(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103109516 A
(43)申请公布日 2013.05.15

(21)申请号 201180044488.2
(22)申请日 2011.09.14
(30)优先权数据
12/882,795 2010.09.15 US
(85)PCT申请进入国家阶段日
2013.03.15
(86)PCT申请的申请数据
PCT/EP2011/065945 2011.09.14
(87)PCT申请的公布数据
WO2012/035067 EN 2012.03.22
(71)申请人 国际商业机器公司
地址 美国纽约阿芒克
(72)发明人 M. 肖伊克尔 J. 克林克
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邸万奎
(51)Int.Cl.
H04L 29/12(2006.01)
G06F 9/455(2006.01)

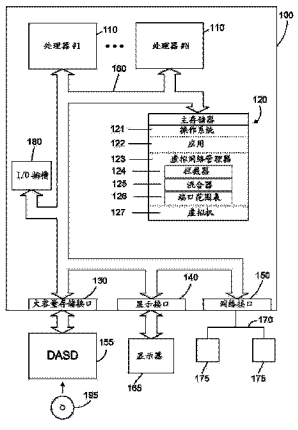
权利要求书2页 说明书9页 附图5页

(54)发明名称

共享单个IP地址的多虚拟机

(57)摘要

提供了允许多个虚拟机在外部网络地址空间上共享同一IP地址的方法和装置。虚拟机驻留在一个或多个物理主机计算机系统上。虚拟网络管理器处理来自主机计算机上的物理接口的网络流量，并基于目的地端口号，将网络数据转发到适当的虚拟机。外部网络上的数据分组各自具有目的地和源端口号。虚拟网络管理器使用端口范围表，其将每个虚拟机与用于传入数据分组的、目的地端口号的范围相关联。每个虚拟机被分配端口范围表中唯一的目的地端口范围，并且，基于数据分组中的目的地端口号，外部网络上的传入数据流量被路由到接收虚拟机。



CN 103109516 A

1. 一种装置，包括：

主机计算机系统，具有处理器和存储器；

物理接口，具有将所述主机计算机连接到外部网络的单个因特网协议（IP）地址；

所述存储器中的多个虚拟机，各自具有虚拟机号；

所述物理接口上接收的数据分组，具有目的地端口号；

虚拟网络管理器，用于取决于所述数据分组中的目的地端口号而将所述数据分组路由到所述多个虚拟机中的唯一一个。

2. 根据权利要求 1 所述的装置，还包括端口范围表，其具有多个端口范围和用于每个端口范围的对应的虚拟机号，并且，其中所述虚拟网络管理器通过选择与包括所述数据分组中的目的地端口号的端口范围相对应的、存储在所述端口范围表中的所述虚拟机号，来确定所述多个虚拟机中的唯一一个的虚拟机号。

3. 根据权利要求 1 所述的装置，还包括防火墙，保护所述主机计算机不受所述外部网络影响。

4. 根据权利要求 1 所述的装置，其中所述多个虚拟机位于多个主机计算机系统上。

5. 根据权利要求 1 所述的装置，其中所述虚拟网络管理器将所述数据分组转发到虚拟网络上的所述虚拟机。

6. 根据权利要求 1 所述的装置，其中所述数据分组符合从以下协议中选择的协议：TCP（传输控制协议）以及用户数据报协议（UDP）。

7. 根据权利要求 1 所述的装置，其中将所述虚拟机的临时端口配置为使用所述端口范围表中的分配给所述虚拟机的端口号。

8. 一种用于将数据发送到主机计算机系统上的虚拟机的方法，所述方法包括以下步骤：

配置具有单个因特网协议（IP）地址的多个虚拟机；

配置虚拟网络管理器，其具有端口范围表，所述端口范围表具有多个端口范围、以及用于每个端口范围的对应的虚拟机号；以及

取决于数据分组中的目的地端口号，将传入数据分组从物理接口路由到所述多个虚拟机中的唯一一个。

9. 根据权利要求 8 所述的方法，其中路由所述传入数据分组的步骤还包括：

确定与所述端口范围表中的包括所述数据分组中的目的地端口号的端口范围相对应的虚拟机号，并将所述数据分组路由到具有所确定的虚拟机号的所述唯一一个虚拟机。

10. 根据权利要求 8 所述的方法，还包括以下步骤：

在所述传入数据分组不被防火墙允许的情况下，丢弃所述传入数据分组；以及

如果所述分组不符合从 TCP（传输控制协议）以及用户数据报协议（UDP）中选择的协议，则返回所述传入数据分组；以及

将所述虚拟机的临时端口配置为使用所述端口范围表中的分配给所述虚拟机的端口号。

11. 根据权利要求 8 所述的方法，其中所述虚拟网络管理器将所述数据分组转发到虚拟网络上的所述虚拟机。

12. 根据权利要求 8 所述的方法，其中所述多个虚拟机位于多个主机计算机上。

13. 一种包括计算机程序代码的计算机程序，在其被载入计算机系统并执行时，执行根据权利要求 8 至 12 中的任一个的方法的所有步骤。

共享单个 IP 地址的多虚拟机

技术领域

[0001] 本发明涉及计算机系统，并且，更具体地，涉及在驻留于一个或多个物理主机计算机的多个虚拟机之间共享单个 IP 地址。

背景技术

[0002] 单个主机计算机可保持被称为虚拟机的计算机的多个虚拟实例。虚拟机有时被定义为真实机的有效且隔离的副本。由此，虚拟机是驻留在物理主机计算机上的虚拟计算机的副本或实例。虚拟机有时也被称为逻辑分区。虚拟机系统的本质优点在于，多个操作系统(OS)环境可以彼此隔离的方式共存于同一计算机上。另外，虚拟机可提供与真实机不同的指令集架构。虚拟机可被用来改善应用服务开通(provisioning)、维护、高可用性和灾难复原。

[0003] 典型地，驻留在物理主机计算机上的虚拟机必须共享主机计算机的物理网络接口。主机计算机的物理网络接口连接到外部网络。如在这里所使用的，外部网络是驻留在单个物理机外部的任意网络，且可以 / 可以不通过一系列防火墙间接接触。在一些情况下，将来自外部网络地址空间的单个 IP 地址分配给主机计算机的物理接口是有利的。驻留在主机的虚拟机使其自身的虚拟网络接口经由主机物理接口连接到同一外部网络。在现有技术中，已存在使多个虚拟机使用同一物理网络接口的各种方法。

[0004] US7782878 公开了由第二网络设备共享分配给第一网络设备的 IP 地址，使得源自第二网络设备的分组呈现为源自第一网络设备。网络设备通过使用计算机的 IP 地址、从一个或多个指定端口发送消息，来完成此任务，其中，所述指定端口未被该计算机使用。

[0005] US20090106404 公开了用于动态配置虚拟因特网协议地址的方法。在正常情况下，在 IP 地址指定连接到局域网(LAN)的节点时，IP 地址中的某些或全部一般会指定 LAN 的接入点。然而，除了 IP 地址之外，还可使用“端口”指定来指定接入点(LAN)内的节点。即，可使用 IP 地址来指定 LAN 的因特网接入点，并使用端口来指定连接到该接入点处的因特网的 LAN 之内的节点。因特网接入点将在因特网上接收到的分组的 IP 地址(以及端口，如果包括的话)变换为局域网地址，其也可为 IP 地址。

[0006] US74478042 公开了在局域 IP 网络上的多重无线通信(multi-telecommunication)的方法。在此方法中，由多个终端共享每个 IP 地址。局域 IP 网络 101 通过内部 IP 地址来识别每个终端，即，10.0.0.0 至 10.0.255.255。每个终端被分配不同的端口号，以在局域 IP 网络 101 的终端之间进行区分。这里，端口表示 TCPfuDP 端口，而不是物理或硬件上的含义。通常，IP 网络分配特定端口来处理 HTTP、E-mail 和 FTP，并具有多个保留端口。将这些保留的端口用作 ID 来识别连接到局域 IP 网络的终端。

[0007] KR2002007477A2 公开了使用端口号来共享 IP 地址的装置。共享 IP 地址的装置被提供用来防止 IP 地址的浪费，并通过使用在 TCPAJDP/IP 报头中包括的端口号来提高速度。

[0008] 然而，上面的现有技术均不能克服如何跨越多个虚拟机而共享单个 IP 地址的问题。

发明内容

[0009] 这里的公开和权利要求针对于在外部网络地址空间上被共同分配同一 IP 地址的多个虚拟机(虚拟计算机)。虚拟机驻留在一个或多个物理主机计算机系统上。虚拟网络管理器处理来自主机计算机上的物理接口的网络流量,并基于目的地端口号,将网络数据转发到适当的虚拟机。外部网络上的数据分组各自具有目的地和源端口号。虚拟网络管理器使用端口范围表,其将每个虚拟机与用于传入数据分组的目的地端口号的范围相关联。每个虚拟机被分配端口范围表中唯一的目的地端口范围,并且,外部网络上的传入数据流量基于数据分组中的目的地端口号而被路由到接收虚拟机。

[0010] 从第一方面看,本发明提供了一种装置,包括 :主机计算机系统,具有处理器和存储器 ;物理接口,具有将主机计算机连接到外部网络的单个因特网协议(IP)地址 ;存储器中的多个虚拟机,各自具有虚拟机号 ;在物理接口上接收的数据分组,具有目的地端口号 ;虚拟网络管理器,用于取决于数据分组中的目的地端口号,将数据分组转发到多个虚拟机中的唯一一个。

[0011] 优选地,本发明提供了装置,还包括端口范围表,其具有多个端口范围和用于每个端口范围的对应的虚拟机号,并且,其中虚拟网络管理器通过选择与包括数据分组中的目的地端口号的端口范围相对应的、存储在端口范围表中的虚拟机号,来确定所述多个虚拟机中的唯一一个的虚拟机号。

[0012] 优选地,本发明提供了装置,还包括防火墙,保护主机计算机不受外部网络影响。

[0013] 优选地,本发明提供了装置,其中所述多个虚拟机位于多个主机计算机系统上。

[0014] 优选地,本发明提供了装置,其中虚拟网络管理器将数据分组转发到虚拟网络上的虚拟机。

[0015] 优选地,本发明提供了装置,其中数据分组符合从以下协议中选择的协议 :TCP(传输控制协议)以及用户数据报协议(UDP)。

[0016] 优选地,本发明提供了装置,其中将虚拟机的临时端口配置为使用所述端口范围表中的分配给所述虚拟机的端口号。

[0017] 从第二方面看,本发明提供了一种用于将数据发送到主机计算机系统上的虚拟机的方法,所述方法包括以下步骤 :配置具有单个因特网协议(IP)地址的多个虚拟机 ;配置虚拟网络管理器,其具有端口范围表,所述端口范围表具有多个端口范围、以及用于每个端口范围的对应的虚拟机号 ;以及取决于数据分组中的目的地端口号,将所述传入数据分组从物理接口路由到所述多个虚拟机中的唯一一个。

[0018] 优选地,本发明提供了方法,其中,在计算机存储器中存储的计算机软件程序中实施、并由计算机处理器执行所述方法的步骤。

[0019] 优选地,本发明提供了方法,其中,路由传入数据分组的步骤还包括 :确定与所述端口范围表中的包括所述数据分组中的目的地端口号的端口范围相对应的虚拟机号,并将所述数据分组路由到具有所确定的虚拟机号的唯一一个虚拟机。

[0020] 优选地,本发明提供了方法,还包括以下步骤 :在传入数据分组不被防火墙允许的情况下,丢弃传入数据分组 ;以及如果分组不符合从 TCP (传输控制协议)以及用户数据报协议(UDP)中选择的协议,则返回传入数据分组 ;以及将虚拟机的临时端口配置为使用所

述端口范围表中的分配给所述虚拟机的端口号。

[0021] 优选地，本发明提供了方法，其中，虚拟网络管理器将数据分组转发到虚拟网络上的虚拟机。

[0022] 优选地，本发明提供了方法，其中，所述多个虚拟机位于多个主机计算机上。

[0023] 从第三方面看，本发明提供了一种用于将数据发送到主机计算机系统上的虚拟机的方法，所述方法包括以下步骤：配置具有单个因特网协议（IP）地址的位于至少一个物理主机计算机上的多个虚拟机；配置虚拟网络管理器，其具有端口范围表，所述端口范围表具有多个端口范围、以及用于每个端口范围的对应的虚拟机号；以及通过确定与所述端口范围表中的包括所述数据分组中的目的地端口号的端口范围相对应的虚拟机号、并将所述数据分组路由到具有所确定的虚拟机号的唯一一个虚拟机，基于数据分组中的目的地端口号而将传入数据分组从物理接口路由到所述多个虚拟机中的唯一一个；在传入数据分组不被防火墙允许的情况下，丢弃传入数据分组；以及如果分组不符合从 TCP（传输控制协议）以及用户数据报协议（UDP）中选择的协议，则返回传入数据分组；以及将虚拟机的临时端口配置为使用所述端口范围表中的分配给所述虚拟机的端口号；其中，在虚拟网络上路由数据分组；并且，其中，在计算机存储器中存储的计算机软件程序中实施、并由计算机处理器执行所述方法的步骤。

[0024] 从第四方面看，本发明提供了一种制品，其包括在有形计算机可读存储介质上存储的软件，所述软件包括：虚拟网络管理器，其取决于数据分组中的目的地端口号，将在物理接口上接收到的具有目的地端口号的数据分组转发到多个虚拟机中的唯一一个，其中，所述多个虚拟机共享物理接口，其具有将主机计算机连接到外部网络的单个因特网协议（IP）地址。

[0025] 优选地，本发明提供了一种制品，其中，虚拟网络管理器还包括端口范围表，所述端口范围表具有多个端口范围、以及用于每个端口范围的对应的虚拟机号，并且，其中虚拟网络管理器通过选择与包括数据分组中的目的地端口号的端口范围相对应的、存储在端口范围表中的虚拟机号，来确定所述多个虚拟机中的唯一一个的虚拟机号。

[0026] 优选地，本发明提供了一种制品，其中，防火墙保护主机计算机不受外部网络影响。

[0027] 优选地，本发明提供了一种制品，其中，所述多个虚拟机位于多个主机计算机上。

[0028] 优选地，本发明提供了一种制品，其中，虚拟网络管理器将数据分组转发到虚拟网络上的虚拟机。

[0029] 优选地，本发明提供了一种制品，其中，数据分组符合从以下协议中选择的协议：TCP（传输控制协议）以及用户数据报协议（UDP）。

[0030] 优选地，本发明提供了一种制品，其中，将虚拟机的临时端口配置为使用所述端口范围表中的分配给所述虚拟机的端口号。

附图说明

[0031] 现在，通过仅仅示例的方式，参照附图来描述本发明的优选实施例，附图中：

[0032] 图 1 是根据本发明的优选实施例的计算机系统的框图，其中，如在这里描述的，虚拟网络管理器利用端口范围表来使多个虚拟计算机能够使用单个网络 IP 地址；

[0033] 图 2 是示出根据本发明的优选实施例的、虚拟网络管理器如何将数据分组路由到驻留在主机计算机上的多个虚拟机的框图；

[0034] 图 3 是根据本发明的优选实施例的、表示这里描述的在网络上发送的数据分组的框图；

[0035] 图 4 是根据本发明的优选实施例的、示出端口范围表的示例的框图；

[0036] 图 5 是类似于图 1 的框图，其示出了根据本发明的优选实施例的多个物理端口，其中虚拟机利用同一 IP 地址；

[0037] 图 6 是根据本发明的优选实施例的、在多个虚拟机之间共享单个 IP 地址的方法流程图；以及

[0038] 图 7 是根据本发明的优选实施例的方法流程图的示例，其用于根据图 6 中的步骤 630，基于端口范围表来将传入数据路由到多个虚拟机。

具体实施方式

[0039] 这里描述了多个虚拟机用来共享外部网络地址空间上的同一 IP 地址的装置和方法。虚拟机驻留在一个或多个物理主机计算机系统上。虚拟网络管理器处理来自主机计算机上的物理接口的网络流量，并基于目的地端口号而将网络数据转发到适当的虚拟机。外部网络上的数据分组各自具有目的地和源端口号。虚拟网络管理器使用端口范围表，其将每个虚拟机与用于传入数据分组的、某个范围的目的地端口号相关联。每个虚拟机被分配端口范围表中唯一的目的地端口范围，并且，基于数据分组中的目的地端口号，外部网络上的传入数据流量被路由到接收虚拟机。

[0040] 参照图 1，计算机系统 100 是计算机系统的一个适当的实施方式，其包括这里描述的虚拟网络管理器。计算机系统 100 是国际商业机械公司(IBM®)的 Power System，其可运行多个操作系统，包括IBM® i操作系统、以及 Linux 操作系统(Linux 是 Linus Torvalds 在美国和 / 或其它国家的注册商标)。然而，本领域的技术人员将理解的是，这里的公开同样适用于能够连接到外部网络的任何计算机系统。如图 1 所示，计算机系统 100 包括一个或多个处理器 110、主存储器 120、大容量存储接口 130、显示接口 140、以及网络接口 150、和多个 I/O 插槽 180。通过使用系统总线 160 来互连这些系统组件。大容量存储接口 130 用来将具有诸如直接存取存储设备 155 的计算机可读介质的大容量存储设备连接到计算机系统 100。直接存取存储设备 155 的一个特定类型是可读写 CD-RW 驱动器，其可向 / 从 CD-RW195 存储 / 读取数据。注意，大容量存储接口 130、显示接口 140、以及网络接口 150 实际上可在耦接到 I/O 插槽 180 的适配器中实现。I/O 适配器是一个适当的网络接口 150，其可在外部卡中实现，所述外部卡被插入到 I/O 插槽 180 之一。另外，诸如调制解调器的其它 I/O 设备可被插入到 I/O 插槽 180 之一。

[0041] 优选地，主存储器 120 包含操作系统 121。优选地，操作系统 121 为诸如 AIX 或 Linux 的多任务操作系统；然而，本领域的技术人员将理解的是，本公开的精神和范围不限于任一操作系统。可使用任何适用的操作系统。操作系统 121 是复杂的程序，其包含低级代码来管理计算机系统 100 的资源。这些资源中的一些是处理器 110、主存储器 120、大容量存储接口 130、显示接口 140、网络接口 150、系统总线 160、以及 I/O 插槽 180。每个虚拟机也可具有操作系统。每个虚拟机或分区中的操作系统作为虚拟机中的操作系统可以相同，

或可为完全不同的操作系统。由此，一个虚拟机可运行 AIX 操作系统，而不同的虚拟机可运行 AIX 的另一个实例，可能是不同的版本或具有不同的环境设置(例如，时区或语言)。以这种方式，虚拟机可在同一物理计算机系统上提供完全不同的计算环境。存储器还包括软件应用 122。存储器包括虚拟网络管理器 123。虚拟网络管理器包括拦截器 124、混合器 125、以及端口范围表 126。存储器还包括一个或多个虚拟机或计算机 127。下面进一步描述存储器中的这些实体中的每个。

[0042] 虚拟机 127 被示出为驻留在主存储器 120 内。然而，本领域的技术人员将理解的是，虚拟机(或逻辑分区)是包括除了存储器之外的资源的逻辑构造。典型地，虚拟机 127 指定存储器的一部分、连同处理器能力以及诸如 I/O 插槽 180 和可驻留在 I/O 插槽 180 中的 I/O 适配器的其它系统资源的分配。由此，一个虚拟机可被定义为包括两个处理器、以及存储器 120 的一部分、连同一个或多个 I/O 处理器，所述 I/O 处理器可提供大容量存储接口 130、显示接口 140、网络接口 150 或到插入 I/O 插槽 180 中的 I/O 适配器或其它设备(如调制解调器)的接口的功能。随后，另一个虚拟机可被定义为包括三个其它处理器、存储器 120 的不同部分、以及一个或多个 I/O 处理器。图 1 中示出虚拟机，其用来象征性地表示虚拟机或逻辑分区，其可包括计算机系统 100 内的存储器 120 之外的系统资源。

[0043] 计算机系统 100 利用公知的虚拟寻址机制，其允许计算机系统 100 的程序如同它们仅具有对大的单个存储实体的访问那样工作，而不是访问多个较小的存储实体，诸如主存储器 120 和 DASD 设备 155。因此，尽管将操作系统 121、应用 122、虚拟网络管理器 123 和虚拟机 127 示出为驻留在主存储器 120 中，但本领域的技术人员将认识到，这些部件不一定全部被同时完全包含在主存储器 120 中。也应注意的是，术语“存储器”在这里一般用来表示计算机系统 100 的整个虚拟存储器，并可包括耦接到计算机系统 100 的其它计算机系统的虚拟存储器。

[0044] 可从一个或多个微处理器和 / 或集成电路构造处理器 110。处理器 110 执行在主存储器 120 中存储的程序指令。主存储器 120 存储处理器 110 可访问的程序和数据。当计算机系统 100 启动时，处理器 110 最初执行组成操作系统 121 的程序指令，之后执行组成应用 122 和虚拟网络管理器 123 的程序指令。

[0045] 尽管计算机系统 100 被示出为仅包含单个处理器和单个系统总线，但本领域的技术人员将理解的是，可使用具有多个处理器和 / 或多个总线的计算机系统来实现虚拟网络管理器。另外，优选使用的接口各自包括独立的完全编程的微处理器，其被用来从处理器 110 卸载计算密集的处理。然而，本领域的技术人员将理解的是，也可使用 I/O 适配器来执行这些功能。

[0046] 显示接口 140 被用来将一个或多个显示器 165 直接连接到计算机系统 100。可为非智能(即，dumb)终端或完全可编程的工作站的这些显示器 165 被用来向系统管理员和用户提供与计算机系统 100 通信的能力。然而，注意，尽管提供了显示接口 140 来支持与一个或多个显示器 165 的通信，但计算机系统 100 不一定需要显示器 165，这是因为，所有所需的与用户和其他处理的交互可经由网络接口 150 (例如，基于 web 客户端的用户)发生。

[0047] 网络接口 150 被用来将计算机系统 100 经由网络 170 连接到其它计算机系统或工作站 175。网络接口 150 广义上代表互连电子设备的任何适当方式，而不考虑网络 170 是否包括当前的模拟和 / 或数字技术、或经由将来的一些网络机制。另外，可使用很多不同的网

络协议来实现网络。这些协议是专门的计算机程序，其允许计算机跨越网络通信。TCP（传输控制协议）和用户数据报协议（UDP）是适用的网络协议的示例。

[0048] 图 2 示出了主机计算机的框图，其中多个虚拟机共享外部网络地址空间上的同一 IP 地址。图 2 中的主机计算机 100 是上面参照图 1 描述的主机计算机、或类似的计算机系统。主机计算机 100 通过物理网络 214 连接到网络云 212。网络云表示连接在一起并与主机计算机 100 通信的计算机的外部网络。来自网络云 212 中的其他计算机的数据通信通过防火墙 216 流向主机计算机 100。根据不同的数据协议，以数据分组的形式，在网络 214 上将数据发送到主机计算机。虚拟网络管理器 123 将数据分组路由到驻留在主机计算机 100 上的多个虚拟机 127A、127B。虚拟网络管理器 123 在物理接口 216 上接收数据分组，并随后使用虚拟接口 220，将数据分组发送到适当的虚拟机。虚拟网络管理器具有 ：拦截器 124，其管理传入数据 ；以及混合器 125，其管理传出数据。混合器 125 从虚拟机 127A、127B 接收传出分组，并将它们发送到外部网络 212。拦截器 124 拦截到共享地址的传入流量，并取决于目的地端口而将其经由虚拟接口发送到目的地虚拟机，或者，如果目的地端口不匹配任一分配的端口范围，则将其返回到主机网络堆栈。拦截器使用端口范围表 126 来确定将每个数据分组发送到何处。拦截器查看数据分组中的目的地端口号，并将数据分组发送到这样的虚拟机，该虚拟机被分配用来通过由端口范围表 126 所确定的该特定目的地端口号接收数据分组。

[0049] 图 3 是这样的框图，其表示用于在外部网络上的数据通信的数据分组的高度简化图。数据分组可为本领域公知的 TCP 或 UDP 数据分组。数据分组 300 包括 IP 地址和目的地端口号 312。这里未描述数据分组的其它元素 314，但其在本领域中是公知的。

[0050] 图 4 示出表示虚拟网络管理器 123 （图 2）中的拦截器 124 （图 2）使用的端口范围表 126 的一个适用实施方式的表。优选地，端口范围表 126 是在存储器、数据存储设备或两者中存储的记录的文件。端口范围表 126 包括多个目的地端口范围 410、以及对于每个端口范围的关联的虚拟机 412。端口范围 410 定义一个或多个目的地端口号，其被虚拟网络管理器用来将数据路由到对应的虚拟机 412。在示出的例子中，端口范围 0-25414 与虚拟机 1416 相关联，端口范围 26-80418 与虚拟机 2420 相关联。端口范围表 126 可包括如由与其它虚拟机 424 相关联的“其它”范围 422 所指示的任意数目的其它端口范围。可以任意适用格式存储端口范围表 126，以示出这里描述的端口范围和虚拟机之间的逻辑条件。可在主机计算机上关闭全部端口范围，以禁用整个虚拟机的分组，由此在管理主机上的虚拟机时简化系统管理。

[0051] 对于 TCP 和 UDP 协议，单个 IP 地址具有有限数目的目的地端口，且在使用一个 IP 地址时，端口号一般不会在应用之间冲突。一个 IP 地址可仅允许虚拟机上的一个应用成为到特定端口的通信的接收器。例如，只有一个虚拟机可使用 TCP 端口 21 用来通信，其中如这里所述，仅存在一个 IP 地址。通过允许虚拟机可见的地址空间属于外部网络地址空间，虚拟机的地址空间对包括点对点协议和 IP 电话（VoIP）协议的所有协议是透明的。

[0052] 混合器 125 和拦截器 124 二者都位于主机防火墙 216 之后，由此保护虚拟机不受外部威胁。主机系统和客户端系统的防火墙可保持不变。由于共享的 IP 地址对于主机来说被视为“本地的”，所以，其将任何分组规则视为如同其为本地规则，并将其指向本地应用。不需要次级防火墙或规则集，这是由于仅使用于一个 IP 地址。

[0053] 在上述优选示例中，所有虚拟机被配置为使用网络接口上的同一 IP 地址。每个虚拟机被分配唯一的端口范围，其可包括一个或多个不连续的范围。正在接受传入的 TCP 或 UDP 分组的所有应用被配置为仅使用来自分配的范围的端口，这是由于仅这些端口将是已知的传入 / 传出端口。虚拟机操作系统可被配置为使用来自分配的范围的临时端口（ephemeral port）。临时端口被用作传出 TCP 和 UDP 中的暂时端口。虚拟机在端口范围表中的分配给虚拟机的相同的端口范围中，分配传出消息上的源端口，使得返回消息将返回到适当的虚拟机。主机被配置为拦截发送到被分配到虚拟机的共享 IP 地址的分组，并基于分组目的地端口号，将其转发到目的地机。典型地，所有传出分组未修改便被传送到外部网络。如果主机也使用共享的 IP 地址，则将唯一的端口范围分配给主机。在此情况下，主机从此范围中分配永久和临时端口。主机接收的用于共享地址的分组被拦截器拦截，并指向虚拟机。如果主机使用共享 IP，则将一个虚拟机端口范围未匹配的所有分组返回到主机网络堆栈。

[0054] 图 5 示出了计算机系统的框图，其中多个虚拟机共享外部网络地址空间上的同一 IP 地址。图 5 的计算机系统类似于图 2 中示出的系统，但其示出了该系统可被如何调整为多个物理主机计算机的例子。在图 5 中，主机计算机 510A 具有虚拟网络管理器 123，其类似于图 2 中描述的主机计算机 100。与图 2 中的系统相反，图 5 中的虚拟网络管理器 123 与驻留在一个或多个其它主机上的虚拟机通信。在示出的例子中，虚拟网络管理器 123 将数据分组发送到主机 B510B 上的虚拟机 A125A 和虚拟机 B125B、以及主机 C510C 上的虚拟机 C125C 和虚拟机 D125D。在此情况下，虚拟网络管理器处理物理网络 512（而不是主机计算机 510A、510B、510C 之间的虚拟网络）的、到不同的物理主机计算机上的虚拟机的通信。对其它主机计算机上的虚拟机的连接可使用任意适用的物理网络连接。此架构允许虚拟机迁移到不同的物理主机，而不需要改变 IP 地址。

[0055] 图 6 示出了方法 600，其用于将外部网络上的同一 IP 地址分配给多个虚拟计算机，如这里所述。优选地，由虚拟网络管理器 123（图 1）执行方法 600 中的步骤，但是还可由与计算机系统相关联的其它软件或系统管理器来执行部分所述方法。首先配置多个虚拟机来使用单个 IP 地址（步骤 610）。接下来，配置具有用于每个虚拟机的端口范围的端口范围表（步骤 620）。随后，配置每个虚拟机的临时端口，以使用端口范围表中为虚拟机分配的端口范围中的源端口号（步骤 630）。随后，基于数据分组中的目的地端口号，将物理接口上的传入数据路由到多个虚拟机（步骤 640）。随后，完成该方法。

[0056] 图 7 示出了方法 630，其用于基于端口范围表，将物理接口上的数据路由到多个虚拟机。方法 630 是根据前述段落中描述的示例来执行图 6 中的步骤 630 的示例。优选地，由虚拟网络管理器 123（图 1）执行方法 630 中的步骤，但是还可由与计算机系统相关联的其它软件来执行部分所述方法。对于物理接口上的每个新的传入数据分组执行方法 630（步骤 710）。接下来，防火墙检查数据分组（步骤 720）。如果防火墙不允许该数据分组（步骤 720= 否），则丢弃该数据分组（步骤 730），并且方法返回到步骤 710。如果防火墙允许该数据分组（步骤 720= 是），则检查该数据分组是否符合 TCP 或 UDP 协议（步骤 740）。如果该数据分组不符合 TCP 或 UDP 协议（步骤 740= 否），则返回该分组（步骤 750），并返回到步骤 710。如果该数据分组符合 TCP 或 UDP 协议（步骤 740= 是），则确定该分组的目的地端口号是否匹配端口范围表中用于虚拟机的端口范围中的目的地端口号（步骤 760）。如果该分组的目的地端

口号不匹配端口范围表中的目的地端口号(步骤 760= 否),则返回该分组(步骤 750),并返回到步骤 710。如果该分组的目的地端口号匹配端口范围表中的目的地端口号(步骤 760= 是),则取决于该数据分组中的目的地端口号,将该数据分组转发到唯一一个虚拟机(步骤 770),并返回到步骤 710。在上述实施例中,通过选择在与包括该数据分组中的目的地端口号的端口范围相对应的端口范围表中存储的虚拟机号,来确定用来转发该分组的唯一虚拟机的虚拟机号。

[0057] 附图中的流程图和框图显示了根据本发明的多个实施例的系统、方法和计算机程序产品的可能实施方式的架构、功能和操作。在这点上,流程图或框图中的每个框可以代表模块、程序段或代码的一部分,所述模块、程序段或代码的一部分包含一个或多个用于实现指定逻辑功能的可执行指令。也应当注意,在一些作为替换的实施方式中,框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续示出的框实际上可以基本同时地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和 / 或流程图中的每个框、以及框图和 / 或流程图中的框的组合,可以用执行指定功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0058] 所属技术领域的技术人员知道,本发明可以实现为系统、方法或计算机程序产品。因此,本公开可以具体实现为以下形式,即 :可以是完全的硬件、也可以是完全的软件(包括固件、驻留软件、微代码等),还可以是硬件和软件结合的形式,本文一般称为“电路”、“模块”或“系统”。此外,在一些实施例中,本发明还可以实现为在一个或多个计算机可读介质中的计算机程序产品的形式,该计算机可读介质中包含计算机可读的程序代码。

[0059] 可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括 :便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或闪存)、光纤、便携式压缩磁盘只读存储器 (CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括——但不限于——电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括——但不限于——无线、电线、光缆、RF 等等,或者上述的任意合适的组合。

[0060] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如 Java(Java 和所有基于 Java 的商标和标志是 Oracle 和 / 或其子公司的商标或注册商标)、Smalltalk、C++,还包括常规的过程式程序设计语言—诸如”C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远

程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网 (LAN) 或广域网 (WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。下面将参照本发明实施例的方法、装置(系统)和计算机程序产品的流程图和 / 或框图描述本发明。应当理解，流程图和 / 或框图的每个方框以及流程图和 / 或框图中各方框的组合，都可以由计算机程序指令实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器，从而生产出一种机器，这些计算机程序指令通过计算机或其它可编程数据处理装置执行，产生了实现流程图和 / 或框图中的方框中规定的功能 / 操作的装置。也可以把这些计算机程序指令存储在能使得计算机或其它可编程数据处理装置以特定方式工作的计算机可读介质中，这样，存储在计算机可读介质中的指令就产生出一个包括实现流程图和 / 或框图中的方框中规定的功能 / 操作的指令装置的制造品。也可以把计算机程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机或其它可编程装置上执行的指令能够提供实现流程图和 / 或框图中的方框中规定的功能 / 操作的过程。

[0061] 本领域的技术人员将理解的是，可在权利要求的范围内有很多变化。尽管这里描述了关于时间的示例，但这些其它类型的阈值显然可被包括在权利要求的范围内。由此，尽管以上具体示出并描述了本公开，但本领域的技术人员将理解的是，可在其中作出形式和细节上的这样的和其它的改变，而不会背离权利要求的范围。

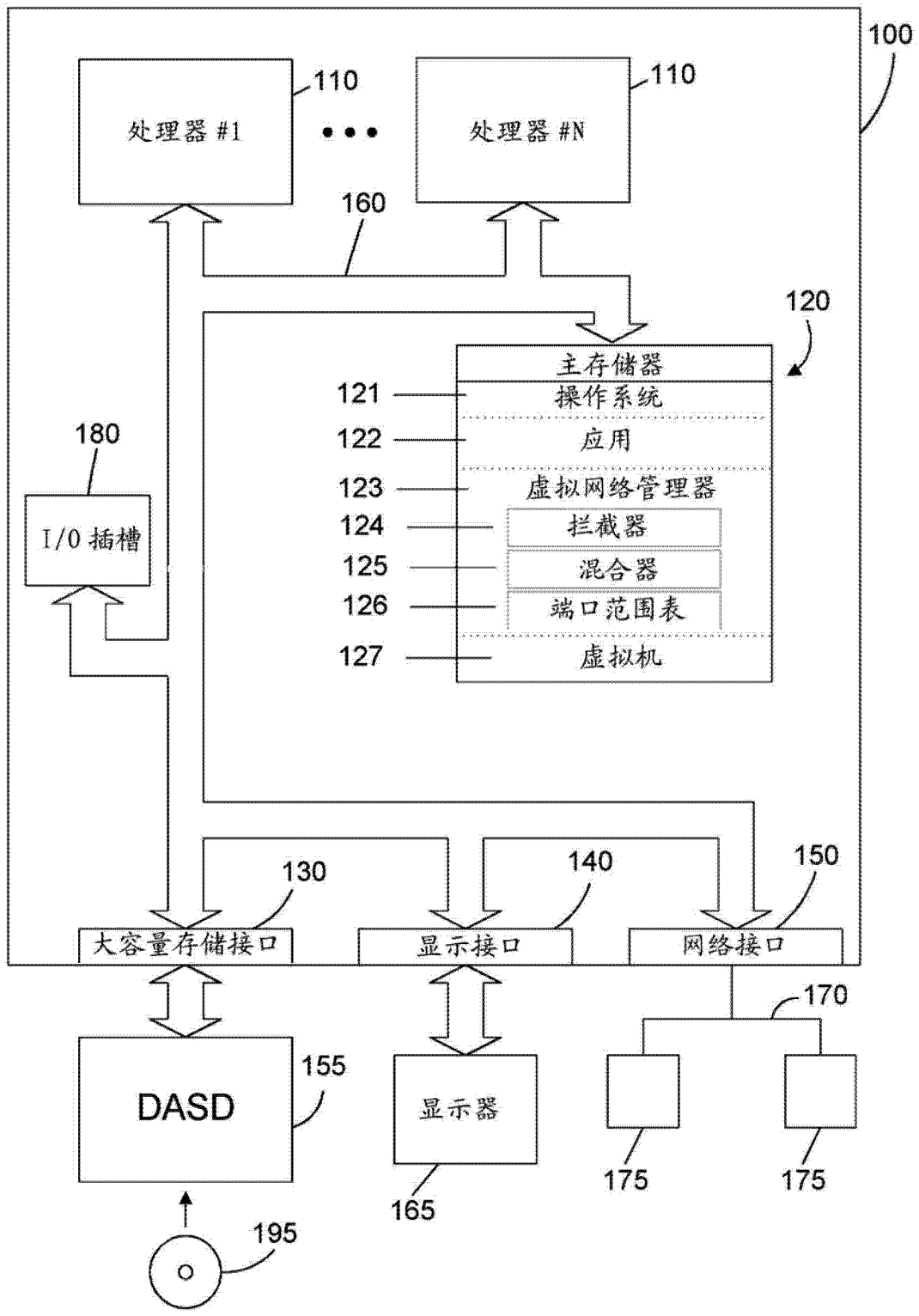

100
处理器 #1
110
处理器 #N
110
160
120
主存储器
121
操作系统
122
应用
123
虚拟网络管理器
124
拦截器
125
混合器
126
端口范围表
127
虚拟机
180
I/O 插槽
130
140
150
大容量存储接口
显示接口
网络接口
170
DASD
155
显示器
165
175
175
195

图 1

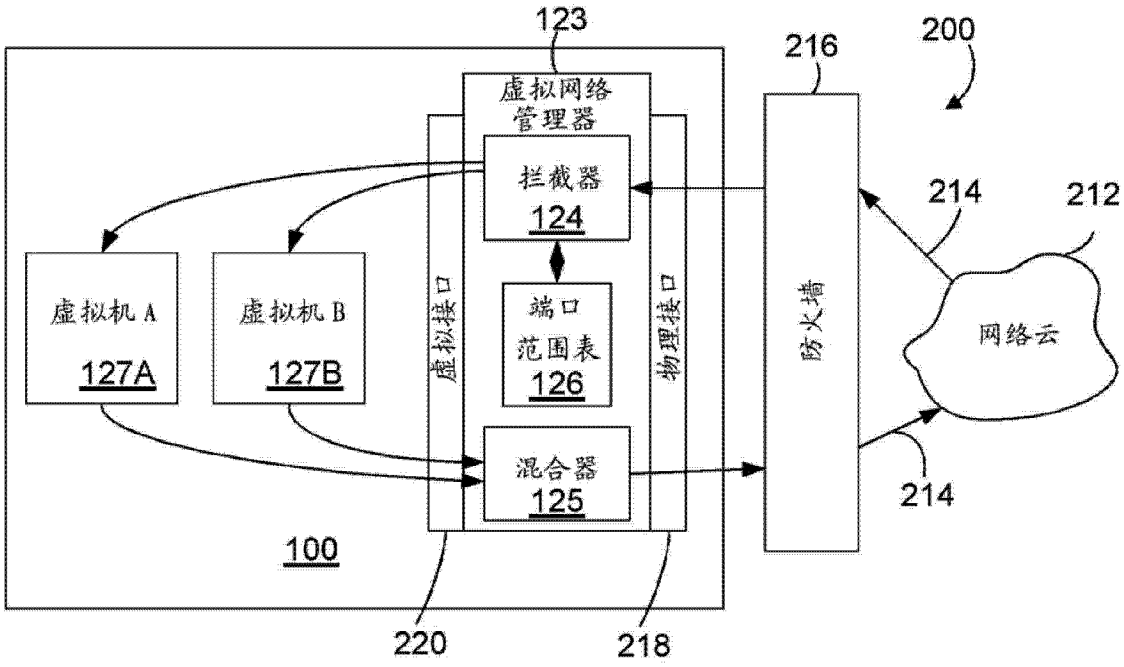

123
216
200
虚拟网络管理器
拦截器
124
214
212
虚拟机 A
127A
虚拟机 B
127B
虚拟接口
端口范围表
126
物理接口
防火墙
网络云
混合器
125
214
100
220
218

图 2

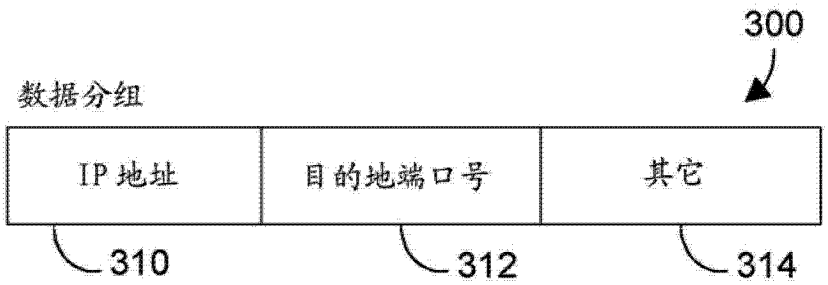

300
数据分组
IP 地址
目的地端口号
其它
310
312
314

图 3

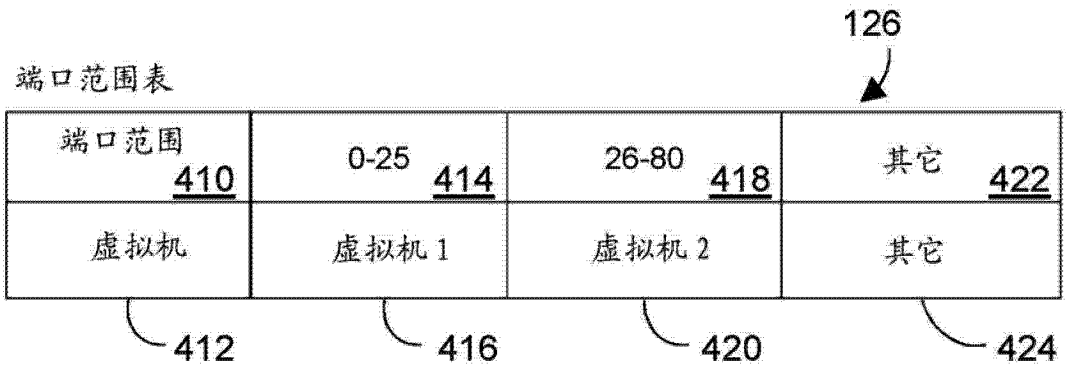

126
端口范围表
端口范围
410
0-25
414
26-80
418
其它
422
虚拟机
虚拟机 1
虚拟机 2
其它
412
416
420
424

图 4

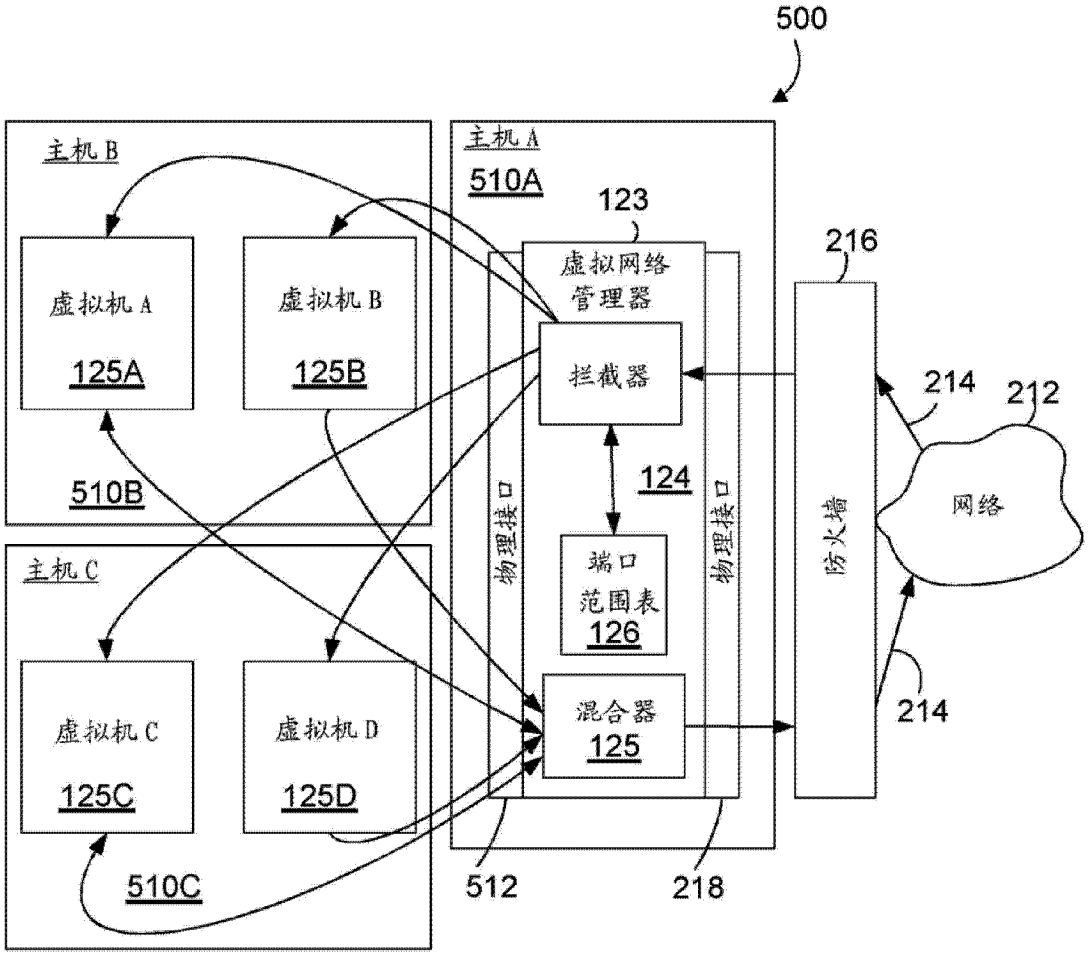

500
主机 B
虚拟机 A
125A
虚拟机 B
125B
510B
主机 C
虚拟机 C
125C
虚拟机 D
125D
510C
主机 A
510A
123
虚拟网络
管理器
拦截器
124
端口
范围表
126
混合器
125
物理接口
物理接口
512
218
216
防火墙
214
212
网络
214

图 5

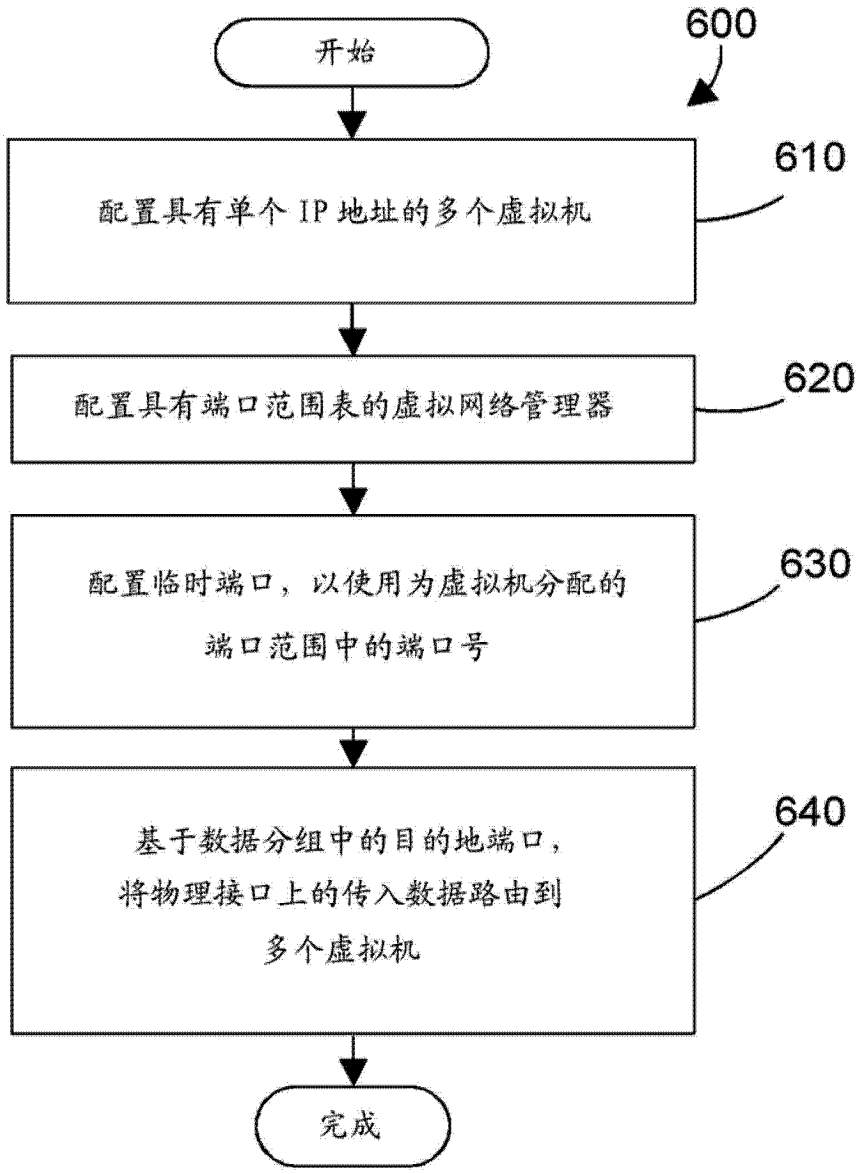

开始
600
610
配置具有单个 IP 地址的多个虚拟机
620
配置具有端口范围表的虚拟网络管理器
630
配置临时端口，以使用为虚拟机分配的端口范围中的端口号
640
基于数据分组中的目的地端口，将物理接口上的传入数据路由到多个虚拟机
完成

图 6

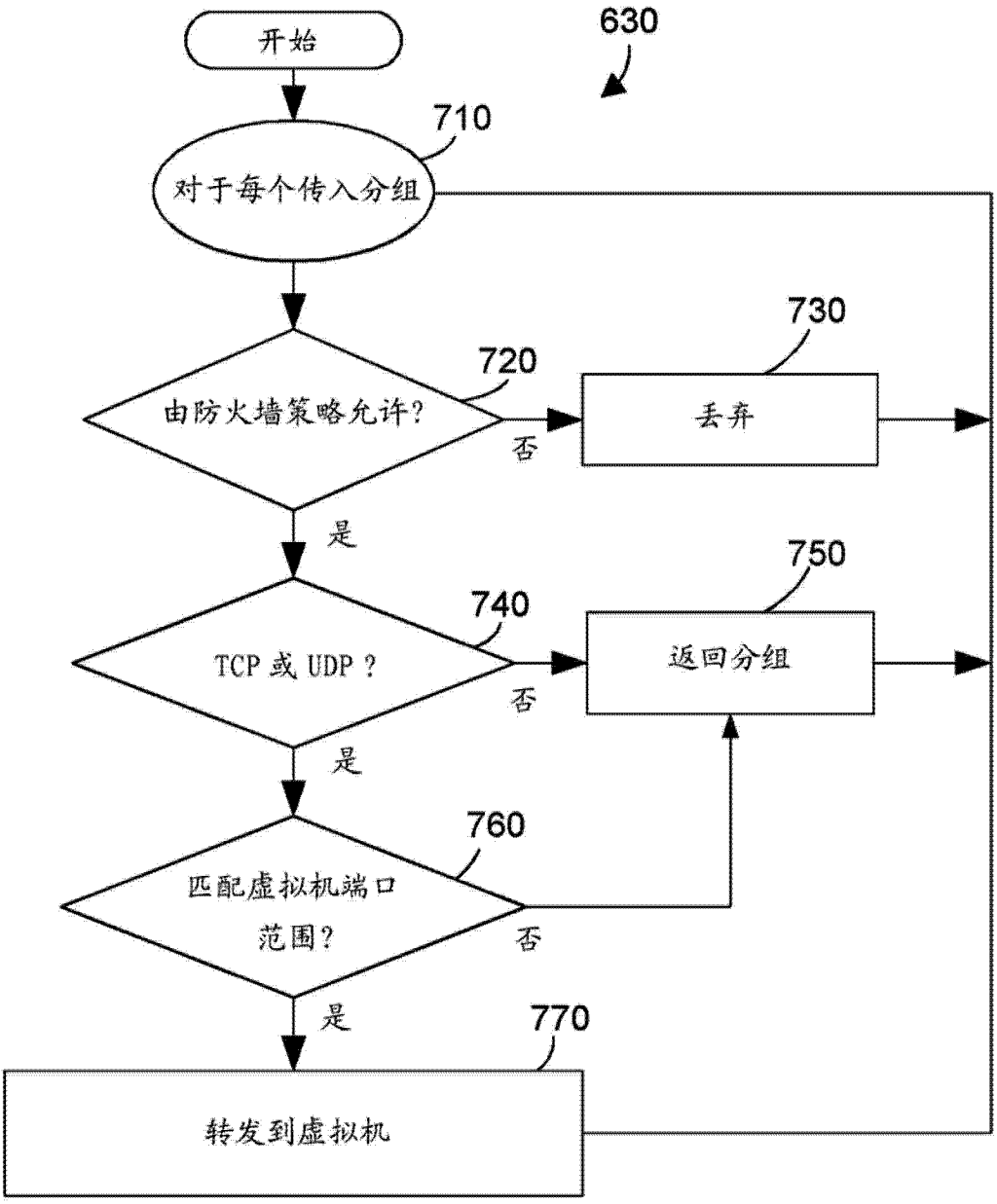

开始
630
710
对于每个传入分组
720
由防火墙策略允许?
否
730
丢弃
是
740
TCP 或 UDP ?
否
750
返回分组
是
760
匹配虚拟机端口
范围?
否
是
770
转发到虚拟机

图 7