



[12] 发明专利说明书

专利号 ZL 02828446.1

[45] 授权公告日 2007 年 4 月 18 日

[11] 授权公告号 CN 1311326C

[22] 申请日 2002.12.23 [21] 申请号 02828446.1

[30] 优先权

[32] 2002.1.9 [33] US [31] 10/045,883

[86] 国际申请 PCT/US2002/041079 2002.12.23

[87] 国际公布 WO2003/060688 英 2003.7.24

[85] 进入国家阶段日期 2004.9.2

[73] 专利权人 思科技术公司

地址 美国加利福尼亚州

[72] 发明人 桑贾亚·库马尔 马纳斯·巴鲁阿
约翰·L·伯内特

[56] 参考文献

WO0180013A1 2001.10.25

审查员 赵小宁

[74] 专利代理机构 北京东方亿思知识产权代理有限公司

代理人 王 怡

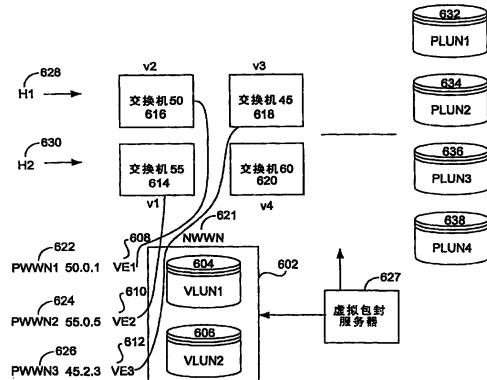
权利要求书 8 页 说明书 26 页 附图 14 页

[54] 发明名称

通过虚拟包封在存储区域网络内实现存储虚
拟化的方法和装置

[57] 摘要

本发明公开了用于在存储区域网络的网络设备上实现存储虚拟化的方法和装置。创建虚拟包封，使其具有一个或多个虚拟包封端口，并适于表示一个或多个存储虚拟单元。每个虚拟存储单元都表示存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置。虚拟包封的每个虚拟包封端口都与存储区域网络内的网络设备的端口相关联。然后向每个虚拟包封端口分配地址或标识符。



1. 一种在存储区域网络内实现存储虚拟化的方法，包括：

创建虚拟包封，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；

将所述虚拟包封的虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联，以使得所述存储区域网络内的一个或多个网络设备与所述虚拟端口相关联；以及

向所述虚拟端口中的每一个都分配地址或标识符；

其中“将所述虚拟包封的所述虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联”包括从第一网络设备向所述存储区域网络内的第二网络设备的物理端口发送消息，以指示所述第二网络设备的物理端口去处理指向分配给所述关联虚拟端口的地址或标识符的消息，从而使得所述第一网络设备指示所述第二网络设备的物理端口代表所述虚拟端口进行操作。

2. 如权利要求 1 所述的方法，还包括：

选择要被包括在所述虚拟包封中的虚拟端口数量。

3. 如权利要求 1 所述的方法，其中，“将所述虚拟包封的所述虚拟端口中的每一个都与所述存储区域网络内的第二网络设备的端口相关联”包括：

将所述虚拟端口与所述存储区域网络内的一个或多个网络设备的端口相关联。

4. 如权利要求 1 所述的方法，还包括：

将一个或多个虚拟存储单元分配到所述虚拟包封。

5. 如权利要求 4 所述的方法，其中，所述一个或多个虚拟存储单元中的每一个都包括 VLUN 或所述存储区域网络上的存储的其他虚拟表示。

6. 一种在存储区域网络内实现存储虚拟化的装置，包括：

用于创建虚拟包封的装置，所述虚拟包封具有一个或多个虚拟端口，

并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；

用于将所述虚拟包封的虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联，以使得所述存储区域网络内的一个或多个网络设备与所述虚拟端口相关联的装置；以及

用于向所述虚拟端口中的每一个都分配地址或标识符的装置；

其中所述用于将所述虚拟包封的虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联的装置包括用于从第一网络设备向所述存储区域网络内的第二网络设备的物理端口发送消息，以指示所述第二网络设备的物理端口去处理指向分配给所述关联虚拟端口的地址或标识符的消息，从而使得所述第一网络设备指示所述第二网络设备的物理端口代表所述虚拟端口进行操作的装置。

7. 一种适于在存储区域网络内实现存储虚拟化的网络设备，包括：

处理器；以及

存储器，所述处理器和存储器中至少有一个适于：

创建虚拟包封，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；

将所述虚拟包封的虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联，以使得所述存储区域网络内的一个或多个网络设备与所述虚拟端口相关联；并且

向所述虚拟端口中的每一个都分配地址或标识符；

其中“将所述虚拟包封的所述虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联”包括从第一网络设备向所述存储区域网络内的第二网络设备的物理端口发送消息，以指示所述第二网络设备的物理端口去处理指向分配给所述关联虚拟端口的地址或标识符的消息，从而使得所述第一网络设备指示所述第二网络设备的物理端口代表所述虚拟端口进行操作。

8. 如权利要求 7 所述的网络设备，其中所述存储区域网络是虚拟存储区域网络。

9. 如权利要求 7 所述的网络设备，其中节点全球范围名称与所述虚拟包封相关联。

10. 如权利要求 7 所述的网络设备，其中端口全球范围名称被分配给所述虚拟端口中的每一个，以使得所述端口全球范围名称与所述存储区域网络内的网络设备的关联物理端口相关联。

11. 如权利要求 7 所述的网络设备，其中，所述存储区域网络内的第二网络设备的物理端口是光纤信道设备的端口。

12. 如权利要求 7 所述的网络设备，其中 FCID 被分配给所述虚拟端口中的每一个。

13. 如权利要求 7 所述的网络设备，其中，所述虚拟包封的虚拟端口数量大于所述存储区域网络内的每个网络设备的端口数量。

14. 如权利要求 7 所述的网络设备，其中，“将所述虚拟包封的所述虚拟端口中的每一个都与所述存储区域网络内的网络设备的端口相关联”包括：

向所述存储区域网络内的网络设备的端口发送绑定消息，以将所述存储区域网络内的网络设备的端口绑定到所述虚拟端口中的一个或多个。

15. 如权利要求 14 所述的网络设备，还包括：

向所述存储区域网络内的一个或多个网络设备的一个或多个其他端口发送陷入消息，以指示所述存储区域网络内的一个或多个网络设备的一个或多个其他端口去陷入指向所述虚拟端口之一的消息。

16. 如权利要求 7 所述的网络设备，其中所述虚拟存储单元中的一个或多个中的每一个都包括 VLUN 或所述存储区域网络上的存储的其他虚拟表示。

17. 一种在存储区域网络内进行 LUN 映射的方法，包括：

访问具有一个或多个条目的 LUN 映射表，所述条目中的每一个都标识出所述存储区域网络内的发起者、虚拟包封中的一个或多个虚拟端口构成的组中的一个或多个虚拟端口，并且所述条目还将所指定的逻辑单元与

一个或多个虚拟存储单元相关联，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置，其中所述虚拟包封适于表示所述的由一个或多个虚拟存储单元构成的组，并且每个所述虚拟端口都与所述存储区域网络内的网络设备的端口相关联，其中所述网络设备的物理端口已从另一网络设备接收到消息，所述消息指示所述物理端口去处理指向所述关联虚拟端口的消息；以及

当通过所述关联虚拟端口之一，从所述发起者接收到对所指定的逻辑单元的请求时，标识出所述 LUN 映射表中的条目之一，并利用该条目中指定的一个或多个虚拟存储单元来服务于该请求。

18. 一种在第一网络设备中的用于在存储区域网络内实现存储虚拟化的方法，包括：

向所述存储区域网络内的第二网络设备的物理端口发送虚拟化消息，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；以及

响应于所述虚拟化消息，从所述第二网络设备的所述物理端口接收虚拟化响应。

19. 如权利要求 18 所述的方法，还包括：

接收分配给所述虚拟端口的地址或标识符。

20. 如权利要求 18 所述的方法，其中所述虚拟化消息表明所述物理端口将处理指向分配给所述虚拟端口的地址或标识符的消息。

21. 如权利要求 20 所述的方法，其中所述地址或标识符是 FCID。

22. 一种适于在存储区域网络内的第一网络设备中实现存储虚拟化的装置，包括：

用于向所述存储区域网络内的第二网络设备的物理端口发送虚拟化消息的装置，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络

的一个或多个物理存储单元上的一个或多个物理存储位置；以及
用于响应于所述虚拟化消息，从所述第二网络设备的所述物理端口接收虚拟化响应的装置。

23. 一种适于在存储区域网络内的第一网络设备中实现存储虚拟化的装置，包括：

处理器；

存储器，所述处理器和存储器中至少有一个适于：

向所述存储区域网络内的第二网络设备的物理端口发送虚拟化消息，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；并且

响应于所述虚拟化消息，从所述第二网络设备的所述物理端口接收虚拟化响应。

24. 如权利要求 23 所述的装置，其中所述虚拟端口由 NWWN 和 PWWN 来标识。

25. 如权利要求 23 所述的装置，其中所述虚拟化响应表明所述物理端口被配置成处理指向所述虚拟包封的虚拟端口的消息。

26. 如权利要求 23 所述的装置，其中所述虚拟化消息表明所述物理端口要获得分配给所述虚拟端口的地址或标识符。

27. 如权利要求 26 所述的装置，其中所述虚拟化消息是绑定消息或陷入消息。

28. 如权利要求 26 所述的装置，其中所述虚拟化响应包括分配给所述虚拟端口的地址或标识符。

29. 如权利要求 23 所述的装置，其中所述虚拟化消息表明所述物理端口要从 DNS 服务器获得分配给所述虚拟端口的地址或标识符。

30. 如权利要求 26 所述的装置，其中所述地址或标识符是 FCID。

31. 一种在存储区域网络内的第一网络设备中实现存储虚拟化的方法，包括：

在所述第一网络设备的物理端口处接收来自所述存储区域网络内的第二网络设备的虚拟化消息，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；以及

响应于所述虚拟化消息，从所述第一网络设备的所述物理端口发送虚拟化响应到所述第二网络设备。

32. 如权利要求 31 所述的方法，还包括：

获得并存储分配给所述虚拟端口的所述地址或标识符。

33. 如权利要求 32 所述的方法，还包括：

发送分配给所述虚拟端口的地址或标识符。

34. 如权利要求 32 所述的方法，其中所述地址或标识符是 FCID。

35. 如权利要求 31 所述的方法，还包括：

处理指向分配给所述虚拟端口的地址或标识符的消息。

36. 如权利要求 31 所述的方法，还包括：

处理指向所述虚拟包封的虚拟端口的消息。

37. 如权利要求 32 所述的方法，还包括：

处理指向分配给所述虚拟端口的地址或标识符的消息。

38. 如权利要求 31 所述的方法，还包括：

接收一个报告消息，该消息请求标识出由分配给所述虚拟端口之一的地址或标识符所支持的虚拟存储单元中的一个或多个；以及

发送应答消息，该消息标识了所述虚拟存储单元中的一个或多个。

39. 如权利要求 38 所述的方法，其中所述标识符或地址是 FCID。

40. 如权利要求 38 所述的方法，其中，所述应答消息中所标识出的虚拟存储单元中的一个或多个是对发送所述报告消息的发起者来说可见的那些虚拟存储单元。

41. 一种适于在存储区域网络内的第一网络设备中实现存储虚拟化的网络设备，包括：

用于在第一网络设备的物理端口处接收来自所述存储区域网络内的第二网络设备的虚拟化消息的装置，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；以及

用于响应于所述虚拟化消息，从所述第一网络设备的所述物理端口向所述第二网络设备发送虚拟化响应的装置。

42. 一种适于在存储区域网络内的第一网络设备中实现存储虚拟化的网络设备，包括：

处理器；以及

存储器，所述处理器和存储器中至少有一个适于：

在第一网络设备的物理端口处接收来自所述存储区域网络内的第二网络设备的虚拟化消息，所述虚拟化消息指示所述物理端口处理指向虚拟包封的虚拟端口的消息，所述虚拟包封具有一个或多个虚拟端口，并适于表示一个或多个虚拟存储单元，所述虚拟存储单元中的每一个都表示所述存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置；并且

响应于所述虚拟化消息，从所述第一网络设备的所述物理端口向所述第二网络设备发送虚拟化响应。

43. 如权利要求 42 所述的网络设备，其中，所述虚拟化消息表明所述物理端口要获得分配给所述虚拟端口的地址或标识符。

44. 如权利要求 42 所述的网络设备，其中，所述虚拟化消息表明所述物理端口要从 DNS 服务器获得分配给所述虚拟端口的地址或标识符。

45. 如权利要求 42 所述的网络设备，其中，所述虚拟化消息表明所述物理端口将处理指向分配给所述虚拟端口的地址或标识符的消息。

46. 如权利要求 45 所述的网络设备，其中所述地址或标识符是 FCID。

47. 如权利要求 42 所述的网络设备，其中，所述虚拟存储单元中的一

个或多个包括 VLUN 或所述存储区域网络上的存储的其他虚拟表示。

通过虚拟包封在存储区域网络内实现存储虚拟化的方法和装置

技术领域

本发明涉及网络技术。更具体地说，本发明涉及支持存储区域网络内的存储虚拟化的方法和装置。

背景技术

近年来，存储设备的容量的增长速度未能赶上对存储的需求的增长。因此，一个给定的服务器或其他主机必须访问多个物理上不同的存储节点（一般是磁盘）。为了解决这些存储限制，开发了存储区域网络（SAN）。一般地说，存储区域网络是一种高速专用网络，其代表一个更大的用户网络而互连不同的数据存储设备和关联数据主机。然而，尽管 SAN 使得存储设备可被配置为供网络内的不同网络设备和/或实体使用，但是数据存储需求却经常是动态而非静态的。

图 1A 示出了一种示例性的传统存储区域网络。更具体地说，在存储区域网络 102 内，可以将一组主机（例如服务器或工作站）104、106、108 耦合到存储设备（例如磁盘）池。按 SCSI 的话说，主机可被看作为“发起者”，而存储设备可看作为“目标”。例如，可通过一组存储阵列或磁盘阵列 110、112、114 来实现存储池。每个磁盘阵列 110、112、114 还对应于一组磁盘。在这一示例中，第一磁盘阵列 110 对应于磁盘 116、118，第二磁盘阵列 112 对应于磁盘 120，而第三磁盘阵列 114 对应于磁盘 122、124。不是让所有主机 104—108 都可访问所有磁盘 116—124，而是需要通过磁盘阵列 110、112、114 而对每个主机 104—108 实现存储（例如磁盘）的动态和不可见的分配。也就是说，可通过虚拟存储器（例如虚拟磁盘）的概念来分配物理存储器（例如物理磁盘）。这使得可将异构的发起者连接到分布式的异构目标组（存储池），其连接方式可实现存储的动态和透明分配。

虚拟存储器的概念传统上已被用于通过在物理存储器中的物理地址和虚拟存储器中的虚拟地址之间的翻译来实现物理存储器的虚拟化。近来，

“虚拟化”的概念已通过各种机制而实现在存储区域网络中。虚拟化在存储网络上实现物理存储和虚拟存储的相互转换。主机（发起者）将虚拟磁盘视为目标。虚拟磁盘以已定义但具有一定灵活性的方式来表示可用的物理存储。虚拟化向主机提供了可用物理存储的一种表示，其不受限于存储的特定物理设置/分配。

一种早期技术即独立磁盘冗余阵列（RAID）提供了虚拟化的一些受限特征。已实现若干 RAID 子类型。在 RAID1 中，一个虚拟磁盘可对应于两个存储了相同数据（或支持相同数据的恢复）的物理磁盘 116、118，从而可在存储区域网络内支持冗余。在 RAID0 中，单个虚拟磁盘分片在多个物理磁盘上。一些其他的虚拟化包括级联（concatenation）、备用（sparing）等等。虚拟化的一些方面近来已通过在存储区域网络内的各种位置内的虚拟化功能而实现了。三种这样的位置已获得一定程度的接受：主机（例如 104—108）中的虚拟化、磁盘阵列或存储阵列（例如 110—114）中的虚拟化以及独立于主机和存储池的存储用具 126 中的虚拟化。不幸地是，这些实现方案中的每一种都具有一些不期望的性能限制。

存储阵列中的虚拟化是如今所使用的最常见的存储虚拟化方案之一。通过这一方法，可以在特定存储子系统（例如磁盘阵列）的存储空间上创建多个虚拟卷。在存储子系统级上创建虚拟卷提供了主机独立性，这是因为存储池的虚拟化对主机来说是不可见的。另外，存储系统级的虚拟化可实现存储器访问的优化，因而可获得高性能。然而，这一虚拟化方案一般只可对同构存储环境实现统一的管理结构，甚至只具有有限的灵活度。而且，由于虚拟化是在存储子系统层级上执行的，因此在存储子系统级上设置的物理-虚拟限制被强加到存储区域网络中的所有主机上。而且，每个存储子系统（或磁盘阵列）是独立地进行管理。因此，存储级的虚拟化很少使得虚拟卷可跨越多个存储子系统（例如磁盘阵列），因此限制了基于存储的方法的可扩展性。

当在每个主机上实现虚拟化时，可以跨越多个存储子系统（例如磁盘

阵列）。基于主机的方法具有一个额外的优点，即对一个主机的限制不影响存储区域网络中其他主机的运行。然而，主机级的虚拟化需要有一个运行在每个主机（例如服务器）上来实现虚拟化功能的软件层。因此，这一软件的运行影响了运行这一软件的主机的性能。这一方法的另一主要难点在于它将可用的存储提前划分给不同的主机。由于这一划分是在主机级上支持的，并且每个主机的虚拟化功能独立于存储区域网络内其他主机地执行，因此难于在各主机之间协调存储访问。因此，基于主机的方法不能提供足够程度的安全性。由于这一安全性限制，难于实现多种冗余方案例如 RAID，这些冗余方案需要在读和写操作期间对存储器进行“锁定”。另外，当进行镜像时，主机必须多次复制数据，增加了其输入输出和 CPU 负载，并增加了 SAN 上的流量。

在位于主机和存储设备之间的存储区域网络用具中进行虚拟化，这可以解决基于主机和基于存储的方法中的一些难题。所述存储用具全局地管理物理存储到虚拟卷地映射和分配。一般地，存储用具管理一个中心表，该表提供物理到虚拟的当前映射。这样，基于存储用具的方法使得可在存储区域网络上实现同时独立于主机和存储子系统的虚拟卷，因而提供了更高程度的安全性。而且，这一方法支持跨越多个存储子系统的虚拟化。这一一体系结构的许多实现的主要缺点在于每个主机的每次输入/输出（I/O）都要发送通过该存储区域网络用具，造成了明显的性能降低和存储区域网络瓶颈。这在支持诸如 RAID 等冗余方案的系统中尤其不利，因为数据必须被映射为跨越多个磁盘。在另一种基于存储用具的方法中，所述用具确保所有主机都接收到所述表的当前版本。因此，为了使得主机可从所述用具接收到该表，需要一种从该用具到主机的软件“垫片(shim)”，这增加了系统的复杂度。而且，由于所述软件层实现在主机上，也就出现了许多基于主机的方法的缺点。

考虑到上述内容，如果网络内各种存储设备或其一些部分可在逻辑上动态分配到各种设备和/或实体，这将是非常可取的。而且，如果可以实现这样一种机制来在 SAN 内支持存储虚拟化而又没有传统虚拟化方法的缺点，那将是很有益的。

发明内容

在此公开了用于在存储区域网络内实现存储虚拟化的方法和装置。这是通过使用一个或多个能被置于主机和存储设备之间的数据路径中的网络设备来实现的。结果，存储设备和主机都不需要额外的软件或硬件来支持存储虚拟化。因此，本发明优于基于主机的方法，后者要求每个主机都需要额外的软件来实现虚拟化功能。而且，本发明使得多个网络设备可同时管理各存储设备的虚拟化。重要的是，基于交换机的虚拟化可逐个端口地实现。交换机上任意数量的端口都可管理它自己的流量的虚拟化。这使得网络的虚拟化能力可随着端口数量而扩展。由于在任何网络系统中都存在大量端口，因此几乎总是会有足够的带宽来用于虚拟化。因此，可以实现存储虚拟化而又不出现传统虚拟化方案中的许多缺点。

根据本发明的一个方面，创建一种虚拟包封（virtual enclosure），其具有一个或多个虚拟包封端口，并适于表示一个或多个虚拟存储单元。也就是说，所述虚拟包封用来“包封”所选择的虚拟存储单元，这些单元可通过虚拟包封端口来访问。每个虚拟存储单元都表示存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置。另外，虚拟包封的每个虚拟包封端口都与存储区域网络内的网络设备的端口相关联。然后，将一个地址或标识符分配给每个虚拟包封端口。例如，所述地址或标识符可以是光纤信道标识符（FCID）。这样，指向虚拟包封端口（或其所分配的地址/标识符）的消息（例如分组或帧）可由与该虚拟包封端口相关联的端口来处理。

根据本发明的各个实施例，虚拟包封实现在光纤信道网络内部。因此，一个节点全球范围名称（Node World Wide Name, NWWN）与该虚拟包封相关联。另外，一个端口全球范围名称（Port World Wide Name, PWWN）与每个虚拟包封端口相关联。

根据本发明的另一个方面，指示存储区域网络内的网络设备的端口代表虚拟包封端口来处理消息。这可以两种方式实现。第一，可指示该端口将它自己“绑定”到该虚拟包封端口。也就是说，该端口起到虚拟包封端

口的作用，并且所有指向该虚拟包封端口并且被该端口接收的消息都由该端口处理。第二，可指示所述端口起到“陷入端口（trapping port）”的作用。更具体地说，除了绑定到虚拟包封端口的端口之外，一个或多个其它端口也可处理它们所接收的指向所述虚拟包封端口的消息。陷入端口优选地是与主机直接相连的端口，因此可以跟踪它所接收的请求以及与这些请求相关联的响应。在多个端口之间代表单个虚拟包封端口进行的绑定和陷入优选地是在一个中心位置例如虚拟包封服务器处进行协调。

各种网络设备可被配置或改装成用于执行所公开的虚拟化处理。这些网络设备包括但不局限于服务器（例如主机）、路由器和交换机。而且，用于上述虚拟化处理的功能可用软件及硬件来实现。

本发明的另一个方面涉及包括机器可读介质的计算机程序产品，该介质上提供了程序指令来整体或部分地实现上述方法和技术。本发明的任何方法都可整体或局部地表示为可在这种机器可读介质上提供的程序指令。另外，本发明涉及在此描述的所生成和/或使用的数据的各种组合和/或设置。例如，具有在此描述的格式并在合适的介质上提供的分组或帧是本发明的一部分。

在下面对本发明的详细描述中，将结合下述附图描述本发明的这些以及其他特征。

附图说明

图 1A 的框图示出了能够实现现有虚拟化功能的若干实施例的示例性传统存储区域网络。

图 1B 的框图示出了可在其中实现本发明的若干实施例的示例性存储区域网络。

图 2 的框图示出了可根据本发明的若干实施例来实现的虚拟化模型。

图 3A 的框图示出了可在其中实现本发明的若干实施例的示例性虚拟化交换机。

图 3B 的框图示出了可在其中实现本发明的若干实施例的示例性标准交换机。

图 4 的事务流程图示出了对每个 SCSI 目标端口实现节点全球范围名称（NWWN）和端口全局范围名称（PWWN）的传统方法。

图 5 的框图示出了根据本发明一个实施例的示例性虚拟包封。

图 6 示出了一种示例性系统，其中通过根据本发明的若干实施例，将虚拟包封端口绑定到若干虚拟化端口，从而实现虚拟包封。

图 7 的处理流程图示出了根据本发明的若干实施例，创建虚拟包封的方法。

图 8 示出了根据本发明的若干实施例，可与虚拟包封端口相关联的传统光纤信道标识符（FCID）。

图 9 的事务流程图示出了根据本发明的若干实施例，协调虚拟化端口的虚拟包封绑定和陷入功能的一种方法。

图 10 示出了根据本发明的若干实施例，可由虚拟化端口维护的一个示例性表，该表表示由该虚拟化端口处理的 FCID。

图 11 的事务流程图示出了根据本发明的若干实施例，在主机和一个或多个虚拟化端口（例如虚拟包封端口、陷入端口）之间建立通信，以使得该主机可访问一个或多个 LUN 的一种方法。

图 12 示出了一种示例性 LUN 映射表，该表可用于在图 11 的步骤 1128 处执行 LUN 映射。

图 13 示出了对应于图 12 的 LUN 映射表的虚拟包封。

具体实施方式

在下面的描述中，给出了大量具体细节以透彻地理解本发明。然而，对本领域内的技术人员来说很明显没有这些具体细节中的一些或全部也可实施本发明。在其他情形下，未详细示出一些公知处理步骤以免不必要的混淆本发明。

根据本发明的若干实施例，存储区域网络内的存储虚拟化可通过创建具有一个或多个虚拟包封端口的虚拟包封来实现。所述虚拟包封部分是通过一个或多个网络设备实现的，所述网络设备在此称为虚拟化交换机。更具体地说，虚拟化交换机（或更具体地说是虚拟化交换机内的虚拟化端

口) 可代表虚拟包封端口之一来处理消息如分组或帧。因此, 本发明的实施例可被应用于指向虚拟包封端口的分组或帧, 下面将更详细地描述。为了方便起见, 下面的讨论将针对于帧来描述本发明的实施例。交换机对帧进行操作, 并使用关于 SAN 的信息来进行交换决策。

注意, 虚拟化交换机所接收和发送的帧具有对于标准协议例如以太网或光纤信道而指定的帧格式。因此, 传统上用来生成这些帧的软件和硬件可与本发明一起使用。根据本发明, 还采用了附加的硬件和/或软件来修改和/或生成与所述标准协议兼容的帧。本领域内的技术人员将会理解如何开发必需的硬件和软件来实现下述虚拟化。

很明显, 所述合适的网络设备应该用合适的软件和/或硬件来配置, 以执行虚拟化功能。当然, 不是存储区域网络内的所有网络设备都需要配置有虚拟化功能。相反地, 可选择一些交换机和/或端口进行虚拟化功能的配置, 或将其改装成适于该功能。类似地, 在各实施例中, 可以通过选择不同模式来启用或禁止这一虚拟化功能。而且, 将网络设备所选择的端口配置为能够执行虚拟化(或者是持续地, 或者只是在处于启用虚拟化的状态中时) 是所期望的。

存储区域网络内采用的标准协议(即用于使数据成帧的协议)一般(但非必然)与网络所携带的“流量类型”同义。如下所述, 按照某些封装格式来定义流量类型。流量类型的例子一般是层 2 或对应的层格式, 例如以太网、光纤信道和 InfiniBand。

如上所述, 存储区域网络(SAN)是一种代表一个更大的用户网络, 互连具有关联网络主机(例如数据服务器或终端用户机器)的不同数据存储设备的高速专用网络。SAN 由系统的物理配置所定义。也就是说, SAN 中的这些设备必须在物理上互连。

在如图 1B 中所示的存储区域网络 131 内, 可以实现多个存储设备 132、134、136、138、140 和 142, 它们可以是同构的(例如相同的设备类型、大小或配置)或异构的(例如不同的设备类型、大小或配置)。可响应于主机 144 和 146 发送的命令而从存储设备 132—142 的各个部分读数据或对之写数据。这些存储设备和主机之间的通信是通过将存储设备与主

机耦合在一起而实现的，所述耦合通过一个或多个交换机、路由器或其他配置来执行交换功能的网络节点来实现。在这一示例中，交换机 148、150 和 152 通过交换机间链路 154 和 156 来相互通信。

如上所述，本发明涉及存储网络中的“虚拟化”。与现有方法不同，本发明中的虚拟化是通过创建并实现虚拟包封来实现的。这部分地是通过使用存储区域网络的交换机或其他“内部”网络节点来实现所述虚拟包封来完成的。而且，本发明的虚拟化一般是逐个端口地实现。也就是说，多端口虚拟化交换机将具有独立地实现在其一个或多个端口上的虚拟化。各端口具有若干专用逻辑，以用于处理该端口所处理的分组或帧的虚拟化功能。这使得虚拟化处理可随着端口数量而扩展，并且，与基于主机或基于存储的虚拟化方案相比，可提供多得多的带宽来用于虚拟化。在这些现有的方法中，主机和网络结构（network fabric）之间或存储节点和网络结构之间的连接数量是受限的——至少与网络结构中的端口数量相比是这样的。

在本发明的一个特定且优选的实施例中，虚拟化逻辑分别实现在给定交换机的各端口处——而非集中式地处理交换机的所有端口。这使得虚拟化处理能力可逐个端口地与交换机的准确需求紧密地匹配。如果对（服务于大量端口的）整个交换机采用中央处理器，则该处理器必须被设计/选择来处理所有端口处的最大流量。对于许多应用而言，这意味着极高的处理需求和非常巨大/昂贵的处理器。如果该中央处理器太小，则交换机将经常不能跟上网络的交换/虚拟化需求。

虚拟化可采用许多形式。一般地，它可被定义为对存储网络上的物理存储和虚拟存储进行相互关联的逻辑或过程。主机可以获得可用物理存储的一种表示，其不受限于该存储设备所固有的物理设置或分配。被虚拟化所克服的物理限制的一个示例包括构成性物理存储块的大小和位置。例如，小型计算机系统接口（SCSI）标准所定义的逻辑单元具有精确的物理大小（例如 36Gb 和 72GB）。虚拟化以比物理逻辑单元的规定大小更小或更大的虚拟逻辑单元来表示存储。而且，虚拟化可以提供一种虚拟逻辑单元，其包括来自两个或更多不同物理逻辑单元的区域，它们有时是来自不

同供应商的设备。优选地，虚拟化操作至少对一些网络实体（例如主机）是透明的。

按照一些通常意义，存储区域网络上的虚拟化与典型计算机系统的虚拟存储器类似。然而，网络上的虚拟化产生了大得多的复杂度并带来了大得多的灵活性。所述复杂度直接来源于下述事实，即存在多个分别互连的网络节点。虚拟化必须跨越这些节点。所述节点包括主机、存储子系统和交换机（或相当的网络流量控制设备例如路由器）。所述主机和/或存储子系统经常是异构的，由不同供应商提供。供应商可能采用了截然不同的协议（标准协议或专有协议）。因此，在许多情形下，虚拟化提供了将异构的发起者（例如主机或服务器）连接到分布式的异构目标（存储子系统）组的能力，实现了动态且透明的存储分配。

网络专用的虚拟化操作的例子包括下述操作：RAID 0 到 RAID 5、来自物理存储器的两个或更多不同逻辑单元的存储器的级联、备用（失效物理介质的自替换）、物理存储器的远程镜像、信息（例如错误和/或统计）写日志、多个物理存储器系统间的负载平衡、条带化（例如 RAID 0）、安全性措施例如用于访问物理存储器的访问控制算法、虚拟存储器块的大小重新设置、使得任意逻辑单元（LUN）可作为引导设备的 LUN 映射、物理存储器的备份（时间点（point in time）拷贝）等等。这些仅仅是虚拟化功能的示例。本发明并不限制于这一全集或其任何特定子集。

在此的一些讨论中，本发明的虚拟化交换机的功能是按照 SCSI 协议来描述的。这是因为许多商用存储区域网络运行 SCSI 协议来访问存储站点。存储区域网络经常采用光纤信道（FC-PH（ANSI X3.230-1994，光纤信道—物理和信令接口）作为更低层的协议，并在光纤信道之上运行 IP 和 SCSI。注意，本发明并不局限于这些协议中的任何一个。例如，可用以太网、InfiniBand 等来替换光纤信道。而且，更高层的协议不一定包括 SCSI。例如，这可包括 FC 上的 SCSI、iSCSI（IP 上的 SCSI）、并行 SCSI（并行缆线上的 SCSI）、串行 SCSI（串行缆线上的 SCSI）以及 SCSI 的所有其他变体。

由于 SCSI 非常普遍地使用在存储区域网络中，因此在此使用的许多

术语都是 SCSI 术语。使用 SCSI 术语（例如“发起者”和“目标”）并不意味着所描述的过程或装置必须采用 SCSI。在做进一步描述之前，有必要对这一讨论中将要使用的若干 SCSI 术语进行解释。首先，“发起者”是请求另一个设备执行一项操作的设备（通常是主机系统）。一般地，在本文献的上下文中，主机发起者将请求对虚拟或物理存储器的一个区域进行读或写操作。其次，“目标”是执行发起者所请求的操作的设备。例如，目标物理存储器磁盘将获得或写下主机发起者一开始所请求的数据。注意，尽管主机发起者可提供对具有虚拟地址的“虚拟”目标进行读或对之写的指令，但是本发明的虚拟化交换机在对该目标发出指令前必须首先将这些指令转换成物理目标地址。

目标可被划分成物理或虚拟“逻辑单元”。这些是通过该目标可以寻址的特定设备。例如，物理存储子系统可被组织为具有多个不同逻辑单元。在本文献中，主机将虚拟存储器视为不同的虚拟逻辑单元。在此有时将逻辑单元称为“LUN”。在 SCSI 标准中，LUN 表示逻辑单元号。但在通常的术语中，LUN 也表示逻辑单元本身。

虚拟化的中心概念是“虚拟化模型”。这是存储子系统（例如磁盘阵列）上提供的物理存储借以与网络上的主机或其他发起者所看到的虚拟存储建立关系的方式。尽管所述关系可以具有许多形式，也可由不同术语给出其特征，但在此将使用基于 SCSI 的术语，如上所述。因此，存储区域网络的物理侧将被描述为物理 LUN。反过来，主机侧可看到一个或多个作为物理 LUN 的虚拟表示的虚拟 LUN。物理 LUN 到虚拟 LUN 的映射逻辑上可能发生在一个、两个或更多的层级上。最后，存在一种可由本发明的交换机使用来在物理 LUN 地址和虚拟 LUN 地址之间进行相互转换的映射功能。

图 2 的框图示出了根据本发明的若干实施例，可在存储区域网络内实现的虚拟化模型的一个示例。如图所示，存储区域网络的物理存储由一个或多个物理 LUN 构成，在此示出为物理磁盘 202。每个物理 LUN 是能够包含存储成一个或多个连续块的数据，所述块可分别被直接访问。例如，物理 LUN 内的存储器的每个块可被表示为块 204，可称为磁盘单元

(DUnit)。

通过映射功能 206，可以将与物理 LUN 202 相关联的物理 LUN 地址转换成虚拟 LUN 地址，反之亦然。更具体地说，如上所述，所述虚拟化以及映射功能可在一个或多个层级上发生。例如，如图所示，在第一虚拟化层级处，一个或多个虚拟 LUN 208 中的每一个都表示一个或多个物理 LUN 202 或其一些部分。一起构成单个虚拟 LUN 208 的物理 LUN 202 不一定是连续的。类似地，被映射为虚拟 LUN 208 的物理 LUN 202 不一定位于单个目标内。因此，通过虚拟化，可创建表示位于物理上不同的目标内的物理存储器的虚拟 LUN 208，这些目标可来自不同的供应商，因此，可支持不同协议和流量类型。

尽管可用单个层级来实现所述虚拟化模型，但是本发明的不同实施例也可支持具有任意数量的层级的层次设置。例如，如图所示，图 2 的虚拟模型内的第二虚拟化层级称为高级 VLUN 或卷 210。一般地，发起者设备在访问数据时只“看到” VLUN 210。根据本发明的若干实施例，多个 VLUN 被“包封”在一个虚拟包封内，以使得只有该虚拟包封可被发起者“看到”。也就是说，虚拟包封所包封的 VLUN 对发起者来说是不可见的。

在这一示例中，VLUN 210 被实现为虚拟 LUN 208 的“逻辑” RAID 阵列。而且，还可以例如通过使用条带化和/或镜像来进一步实现这一虚拟化层级。另外需要注意，不必指定虚拟化层级的数量来支持映射功能 206。相反地，可以例如通过递归映射功能来实现任意数量的层级的虚拟化。例如，不同层级的节点可被构建或维护在树型数据结构、链接表或其他可被遍历的合适的数据结构中。

因此，每个发起者可通过位于该层次虚拟化模型的任意层级中的节点来访问物理 LUN。实现在给定存储区域网络内的层次模型的给定虚拟化层级内的节点对于一个被许可的发起者组（未示出）来说既可见又可访问。然而，根据本发明的若干实施例，这些节点包封在虚拟包封中，因此对于被许可的发起者组来说不再可见。在可对特定虚拟化层级内的节点（例如 VLUN）执行某些功能（例如读、写）之前，需要创建所述节点。这例如

可通过特定发起者的主引导记录来实现。另外，可针对特定虚拟化层级内的特定节点（例如 VLUN），向不同发起者分配读和/或写特权。按照这种方式，特定虚拟化层级内的节点可被所选择的发起者访问。

如上所述，存储区域网络内的各交换机可以是支持虚拟化功能的虚拟化交换机。图 3A 的框图示出了可在其中实现本发明的若干实施例的示例性虚拟化交换机。如图所示，智能虚拟化端口通过双向连接器 302 接收数据或消息。另外，虚拟化端口适于代表虚拟包封端口来处理消息，下面将更详细地描述。与进入端口相关联，提供了介质访问控制（MAC）模块 304，其使得可接收各种协议例如以太网或光纤信道的帧。另外，虚拟化拦截交换机 306 确定一个进入分组中指定的地址是否与对某个虚拟存储单元的虚拟存储位置的访问有关，该虚拟存储单元表示存储区域网络的一个或多个物理存储单元上的一个或多个物理存储位置。例如，所述虚拟存储单元可以是包封在虚拟包封内的虚拟存储单元（例如 VLUN）。

当虚拟化拦截交换机 306 确定进入帧中指定的地址涉及对虚拟存储位置而非物理存储位置的访问时，该帧由能够执行上述映射功能的虚拟化处理器 308 处理。更具体地说，虚拟化处理器 308 获得一个或多个物理存储位置和虚拟存储位置之间的虚拟-物理映射。按照这种方式，虚拟化处理器 308 可查找物理或虚拟地址，视情况而定。例如，可能需要执行从物理地址到虚拟地址的映射，或者需要执行从虚拟地址到一个或多个物理地址的映射。

获得虚拟-物理映射后，虚拟化处理器 308 然后可利用所获得的映射来生成新的帧或修改现有的帧，从而可将该帧发送到所述虚拟-物理映射指定的发起者或目标。映射功能还可指定该帧需要被复制多次，例如在镜像写的情况下。更具体地说，视情况而定地修改源地址和/或目的地地址。例如，对于来自目标的数据，虚拟化处理器将最初是物理 LUN 地址的源地址替换为对应的虚拟 LUN 和地址。在目的地地址中，端口将它自己的地址替换为发起者的地址。对于来自发起者的数据，端口将源地址从发起者的地址改变为该端口自己的地址。它还将目的地地址从虚拟 LUN/地址改变为对应的物理 LUN/地址。所述新的或已修改的帧然后可被提供给虚拟

化拦截交换机 306，以使该帧可被发送到其预期目的地。

当虚拟化处理器 308 获得并应用所述虚拟-物理映射时，所述帧或关联数据可存储在临时存储器位置（例如缓冲区）310 中。另外，可能需要或希望存储正被发送或接收的数据，直到已确认所预期的读或写操作已成功完成。例如，可能希望将大量数据写到虚拟 LUN，所述数据必须以多个帧的形式被分别发送。因此，可能希望对该数据进行临时缓冲，直到接收到该数据的接收确认。作为另一个例子，可能希望从虚拟 LUN 读大量数据，所述数据必须以多个帧的形式被分别接收。而且，接收这一数据的顺序可能与该数据应被传送到读命令的发起者的顺序不一致。在此情形下，在将数据发送到发起者之前对之进行缓冲可能是有益的，以使数据在发送之前可被重新排序。类似地，可能希望在必须验证已被发送到发起者（或目标）的数据的完整性时，对数据进行缓冲。

所述新的或已修改的帧然后由转发引擎 312 接收，转发引擎 312 从该帧的各个字段获得信息，例如源地址和目的地地址。转发引擎 312 然后访问转发表 314，以确定所述源地址是否可访问所指定的目的地地址。更具体地说，转发表 314 可包括物理 LUN 地址以及虚拟 LUN 地址。转发引擎 312 还确定交换机的合适端口以通过其发送该帧，并为该帧生成合适的路由标签。

将帧进行合适的格式化以用于发送之后，在发送之前由缓冲队列模块 316 接收该帧。不是将帧在接收时就进行发送，而是可能希望将帧临时存储在缓冲区或队列 318 中。例如，可能希望基于服务质量而将分组临时存储在一组队列中的一个队列中，其中每个队列都对应于不同的优先级。然后通过交换结构 320 将帧发送到合适的端口。如图所示，外发端口具有它自己的 MAC 模块 322 和双向连接器 324，通过它们发送帧。

如上所述，不是存储区域网络中的所有交换机都必须是虚拟化交换机。也就是说，交换机可以是标准交换机，其中任意端口都未实现“智能的”虚拟化功能。图 3B 的框图示出了其中可实现本发明的若干实施例的示例性标准交换机。如图所示，标准端口 326 具有 MAC 模块 304。然而，未实现诸如图 3 所示的虚拟化拦截交换机和虚拟化处理器。在进入端

口处接收的帧只是由转发引擎 312 和它的关联转发表 314 进行处理。在发送之前，可将帧排队 316 在缓冲区或队列 318 中。然后通过交换结构 320 将帧转发到外发端口。如图所示，外发端口也具有关联 MAC 模块 322 和双向连接器 324。当然，每个端口都可支持多种协议。例如，外发端口可以是也支持虚拟化的 iSCSI 端口（即支持以太网上的基于 IP 的 SCSI 的端口），还可以是并行 SCSI 和串行 SCSI。

虽然上面参考图 3A 和 3B 所述的网络设备被描述为交换机，但是这些网络设备仅仅是示例性的。因此，也可实现其他网络设备例如路由器来接收、处理、修改和/或生成具有如上所述功能的分组或帧以在存储区域网络中进行传输。而且，上述网络设备仅仅是示例性的，因此也可实现其他类型的网络设备来执行所公开的虚拟化功能。

一般地，SCSI 目标可由 SCSI 发起者（例如主机）直接访问。也就是说，SCSI 目标例如 PLUN 对正在访问这些 SCSI 目标的主机来说是可见的。类似地，即使实现了 VLUN，VLUN 对 SCSI 发起者来说也是可见且可访问的。因此，每个主机一般都必须识别对它来说可用的 SCSI。更具体地说，主机一般确定哪些 SCSI 目标端口对它来说是可用的。主机然后向这些 SCSI 端口中的每一个询问，想了解通过这些 SCSI 目标端口可使用哪些 VLUN。

在光纤信道网络内，所有的光纤信道设备都具有全球范围名称（WWN）。更具体地说，节点 WWN（NWWN）是连接到特定端口的节点的 WWN。也就是说，NWWN 是连接到交换机端口的系统、存储设备或子系统的 WWN。在节点 WWN 之外，端口 WWN（PWWN）用作为特定端口的给定名称。特定交换机端口的光纤信道网络 ID（FCID）用于表示端口的物理位置。每个光纤信道设备可具有多个端口，每个端口都唯一地由一个 NWWN 和 PWWN 标识。

不幸地是，传统的光纤信道 WWN 术语的应用存在若干相关联的缺点。例如，必须为光纤信道设备的每个端口都分配 NWWN 和 PWWN。然而，可能不希望使得每个端口的 NWWN 和 PWWN 对于发起者例如主机来说都是可见的。而且，可用端口的数量被限制为特定存储设备、子系统

或交换机内的端口的数量。类似地，存储设备、子系统或交换机可具有比特定存储虚拟化方案中所需的端口数量多得多的端口。然而，虚拟化端口的实现是很昂贵的，因此不希望“浪费”这些智能端口。因此，根据本发明，虚拟化端口的使用可以是按需进行。也就是说，可选择端口用于实现一个或多个虚拟包封，这是通过将这些端口绑定到虚拟包封端口或通过将中心端口实现为陷入端口来完成的。结果，生产起来最为昂贵的那些端口可得到最大程度的使用。

在本发明的一个实施例中，网络例如光纤信道网络中的虚拟化的实现不受限于存储子系统中可访问端口的数量。而且，SAN 内的端口可按需选择及分配，以用于特定存储虚拟化方案。下面将更详细地描述本发明的若干实施例。

为了理解本发明是如何应用到光纤信道网络中的，图示出 WWN 术语在光纤信道网络中的传统应用是有帮助的。图 4 的事务流程图示出了为每个 SCSI 目标端口实现节点全球范围名称 (NWWN) 和端口全球范围名称 (PWWN) 的传统方法。如图所示，主机 402、交换机 404、域名系统 (DNS) 服务器 406 和 SCSI 目标端口 408 之间的交互通过被标签的对应垂直线所表示出来。如图所示，为了是光纤信道节点例如主机 402 可建立到结构交换机 404 的逻辑连接，主机 402 执行结构登录 (FLOGI) 410。与使用固定介质访问控制 (MAC) 地址的许多 LAN 技术不同，光纤信道使用称为 FCID 的地址标识符，该标识符可在登录期间动态分配。这样，在 412 处，交换机 404 向主机 402 提供一个 FCID。一旦向主机分配了主机 FCID，主机就可在方框 414 通过 SCSI REPORT 命令向 DNS 服务器 406 进行 DNS 查询，该命令请求确定 SCSI 目标是否可用。更具体地说，所述 DNS 查询确定对主机 FCID 可见的那些 SCSI 目标。在 416，DNS 服务器 406 然后将 SCSI 目标端口的 FCID 提供给主机 402。

在主机获得对它可用的那些 SCSI 目标端口的 FCID 之后，在 418，它向（由其 FCID 标识出的）可用的 SCSI 目标端口之一发送光纤信道处理逻辑命令。这一处理逻辑实现了一个映射层，将光纤信道“映射”到 SCSI。完成后，SCSI 目标端口 408 在 420 发送光纤信道接受消息。由于光纤信道

被映射到 SCSI，因此主机可以发送 SCSI 命令到 SCSI 目标。

由于主机 402 可以发送 SCSI 命令到 SCSI 目标端口 408，因此它在 422 可以通过将 SCSI 处理登录命令发送到 SCSI 目标端口 408 来执行 SCSI 处理登录。SCSI 目标端口 408 然后发送 SCSI 接受命令 424。由此可在主机和 SCSI 目标之间建立经由 SCSI 协议进行的通信。例如，主机可以确定哪些 LUN 对它可用，并对它可用的 LUN 进行读和写。

由于主机 402 知道了哪些 SCSI 目标端口对它可用，并可与这些端口中的每一个进行通信，因此它可以在 426 发送 SCSI REPORT LUN 命令到 SCSI 目标端口 408，以确定对所述主机 FCID 可见的那些 LUN。SCSI 目标端口 408 在 428 确定哪些 LUN 对该主机 FCID 是可见的，并发送一个 LUN（例如 PLUN 或 VLUN）列表。然后在 430，主机 402 可通过 SCSI 目标端口 408 向特定 PLUN 或 VLUN 发送 SCSI 读和写命令。

根据本发明的若干实施例，通过创建“虚拟包封”而在存储区域网络中实现了存储虚拟化。图 5 的框图示出了根据本发明一个实施例的示例性虚拟包封。虚拟包封 502 是一个适于“包封”或代表一个或多个虚拟存储单元的虚拟实体。例如，所述虚拟存储单元中的一个或多个中的每一个都可包括 SAN 上的 VLUN 或其他虚拟存储表示。如上所述，每个虚拟存储单元都表示存储区域网络的一个或多个物理存储单元 504 上的一个或多个物理存储位置。通过创建虚拟包封，可以按需实现上述各种虚拟化端口以支持特定存储区域网络内的虚拟化。更具体地说，所述虚拟包封具有一个或多个“虚拟包封端口”，其中每一个虚拟包封端口都与该存储区域网络内的网络设备的一个端口（例如虚拟化端口）相关联。例如，可静态或动态地指示网络设备的端口去处理发送到虚拟包封端口的消息。还将一个地址或标识符分配到每个虚拟包封端口。这样，发送到虚拟包封端口的消息（例如分组或帧）可通过这一地址或标识符来标识，从而使得一个端口可代表特定的虚拟包封端口来拦截并处理消息。例如，可将一个 FCID 分配到光纤信道网络中使用的每个虚拟包封端口，或与诸如 SAN 之类的网络内的各种光纤信道设备一起使用。按照这种方式，可以创建虚拟包封来表示一个或多个虚拟存储单元。

在 SAN 内，可以创建不同的虚拟 SAN (VSAN)。在单个存储区域网络内实现虚拟存储区域网络 (VSAN) 的一种方法已参考美国专利申请 No._____ (律师案卷号 No.ANDIP001) 进行了更详细的描述，该申请的名称为 “Methods and Apparatus for Encapsulating a Frame for Transmission in a Storage Area Network”，由 Edsall 等人与 2001 年 12 月 26 日递交，该申请通过引用而包含于此以用于各种目的。也就是说，可能希望或必须将物理存储单元分布在不同的 VSAN 之间。因此，当虚拟包封端口被绑定到虚拟化端口时，这些所选择的虚拟化端口可被分布在多个 VSAN 之间。

每个虚拟包封可具有任意数量的虚拟包封端口。也就是说，希望使得虚拟包封端口的数量是可以选择的。例如，负责创建并维护虚拟包封定义的系统管理员可选择适当数量的虚拟包封端口。应注意，虚拟包封内的虚拟包封端口的数量并不受限于存储区域网络内特定网络设备内的端口数量。更具体地说，每个虚拟包封端口与存储区域网络内的网络设备的一个端口相关联。也就是说，单个虚拟包封的虚拟包封端口可同时与存储区域网络内多个不同网络设备而非单个设备的端口（例如虚拟化端口）相关联。另外，网络设备的单个端口例如虚拟化端口可同时与多个虚拟包封端口相关联或绑定到所述虚拟包封端口。因此，可用于虚拟存储单元的虚拟化的端口的数量几乎没有限制。

如上所述，将一个地址或标识符分配到每个虚拟包封端口。理论上，这一地址或标识符可以是之前已被分配到存储区域网络某个端口的地址或标识符，所述某个端口之后与该虚拟包封端口相关联。然而，由于单个虚拟化端口可绑定到多个虚拟包封端口，因此之前分配给所述端口（例如虚拟化端口）的地址或标识符将不再唯一地标识虚拟包封端口。因此，将所述地址或标识符分配到虚拟包封端口以唯一地表示该虚拟包封端口。此时，将所述地址或标识符提供给与该虚拟包封端口相关联的虚拟化端口。根据一个实施例，所述虚拟包封使用在光纤信道网络中，因此每个光纤信道设备都具有 NWWN。根据本发明的各个实施例来利用这一术语，以实现虚拟包封。因此，NWWN 和 PWWN 一起可用作唯一地表示虚拟包封端

口的地址或标识符。更具体地说，NWWN 与虚拟包封相关联。另外，将 PWWN 分配到每个虚拟包封端口。NWWN 和 PWWN 一起标识虚拟包封端口，直到它被分配了一个地址或标识符例如 FCID。

创建虚拟包封之后，可将一个或多个虚拟存储单元分配到该虚拟包封。如上所述，每个虚拟存储单元都可以是 VLUN 或存储区域网络上的其他虚拟存储表示。按照这种方式，虚拟包封“包封”了所述虚拟存储单元，从而需要主机通过虚拟包封来访问这些虚拟存储单元。按照这种方式，可将 VLUN 对于主机“隐藏”起来。也就是说，通过访问 PWWN，主机仅可访问虚拟包封而不能访问具体设备或 VLUN。更具体地说，VLUN 看起来像位于一组虚拟包封端口之后的逻辑单元。这样，用于创建 VLUN 的 PLUN 对主机隐藏起来。

如上所述，可用适于实现虚拟化功能的虚拟化交换机以及标准交换机来实现存储区域网络。每个虚拟化交换机都可包括一个或多个“智能”虚拟化端口以及一个或多个标准端口。图 6 示出了根据本发明若干实施例的一个示例性系统，在其中可通过将虚拟包封端口绑定到若干虚拟化端口来实现虚拟包封。如图所示，虚拟包封 602 “包封”了两个虚拟存储单元 VLUN1 604 和 VLUN2 606。在这一示例中，虚拟包封 602 具有 3 个虚拟包封端口：VE1 608、VE2 610 和 VE3 612。另外，还示出了存储区域网络内的 4 个网络设备。更具体地说，示出了 4 个虚拟化交换机 614、616、618 和 620。每个虚拟化交换机都具有一个或多个虚拟化端口，如上参考图 3A 所述。然而，为了简化图示，每个虚拟化交换机都被示出为具有单个虚拟化端口，分别标记为 v1、v2、v3 和 v4。每个虚拟化端口都具有关联 PWWN（未示出）。交换机之间的通信可通过两个交换机（或两个端口）之间的交换机间链路来完成。

可唯一地表示每个虚拟包封端口。更具体地说，在光纤信道网络内，虚拟包封 602 由 NWWN 621 所标识。另外，一旦每个虚拟包封端口与虚拟化端口相关联之后，虚拟包封端口 VE1 608、VE2 610 和 VE3 612 中的每一个就都可由 PWWN 以及其 FCID 来进一步标识，分别标记为 PWWN1 622、PWWN2 624 和 PWWN3 626。更具体地说，虚拟包封端口可通过

NWWN 和 PWWN 来标识，直到向虚拟包封端口分配了 FCID。下面将参考图 8 来更详细地描述 FCID。如图所示，所分配的 FCID 还标识了与对应的虚拟包封端口相关联的虚拟化交换机。这是因为在光纤信道中，交换机被视为“域”。因此，该交换机中的任意端口的 FCID 的第一个字节都与域 ID 相同。例如，分配给第一虚拟包封端口 VE1 608 的 FCID 的第一个字节标识了虚拟化交换机 616，示出为交换机 50，而分配给第三虚拟包封端口 VE3 612 的 FCID 的第一个字节标识了虚拟化交换机 618，示出为交换机 45。

虚拟包封例如虚拟包封 602 的创建还可由网络设备例如虚拟包封服务器 627 来执行。例如，可由系统管理员来创建虚拟包封 602。创建后，可将各种 VLUN 例如 VLUN 604 和 606 分配给虚拟包封 602。需要的话，可随后将这一分配修改为包括其他 VLUN，从该虚拟包封内删除 VLUN，或修改 VLUN 到虚拟包封 602 的分配。在创建、修改和维护虚拟包封之外，虚拟包封服务器 627 还可以向虚拟化交换机的虚拟化端口通知它们与对应的虚拟包封端口之间的关联。按照这种方式，可向虚拟化端口通知它们的以下职责，即拦截并处理指向那些对应虚拟包封端口的分组（或帧）。

一旦已创建虚拟包封，一个或多个主机 628、630 就可通过虚拟包封 602 访问存储区域网络内的数据。更具体地说，主机 628、630 可访问与虚拟存储单元（在此示出为 VLUN1 604 和虚拟包封 602）相对应的各个物理存储设备（称为物理存储单元）。例如，主机可通过向虚拟包封所包封的 VLUN 内（并且通过虚拟包封端口而可由该主机获得）的虚拟地址发送分组、帧或消息，从存储区域网络内的各个 PLUN 632、634、636、638 读数据或对之写数据。

如上所述，可创建虚拟包封以在各种网络环境下使用。图 7 的处理流程图示出了根据本发明的若干实施例来创建虚拟包封的方法。在这一示例中，该虚拟包封用在光纤信道网络中。因此，如在方框 702 所示，将一个 NWWN 与虚拟包封相关联。另外，在方框 704 选择虚拟包封的虚拟包封端口的数量。这些虚拟包封端口中的每一个都可由 PWWN 来标识，直到在方框 706 将它们绑定到虚拟化端口，并在方框 708 分配 FCID。生成虚

拟包封之后，在 710 将一个或多个 VLUN 分配到虚拟包封。这样，当主机在方框 712 登录到 SAN 中时，该主机可以发出 SCSI 读和写命令，以通过虚拟包封来访问物理存储单元。

在光纤信道网络内，每个 SCSI 目标设备都被分配了 NWWN。而且，每个 SCSI 目标端口都被分配了 PWWN。另外，光纤信道标识符（FCID）标识了每个 SCSI 目标端口的物理位置，因此与 PWWN 相关联。图 8 示出了根据本发明的若干实施例，可与虚拟包封端口相关联的传统 FCID。FCID 是一个 3 字节地址标识符，标识出交换机 802 例如虚拟化交换机、网络内的区域 804 以及交换机 802 的端口 806 例如虚拟化端口。

如上所述，为了创建虚拟包封，将每个虚拟包封端口“绑定”到虚拟化端口。根据本发明的若干实施例，由独立的网络设备来协调将虚拟包封端口绑定到虚拟化端口的工作。例如，这一网络设备可以是负责生成虚拟包封的虚拟包封服务器。也就是说，虚拟包封服务器对被绑定到虚拟包封端口、并因此应处理指向该虚拟包封端口的（由该虚拟化端口所接收的）所有消息的虚拟化端口进行指示。

除了将单个虚拟化端口绑定到虚拟包封端口之外，可能还希望使得另外的端口可“陷入”指向该虚拟包封端口的消息。例如，接收指向虚拟包封端口的虚拟化端口可比“绑定”到该虚拟包封端口的虚拟化端口离主机更近，因此能够提供更及时、有效的服务。另外，可能不希望将所有的消息都路由到被绑定到虚拟包封端口的单个虚拟化端口，因为这可能对有限数量的端口产生过重的负载，从而导致低效的服务。因此，根据本发明的若干实施例，虚拟包封服务器指示各个虚拟化端口“陷入”指向一个或多个虚拟包封端口的消息。按照这种方式，就可以利用 SAN 内其他虚拟化端口处理消息的能力。因此，即使在虚拟化端口未绑定到虚拟包封端口时，虚拟化端口也可对虚拟包封进行服务。

“陷入”虚拟化端口优选地是 SAN 中的“外部”节点而非内部节点。也就是说，虚拟化端口应直接连接到主机，而非通过一个或多个其他端口（例如标准或虚拟化端口）间接地连接。这一直接连接尤其重要，因为内部节点可从主机接收消息或请求，但是该内部节点可能不接收来自该

目标、指向该主机的消息，因为不能确保有相同的返回路径。因此，虚拟化端口将不能完成这一“通信回路”，因此就无法得知主机请求是否已得到了服务。

图 9 中示出了一种方法，用于根据本发明的若干实施例，协调虚拟化端口的虚拟包封绑定和陷入功能。虚拟包封服务器处执行的步骤由垂直线 902 表示，而在虚拟化端口 1-3 处执行的步骤分别由垂直线 904、906 和 908 表示。DNS 服务器和关联交换机分别由垂直线 912 和 910 表示。DNS 服务器 912 经常包括在交换机 910 内。虚拟包封服务器 902 可向 SAN 内的各端口发送各种虚拟化消息，以实现 SAN 内的存储虚拟化。例如，如上所述，虚拟化消息可以是绑定消息或陷入消息，其标识了虚拟包封端口的 PWWN。绑定消息和陷入消息之间的基本区别在于绑定消息表明 FCID 将动态地分配给虚拟包封端口，而陷入消息表明将获得之前已分配给另一个虚拟包封端口的 FCID，以使得指向该 FCID 的消息可由接收端口陷入。如在 914 所示，虚拟包封服务器发送绑定消息 914，指示第一虚拟化端口（虚拟化端口 1 904）处理指向第一虚拟包封端口 VEP1 的所有消息，这些消息由虚拟化端口 1 904 接收。每个虚拟包封端口例如 VEP1 都由其 PWWN 唯一地标识。虚拟化消息例如绑定或陷入消息还可进一步表明接收虚拟化端口将获得分配到该虚拟包封端口的地址或标识符。例如，虚拟化消息可表明将从 DNS 服务器获得所述地址或标识符，其可以是已指定或未指定的。

接收到绑定消息后，虚拟化端口 1 904 在 916 将 FLOGI 消息发送到交换机 910，以建立与交换机 910 的连接。如上所述，在登录期间动态地分配 FCID。因此，交换机 910 向第一虚拟化端口 VEP1 分配了一个 FCID 即 FCID1，其在 918 被提供给 DNS 服务器 912，服务器 912 然后将虚拟包封端口 1 VEP1 与该 FCID 即 FCID1 相关联。交换机 910 然后在 920 发送“接受（ACCEPT）”消息，表明 FCID1 现在已由 DNS 服务器 912 与第一虚拟包封端口 VEP1 相关联。另外，如图所示，该“接受”消息还向虚拟化端口 904 提供已被分配的 FCID。虚拟化端口跟踪这些虚拟包封端口，该虚拟化端口已与这些虚拟包封端口相互绑定，并负责为这些虚拟包

封端口陷入消息。为了维护这一虚拟包封端口信息，虚拟化端口然后将所述 FCID 即 FCID1 存储在例如下面参考图 10 所述的虚拟化端口表中。还在 922 执行 DNS REGISTRY (DNS 注册)，以将 VEP1 理解 SCSI 协议这一情况通知给 DNS 服务器 912。DNS 服务器然后在 914 发送“接受”消息。然后在 926 从虚拟化端口向虚拟包封服务器发送虚拟化响应，表明虚拟化端口现在已被配置为处理指向虚拟包封的虚拟包封端口的消息。在这一示例中，所述虚拟化响应表明虚拟化端口现在已绑定到虚拟包封端口。另外，分配到虚拟包封端口 VEP1 的 FCID 也可被提供给虚拟包封服务器，以使得虚拟包封服务器可将 FCID 分配给虚拟包封端口。更具体地说，可以在虚拟化响应中提供 FCID。按照这种方式，虚拟包封服务器就获得了它可使用的 SCSI 目标端口的 FCID。

在将虚拟包封端口绑定到 SAN 内的虚拟化端口之外，虚拟包封服务器 902 还可通过 SAN 内地其他虚拟化端口来建立陷入，如上所述。例如，如图所示，在 928，发送陷入消息，表明虚拟化端口 2 906 将处理指向分配到特定虚拟包封端口的地址或标识符的消息。由于虚拟包封服务器 902 已获得了分配到该虚拟包封端口 VEP1 的 FCID，因此可以在陷入消息中提供该 FCID。或者，可以从 DNS 服务器获得该 FCID，这将在此示例中进行描述。在这一示例中，指示虚拟化端口 906 处理指向所指定的虚拟包封端口（例如 VEP1）消息，这些消息由虚拟化端口 906 接收。也就是说，指示虚拟化端口 906 处理指向分配到该虚拟包封端口的地址或标识符的消息。类似地，在 930 发送第二陷入消息到虚拟化端口 3 908，表明该虚拟化端口将处理指向第一虚拟包封端口的消息。

当虚拟化端口 2 906 在 928 接收到陷入消息时，该虚拟化端口在 932 发送 GET_FCID 消息到 DNS 服务器 912，以获得分配到第一虚拟包封端口 VEP1 的地址或标识符。它在 934 接收到所述地址或标识符之后，在 936 存储该地址或标识符。更具体地说，它可更新以下图 10 中所述的表。所述虚拟化端口然后在 938 向主机发送虚拟化响应，以响应所述虚拟化消息。例如，所述虚拟化响应可表明所述虚拟化端口已成功（或不成功）地被配置来处理指向所述虚拟包封端口的消息。所述虚拟化端口现在可以陷

入它所接收的、指向所述虚拟包封端口的消息，如在 940 所示。

类似地，当虚拟化端口 3908 在 930 接收到陷入消息时，该虚拟化端口在 942 将 GET_FCID 消息发送到 DNS 服务器 912，以获得分配给第一虚拟包封端口 VEP1 的地址或标识符。它在 944 接收到该地址或标识符之后，在 946 存储该地址或标识符。该虚拟化端口在 948 发送虚拟化响应，表明所述虚拟化端口已成功（或不成功）地被配置为陷入端口，并在 950 开始陷入指向该虚拟化端口的消息。

如上所述，SAN 内的端口例如虚拟化端口可被配置为代表多个虚拟包封端口来处理消息。更具体地说，单个虚拟化端口可被绑定到多个虚拟包封端口，并可被配置为用于多个虚拟包封端口的陷入端口。图 10 示出了根据本发明若干实施例的一个示例性的表，其可由虚拟化端口维护，表明将由该虚拟化端口处理的 FCID。如图所示，虚拟化端口表 1000 可由虚拟化端口维护，以跟踪与之绑定或被配置来为之陷入消息的那些虚拟包封端口 1002。对于每个虚拟包封端口 1002，它维护相关联的 FCID。按照这种方式，虚拟化端口可标识出它所负责的那些 FCID。当分组指向该虚拟化端口不对之负责的 FCID 时，虚拟化端口只是转发该分组。

配置了一个或多个虚拟化端口来代表虚拟包封端口处理分组后（例如陷入或绑定端口），它们就可用作为发起者例如主机的 SCSI 目标。图 11 的事务流程图示出了根据本发明的实施例，在主机和一个或多个虚拟化端口（例如绑定到一个或多个虚拟包封端口的端口或陷入端口）建立通信，以使得主机可以访问一个或多个 LUN 的方法。如图所示，主机 1102、交换机 1104、域名系统（DNS）服务器 1106 和虚拟化端口 1108 之间的交互由被标记的对应垂直线表示。如图所示，光纤信道节点例如主机 1102 为了建立到结构交换机 1104 的逻辑连接，它执行结构登录（FLOGI）1110。如上所述，光纤信道使用称为 FCID 的地址标识符，该标识符在登录期间动态地分配。这样，交换机 1104 在 1112 向主机 1102 提供 FCID。向主机分配了主机 FCID 之后，主机可在步骤 1114 通过 SCSI REPORT（报告）命令对 DNS 服务器 1106 进行 DNS 查询，请求对该主机可用因而可见的 SCSI 目标。更具体地说，DNS 查询确定对该主机 FCID 可见的 SCSI 目

标。然后 DNS 服务器 1106 在 1116 向主机 1102 提供作为潜在目标端口的一个或多个虚拟包封端口的 FCID。

主机获得对它来说可用的那些 SCSI 目标端口的 FCID 之后，它在 1118 发送光纤信道处理登录命令到（由其 FCID 标识的）可用的虚拟包封 SCSI 目标端口中的一个或多个。如上所述，虽然分组指向了分配给虚拟包封端口的 FCID，但是，可能是由绑定到该虚拟包封端口或代表该虚拟包封端口进行陷入的虚拟化端口来实际处理这些分组。这一处理登录实现了一个映射层，将光纤信道“映射”到 SCSI。完成后，（多个）SCSI 虚拟包封端口 1108 在 1120 发送光纤信道接受消息。由于光纤信道被映射到 SCSI，因此主机可以将 SCSI 命令发送到所述（多个）SCSI 目标虚拟包封端口。

由于主机 1102 可以向（多个）虚拟包封端口 1108 发送 SCSI 命令，因此它通过将 SCSI 处理登录命令发送到 SCSI 目标虚拟包封端口 1108，从而可在 1122 执行 SCSI 处理登录。SCSI 虚拟包封端口 1108 然后发送 SCSI 接受命令 1124。因此通过 SCSI 协议在主机和 SCSI 目标虚拟包封端口之间建立了通信。例如，主机可以确定哪些 LUN 对它来说是可用的，并对那些对它可用的 LUN 进行读和写。

由于主机 1102 知道哪些 SCSI 目标（以及虚拟包封端口）对它来说是可用的，并且可以与这些端口中的每一个进行通信，因此，它可以在 1126 发送“SCSI 报告 LUN”命令到（多个）SCSI 目标虚拟包封端口 1108，以确定对该主机 FCID 可见的那些 LUN。例如，这些 LUN 可能仅仅是虚拟包封的那些 VLUN，或者可能是那些 VLUN 的子集。更具体地说，这一“报告”消息可被发送到分配给所述虚拟包封端口的 FCID。接收 SCSI 目标虚拟包封端口 1108 在 1128 确定哪些 LUN 对所述主机 FCID 是可见的，并在 1130 发送指示了一个或多个可用 LUN（例如 PLUN 或 VLUN）的应答消息。需要注意，接收虚拟包封端口实际上可能是绑定到虚拟包封端口的虚拟化端口或代表该虚拟包封端口进行陷入的虚拟化端口。因此，这些虚拟化端口还负责在 1128 执行 LUN 映射。下面将参考图 12 详细描述一种 LUN 映射方法。主机 1102 然后在 1132 通过虚拟包封端口 1108 发送

SCSI 读和写命令到特定的 VLUN。

可以任何通信协议来实现诸如陷入和绑定消息等虚拟化消息。所实现的协议优选地是可靠的通信协议，例如 TCP 套接口或运行在 TCP/IP 上的动态即时化协议（DIP）。

图 12 示出了可在图 11 的步骤 1128 处用于执行 LUN 映射的示例性 LUN 映射表。如图所示，LUN 映射表 1200 可用于为每个发起者（例如主机）1202 标识出那些通过虚拟包封的一个或多个虚拟包封端口 1206（例如 FCID）可见的那些 VLUN 1204。例如，一个指定的逻辑单元 1208 例如 LUN0 可用来表示引导盘。由于可能希望为每个主机提供一个不同的引导盘，因此所指定的逻辑单元 1208 与一个或多个 VLUN 1204 相关联，所述 VLUN 1204 通过所指定的虚拟包封端口 1206 而对主机 1202 可用。对特定主机 1202 可用的虚拟包封端口 1206 可被指定，或者可使用通配符来表明所有的虚拟包封端口对该主机来说都是可用的。因此，当通过虚拟包封端口之一从该主机接收到对指定的逻辑单元 1208 的请求时，与该指定的逻辑单元 1208 相关联的 VLUN 被利用来服务于该请求。

图 13 表示对应于图 12 的 LUN 映射表的虚拟包封。如图所示，虚拟包封 1302 表示 4 个 VLUN：A 1304、B 1306、C 1308 和 D 1310。虚拟包封 1302 具有两个虚拟包封端口，VEP1 1312 和 VEP2 1314。如图 12 所示，主机 H1 在任何虚拟包封端口上都将 LUN0 视为 VLUN A，主机 H2 在任何虚拟包封端口上都将 LUN0 视为 VLUN B，主机 H3 在任何虚拟包封端口上都将 LUN0 视为 VLUN C，主机 H4 只在虚拟包封端口 0 上将 LUN0 视为 VLUN D，而主机 H5 只在虚拟包封端口 1 上将 LUN0 视为 VLUN C。按照这种方式，所述 VLUN 的身份对主机来说是不可见的。因此，本发明提供了附加的存储虚拟化层级。

LUN 映射表优选地维护在中心位置例如虚拟包封服务器处。然而，根据一个实施例，也可提供 LUN 映射表并周期性地分发到存储区域网络内的合适网络设备（例如虚拟化端口）。例如，LUN 映射表可在主机登录时被分发到某个虚拟包封端口。换言之，向虚拟化端口提供了一个 LUN 映射（map），其对应于通过所述虚拟包封服务器已登录的主机。

尽管在此已示出并描述了本发明的示例性实施例和应用，但是可在本发明的原理、范围和精神的范围内作出许多变动和修改，这些变动和修改对本领域内的技术人员来说在阅读了本申请之后将会变得很清楚。例如，本发明被描述为应用到帧上。然而，应该理解到，本发明并不局限于这种实现，而是可同样应用到分组。而且，可应用本发明而不考虑其实现所处的上下文和系统。因此，一般地说，多个端口的绑定和陷入的协调控制并不一定需要如上所述地使用虚拟包封服务器来执行，而是可以其他方式来执行。

另外，尽管描述了示例性的交换机，但是上述实施例也可实现在多种网络设备（例如服务器）以及多种介质中。例如，用于实现上述发明的指令和数据可以存储在磁盘驱动器、硬盘驱动器、软盘、服务器计算机或远程联网的计算机上。因此，所述实施例应被理解为示例性的而非限制性的，本发明不应局限于此处所给出的细节，而是可以在所附权利要求的范围和等同物之内作出修改。

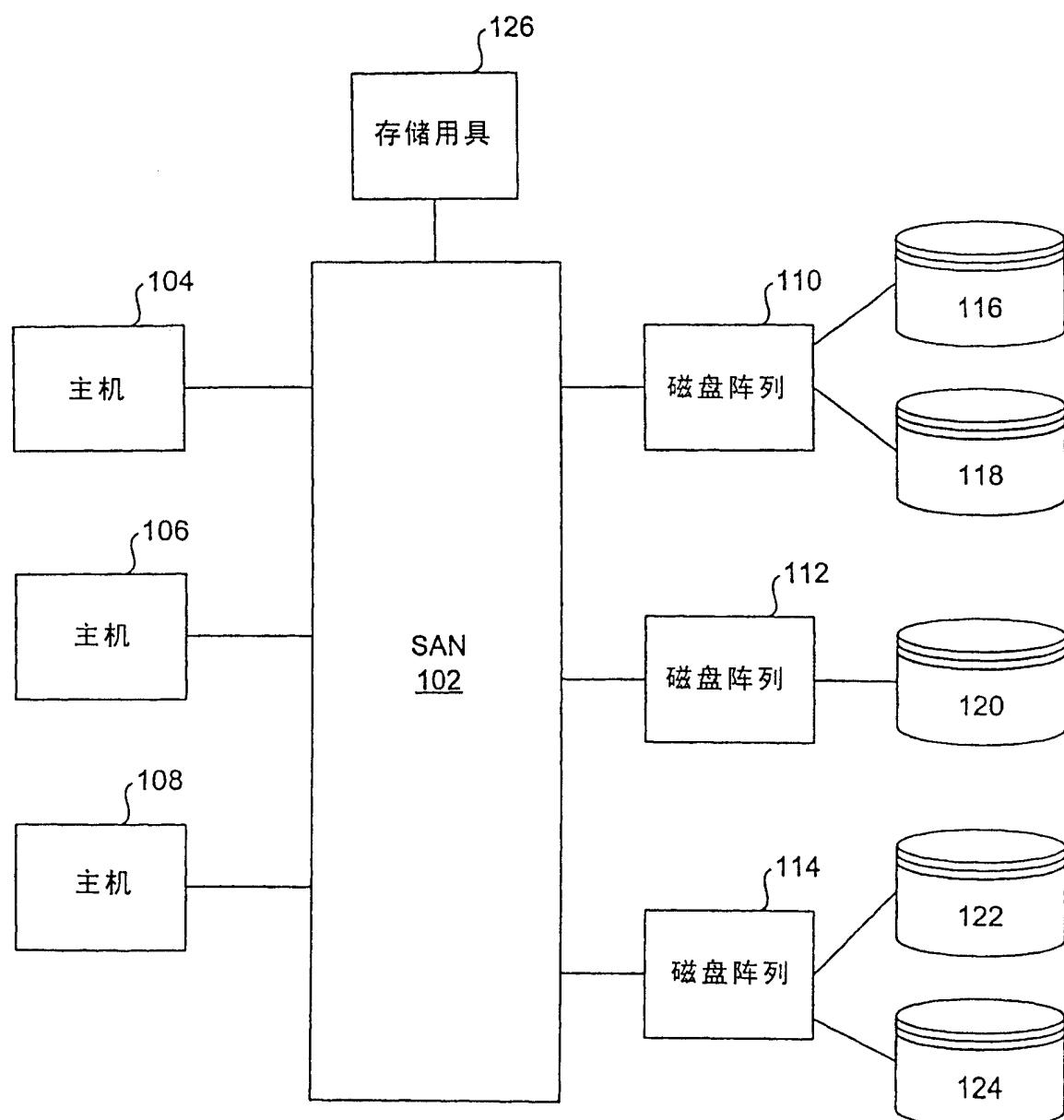


图1A

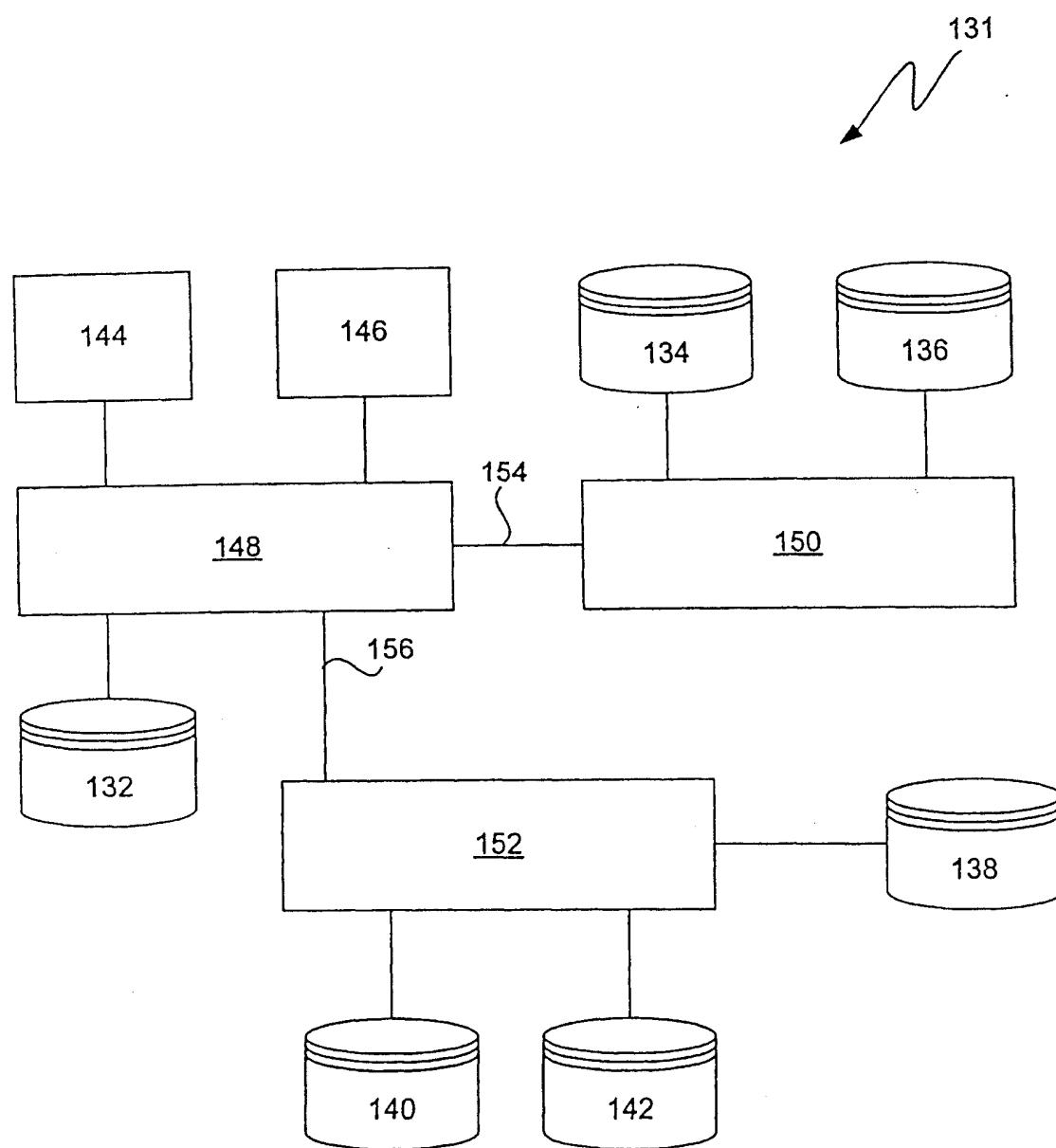


图1B

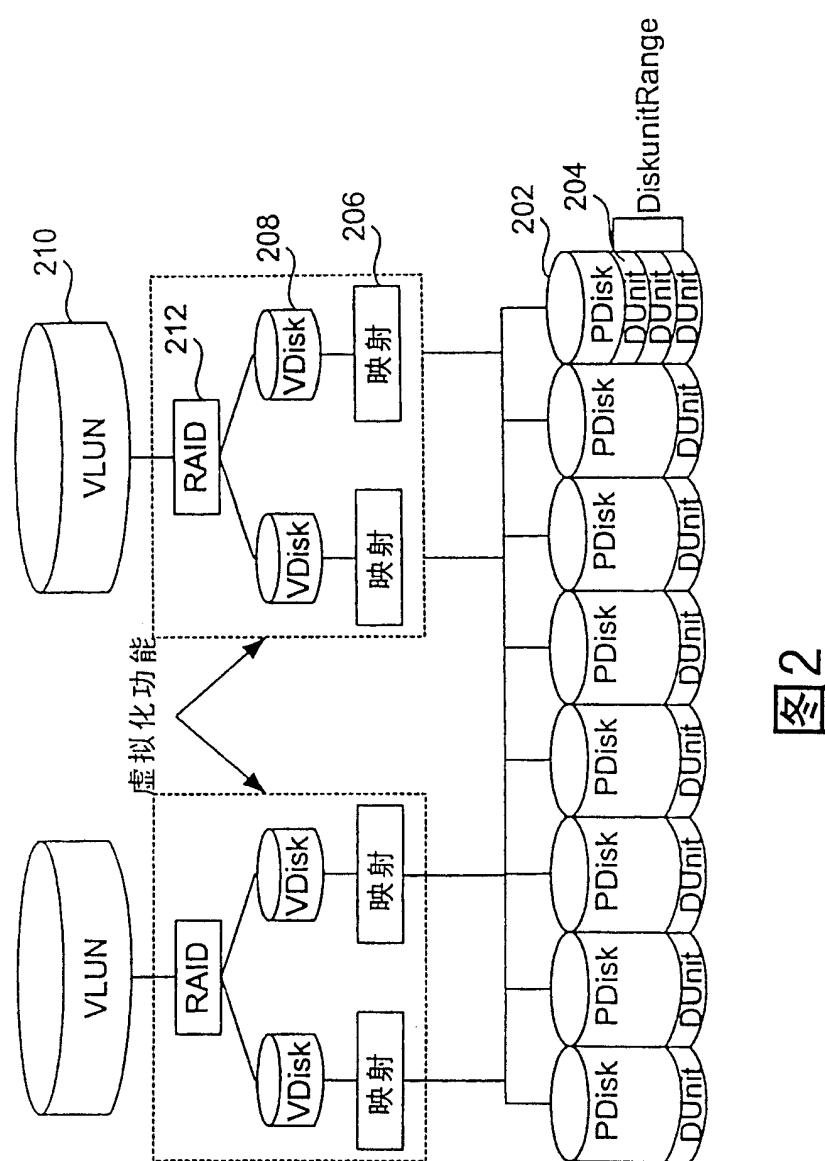


图2

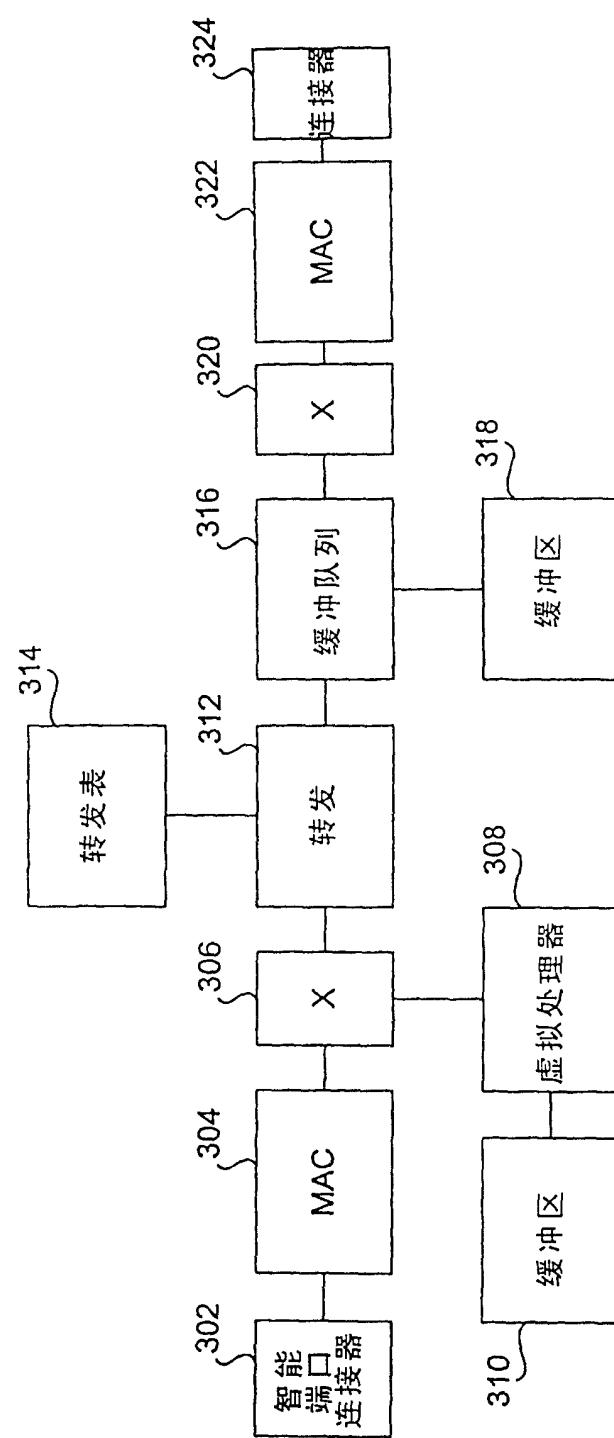


图3A

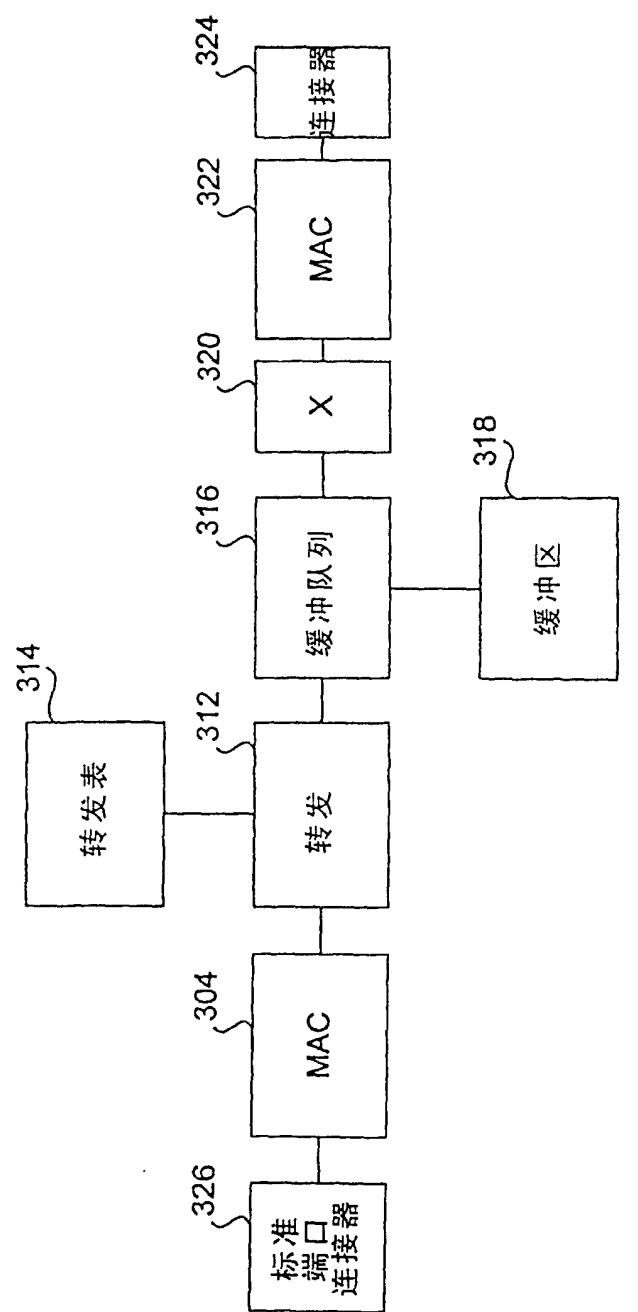


图3B

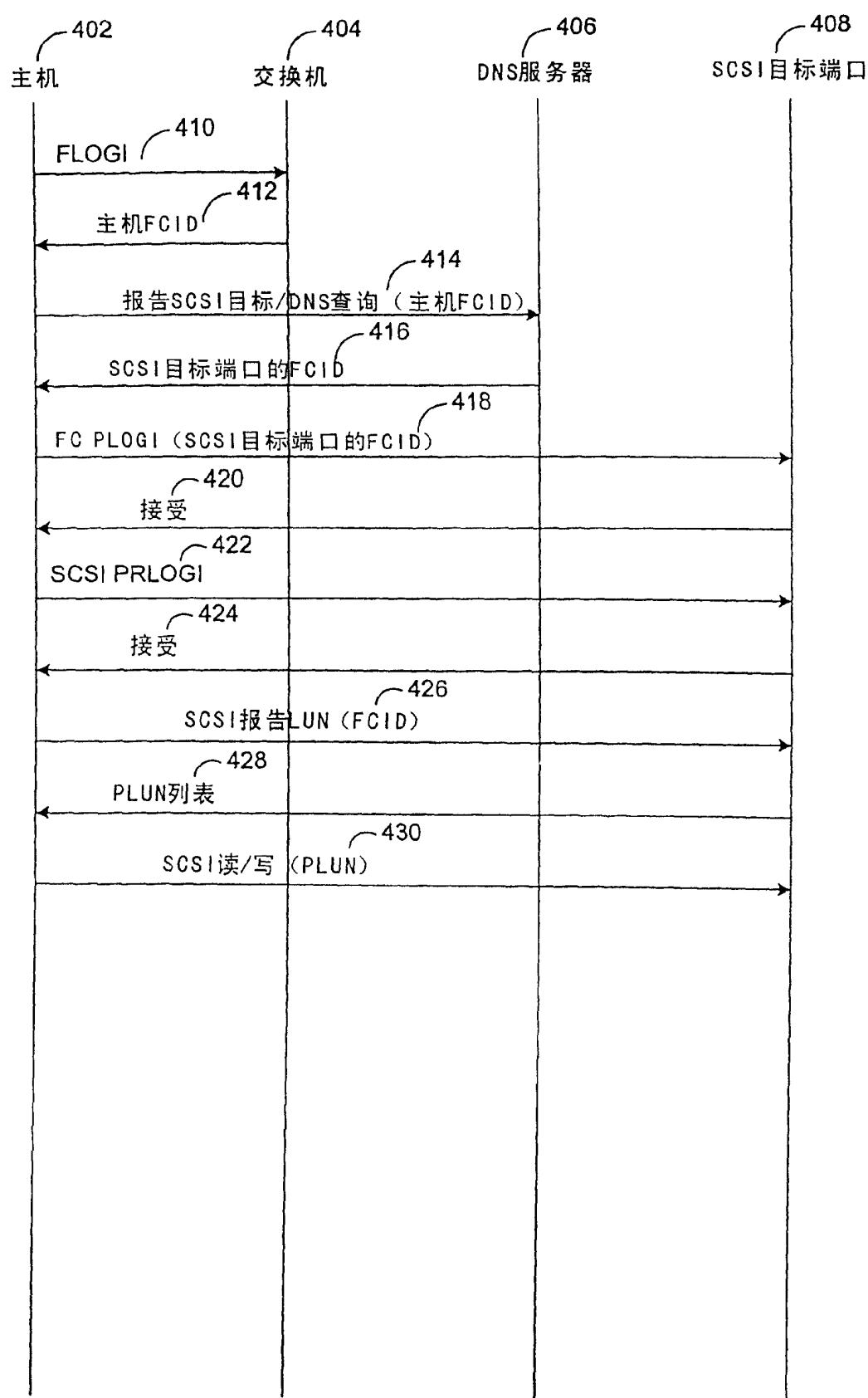


图 4

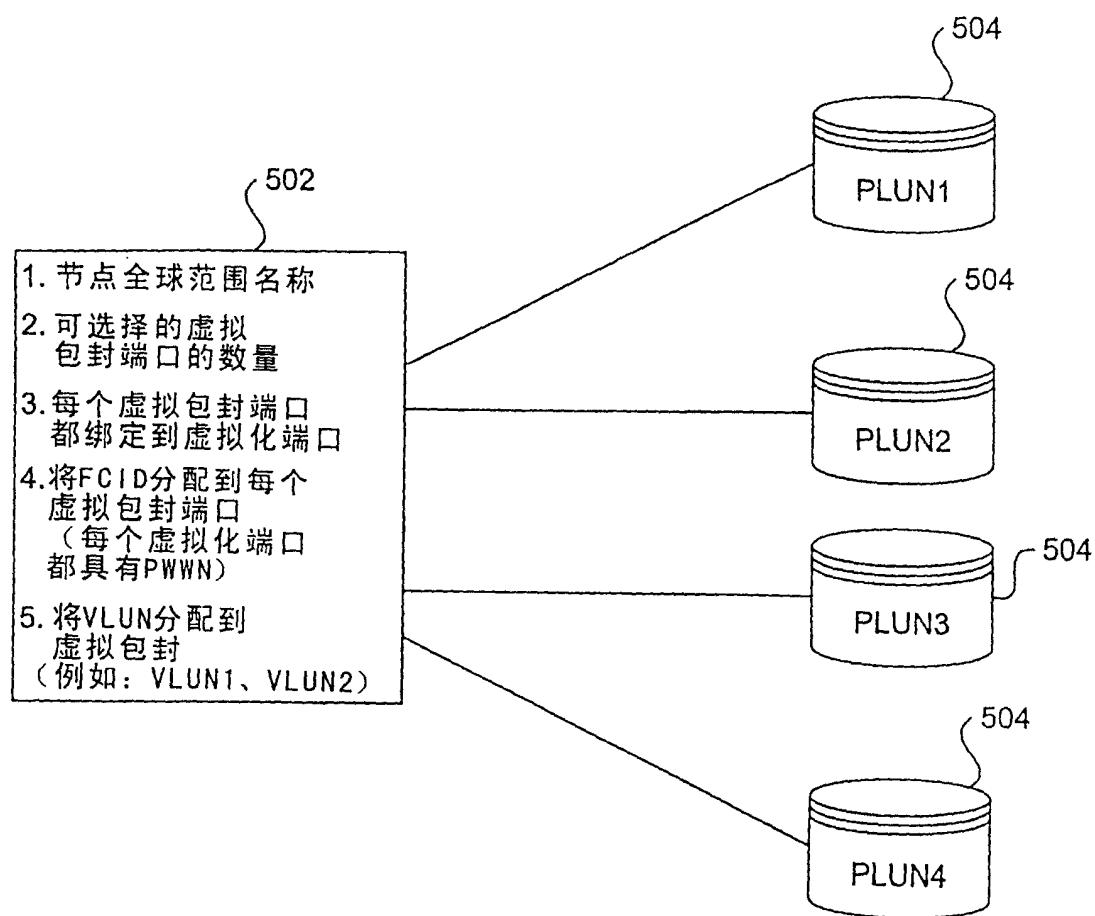


图5

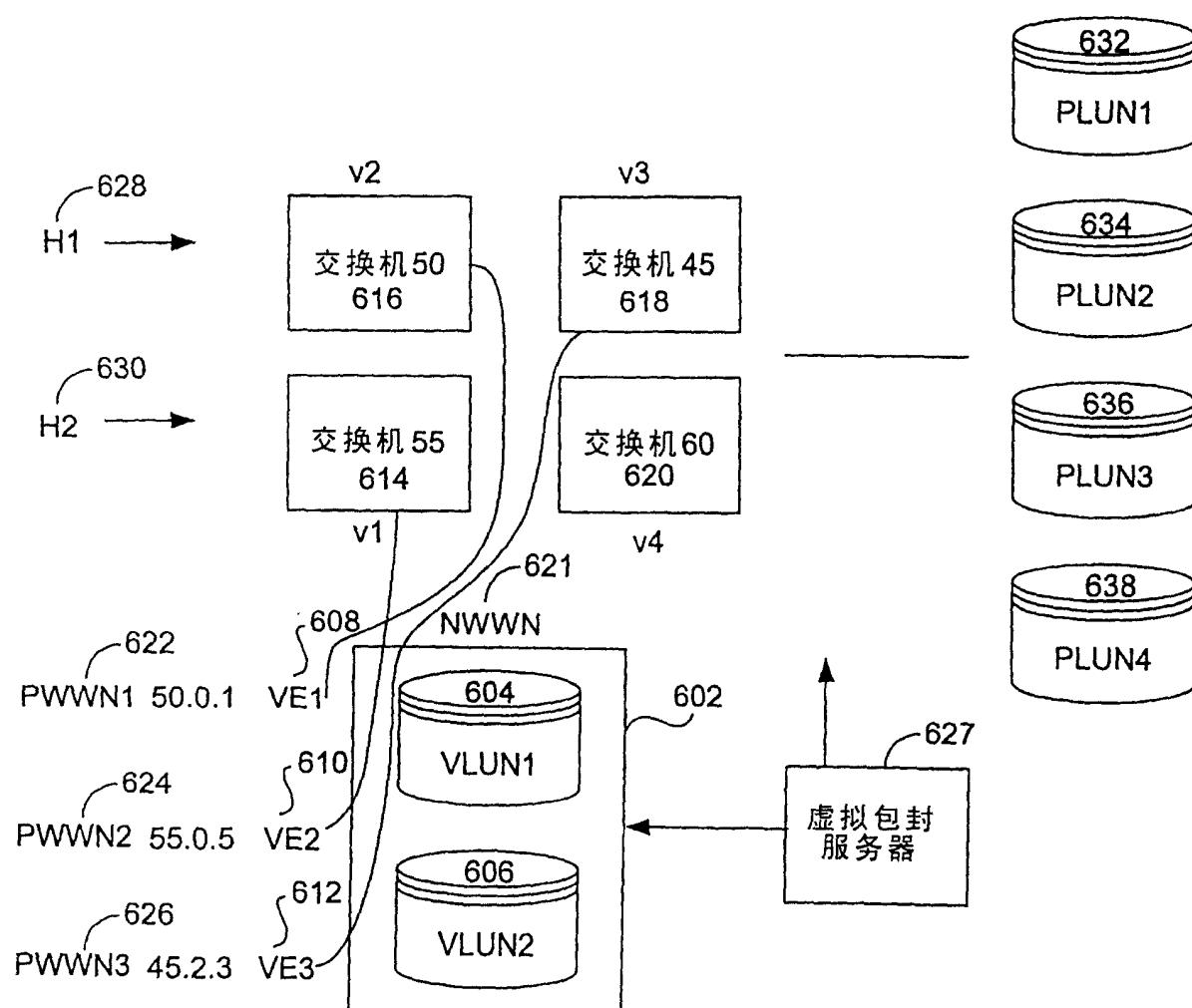


图6

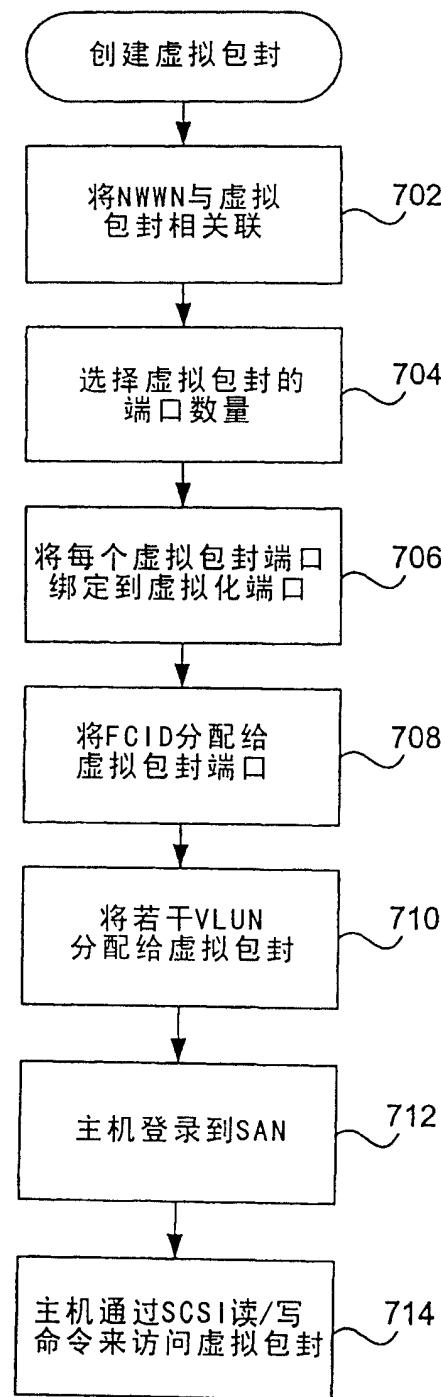


图7

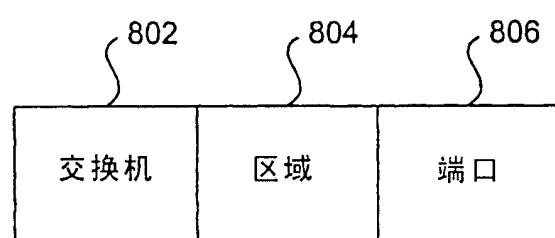


图8

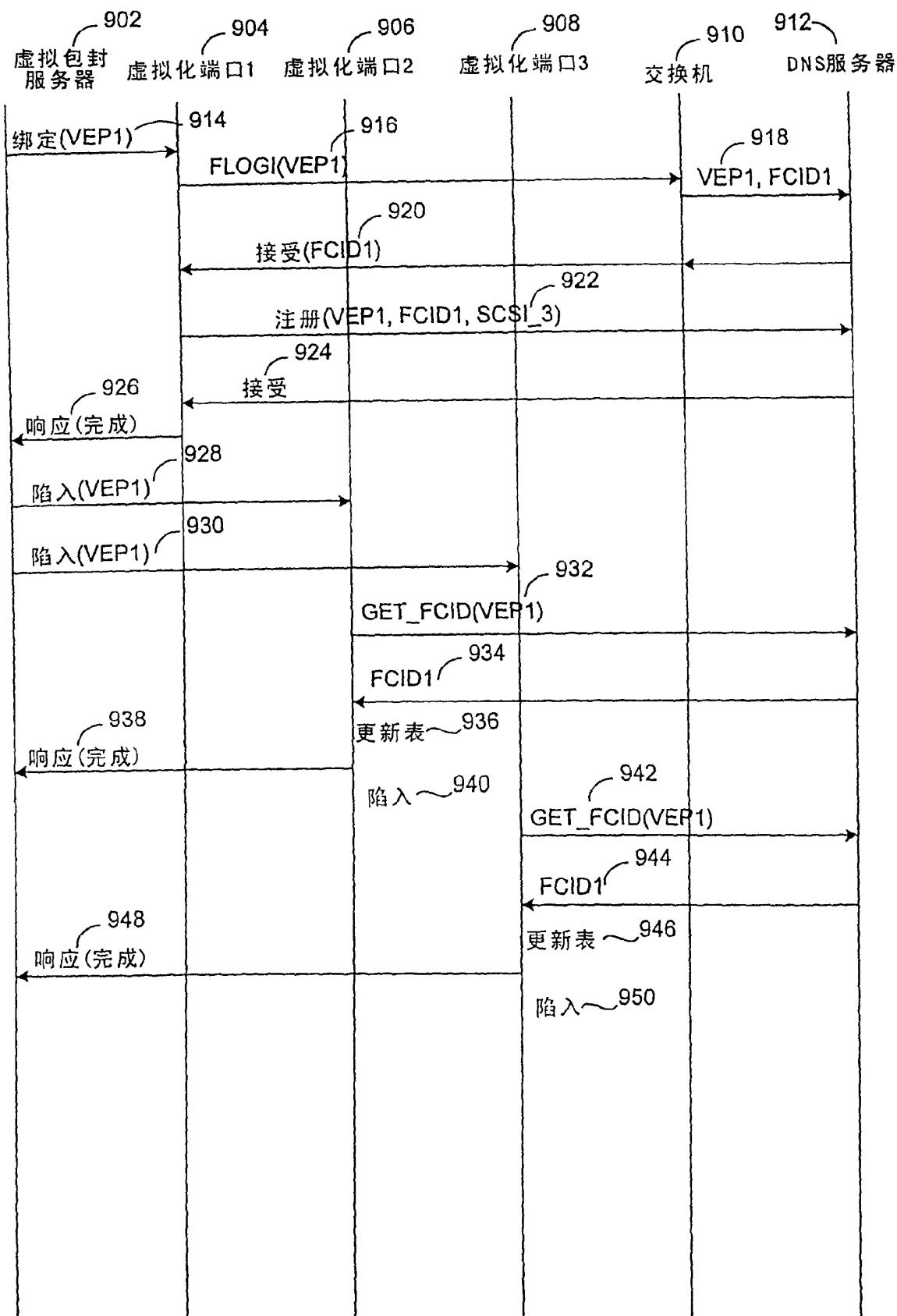


图9

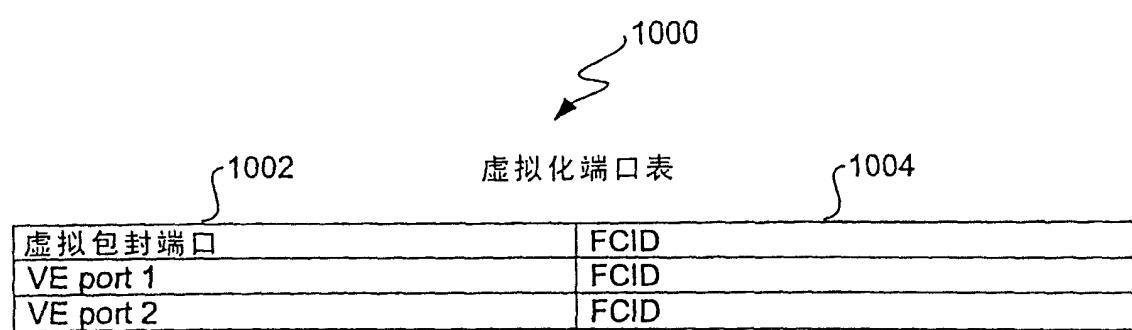


图10

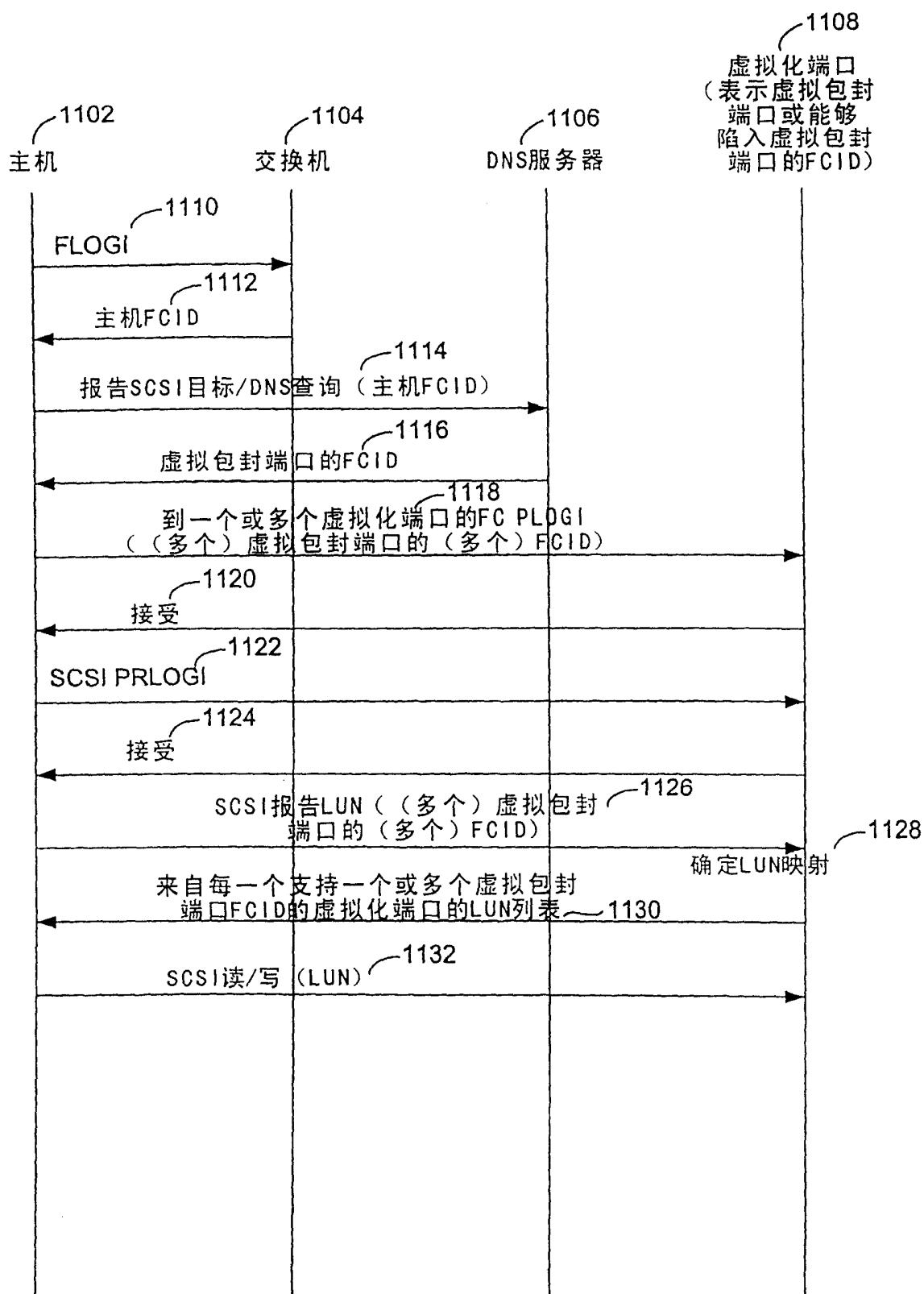


图 11

主机	VE端口	LUN #	VLUN
H1	*	0	A
H2	*	0	B
H3	*	0	C
H4	0	0	D
H4	1	0	C

图 12

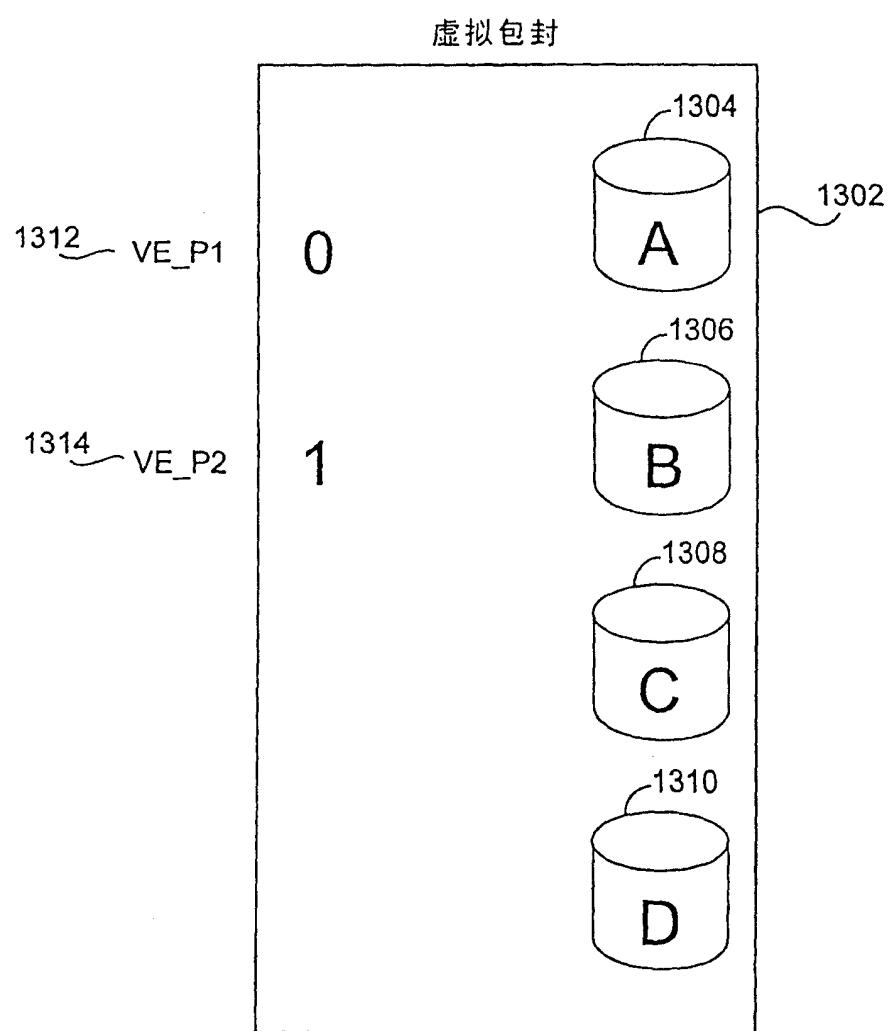


图 13