 可以包括 Nortel 负载平衡装置。任意一个或者多个这些设备 500A-500N 可以不被设计或者构建为经由 MEP 协议 540 与设备 200 通信。尽管该例总的在以上描述为提供全局负载平衡装置的 Citrix NetScaler 装置 200,但是可以使用任意其它类型的负载平衡装置。

[0185] 除了使用 MEP 540,这些不同设备 500A-500N 的每一个可以经由诸如 SNMP 的网络管理协议提供指标信息。如图 5A 中所示,这些设备 500 可以包括用于经由 MIB 417 提供对象标识符 422A-422N 的代理 416。该示例的进一步实施例并且如结合图 4 所讨论的,使用管理器 / 代理通信模块的设备 200 可以经由网络管理协议查询任意一个这样的设备 500A-500N,以经由 MIB 417 识别、收集和监控所识别的对象。在一些情况中,设备 200 可以使用 SNMP 来与一个或者多个设备 500A-500N 通信。在其他情况中,设备 200 可以使用另一类型的网络管理协议与另一个或者多个设备 500A-500N 通信。仍在另一个情况中,设备 200 可以使用第三类网络管理协议来与又一组一个或者多个设备 500A-500N 通信。

[0186] 设备 200A-200N 可以被认为是与设备 200 同类或者相同类型的设备或者装置。在一个实施例中,设备 200A-200N 是设备 200 的相同产品族。在另一个实施例中,设备 200A-200N 是设备 200 的相同装置版本。在一个情况中,设备 200 和 200A-220N 由同一家公司出品。在一些实施例中,设备 200A-200N 和设备 200 被配置、设计和构建以使用预定协议和 / 或通信模型进行通信。在一个实施例中,设备 200A-200N 和设备 200 被配置、设计和构建为使用专用或者自定义的协议和 / 或通信模型。

[0187] 设备 500A-500N 可以被认为是与设备 200 异类的或者不同类型的设备或者装置。在一个实施例中,设备 500A-500N 由与设备 200 不同的公司出品。在一些实施例中,设备 500A-500N 和设备 500 不是被专有设计为使用预定的协议和 / 或通信模型进行通信。在一个实施例中,设备 500A-500N 和设备 200 不是被配置、设计和构建来使用专用或者自定义协议和 / 或通信模型。在一些情况中,设备 500A-500N 使用网络管理协议而不是使用专用协议来提供指标到其他装置、应用或者服务。

[0188] 现在参考图 5B,描述用于使用多个协议识别、收集和监控从异类网络装置和服务器获取的指标的设备 200 的实施例。设备 200 可以具有被配置、构建或者设计来提供一个或者多个网络 104、104'、104'' 上的多个装置的负载平衡的一个或者多个虚拟服务器 275A-275N。设备 200 可以使用一个或者多个负载监控器 405A-405N 来监控异类装置的每一个的负载。在一个实施例中,设备 200 监控设备 200A-200N 的负载。设备 200 和 / 或负载监控器 405 使用 MEP 协议 540 来从一个或者多个设备 200A-200N 获取指标。在另一个实施例中,设备 200 监控设备 500A-500N 的负载。在其他实施例中,设备 200 监控一个或者多个服务器 106 的负载。仍在另一个实施例中,设备 200 监控服务器群 38 中的服务器之间的负载。设备 200 可以使用一个或者多个网络管理协议来从服务器 106、服务器群 38 和设备

500A-500N 获取指标。

[0189] 设备 200 经由 MEP 协议 540 和网络管理协议从多种诸如设备 500A-500N 和服务器 106 的异类装置和同类装置 200A-200N 收集指标。设备 200 将指标保存在包括诸如存储器中和 / 或磁盘上的文件、数据库、对象或者数据结构的任一类型和形式的数据存储元件的 GSLB (全局服务器负载平衡) 或者全局指标表 530 中。vServer 275 和 / 或负载监控器 405 使用来自 GSLB 指标 530 的一个或者多个指标来提供服务器、服务器群、虚拟服务器和负载平衡装置的全局负载平衡。

[0190] 设备 200 可以收集和监控经由 MEP 协议 540 从一个或者多个设备 200A-200N 获取的指标并且将它们保存在基于 MEP 的指标表 510A-510N 中。在一个实施例中，设备 200 使用第一类或者第一版本的 MEP 协议 540 来获取来自第一设备 200A 的指标并且将指标保存在第一表 510A 中。在另一个实施例中，设备 200 使用第二类或者第二版本的 MEP 协议 540' 来获取来自第二设备 200N 的指标并且将指标保存在第二表 510N 中。

[0191] 设备 200 可以使用任一类型和形式的网络管理协议 (NMP) 收集和监控来自设备 500A-500N 的指标并且将该指标保存在基于 NMP 的指标表 520A-520N 中。在一个实施例中，设备 200 使用 SNMP 协议和通信模型来获取来自第二类型设备 500A 的指标并且将指标保存在基于 NMP 的指标表 520A 中。在一些实施例中，设备 200 使用诸如 CIMP 的第二类网络管理协议来从第二或者第三类设备 500N 获取并且将指标保存在基于 NMP 的指标表 520N 中。在一些实施例中，设备 500A 是与设备 500N 不同类型的设备，但是两种设备都支持同样的网络管理协议用于提供指标。

[0192] 设备 200 还可以使用任一类型和形式的网络管理协议 (NMP) 从服务器 106 和 / 或服务器群 38 收集和监控指标并且将指标保存在基于 NMP 的指标表 520A' -520N' 中。在一个实施例中，设备 200 使用诸如 SNMP 的同样的网络管理协议用于从服务器 106 获取指标，该网络管理协议同样用于从设备 500A-500N 的其中一个获取指标。在另一个实施例中，设备 200 使用和设备 200 从设备 500 获取指标所使用的不相同类型的网络管理协议来从服务器获取指标。

[0193] 设备 200 可以将对于 GSLB 指标 520 的指标保存在对于每个装置的单个表中。例如，设备 200 可以将用于第一设备 200A 的指标保存在第一指标表 510A 中，并且将来自第二设备 520A 的指标保存在第二指标表 520A 中。设备 200 可以将来自服务器 106 的指标保存在服务器指标表 520A' 中。在另一个实施例中，设备 200 将来自服务器群 38 的指标保存到用于服务器群的指标表 520N' 中。

[0194] 设备 200 可以将 GSLB 指标 520 的指标保存在用于每一类协议的单个表中。例如，设备 200 可以将来自多个设备 200A-200N 的所有基于 MEP 的指标保存在第一指标表中。在一些实施例中，设备 200 将基于第一类或者第一版本的 MEP 协议的指标保存在第一表 510A 中并且将基于第二类或者第二版本的 MEP 协议的指标保存在第二表 510N 中。设备 200 可以将来自一个或者多个设备 500A-500N 的所有基于 SNMP 的指标保存在第二指标表中。在另一个例子中，设备可以将来自一个或者多个设备 500A-500N 的根据第二类网络管理协议的指标保存在第三指标表中。

[0195] GSLB 指标 530 可以包括涉及或者关联到设备 200、500、服务器 106 或者服务器群 38 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。全局指标 530

可以包括涉及设备 200、500、和 / 或服务器 106 或者服务器群 38 的网络的任一类型和形式的数据、统计、状态或者信息。全局指标 530 可以包括涉及由设备 200A-200N、500A-500N 所负载平衡的服务 270A-270N 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，全局指标 530 包括有关连接到设备 200A-200N、500A-500N 的任意客户机 102 和 / 或服务器 106 的操作和 / 或性能数据。在一个实施例中，设备 200A-200N、500A-500N 确定关于其连接的或服务的任一客户机 102 或者服务器 106 的操作和 / 或性能信息和建立有关这些客户机 102 和 / 或服务器 106 的指标。在这些实施例中，设备 200A-200N、500A-500N 可以提供这些指标到全局负载平衡设备 200。

[0196] 在一些实施例中，操作和 / 或性能特征提供包括有关设备或者服务器的任意以下的信息的指标 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) 发送的请求的数量；7) 服务的客户机的数量；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，和其状况或者状态。在另一个实施例中，指标 530 包括有关设备 200A-200N、500A-500N 的任意 IP 或者网络层信息的、或者设备 200A-200N、500A-500N 的连接、或者设备 200A-200N、500A-500N 所服务的客户机和 / 或服务器的连接的信息。例如，经由指标 530 提供的信息可以包括设备 200A-200N、500A-500N 的路由表用于执行网络地址转换，诸如用于 SSL VPN 连接。

[0197] 经由配置接口 425，用户可以从全局指标 530 选择一个或者多个指标 430 用于负载监控和确定负载 440。设备 200 可以接收识别来自全局指标 530 的一个或者多个指标的用户选择的信息。设备可以接收第一类型设备的一个或者多个基于 MEP 的指标 510 的用户选择。设备可以接收第二类型的设备的一个或者多个基于 NMP 的指标 520 的用户选择。设备还可以接收用于任一服务器或者服务器群的一个或者多个基于 NMP 的指标 520' 的用户选择。用户可以从全局指标 530 选择指标 430 的任一组合来配置设备 200 以对应于用户选择的指标来执行异类装置的负载平衡。

[0198] 在一个实施例中，设备 200 使用与任意一个或者多个用户选择的指标 430 相组合的设备建立的指标来负载平衡。例如，设备 200 可以对于任一设备 200、500 或者服务器 106 收集和监控连接数量、响应时间、带宽和分组的数量并且使用具有任意用户选择的指标的这些指标来用于负载平衡。经由配置接口 425 并且如结合图 4 所讨论的，设备 200 可以接收来自用户的信息，其识别、指定或者建立用于任一设备建立的指标和 / 或用户选择的指标的权重 435 和 / 或阈值 437。

[0199] 尽管图 5A-5B 的系统总的关于全局服务器负载平衡讨论，但是这些系统可以用于本地负载平衡。设备 200 可以使用从使用多个协议的异类装置、服务器或者服务获取的指标来负载平衡一个或者多个服务或者服务器。使用此处描述的技术，设备 200 可配置地并且灵活地使用由设备支持的指标交换协议和 / 或由网络资源支持的更普遍的网络管理协议来从任一网络资源获取指标，网络资源诸如系统、子系统、应用、服务、装置等等。此外，设备 200 可配置地允许用户从这些异类网络资源选择可用指标的任一组合来执行一个或者多个服务的负载监控和负载平衡。

[0200] F、故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器进行负载平衡

[0201] 现在参考图 6A 和 6B，描述故障切换时用于进行负载平衡的多种系统和方法。一些方面中，图 6A 图 6B 表现故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行

负载平衡的方法和系统。示出了多个实施例，其中，虚拟服务器 275 可以关联或连接到一个或多个备份虚拟服务器 276。一些方面中，虚拟服务器 275 和与虚拟服务器 275 关联的多个备份虚拟服务器 276 可以被系统或者设备 200 视为一个逻辑单元或逻辑链，其中，任何备份虚拟服务器 276 可以接管或者执行虚拟服务器 275 的任何功能。有时，也把虚拟服务器 275 称为 vS 275 或 vServer 275。类似地，有时也把备份虚拟服务器 276 称为 BvS 276 或 BvServer 276。多个实施例中，BvS 276 可以包括 vS 275 的任何和全部特征以及任何和全部功能。

[0202] 图 6A 示出故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行负载平衡的设备 200 的若干实施例。总体而言，多个客户机代理 120A-120A 分别运行在客户机 102A-102N 上。多个服务器 106A-106N 分别在每个服务器 106A-106N 上运行服务 270A-270N。客户机 102 和服务器 106 之间的通信经过网络 104 和 104' 通过设备 200、200' 和 200'' 之一。有时设备 200、200' 和 200'' 称为设备 200。一些实施例中，设备 200 包括各种结构和设置的连接管理机制 710、一个或多个 vServer 275 和与 vServer 275 关联的一个或多个 BvServer 276。

[0203] 连接管理机制 710 也称为 CMM 710，其包括用于控制和管理设备 200 内的通信的软件、硬件或软硬件的任意组合。一些实施例中，CMM 710 包括用于接收、导引或者重定向来自客户机 102 或服务器 106 的请求、数据或指令的逻辑、函数或软件应用。一些实施例中，连接管理机制 710 接收或拦截客户机 102A-102N 和一个或多个服务 270A-270N 之间的传输层连接请求或通信。连接管理机制 710 可包括应用、程序、服务、进程、任务、线程或任何类型和形式的可执行指令。其他实施例中，连接管理机制 710 标示、确定或选择 vServer 275 用于处理从客户机 102 或服务器 106 接收到的通信。一些实施例中，连接管理机制 710 标示、确定或选择 BvS 276 用于处理从客户机 102 或服务器 106 接收到的通信。

[0204] 一些实施例中，连接管理机制 710 确定是否达到或超过了最大动态连接阈值。连接管理机制 710 可以确定是否超过了最大动态连接阈值。若干实施例中，CMM 710 还可以确定是否确立第二虚拟服务器 275N 或备份虚拟服务器 276N，例如泻出 vServer 或 BvServer。在检测到多个第一 vServer 275A 或 BvServer 276A 的活动传输层连接超过阈值（比如动态调整的最大连接阈值）时，连接管理机制 710 可以将接收到的传输层连接请求导引、传输或者提供给第二 vServer 275N 或第二 BvServer 276N 进行处理。一些实施例中，CMM 710 使用动态调整的最大连接阈值来确定何时自动把连接请求从第一 vServer 275A 泻出到备份虚拟服务器 276A 或第二 vServer 275N。一些实施例中，CMM 710 使用动态调整的最大连接阈值来确定何时把意在发送给第一 vServer 275A 的请求重定向到第一备份虚拟服务器 276A、BvS 276N 或任何其他 vS 275 或 BvS 276。

[0205] 一些实施例中，负载监控器 405、CMM 710 或设备 200 中的任一个可以把具体 BvS 276A 和具体 vS 275A 关联。一些实施例中，检测或识别到 vS 275A 不可用，之前由 vS 275A 处理的连接请求或通信业务自动重定向或重分配给 BvS 276A。这种情况下，BvS 276A 接管之前由 vS 275A 处理的连接请求或通信业务的处理。多个实施例中，在接收到 vS 275A 不再可用的信息后，负载监控器 405、CMM 710 或设备 200 动态地或自动地把之前由 vS 275A 处理的连接请求或通信业务重定向到 BvS 276A。多个实施例中，负载监控器 405、CMM 710 或设备 200 把 BvS 276A 分配为用于处理之前由 vS 275A 处理的连接请求或业务的第一备

份虚拟服务器。某些实施例中,检测或识别到 BvS 276A 不可用的情况下,负载监控器 405、CMM 710 或设备 200 把 BvS 276B 分配为用于接管之前由 BvS 276A 处理的连接请求或通信业务的第二备份虚拟服务器。多个实施例中,检测或识别到 vS 275A 不可用的情况下,负载监控器 405、CMM 710 或设备 200 自动地把之前由 vS 275A 处理的连接请求或业务重定向到 BvS 276A。一些实施例中,检测或识别到 BvS 276A 不可用的情况下,负载管理器 405、CMM 710 或设备 200 把之前由 BvS 276A 处理的连接请求或业务重定向到 BvS 276B。

[0206] 其他实施例中,连接管理机制 710 保持客户机 102 或服务器 106 以及处理客户机 102 或服务器 106 的请求的 vServer 275 或 BvServer 276 之间的连接或会话持续性。一些实施例中,即便第一 vServer 275A 的活动连接的数量没有超过最大连接阈值 720,连接管理机制 710 也可选择泄出 vServer 275N 来处理客户机请求。其他实施例中,即便来自其他客户机的请求被导引到泄出 vServer 275N 或 BvServer 276,连接管理机制 710 选择第一 vServer 275A 来处理客户机请求。一些实施例中,连接管理机制 710 可以基于哪个 vServer 275 最近处理了来自客户机 102 或服务器 106 的请求来选择第一 vServer 275A 或第二 vServer 275N。若干实施例中,连接管理机制 710 可以基于哪个 vServer 275 或 BvServer 276 最近处理了来自客户机 102 或服务器 106 的请求来选择第一 BvServer 276A 或第二 BvServer 276N。

[0207] 检测到已超过第一 vServer 275A 和 / 或第二 vServer 275N 的动态调整的最大连接阈值 720 时,一些实施例中,连接管理机制可以确定建立泄出虚拟服务器 275 或备份虚拟服务器 276。检测到已超过第一 vServer 275A 和 / 或第二 vServer 275N 的动态调整的最大连接阈值 720 时,一些实施例中,连接管理机制可以确定不建立另一个泄出虚拟服务器 275N,而是把客户机 102 直接重定向到服务器 106 或者以其他方式绕过设备 200。有时,检测到已超过第一 vServer 275A 和 / 或第二 vServer 275N 或 BvServer 276A 的动态调整的最大连接阈值 720 时,连接管理机制 710 可以决定不建立另一个泄出虚拟服务器 275N 或 BvServer 276N,而是把客户机 102 直接重定向到服务器 106 或者以其他方式绕过设备 200。例如,连接管理机制 710 可以确定已达到了泄出 vServer 275N 或第一 BvServer 276 的动态调整的最大连接阈值 720B,并可以重定向客户机 102,以绕过设备 200,而不是建立第三 vServer 275N 作为泄出或第二 BvServer 276。一些实施例中,检测到已超过第一 vS 275A 和 / 或第二 vS 275N 的动态调整的最大连接阈值 720 时,连接管理机制可以决定建立另一个泄出 BvS 276N。这些实施例中,连接管理机制可以响应于客户机的连接请求向客户机 102 发送让客户机 102 连接的重定向统一资源定位器 (URL)。URL 760 可以识别任一个服务器 106 或服务 270。

[0208] 特定 vS 275 被检测为不可用时与该 vS 275 关联的可接管并实现特定 vS 275 的任何功能的任一个 vS 275 或 BvS 276 可被视为和特定 vS 275 关联的逻辑单元或逻辑链的一部分。一些实施例中,负载监控器 405、CMM 710 或设备 200 把 vS 275A 和与 vS 276A 关联的多个 BvS 276 视为一个单个逻辑单元或一个单个逻辑链。和 vS 275A 关联的单个逻辑单元或单个逻辑链的每个单独部分可以执行 vS 275A 或同一逻辑单元或逻辑链中的任何其他 vS 275 或 BvS 276 的任何功能。

[0209] 多个实施例中, vS 275 可以由于引起 vS 275 停止工作的技术问题而被检测为不可用。若干实施例中,vS 275 由于 vS 275 达到了 vS 275 可以处理的最大业务容量而被检

测为不可用。这些实施例中,即便 vS 275 依然可工作,仍可将 vS 275 检测为不可用。一些实施例中, vS 275 被检测为不可用,虽然进行了检测,仍然保持标记该 vS 275 仍可用的标志或信号。多个实施例中,即便 vS 275 被检测为不可用,虽然进行了检测, CMM 710、封装监控器 405 或设备 200 中的任一个或任一组合可以保持 vS 275 仍然可用的状态、信号或标志。

[0210] 一些实施例中,在 vS 275A 仍被检测为可用时,和 vS 275A 关联的 BvS 276A 收集、产生或保持有关和 vS 275A 关联的业务或请求的指标,一些实施例中,在 vS 275A 仍被检测为可用时,包括 vS 275A 的设备 200 收集、产生或保持有关和 vS 275A 关联的业务或请求的指标,若干实施例中,当 vS 275A 被检测为不可用时,设备 200 或 BvS 276A 获得由设备 200 或 BvS 276A 收集、产生或保持的指标,并使用该指标确定多个负载服务器 275 的负载。多个实施例中,当 vS 275A 被检测为不可用时,和 vS 275A 关联的逻辑链或逻辑单元的任何部分可获得由逻辑链或逻辑单元的任何部分收集、产生或保持的指标并使用该指标确定多个负载服务器 275 的负载。

[0211] 许多实施例中,由于来自和 vS 275A 关联的 BvS 276 的指标被用于确定多个负载服务器 275 的负载,其请求被负载平衡的用户不经历任何由于 vS 275A 被检测为不可用而引起的延迟。利用此处所述的系统和方法,多个虚拟服务器 275 的虚拟服务器 275A 可以出故障或不可用,而不会影响负载平衡或者即便是临时引起延迟。因而,虚拟服务器 275A 出故障不会影响负载平衡,这是由于和虚拟服务器 275A 关联的 BvS 的指标帮助保持所有虚拟服务器 275 的负载平衡,虽然一些一个或多个虚拟服务器 275 不可用。

[0212] 一些实施例中,设备 200 使用来自任何多个虚拟服务器 275 或备份虚拟服务器 276 的指标来确定多个虚拟服务器 275 的负载。多个实施例中,设备 200、负载监控器 405 或 CMM 710 使用第一虚拟服务器 275A 的一部分指标和第一备份虚拟服务器 276A 的一部分指标来确定多个虚拟服务器 275 的负载。多个实施例中,设备 200、负载监控器 405 或 CMM 710 组合任何多个虚拟服务器 275 的指标和备份虚拟服务器 276 的指标来确定多个虚拟服务器 275 的负载。有时,可以组合来自 vS 275A 和多个 BvS 276 的指标或对其进行平均来确定多个 vS 275 的负载,其中, vS 275A 是多个的一部分。一些实施例中,设备 200、负载监控器 405 或 CMM 710 使用来自 vS 275 被检测为不可用时负责接管 vS 275 的功能的任何多个 BvS 276 的指标来确定多个 vS 275 的负载。许多实施例中,设备 200、负载监控器 405 或 CMM 710 通过组合来自 vS 275 被检测为不可用时负责接管 vS 275 的功能的任何多个 BvS 276 的指标或对其进行平均来确定多个 vS 275 的负载。

[0213] 另一个实施例中,设备 200 和 / 或连接管理机制管理多个 vServer 275A-275N 的活动连接数量并对其执行动态泄出技术。一个实施例中,第二 vServer 275B 可以管理从多个客户机 102A-102N 到第二组服务 270A' -270N' 的连接。一些实施例中,设备 200 监控第二 vServer 275B 的第二动态最大连接阈值 720B。一个实施例中,第二 vServer 275B 可以作为第一 vServer 275N 或第三 vServer 的泄出 vServer。

[0214] 监控代理 405 或负载监控器 405 可用于检测或识别可用的 vServer 275 或 BvServer 276。监控代理还可用于检测或识别不可用的 vS 275 或 BvS 276。一些实施例中, CMM 710 可以包括监控代理 405 或包括监控代理 405 的任何和所有功能。多个实施例中,监控代理 405 可以包括 CMM 710 或包括 CMM 710 的任何和全部功能。一些实施例中,监

控代理 405 可用于确立或保持 vServer 275 或 BvServer 276 的状态为可用或不可用。

[0215] 多个实施例中,监控代理 405 可以识别第一 vS 275A 和被识别或选择作为第一 vS 275A 的备份虚拟服务器的多个 BvServer 276。一些实施例中,监控代理 405 或 CMM 710 把第一 vServer 275A 和与第一 vServer 275A 关联的多个 BvServer 276 标识为逻辑单元,或者作为一个单一系统,其中,vServer 275A 或与 vServer 275A 关联的任一个 BvServer 276 可以执行第一 vServer 275A 的任何功能。多个实施例中,监控代理 405 或 CMM 710 标识或者确立与第一 vServer 275A 关联的多个 BvServer 276 之一接管之前由第一 vServer 275 执行的功能的顺序。某些实施例中,与第一 vServer 275A 关联的多个 BvServer 276 之一可以提供用于确定由包括第一 vServer 275 和 BvServer 276 的设备 200 负载平衡的多个服务器的负载的指标。

[0216] 一些实施例中,如果第一 vServer 275A 不可用或被识别为不可用,那么负载监控器 405、CMM 710 或设备 200 可以从多个虚拟服务器以及指定用于执行由第一 vServer 275A 执行的功能的两个备份虚拟服务器第一 BvS 276A 和第二 BvS 276B 中标识第一 vServer 275A。若干实施例中,负载监控器 405、CMM 710 或设备 200 可以检测或识别第一虚拟服务器 275A 不可用,并且响应于该检测或识别,保持第一 vServer 275A 的状态为可用。多个实施例中,负载监控器 405、CMM 710 或设备 200 从第一 BvS 276A 获得指标,并使用从第一 BvS 276A 获得的指标确定多个虚拟服务器的负载。一些实施例中,负载监控器 405 可以使用来自第一 BvS 276A 的指标确定第一 vServer 275A 的负载,该第一 vServer 275A 被识别为不可用。多个实施例中,第一 vServer 275A 和第一 BvS 276A 都被识别或检测为不可用时,保持第一 vServer 275A 的状态为可用,并且用来自第二 BvS 276B 的指标确定 vServer 275A 作为其一部分的多个虚拟服务器的负载。如果第一 BvS 276A 被识别为不可用并且 vServer 275A 被识别为不可用,可以选择第二 BvS 276B。多个实施例中,第一 vS 275A 可以具有分配用于执行第一 vS 275A 的功能并提供用于确定 vS 275A 是其一部分的多个虚拟服务器的负载的指标的任何一个 BvS 276。

[0217] 仍然参看图 6A,设备 200 可包括 CMM 710、两个虚拟服务器 vS 275A 和 vS 275B 以及两个备份虚拟服务器 BvS 276A 和 BvS 276B。BvS 276A 可以选择作为 vServer 275A 的主备份虚拟服务器,BvS 276B 可以选择作为 vServer 275B 的主备份虚拟服务器。监控代理 405 可以监控 vS 275A 和 vS 275B 以及 vS 275A 和 vS 275B 的状态。此外,监控代理 405 可以把 vS 275A 和 BvS 276A 视为单个逻辑单元,其中,vS 275A 和 BvS 276A 中的一个可以执行在 vS 275A 可用时 vS 275A 通常执行的功能。一些实施例中,如果监控代理 405 检测到 vS 275A 不可用,那么监控代理可以从 vS 275B 获得指标以确定 vS 275A 和 vS 275B 的负载。多个实施例中,监控代理 405 在识别 vS 275A 不可用之后,可以从 BvS 276A 获得指标并使用指标来确定 vS 275B 和 BvS 276A 的负载,同时保持 vS 275A 的状态为可用。某些实施例中,负载监控器 405A 可以识别 vServer 275B 为不可用的,相应于该识别,保持 vServer 275B 的状态为可用,响应于该识别,从 BvS 276B 获得指标并使用该指标来确定 vS 275A 和 vS 275B 的负载。若干实施例中,BvS 276B 和 vS 275B 可以被负载监控器 405 视为或识别为单个单元,其中,BvS 276B 或 vS 275B 之一被称为 vS 275B 并且可以执行虚拟服务器 vS 275B 的功能。

[0218] 图 6A 也示出包括多个虚拟服务器 vS 275 以及多个备份虚拟服务器 BvS 276 的设

备 200'。虚拟服务器 vS 275A、vS 275B、vS 275C 到 vS 275N(其中 N 可以为任何数或符号)由两行虚拟服务器备份,第一行有备份虚拟服务器 BvS 276A、BvS 276B 到 BvS 276N,第二行有备份虚拟服务器 BvS 276C、BvS 276D 到 BvS 276N,其中 N 可以为任何数或符号。虚拟服务器 vS 275A 和 vS 275B 具有指定的备份虚拟服务器 BvS 276A。此外,vS 275B 和 vS 275C 由 BvS 276B 备份,并且 vS 275C 到 vS 275N 由 BvS 276N 备份,其中 N 可以任何数字或符号。图 6A 还示出 BvS 276C 备份 BvS 276A, BvS 276D 备份 BvS 276B, 以及 BvS 276N 备份 BvS 276N。因而,如果 vS 276A 或 vS 276B 中的一个被识别为不可用,那么可以指定 BvS 276A 来接管 vS 276A 或 vS 276B 的功能,如果 BvS 276A 被识别为不可用,可指定 BvS 276C 来接管 BvS 276A 的功能。若干实施例中,负载监控器 405 响应于 vS 275A 或 vS 275B 不可用的识别从 BvS 276A 获得指标并使用指标来平衡 vS 275A 到 vS 275N 的负载,其中 BvS 276B 接管识别为不可用的 vS 275 的功能。

[0219] 图 6A 还示出了设备 200"。设备 200" 包括负载平衡虚拟服务器 vS 275B、vS 275C、vS 275D 和 vS 275E 的虚拟服务器 vS 276A 以及 CMM 710。BvS 276A 是虚拟服务器 vS 275B、vS 275C、vS 275D 和 vS 275E 的备份虚拟服务器。BvS 276B 是虚拟服务器 vS 275E 的备份虚拟服务器。此外, BvS 276C 备份 BvS 276A 和 BvS 276B。一些实施例中,如果 vS 275B 到 vS 275E 中的一个被识别为不可用,负载监控器 405 可以从 BvS 276A 获得指标并使用该指标来确定 vS 275B 到 vS 275E 的负载。多个实施例中,如果 vS 275B 到 vS 275E 中的一个被识别为不可用,负载监控器 405 可以从 BvS 276A 获得指标并使用该指标来确定 vS 275B 到 vS 275E 的负载,其中 BvS 276A 会替代或接管识别为不可用的 vS 275 的功能。

[0220] 若干实施例中, vS 275 可以用一个或多个 BvS 276 备份虚拟服务器来备份,其中任何 BvS 276 可以执行 vS 275 的任何功能。一些实施例中,用一个 BvS 276 备份若干 vServer 275。多个实施例中,用第二 BvS 276 备份第一 BvS 276, 第二 BvS 276 可提供用于确定第一 BvS 276 和第二 BvS 276 备份的多个虚拟服务器的负载的指标。虚拟服务器 275 和备份虚拟服务器 276 可以采取任何设置或配置,而且可用于对任何多个服务器或任意量或类型的网络业务进行负载平衡。

[0221] 现在参看图 6B,示出了包括用于故障切换时使用备份虚拟服务器的指标通过多个虚拟服务器执行负载平衡的多个步骤的方法。多个实施例中,所讨论的方法用于故障切换时使用备份虚拟服务器 276A 的指标对多个虚拟服务器 275 进行负载平衡,以对多个虚拟服务器 276 和备份虚拟服务器 276A 进行负载平衡,其中备份虚拟服务器 276A 接管多个 vS 275 中不可用的 vS 275A 的功能。

[0222] 简单概括而言,在方法 600 的步骤 605,负载平衡多个虚拟服务器的设备检测到多个虚拟服务器中的第一虚拟服务器不可用。一些实施例中,设备包括负载监控器 405,其检测虚拟服务器 275 的可用性。多个实施例中,设备包括对另外的多个虚拟服务器 275 进行负载平衡的多个虚拟服务器 275。一些实施中,多个虚拟服务器中的第一虚拟服务器 275A 可以是多个虚拟服务器 275 中的任一个虚拟服务器 275。多个实施例中,虚拟服务器 275A 为多个虚拟服务器 275 提供负载平衡。某些实施例中,设备可以为设备 200、设备 500、客户机 102 或服务器 106。一些实施例中,多个备份虚拟服务器 276 和一个或多个虚拟服务器 275 相关联。

[0223] 在步骤 610,设备识别到一个或多个备份虚拟服务器 276 的至少一个备份虚拟服

务器 276A 可用。一些实施例中，多个备份虚拟服务器 276 可以为任何配置，例如图 6A 所示的多个设备 200、200' 和 200''。一些实施例中，多个备份虚拟服务器 276 中的一些被指派给任意配置的多个虚拟服务器 275 或与之关联。多个实施例中，多个备份虚拟服务器 276 中的一个备份虚拟服务器 276 被指派给特定的虚拟服务器 275 或特定的多个虚拟服务器 275 或与之关联。在一些实施例中，设备 200 识别到备份虚拟服务器 276 是可用的。若干实施例中，和备份虚拟服务器 276 所处的机柜物理分离的设备识别到多个 BvS 276 中的至少一个 BvS 276A 可用。一些实施例中，CMM 710 或负载监控器 405 识别到多个 BvS 276 中的 BvS 276A 可用。

[0224] 在步骤 615，设备响应于该识别保持第一虚拟服务器的状态为可用。一些实施例中，设备响应于步骤 610 的识别保持第一虚拟服务器 vS 275A 的状态为可用。多个实施例中，设备响应于步骤 605 的检测保持第一虚拟服务器 vS 275A 的状态为可用。多个实施例中，设备响应于步骤 610 的识别以及步骤 605 的检测保持 vS 275A 的状态为可用。某些实施例中，设备在步骤 615 保持在步骤 605 被识别为不可用的 vS 275A 的状态为可用，同时把被检测为可用的用于备份 vS 275A 的备份虚拟服务器 BvS 276A 当作 vS 275A，或者作为 vS 275A 的一部分，或者使用 BvS 276A 而不是 vS 275A 来执行 vS 275A 的所有功能。一些实施例中，设备可以把在步骤 610 识别为可用的 BvS 276A 视为或者当作可以完全替代并执行 vS 275A 的所有功能或者作为 vS 275A 的一部分的另一个 vS 275A。

[0225] 在步骤 620，设备从一个或多个备份虚拟服务器的第一备份虚拟服务器获得一个或多个指标。一些实施例中，在步骤 620 从 BvS 276 获得的指标可以包括 vS 276 的所有指标。多个实施例中，从 BvS 276 获得的指标是执行负载平衡必须的所选指标。多个实施例中，在步骤 620 从 BvS 276 获得的指标包括用于执行在步骤 605 被检测为不可用的多个虚拟服务器 276 的 BvS 276、vS276A 以及多个虚拟服务器 276 的任何功能所需的任何指标，以确定多个虚拟服务器 276 的负载。一些实施例中，在步骤 620 从 BvS 276 获得的指标可包括用于执行在步骤 605 被检测为不可用的多个虚拟服务器 276 的 BvS 276、vS 276A 以及多个虚拟服务器 276 的任何功能所需的任何指标，以确定多个虚拟服务器 276 和 BvS 276 的负载。

[0226] 在步骤 625，设备使用从第一备份虚拟服务器获得的指标来确定多个虚拟服务器的负载。一些实施例中，在步骤 625 确定多个虚拟服务器 276 的负载可包括 BvS 276 提供指标，同时不考虑所进行的检测而保持在步骤 605 被检测为不可用的第一虚拟服务器 vS 275A 的状态为可用。一些实施例中，确定多个虚拟服务器的负载可包括辅助任意多个虚拟服务器 275 的任意多个备份虚拟服务器 276 的负载。

[0227] 本领域的技术人员在不偏离本发明的精神和范围的前提下可以进行很多变化和修改。因而，清楚的是，上述任何实施例可以与上述任意其他实施例组合用于表达本发明的任何其他方面。因此，必须清楚理解所示说明性实施例仅是出于示范目的，而不应被看作是限制本发明，本发明由下面的权利要求限定。这些权利要求将被视作包括不仅它们在字面上所阐述的，还包括非实质区别的那些等价元素，尽管它们在除上面的说明中所显示和描述的其它方面上不完全相同。

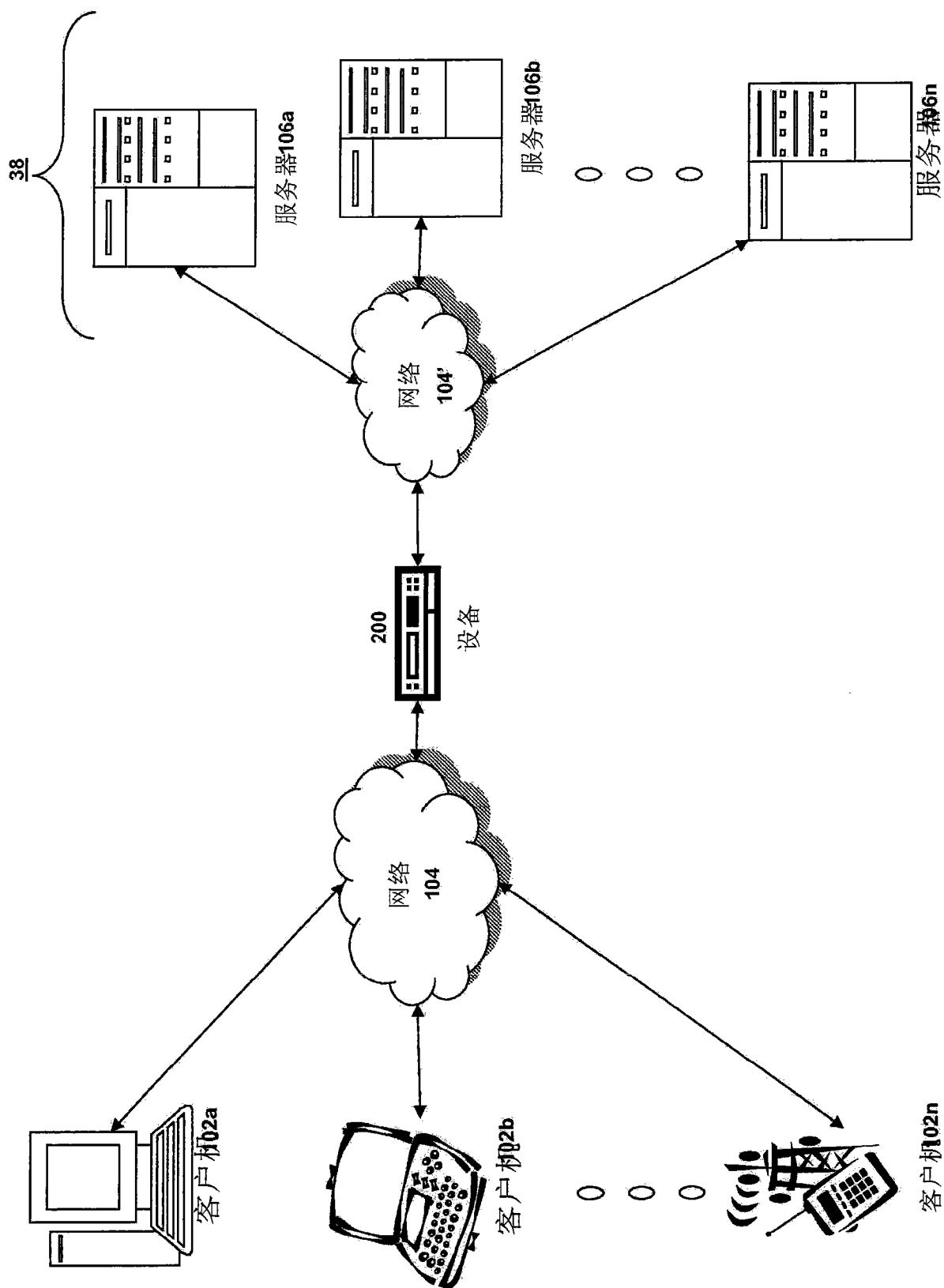


图 1A

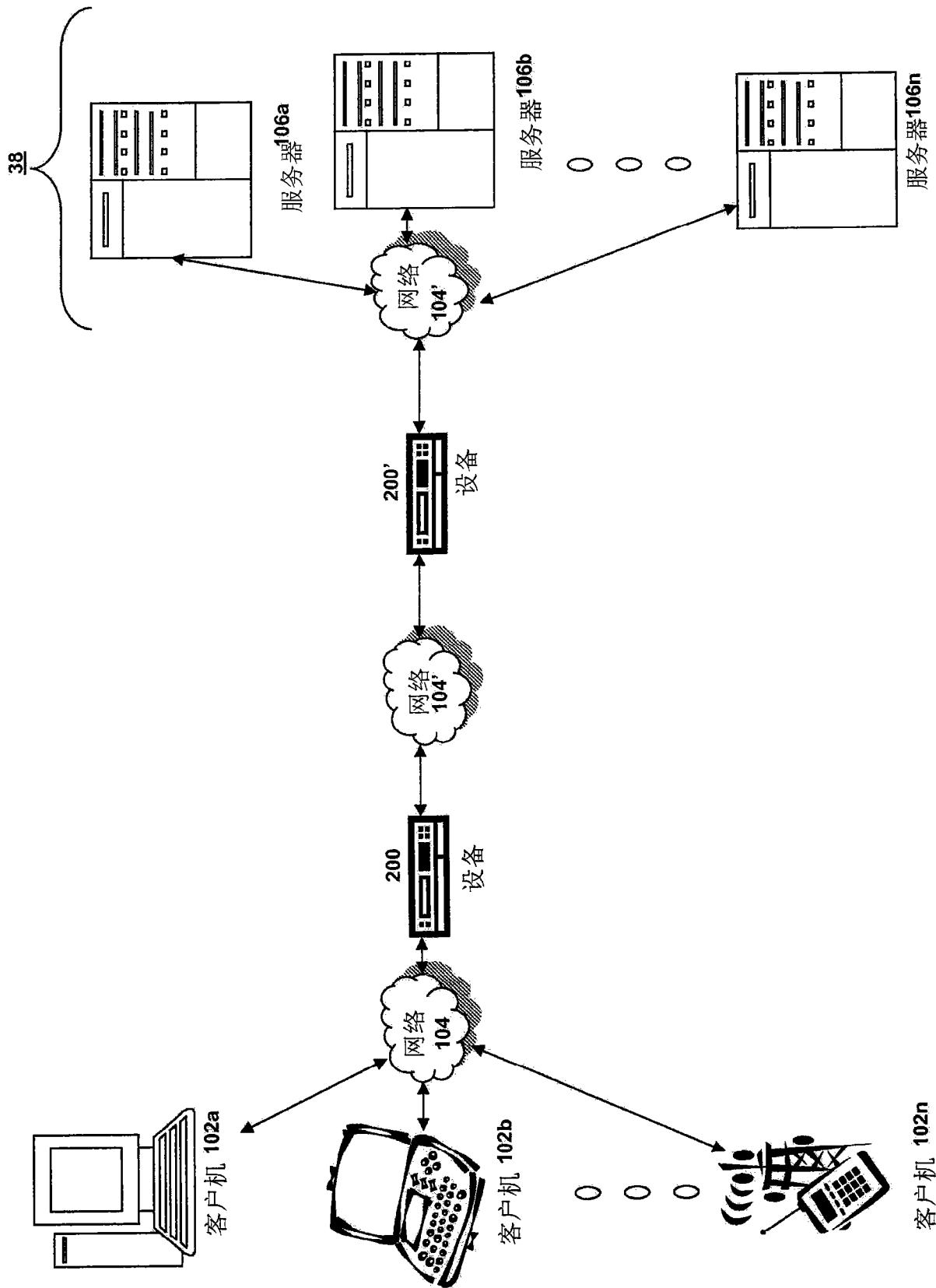


图 1B

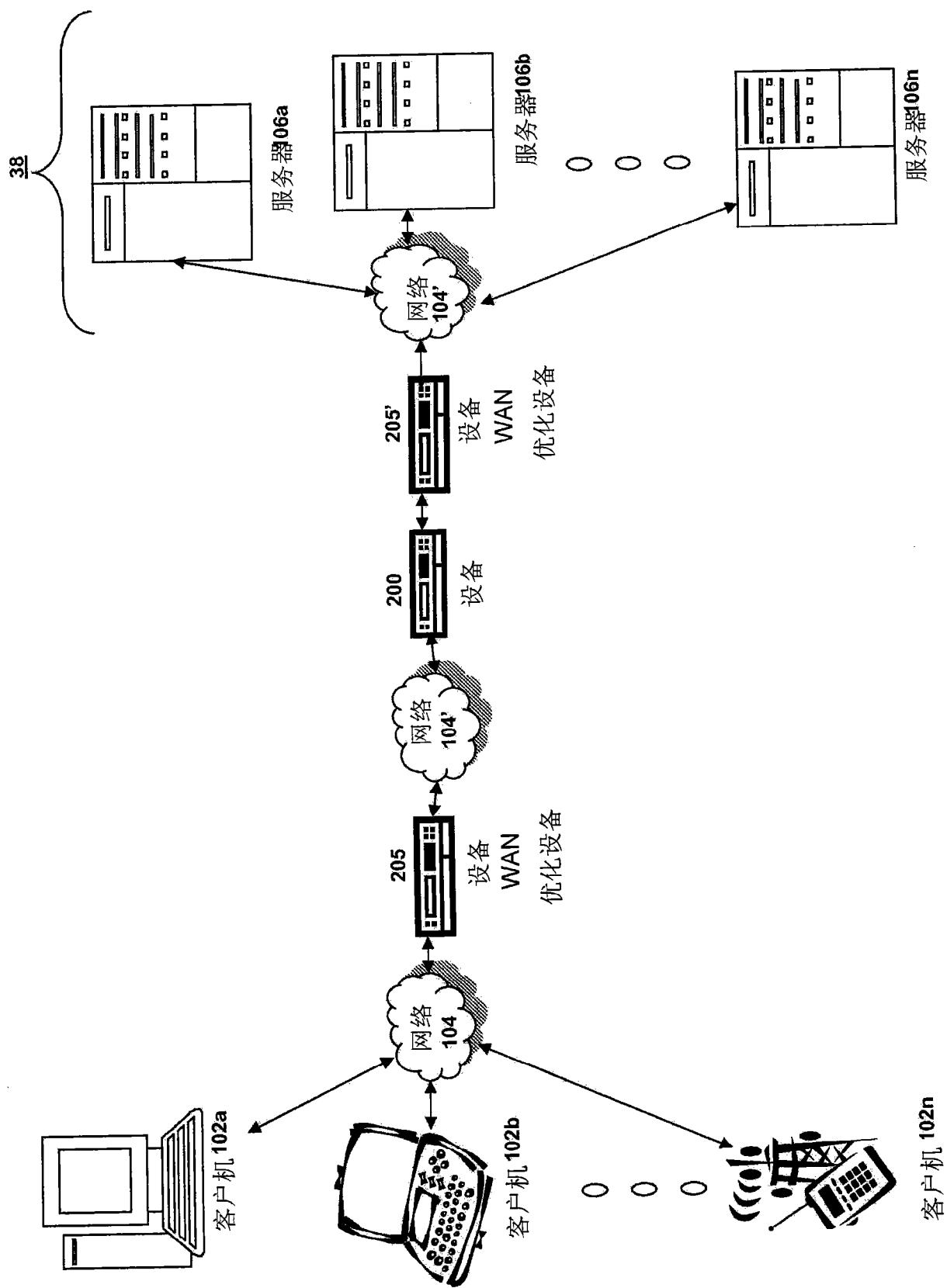


图 1C

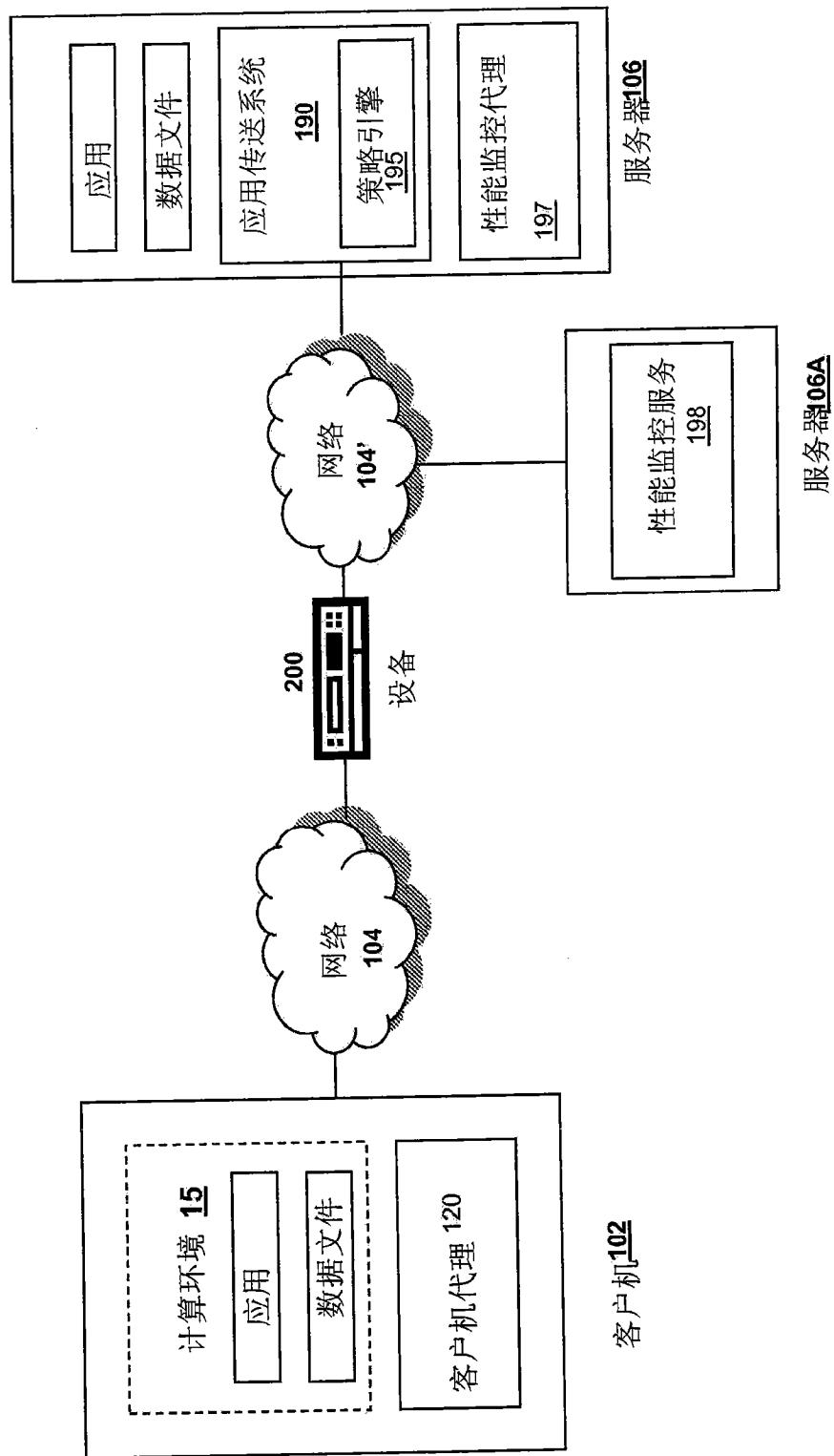


图 1D

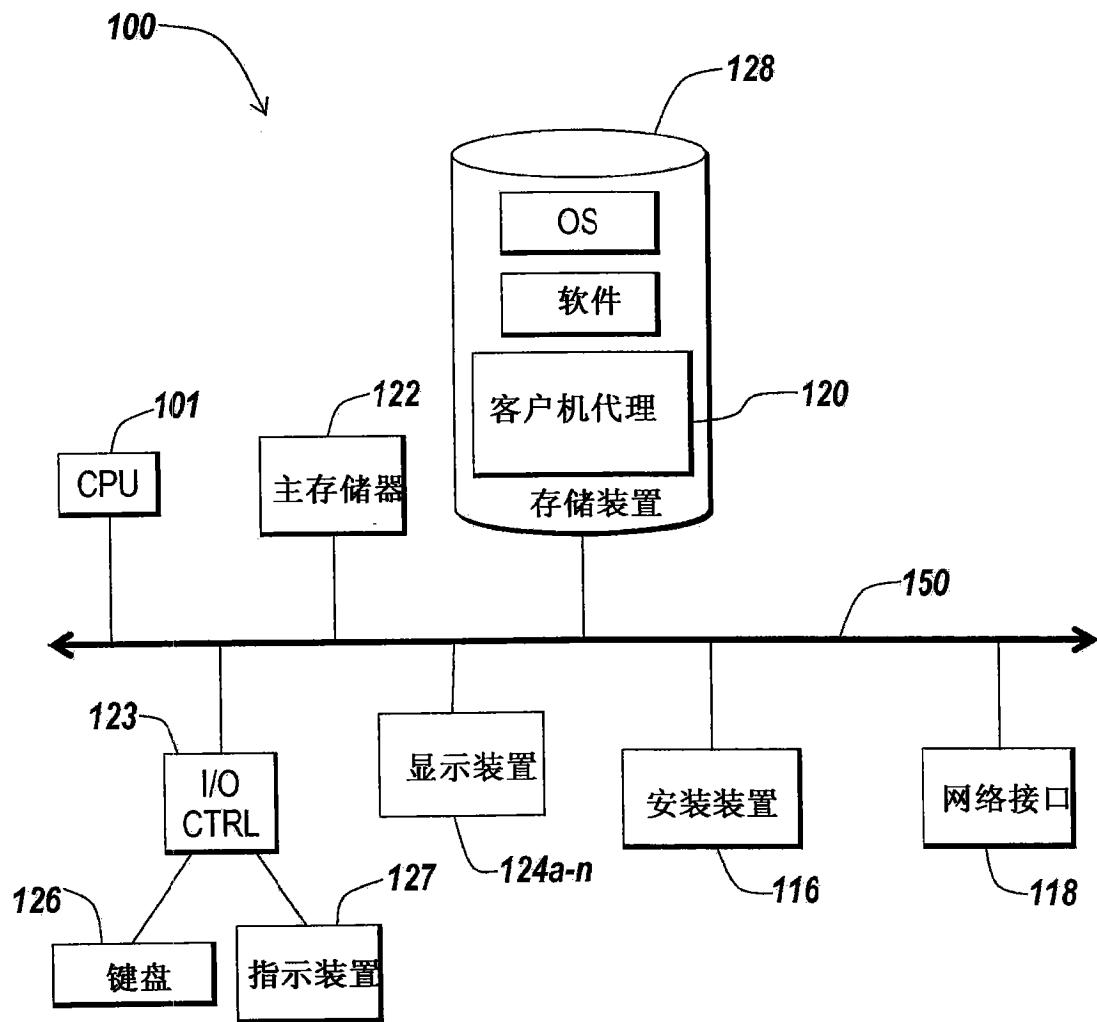


图 1E

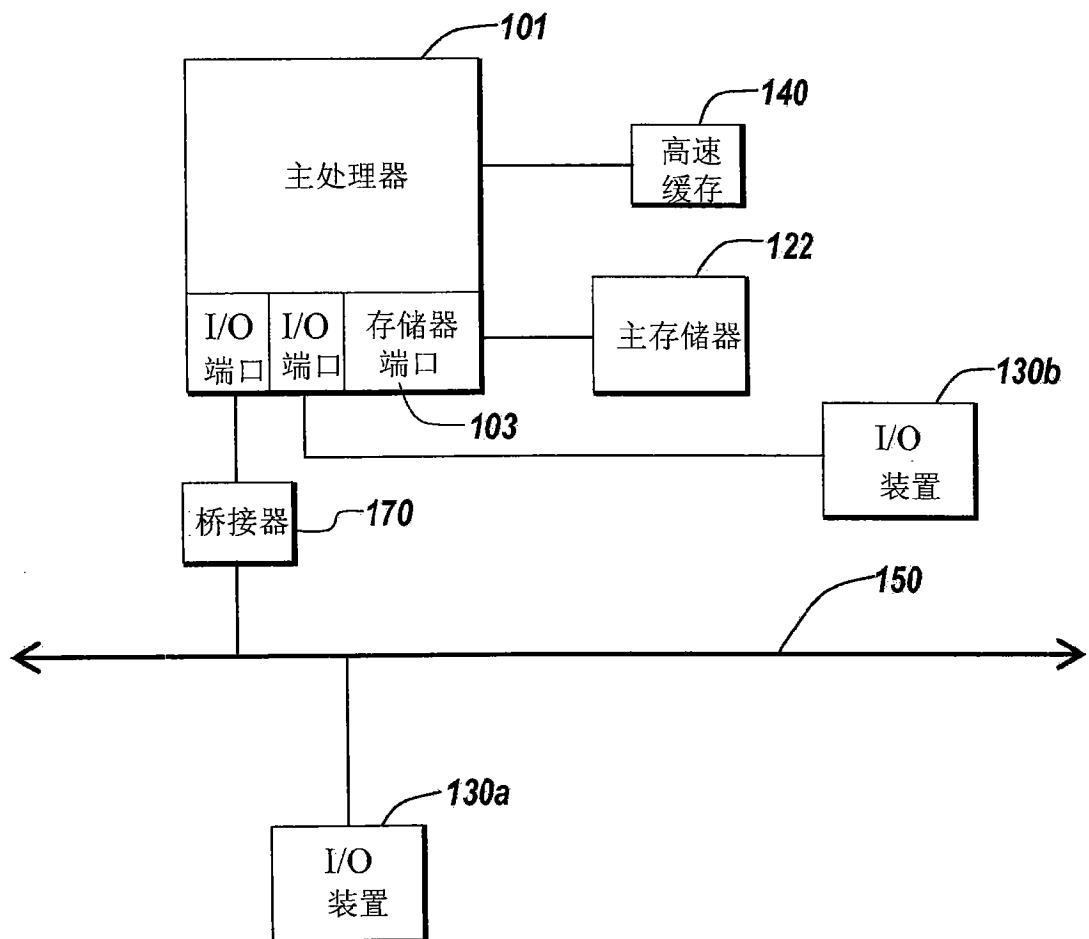


图 1F

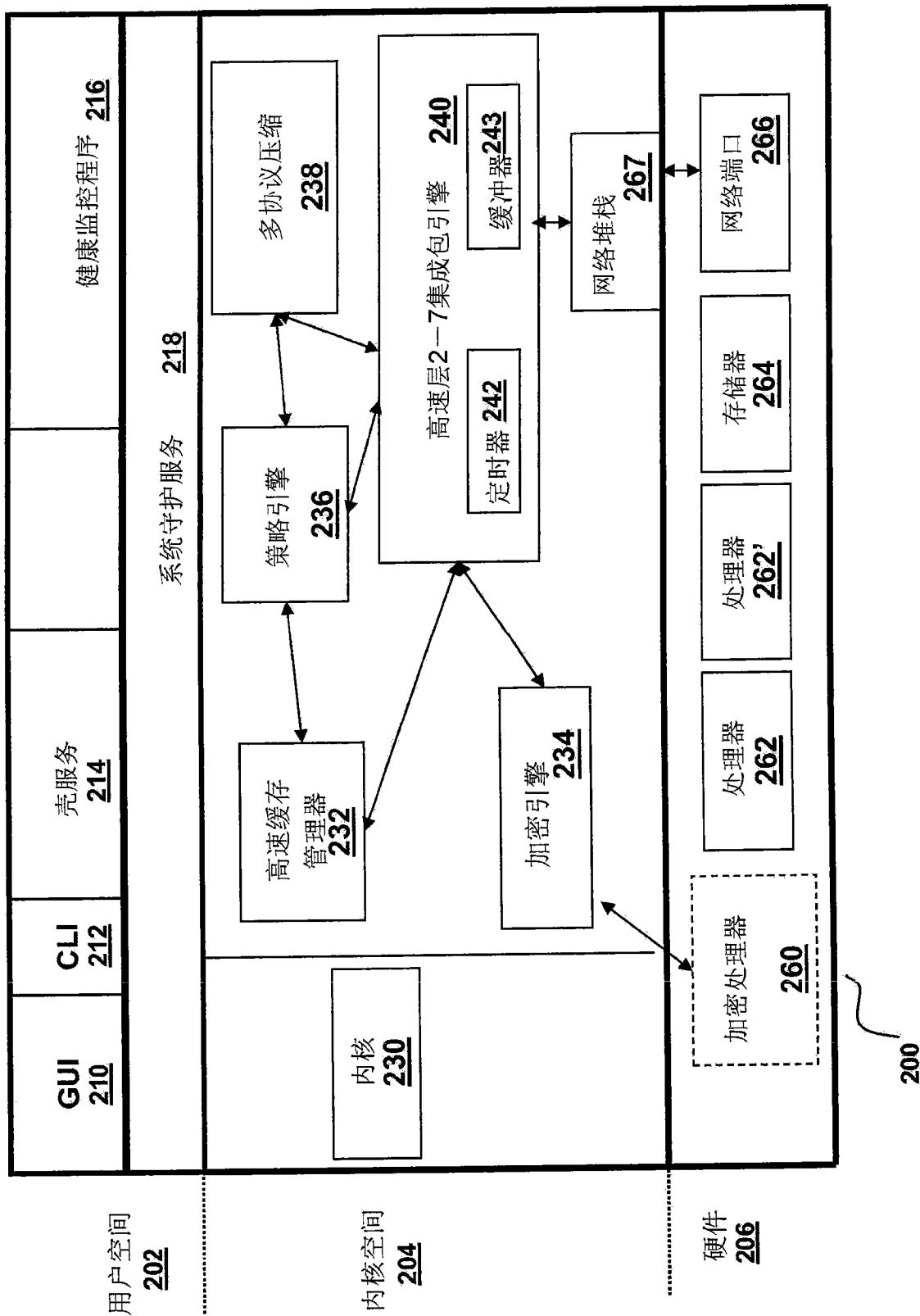


图 2A

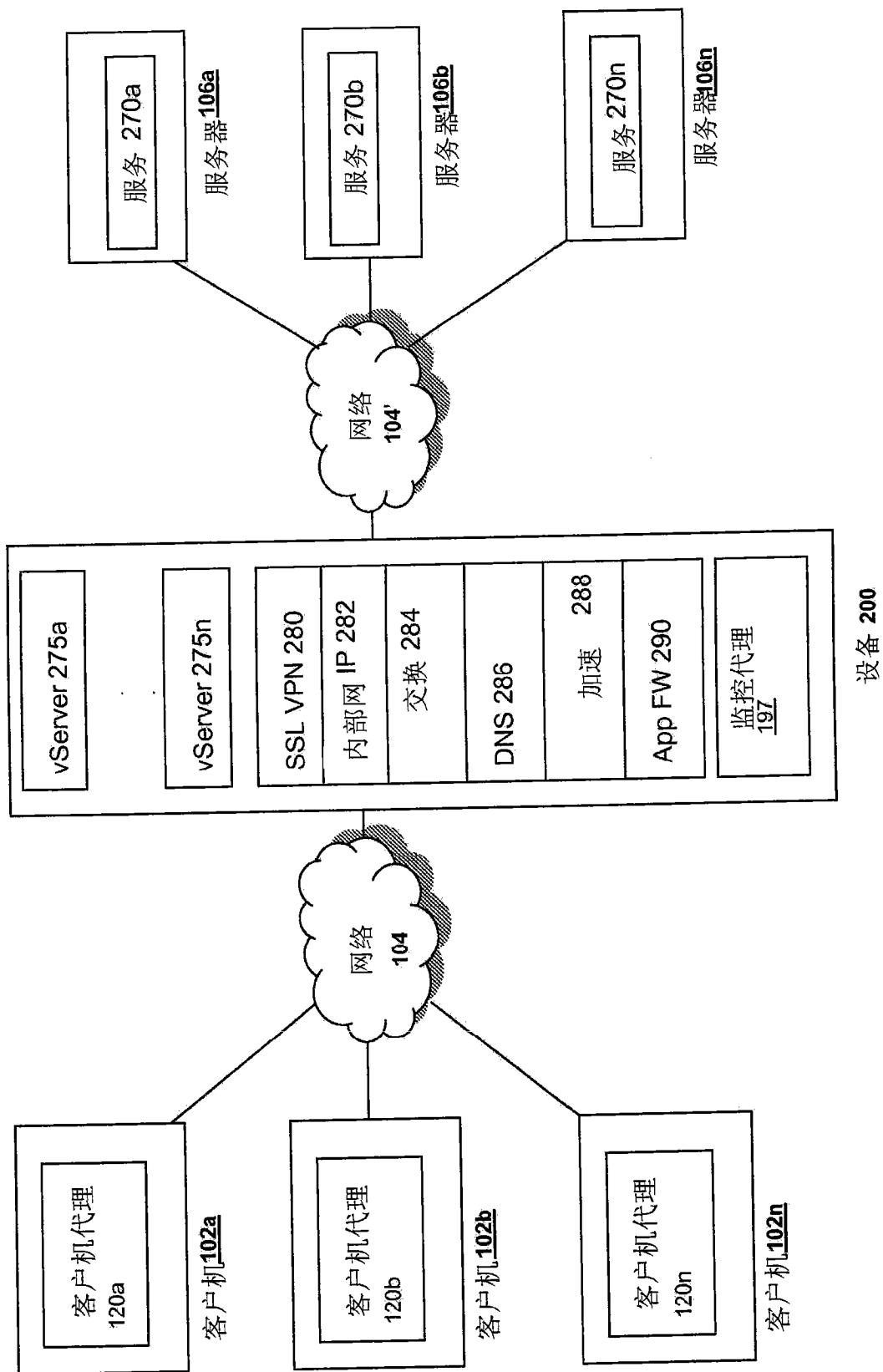


图 2B

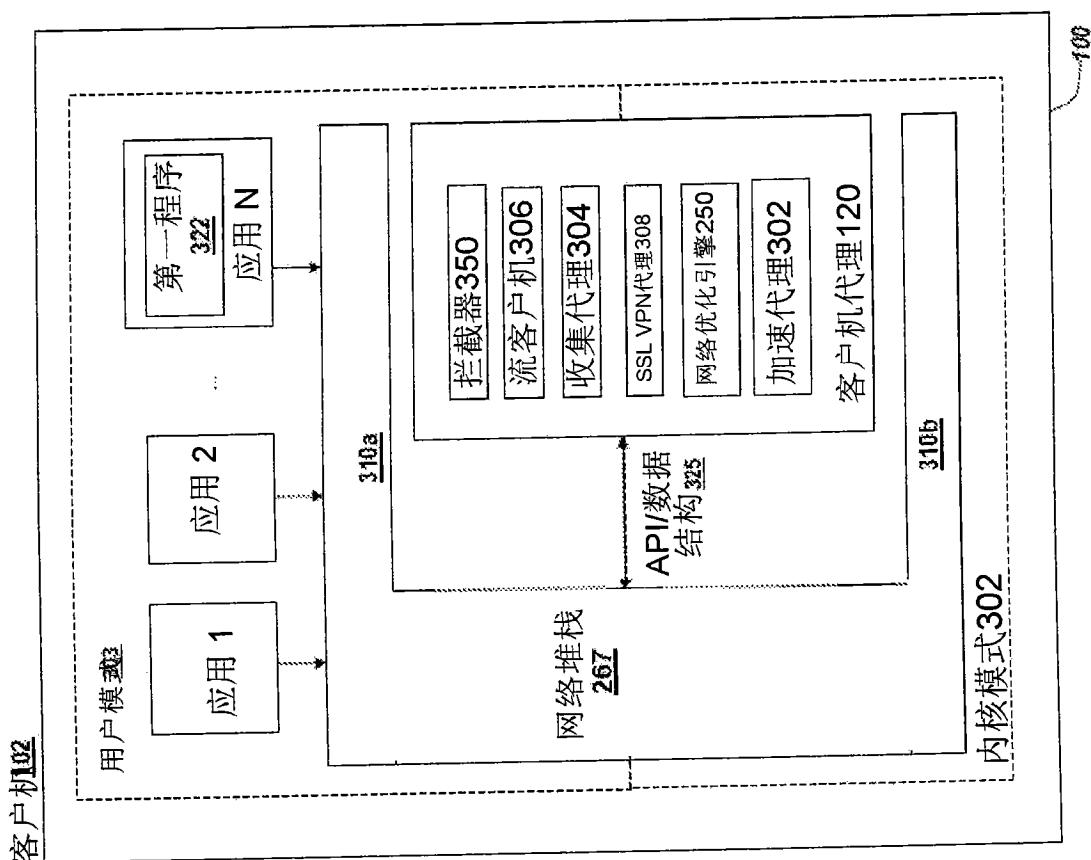


图 3

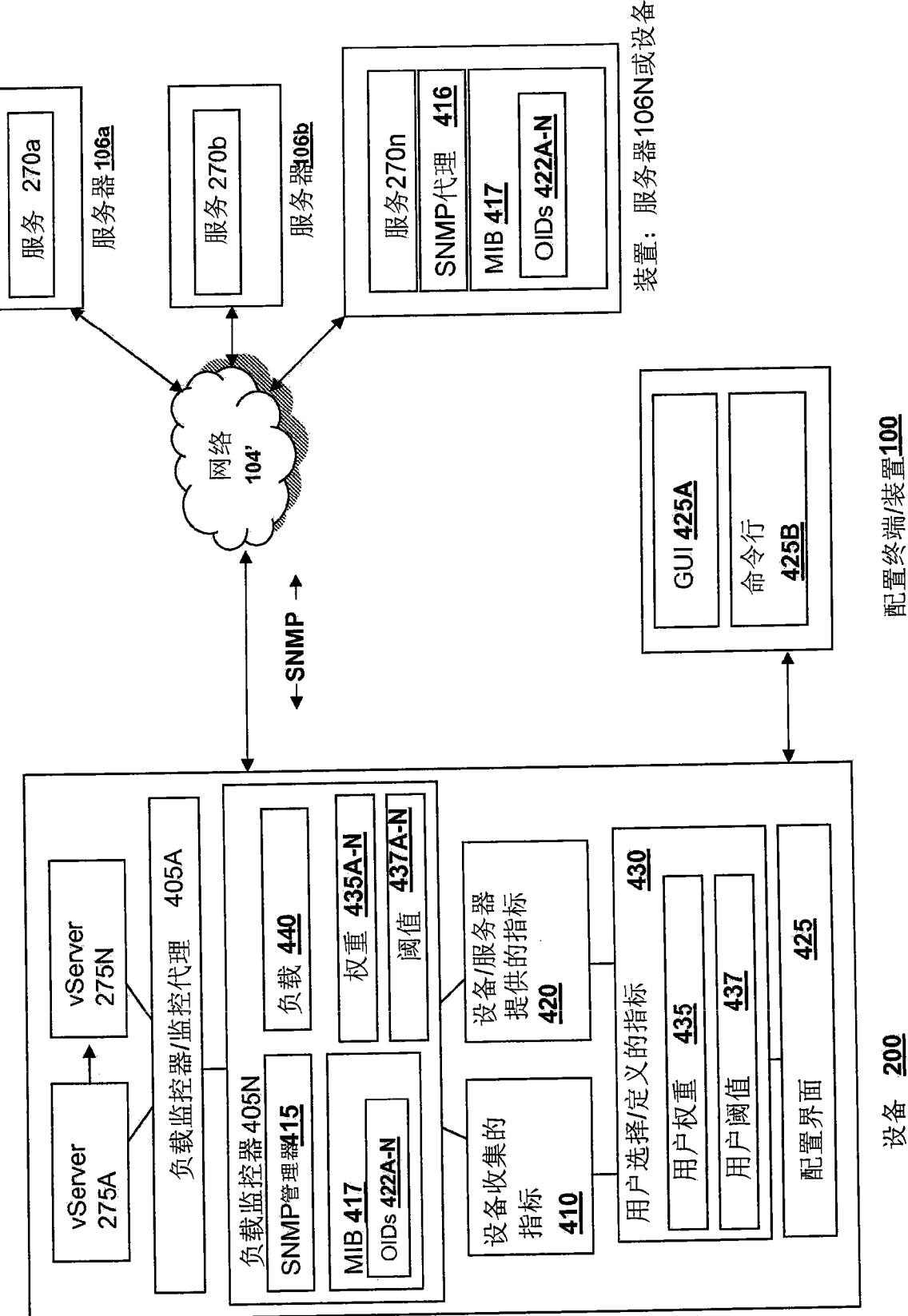


图 4

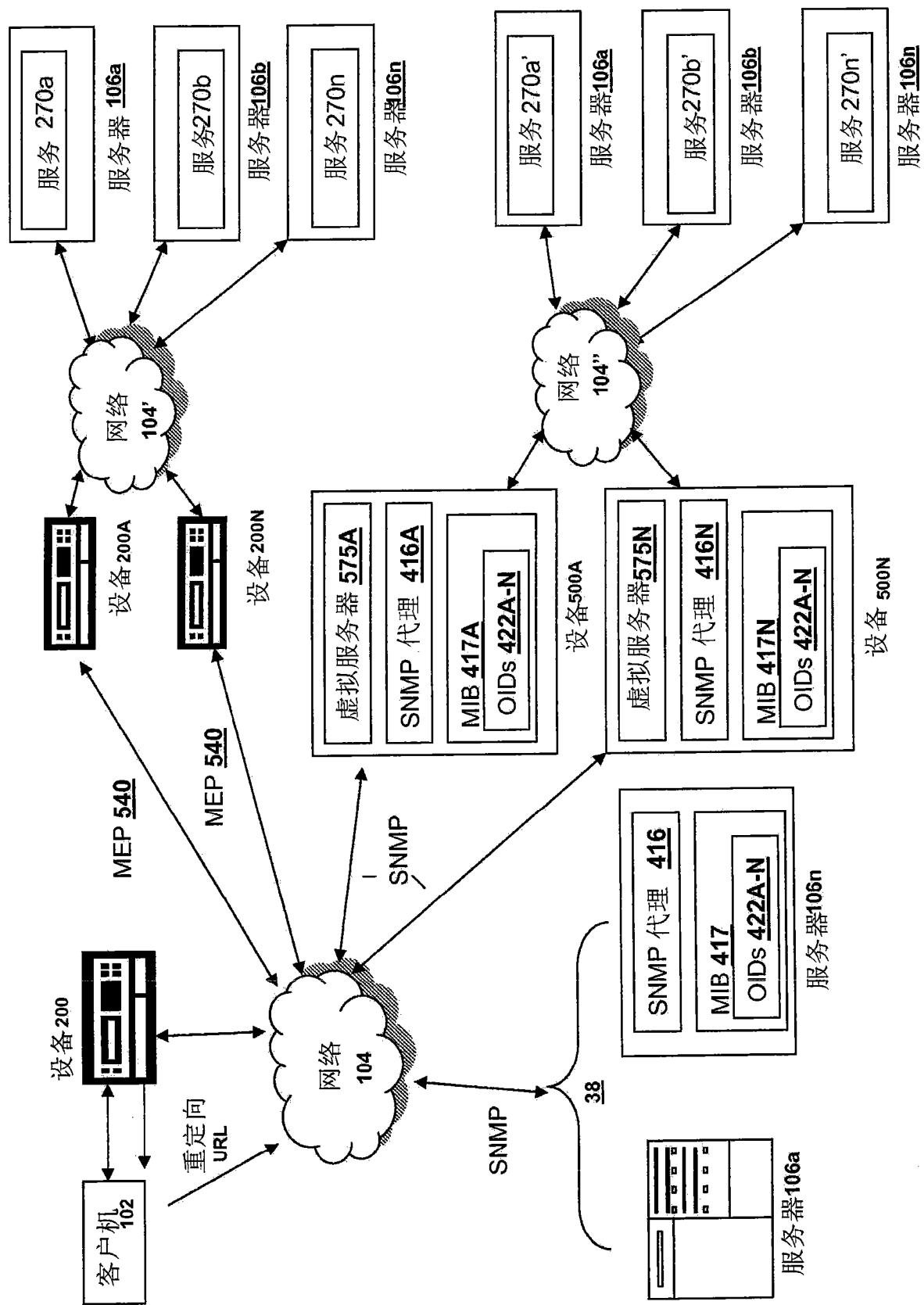


图 5A

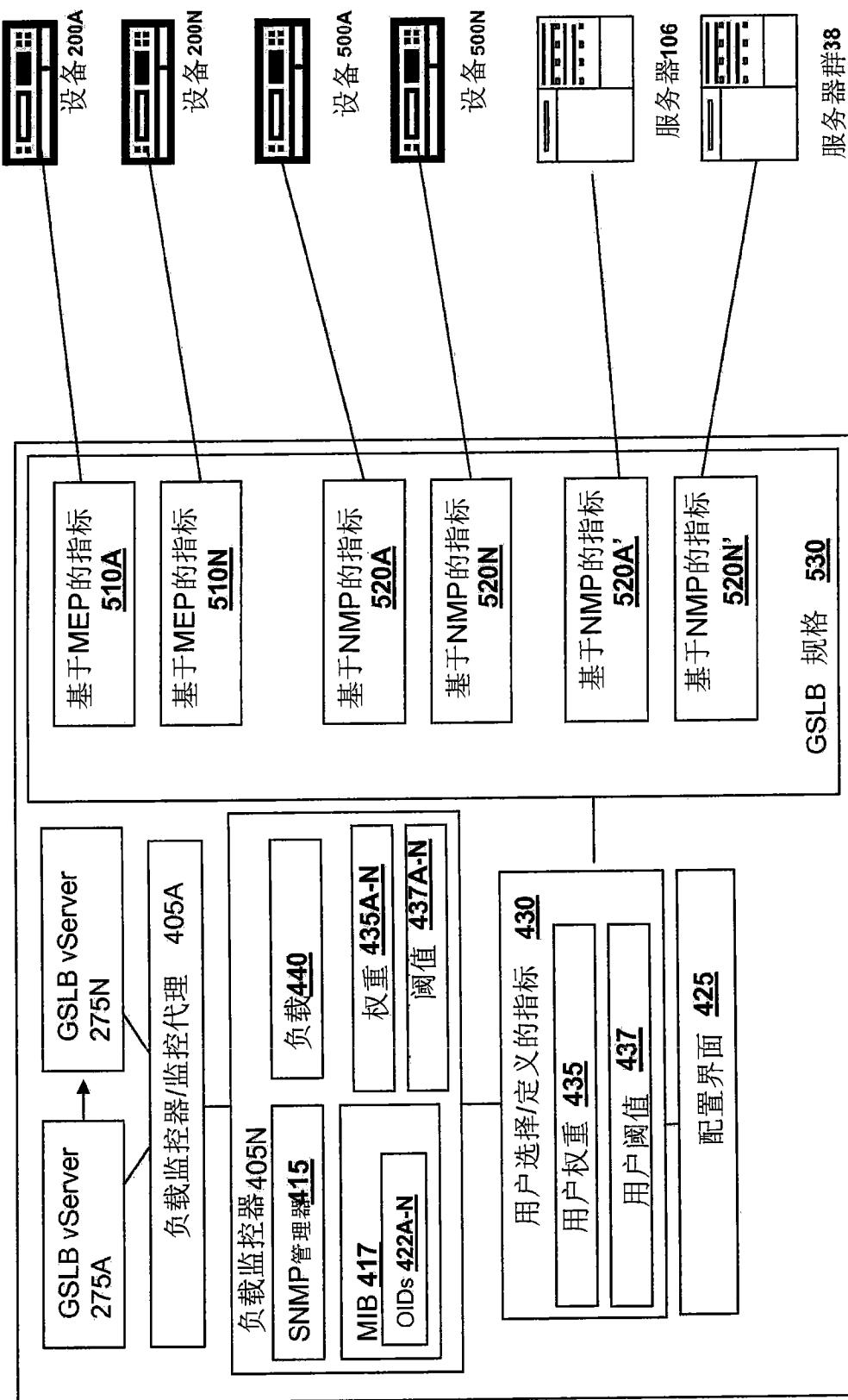


图 5B

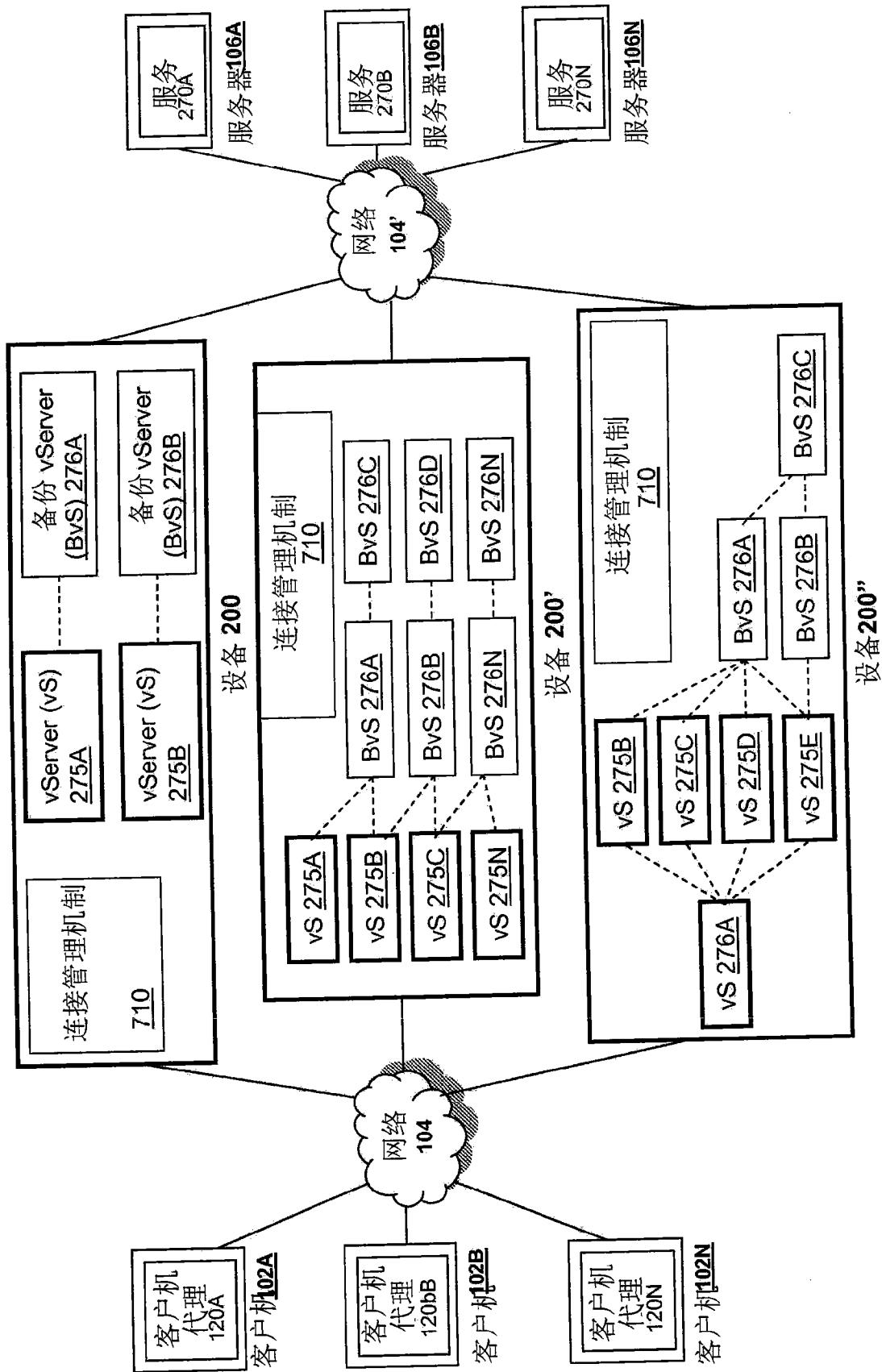


图 6A

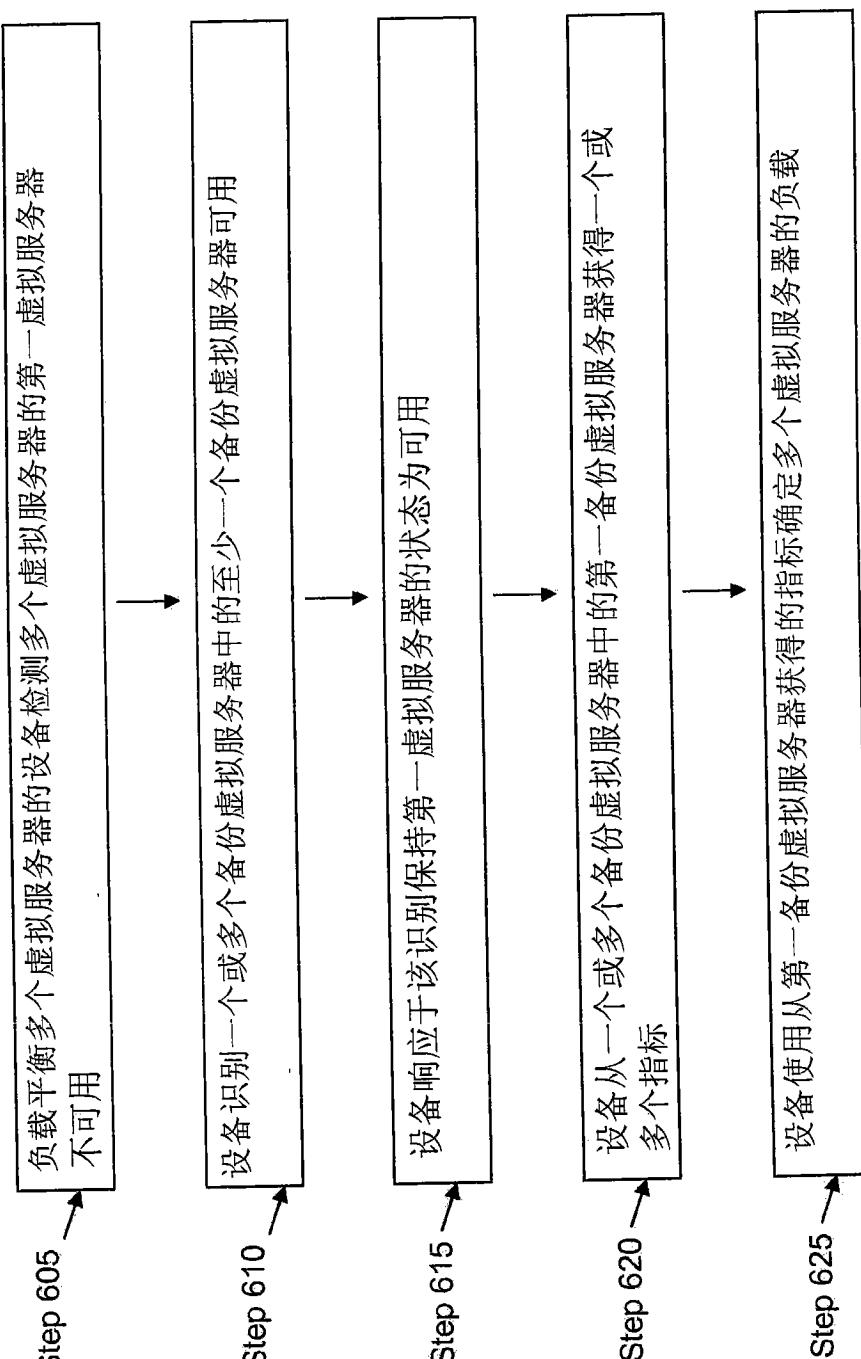
方法 600

图 6B