

虚拟私有云通信系统、系统配置方法及控制器

本申请要求于 2018 年 11 月 30 日提交中国专利局、申请号为
5 201811463985.6 发明名称为“虚拟私有云通信系统、系统配置方法及控制器”
的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及虚拟私有云技术领域，尤其是涉及一种虚拟私有云通信系统、
系统配置方法及控制器。

10 背景技术

虚拟私有云（VPC，Virtual Private Cloud）是一个公共云计算资源的动态
配置池，需要使用加密协议、隧道协议和其他安全程序，在民营企业和云服
务提供商之间传输数据。

VPC 系统利用隧道或其他相类似的网络协议所实现，将云上资源按照租
15 户为粒度来切割，进而对不同的租户提供按需分配的供给能力，同时具有较
强灵活性、隔离性、安全性。目前的虚拟私有云中，云计算服务提供商所提
供的计算资源大多数以虚拟机（VM，Virtual Machine）来交付给租户，该实现方
案是利用 CPU（Central Processing Unit，中央处理器）、Memory（存储器）、
Disk（磁盘）等各资源的虚拟化技术，将原有物理机（VM 的宿主机）进行抽
20 象划分为更细粒度的个体并放置在按租户划分的 VPC 中。

上述方案在一台物理机上虚拟多个 VM 时会引入各个虚拟资源对物理机
原有资源（如 CPU 调度、I/O 读写、和网络带宽）的争抢问题。若一台物理
机只虚拟一个 VM，相对 VM 而言各方面性能有所提升，但虚拟化技术的引
入仍无法达到纯物理机机器原有的性能优势，也无法把整体资源性能发挥到
25 最大化；再者由于近期人工智能行业兴起，对 GPU（Graphics Processing Unit，
图形处理器）需求量非常之大，GPU 的资源虚拟化带来的收益很不明显。

基于上述情况，此时把图像、声音、视频处理等 GPU 消耗型的任务可以
分布在物理机（PM，Physical machine）上处理，而一些控制处理程序可放置
在 VM 中，由 PM 和 VM 做到资源的平衡分配。

此时在超大规模的云环境中租户内通信和租户间隔离显得尤为重要，现有方案中处理通信、隔离利用 VLAN（Virtual Local Area Network，虚拟局域网）来进行，但是由于 VLAN ID（虚拟局域网标识号）有个数限制，当需要搭建的 VPC 超过 VLAN ID 数量的上限值时，便不能搭建更多的 VPC。因此，

5 在云计算服务领域，对云计算提供商来说，由于租户的数量极大，对应的需要搭建的 VPC 的数量远远大于 VLAN ID 数量的上限值，因此，现有技术中采用 VLAN ID 的方法来隔离租户的方法并不能满足在云计算的应用环境。

发明内容

10 有鉴于此，本申请的目的在于提供一种虚拟私有云通信系统、系统配置方法及控制器，以基于网关建立的通信连接，无需受限于 VLAN ID 数量的上限值，为租户分配的 VM 和 PM 的数量可以随着租户的增加而增加，从而一起形成大规模的云环境，满足了当前的业务发展需求。

第一方面，本申请实施例提供了一种虚拟私有云通信系统，包括：至少

15 一个虚拟机 VM 以及与每个所述 VM 通信连接的系统网关；

至少一个物理机 PM 以及与每个所述 PM 通信连接的交换机；

所述系统网关与所述交换机通信连接；

所述系统网关和所述交换机用于基于预设的配置信息使属于同一个虚拟私有云 VPC 内的所述 VM 与所述 PM 之间能够进行通信。

20 可选的，所述配置信息包括与所述 VPC 对应的隔离标签；

所述配置信息还包括与对应的所述 VPC 包括的资源的转发表项；

所述资源包括：VM 和/或 PM。

可选的，所述系统还包括控制器；

所述控制器分别与所述系统网关和所述交换机通信连接；

25 所述控制器用于分别对所述系统网关和所述交换机进行信息配置，生成配置信息，并将所述配置信息分别发送至所述系统网关和所述交换机。

可选的，所述控制器还用于：

基于每个虚拟私有云 VPC 生成与所述 VPC 对应的隔离标签；

获取属于同一个虚拟私有云 VPC 的资源的 IP 地址；所述资源包括 VM 和

/或 PM;

基于资源的 IP 地址建立转发表项;

根据所述转发表项和所述隔离标签生成与所述 VPC 对应的配置信息。

可选的, 所述控制器还用于:

5 基于所述 VM 的 IP 地址建立所述 VM 的转发表项, 和/或

基于所述 PM 的 IP 地址建立所述 PM 的转发表项。

可选的, 所述控制器还用于:

基于所述配置信息管理所述虚拟私有云 VPC 内的资源; 所述资源包括 VM 和/或 PM; 所述管理包括: 增加资源和/或删除资源。

10 可选的, 所述控制器还用于:

接收对所述 VPC 内的资源的管理操作请求; 其中, 所述管理操作请求包括待管理的 VPC 对应的隔离标签;

根据所述隔离标签修改所述系统网关及所述交换机中与所述待管理的 VPC 对应的配置信息。

15 可选的, 所述控制器还用于:

基于资源增加请求增加与资源 IP 地址对应的转发表项; 和/或

基于资源部分删除请求删除与资源 IP 地址对应的转发表项; 和/或

基于资源全部删除请求删除与所述待管理的 VPC 对应的配置信息。

可选的, 其中, 所述系统网关用于:

20 接收所述 VM 的第一报文; 所述第一报文包括隔离标签;

基于所述第一报文中的隔离标签找到与所述隔离标签对应的配置信息, 并基于找到的配置信息将所述第一报文转发至对应的交换机;

所述系统网关还用于:

接收所述交换机的第二报文; 其中, 所述第二报文包括隔离标签;

25 基于所述第二报文中的隔离标签找到与所述隔离标签对应的配置信息, 并基于找到的配置信息将所述第二报文转发至目标 VM。

可选的, 所述交换机用于:

接收所述 PM 的第三报文; 所述第三报文包括隔离标签;

基于所述第三报文中的隔离标签找到与所述隔离标签对应的配置信息,

并基于找到的配置信息将所述第三报文转发至对应的系统网关；

所述交换机还用于：

接收所述系统网关的第四报文；其中，所述第四报文包括隔离标签；

基于所述第四报文中的隔离标签找到与所述隔离标签对应的配置信息，

5 并基于找到的配置信息将所述第四报文转发至目标 PM。

可选的，所述系统网关是通过在服务器中运行相应软件实现的。

第二方面，本申请实施例还提供一种虚拟私有云通信系统的系统配置方法，应用于第一方面及其任一种可能的实施方式所述的虚拟私有云通信系统的系统中的控制器，所述控制器分别与所述系统网关和所述交换机通信连接，

10 所述方法包括：

分别对所述系统网关和所述交换机进行信息配置，生成配置信息；

并将所述配置信息分别发送至所述系统网关和所述交换机；

其中所述配置信息包括与所述 VPC 对应的隔离标签；所述配置信息还包括与对应的所述 VPC 包括的资源的转发表项；所述资源包括：VM 和/或 PM。

15 可选的，所述生成配置信息的步骤，包括：

基于每个虚拟私有云 VPC 生成与所述 VPC 对应的隔离标签；

获取属于同一个虚拟私有云 VPC 的资源的 IP 地址；所述资源包括 VM 和/或 PM；

基于资源的 IP 地址建立转发表项；

20 根据所述转发表项和所述隔离标签生成与所述 VPC 对应的配置信息。

可选的，所述基于资源的 IP 地址建立转发表项的步骤，包括：

基于所述 VM 的 IP 地址建立所述 VM 的转发表项，和/或

基于所述 PM 的 IP 地址建立所述 PM 的转发表项。

可选的，所述方法还包括：

25 基于所述配置信息管理所述虚拟私有云 VPC 内的资源；所述资源包括 VM 和/或 PM；所述管理包括：增加资源和/或删除资源。

可选的，所述方法还包括：

接收对所述 VPC 内的资源的管理操作请求；其中，所述管理操作请求包括待管理的 VPC 对应的隔离标签；

根据所述隔离标签修改所述系统网关及所述交换机中与所述待管理的 VPC 对应的配置信息。

可选的，所述管理操作请求包括资源增加请求、资源部分删除请求、资源全部删除请求中的一种或者多种，所述方法还包括：

- 5 基于资源增加请求增加与资源 IP 地址对应的转发表项；和/或
 基于资源部分删除请求删除与资源 IP 地址对应的转发表项；和/或
 基于资源全部删除请求删除与所述待管理的 VPC 对应的配置信息。

第三方面，本申请实施例还提供一种控制器，包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，所述处理器执行所
10 述计算机程序时实现上述第一方面及其任一种可能的实施方式所述的方法。

第四方面，本申请实施例还提供了一种计算机可读存储介质，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述所述的方法。

第五方面，本申请实施例还提供了一种应用程序，用于在运行时执行：
15 本申请实施例第二方面所提供的虚拟私有云通信系统的系统配置方法。

本申请实施例带来了以下有益效果：

在本申请提供的实施例中，虚拟私有云通信系统包括至少一个虚拟机 VM 以及与每个 VM 通信连接的系统网关；至少一个物理机 PM 以及与每个 PM 通信连接的交换机；系统网关与交换机通信连接；系统网关和所述交换机用于
20 于基于预设的配置信息使属于同一个虚拟私有云 VPC 内的 VM 与 PM 之间能够进行通信。该方式中，由 PM 形成的物理机区域通过交换机接入网络，由 VM 形成的虚拟机区域通过系统网关连接物理机区域对应的交换机，从而建立了物理机区域的 PM 与虚拟机区域的 VM 之间的连接，实现了 VM 与 PM 之间的通信；由此，本申请中基于网关建立的通信连接，无需受限于 VLAN ID
25 数量的上限值，为租户分配的 VM 和 PM 的数量可以随着租户的增加而增加，从而一起形成大规模的云环境，满足了当前的业务发展需求。

本申请的其他特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的目的和其他优点在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

为使本申请的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

5 为了更清楚地说明本申请实施例和现有技术的技术方案，下面对实施例和现有技术中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例提供的一种虚拟私有云通信系统的结构示意图；

10 图 2 为本申请实施例提供的另一种虚拟私有云通信系统的结构示意图；

图 3 为本申请实施例提供的一种虚拟私有云通信系统的通信连接示意图；

图 4 为本申请实施例提供的一种系统配置方法的流程示意图；

图 5 为本申请实施例提供的一种控制器的结构示意图。

具体实施方式

15 为使本申请的目的、技术方案、及优点更加清楚明白，以下参照附图并举实施例，对本申请进一步详细说明。显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

20 目前，现有方案中处理通信、隔离利用 VLAN 来进行，但是由于 VLAN ID 数量限制、交换机硬件结构限制，为租户分配的 VM 与 PM 不能形成大规模的云环境，进而面对越来越多的租户，不能满足当前的业务发展需求。基于此，本申请实施例提供的一种虚拟私有云通信系统、系统配置方法及控制器，基于网关建立 VM 与 PM 之间的通信连接，由于不再利用 VLAN 对局域网进行隔离，因此无需受限于 VLAN ID 数量的上限值，为租户分配的 VM 和 PM

25 的数量可以随着租户的增加而增加，从而一起形成大规模的云环境，满足了当前的业务发展需求

为便于对本实施例进行理解，首先对本申请实施例所公开的一种虚拟私有云通信系统进行详细介绍。

图 1 示出了本申请实施例提供的一种虚拟私有云通信系统的结构示意图。如图 1 所示，该虚拟私有云通信系统包括至少一个虚拟机 VM 10 以及与每个 VM 通信连接的系统网关 12；至少一个物理机 PM 13 以及与每个 PM 通信连接的交换机 14；系统网关与交换机通信连接，系统网关和交换机用于基于预设的配置信息使属于同一个虚拟私有云 VPC 内的 VM 10 与 PM 13 之间能够进行通信。上述 PM 是指除了 VM 宿主机之外的物理机。

该交换机 14 为三层交换机，支持隧道协议，以在后续通过隧道进行数据传输。VM 创建在作为宿主机的物理机上，实现资源虚拟化，可以但不限于用于存储控制处理程序。PM（非 VM 所在的宿主机）可以但不限于用于存储图像、声音、视频处理等 GPU 消耗型的任务信息。同一租户对应的 VM 形成的虚拟机区域和 PM 形成的物理机区域之间可进行数据交换。

在可能的实施例中，上述系统网关是通过在服务器（例如 X86 服务器）中运行相应软件实现的。由于该虚拟私有云通信系统可能对应成千上万的租户，该系统网关通过 X86 服务器集群实现，以形成系统网关集群。

需要说明的是，VM、PM、系统网关及交换机的具体数量，根据实际情况而定，图 1 中仅是示例性的。

该方式中，由 PM 形成的物理机区域通过交换机接入网络，由 VM 形成的虚拟机区域通过系统网关连接物理机区域对应的交换机，从而建立了物理机区域的 PM 与虚拟机区域的 VM 之间的连接，实现了 VM 与 PM 之间的通信；由此本申请中基于网关建立的通信连接，无需受限于 VLAN ID 数量的上限值，为租户分配的 VM 和 PM 的数量可以随着租户的增加而增加，从而一起形成大规模的云环境，满足了当前的业务发展需求。

考虑到不同租户对其 VPC 中的资源（包括 VM 和/或 PM）配置的 IP 可能出现重叠问题，在控制器中保存有配置信息，该配置信息包括用于对 VPC 进行隔离的隔离标签，其中，一个 VPC 对应一个隔离标签。

因此在接收到租户的资源创建请求后，进行逻辑运算，按照不同租户的不同 VPC 来分配隔离标签，以区分不同 VPC 中的 VM 及 PM，以使不同 VPC 之间彼此隔离，互不干扰。基于此，上述配置信息包括与上述 VPC 对应的隔离标签；另外，配置信息还包括与对应的 VPC 包括的资源的转发表项，由此，

系统网关和交换机可以基于该转发表项及隔离标签，实现同一 VPC 的 VM 与 PM 之间的通信。

例如：租户 A 的 VM-A、PM-A 的 IP 分别为 10.0.1.2/24、10.0.1.3/24，标签为 100，租户 B 的 VM-B、PM-B 的 IP 也为 10.0.1.2/24、10.0.1.3/24，标签为 200。假设两个租户的 VM 在虚拟机区域内的同一台宿主机以及两个租户的 PM 对应连接同一台交换机时，当 VM-A 与 PM-A、VM-B 与 PM-B 互相通信时需要经过同一台宿主机，再通过系统网关到达同一台交换机。在该两条通信路径中，系统网关和交换机在通信过程中都是共享的，若不采用隔离技术，则租户 A、租户 B 的 VM 和 PM 通信时可能会出现路径冲突从而导致通信异常。

由于租户可以自行设置机器的 IP，因此存在一种可能的情况，即租户 A 和租户 B 将他们的 VM 或 PM 的 IP 设置成相同的，为了避免将租户 A 的机器和租户 B 的机器混淆，这时对于服务提供商而言则需要区分两个租户的机器。

针对上述问题，控制器可以为每个租户的 VPC 分配隔离标签，然后控制器将隔离标签同 PM、VM 对应的转发表项同时下发至各个系统网关和交换机。当后续租户 A、租户 B 的 VM 都同时与各自的 PM 进行通信时，控制器可以通过该隔离标签封装在转发表项中的方式进行通信路径的隔离。

在上述实施例的图 1 所示的虚拟私有云通信系统的基础上进行改进，参见图 2，本申请还提供了另一种虚拟私有云通信系统，该虚拟私有云通信系统还包括控制器 20，该控制器分别与系统网关和交换机通信连接，对该系统网关和交换机进行信息配置，生成配置信息，并将该配置信息分别发送至系统网关和交换机，从而便于后续数据传输。

在可能的实施例中，上述控制器与 VM 所在的宿主机、PM 对应的带外管理系统连接，根据租户需求通过该宿主机及带外管理系统，进行资源配置和信息配置，并得到配置信息，上述带外管理系统是指对 PM 进行初始化（例如重新安装操作系统）的管理系统，具体过程如下：

（a1）接收租户的资源创建请求。

例如，租户可以通过租户终端（可以为移动终端或者是电脑）直接调用相应的 API（Application Programming Interface，应用程序编程接口），或者是

登录 WEB (World Wide Web, 全球广域网) 控制台调用相应的 API。根据实际需求填写相应需求信息, 如所需 CPU 的类型, 内存大小, 网卡需求等, 从而生成资源创建请求, 并发送至控制器。

(a2) 根据上述资源创建请求为租户分配资源, 该资源构成租户的 VPC。

5 其中 VPC 的资源包括 VM 和/或 PM, 即 VM 和/或 PM 构成租户的 VPC。

控制器在接收到上述资源创建请求后, 进行逻辑计算, 确定需要的资源, 并通过宿主机的管理单元及带外管理系统在资源池 (宿主机及 PM) 里面分配可用资源。如果确定有满足要求的资源, 则进行配置操作, 分配相应数量的 VM 和/或 PM, 该 VM 和/或 PM 构成该租户对应的 VPC; 如果没有满足要求的
10 的资源则返回给客户资源不足信息等信息。

示例性地, 控制器在接收租户的资源创建请求后, 可以根据资源创建请求中需求的 CPU 的类型, 内存大小, 网卡传输速率, 从资源池中选择符合上述需求的 PM 作为目标宿主机, 这便是上面提到的逻辑计算过程, 然后, 控制器可以在目标宿主机中创建 VM。本发明实施例中, 资源池中包括多种类型的 PM, 有的 PM 可以作为宿主机, 有的 PM 可以用于图像、声音、视频处理, 15 这些 PM 中可以仅包含 GPU, 则可以在租户有 GPU 使用需求时, 如图像、声音、视频处理需求时, 可以直接将这些 GPU 作为 PM 分配给租户, 换言之, 这些仅包含 GPU 的 PM 可以作为 PM 的其中一个类别。上述宿主机的管理单元是指一台作为宿主机的 PM 中用于管理自身各 VM 的配置参数的单元, 上述带外管理系统是指对 PM 进行初始化 (例如重新安装操作系统) 的管理系统, 带外管理系统可以独立于图 2 所示的网络运行, 并可以与控制器交互。可以理解是, 由于管理单元用于对宿主机中的 VM 进行管理, 带外管理系统用于对 PM 进行管理, 因此, 控制器可以通过与管理单元与带外管理系统的交互, 在资源池中选择一台符合租户需求的 PM 作为宿主机。
20

25 (a3) 基于每个虚拟私有云 VPC 生成与该 VPC 对应的隔离标签。

其中, 该隔离标签可以通过相应的数字、字母和/或特殊符号等组成。

(a4) 获取属于同一个虚拟私有云 VPC 的资源的 IP 地址。

其中, 该资源包括 VM 和/或 PM, 上述 IP 地址包括 VM 的 IP 地址和 PM 的 IP 地址, 也就是说, 上述所获取的 IP 地址, 是指属于同一 VPC 的 VM 和/

或 PM 的 IP 地址。

具体地，在租户终端在配置过程中，可以对 PM 和 VM 所在的网段进行自定义。例如，通过调用相应的 API，对 VPC 内的 VM 和 PM 进行 IP 配置，并发送相应的 IP 信息至控制器。

- 5 当 VM 与系统网关通信连接时，该 VM 可以自动获取其对应的 IP。当 PM 通过交换机与该系统网关通信时，该 PM 也可以自动获取其对应的 IP。具体地，上述 IP 配置具体可以通过系统网关内的 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器实现，在 VM 和 PM 开机时，VM 和 PM 作为 DHCP 客户机与 DHCP 服务器交互，从而获得相应的 IP。

- 10 (a5) 基于资源的 IP 地址建立转发表项。

其中，该转发表项的建立过程具体包括：基于 VM 的 IP 地址建立 VM 的转发表项，和/或基于 PM 的 IP 地址建立 PM 的转发表项。

由此可以通过上述建立相应的转发表项，后续可以直接根据该转发表项进行数据传输。

- 15 其中，PM 的转发表项包含源 PM 的源 IP 地址以及目标 PM 的目标 IP 地址，VM 的转发表项包含源 VM 的源 IP 地址以及目标 VM 的目标 IP 地址。

(a6) 根据上述转发表项和上述隔离标签生成与 VPC 对应的配置信息。

- 20 在获取到租户的 VPC 的隔离标签，及该 VPC 内 VM 的转发表项和/或 PM 的转发表项后，生成配置信息（该配置信息包含 VM 的转发表项和/或 PM 的转发表项，及隔离标签的信息）。控制器在生成配置信息后，将该配置信息配置到系统网关及交换机，以便于数据传输（即数据报文转发）时使用。

- 25 为了满足租户的多样化需求，便于租户对 VPC 进行控制与管理，提高租户体验，在可能的实施例，上述控制器还用于基于上述配置信息管理虚拟私有云 VPC 内的资源。该管理包括：增加资源和/或删除资源。即通过控制器租户可以添加 VPC 中的 VM 或者 PM，或者删除 VPC 中的 VM 与 PM。

在具体实现过程中，上述控制器还用于：（1）接收对 VPC 内的资源的管理操作请求；其中，该管理操作请求包括待管理的 VPC 对应的隔离标签；（2）根据上述隔离标签修改系统网关及交换机中待管理的 VPC 对应的配置信息。

通过修改配置信息，可以对该 VPC 中的资源进行管理，如需要扩大 VPC

资源时，可以在系统网关及交换机中添加扩展后的资源对应的配置信息，从而后期实现扩展后的 VM 和 PM 的相互通信。

在可能的实施例中，上述管理操作请求可以但不限于包括资源增加请求、资源部分删除请求及资源全部删除请求。基于此，上述控制器还用于基于资源增加请求增加与资源 IP 地址对应的转发表项；和/或基于资源部分删除请求删除与资源 IP 地址对应的转发表项；和/或基于资源全部删除请求删除与待管理的 VPC 对应的配置信息。

例如，上述控制器对资源增加请求的具体处理过程包括：

(b1) 接收租户发送的对 VPC 中资源的资源增加请求。

10 其中该资源增加请求包括待添加 VPC 对应的隔离标签。

例如，租户可以通过租户终端（可以为移动终端或者是电脑）直接调用相应的 API，或者是登录 WEB 控制台调用相应的 API。通过该 API，选择添加 VPC 的 VM 或者 PM。

(b2) 基于资源增加请求增加与资源 IP 地址对应的转发表项。

15 即，在待添加 VPC 中添加资源（VM 和/或 PM）后，为相应的 VM 和/或建立转发表项，并将该转发表项添加至待添加 VPC 的配置信息中。

(b3) 将更新后的配置信息发送至系统网关及交换机。

具体地，可以按照上述配置信息是根据上述步骤（a1）至（a6）的步骤生成的。

20 上述控制器对资源部分删除请求包括：

参见上述步骤（b1）和步骤（b3），在现有的配置信息中删除 VPC 中待删除的资源对应的转发表项，然后将更新后的配置信息发送至系统网关及交换机。

25 而对于资源全部删除请求，控制器可以直接根据该资源全部删除请求中的隔离标签，控制系统网关和交换机中删除待管理的 VPC 的配置信息。

在可能的实施例中，控制器在接收到上述资源全部删除请求或者资源部分删除请求后，通过 VM 对应的宿主机和 PM 对应的带外管理系统，使得相应的 VM 和 PM 由已配置状态变更为未配置状态，以便于后续的循环使用。

由此，通过隔离标签的设置，可以将不同租户的不同 VPC 隔离开来，互

不干扰，为各个 VPC 提供了安全策略防护能力；同时在进行删除操作和添加操作时，可以实现仅对操作的租户对应的 VPC 的配置信息进行更新，而不影响其他租户的配置信息，增加了租户添加和删除 VPC 中 VM 和 PM 的灵活性。

综上所述，在具体应用时，数据在 VM 与 PM 之间的传输过程中，系统网关的作用如下：

在 VM 至 PM 方向的传输过程中，系统网关用于：接收 VM 的第一报文；该第一报文包括隔离标签；基于第一报文中的隔离标签找到与隔离标签对应的配置信息，并基于找到的配置信息将第一报文转发至对应的交换机。

在 PM 至 VM 方向的传输过程中，系统网关还用于接收所述交换机的第二报文；其中，该第二报文包括隔离标签；基于该第二报文中的隔离标签找到与隔离标签对应的配置信息，并基于找到的配置信息将第二报文转发至目标 VM。

交换机的作用如下：

在 PM 至 VM 方向的传输过程中，交换机用于接收 PM 的第三报文；其中，该第三报文包括隔离标签；基于第三报文中的隔离标签找到与隔离标签对应的配置信息，并基于找到的配置信息将第三报文转发至对应的系统网关。

在 VM 至 PM 方向的传输过程中，交换机还用于接收上述系统网关的第四报文；其中，该第四报文包括隔离标签；基于该第四报文中的隔离标签找到与隔离标签对应的配置信息，并基于找到的配置信息将第四报文转发至目标 PM。

为了便于从公共网络中获取相应的数据，在另外的实施例中，上述虚拟私有云通信系统还可以与公共网络如 Internet 连接，在可能的实施例中，参见图 3，该虚拟私有云系统中的 VM 通过网络网关 30 与公共网络连接。而虚拟私有云系统中的 PM 依次通过对应的交换机、系统网关、网络网关 30 与公共网络连接。

在前面描述的系统中，主要涉及到的两个部分：系统网关实现以及配置管理和 PM 的交换机的配置与管理。但是在本申请中的虚拟私有云通信系统中，如 PM 与 PM、PM 与其他网元（包括 VM、Internet（互联网））通信，也在网络转发过程中扮演举足轻重的角色。随着云环境规模增大，通信设备之

间的压力也会线性增加。交换机为线速转发设备，它的压力主要体现在大规模下配置和管理上，而系统网关为 X86 上运行软件实现的网关，性能不及交换机，它的压力则主要体现在网络转发上。

交换机的管理和配置方面：PM 形成的物理机区域在超大规模环境下，交换机上的转发表项也成倍增加，若依赖设备间防洪学习，会在该物理机区域中带来广播风暴，消耗相应带宽。此时若交换机仅支持二层转发设备，即为二层转发设备，为了支持 PM 间跨三层通信则所有的 PM 所需的网关会由系统网关实现，即必须经过系统网关，因此为系统网关带来较大的压力。基于此，在本虚拟私有云通信系统中，交换机为支持隧道协议的三层交换机，支持三层转发，配合 EVPN（Ethernet Virtual Private Network，以太网虚拟专用网）技术来同步交换机间的转发表项，以将 PM 所需的网关从系统网关转移到交换机，此后 PM 之间的通信则可通过交换机直接转发。

系统网关转发性能方面：系统网关的转发性能好坏完全依赖软件架构的实现，若采用 Linux 内核转发，由于 Linux 的网络协议栈庞大和繁冗，在处理网络转发方面势必不理想。而 DPDK（Data Plane Development Kit，数据平面开发套件）技术是能让网络转发逻辑可在 Linux 系统的租户空间上实现，绕过 Linux 网络协议栈让系统网关的转发程序直接操作网卡来获取和发送数据报文，可以极大提高数据处理性能和吞吐量。因此，在后续报文转发过程中，可以采用 DPDK 技术实现。

本申请中的虚拟私有云系统，为物理机区域与虚拟机区域以及公共网络（如 Internet）建立了沟通桥梁，可使虚拟机区域和物理机区域中资源形成大规模的 VPC，无需受限于 VLAN ID 数量的上限值；同时可为 VPC 提供安全策略防护能力，使租户可以按照业务需求，灵活的配比虚拟机和物理机资源。

在上述系统实施例的基础上，本申请实施例还提供了一种虚拟私有云通信系统的系统配置方法，该方法应用于如上述系统实施例中的控制器，如图 4 所示，该虚拟私有云通信系统的系统配置方法，具体包括：

步骤 S401，分别对系统网关和交换机进行信息配置，生成配置信息；

步骤 S402，将配置信息分别发送至系统网关和交换机；

其中该配置信息包括与所述 VPC 对应的隔离标签；该配置信息还包括与对应的 VPC 包括的资源的转发表项；该资源包括：VM 和/或 PM。

上述步骤 S402 中生成配置信息的步骤，包括：基于每个虚拟私有云 VPC 生成与 VPC 对应的隔离标签；获取属于同一个虚拟私有云 VPC 的资源的 IP 地址；基于资源的 IP 地址建立转发表项；根据转发表项和隔离标签生成与 VPC 对应的配置信息。

上述基于资源的 IP 地址建立转发表项的步骤，包括：基于 VM 的 IP 地址建立该 VM 的转发表项，和/或基于 PM 的 IP 地址建立该 PM 的转发表项。

进一步地，上述方法还包括：基于上述配置信息管理虚拟私有云 VPC 内的资源；该管理包括：增加资源和/或删除资源。

进一步地，上述方法还包括：接收对 VPC 内的资源的管理操作请求；其中，上述管理操作请求包括待管理的 VPC 对应的隔离标签；根据隔离标签修改系统网关及交换机中与待管理的 VPC 对应的配置信息。

进一步地，上述管理操作请求包括资源增加请求、资源部分删除请求、资源全部删除请求中的一种或者多种，上述方法还包括：基于资源增加请求增加与资源 IP 地址对应的转发表项；和/或基于资源部分删除请求删除与资源 IP 地址对应的转发表项；和/或基于资源全部删除请求删除与所述待管理的 VPC 对应的配置信息。

进一步地，基于上述实施例二中交换机的管理和配置方面的描述，虚拟私有云通信系统的交换机为三层交换机，支持隧道协议；上述虚拟私有云通信方法还包括：利用 EVPN 技术同步 PM 对应的交换机之间的转发表项，以将 PM 所需的网关从系统网关转移到交换机，此后 PM 之间的通信则可通过交换机直接转发，有效减少了系统网关的转发压力。

参见图 5，本申请实施例还提供一种控制器 100，包括：处理器 40，存储器 41，总线 42 和通信接口 43，所述处理器 40、通信接口 43 和存储器 41 通过总线 42 连接；处理器 40 用于执行存储器 41 中存储的可执行模块，例如计算机程序。

其中，存储器 41 可能包含高速随机存取存储器（RAM，Random Access

Memory), 也可能还包括非易失性存储器(non-volatile memory), 例如至少一个磁盘存储器。通过至少一个通信接口 43 (可以是有线或者无线) 实现该系统网元与至少一个其他网元之间的通信连接, 可以使用互联网, 广域网, 本地网, 城域网等。

5 总线 42 可以是 ISA 总线、PCI 总线或 EISA 总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示, 图 5 中仅用一个双向箭头表示, 但并不表示仅有一根总线或一种类型的总线。

其中, 存储器 41 用于存储程序, 所述处理器 40 在接收到执行指令后, 执行所述程序, 前述本申请实施例任一实施例揭示的流过程定义的装置所执行的
10 方法可以应用于处理器 40 中, 或者由处理器 40 实现。

处理器 40 可能是一种集成电路芯片, 具有信号的处理能力。在实现过程中, 上述方法的各步骤可以通过处理器 40 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 40 可以是通用处理器, 包括中央处理器
15 (Central Processing Unit, 简称 CPU)、网络处理器(Network Processor, 简称 NP) 等; 还可以是数字信号处理器(Digital Signal Processing, 简称 DSP)、专用集成电路(Application Specific Integrated Circuit, 简称 ASIC)、现成可编程门阵列(Field-Programmable Gate Array, 简称 FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理
20 器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成, 或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器, 闪存、只读存储器, 可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 41, 处理器 40 读取存储器 41 中的信息, 结合
25 其硬件完成上述方法的步骤。

本申请实施例提供的虚拟私有云通信系统的系统配置方法及控制器, 与上述实施例提供的虚拟私有云通信系统具有相同的技术特征, 所以也能解决相同的技术问题, 达到相同的技术效果。

本申请实施例还提供了一种计算机可读存储介质, 计算机可读存储介质

内存储有计算机程序，用以执行前述方法实施例中所述的虚拟私有云通信系统的系统配置方法。

本申请实施例所提供的进行系统配置方法的计算机程序产品，包括存储了处理器可执行的非易失的程序代码的计算机可读存储介质，所述程序代码
5 包括的指令可用于执行前述方法实施例中所述的虚拟私有云通信系统的系统配置方法，具体实现可参见方法实施例，在此不再赘述。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的方法及控制器的具体工作过程，可以参考前述系统实施例中的对应过程，在此不再赘述。

10 附图中的流程图和框图显示了根据本申请的多个实施例方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、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规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附
15 图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，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，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动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。

20 在本申请的描述中，需要说明的是，术语“中心”、“上”、“下”、“左”、“右”、“竖直”、“水平”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本申请和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本申请的限制。此外，术语“第一”、“第二”、“第三”仅用于描述目的，
25 而不能理解为指示或暗示相对重要性。除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对步骤、数字表达式和数值并不限制本申请的范围。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，

所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个处理器可执行的非易失的计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，
Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上所述实施例，仅为本申请的具体实施方式，用以说明本申请的技术方案，而非对其限制，本申请的保护范围并不局限于此，尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质脱离本申请实施例技术方案的精神和范围，都应涵盖在本申

请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

5

权 利 要 求

- 1、一种虚拟私有云通信系统，其特征在于，包括：至少一个虚拟机 VM 以及与每个所述 VM 通信连接的系统网关；
至少一个物理机 PM 以及与每个所述 PM 通信连接的交换机；
5 所述系统网关与所述交换机通信连接；
所述系统网关和所述交换机用于基于预设的配置信息使属于同一个虚拟私有云 VPC 内的所述 VM 与所述 PM 之间能够进行通信。
- 2、根据权利要求 1 所述的系统，其特征在于，
所述配置信息包括与所述 VPC 对应的隔离标签；
10 所述配置信息还包括与对应的所述 VPC 包括的资源的转发表项；
所述资源包括：VM 和/或 PM。
- 3、根据权利要求 1 所述的系统，其特征在于，还包括控制器；
所述控制器分别与所述系统网关和所述交换机通信连接；
所述控制器用于分别对所述系统网关和所述交换机进行信息配置，生成
15 配置信息，并将所述配置信息分别发送至所述系统网关和所述交换机。
- 4、根据权利要求 3 所述的系统，其特征在于，所述控制器还用于：
基于每个虚拟私有云 VPC 生成与所述 VPC 对应的隔离标签；
获取属于同一个虚拟私有云 VPC 的资源的 IP 地址；所述资源包括 VM
和/或 PM；
20 基于资源的 IP 地址建立转发表项；
根据所述转发表项和所述隔离标签生成与所述 VPC 对应的配置信息。
- 5、根据权利要求 4 所述的系统，其特征在于，所述控制器还用于，
基于所述 VM 的 IP 地址建立所述 VM 的转发表项，和/或
基于所述 PM 的 IP 地址建立所述 PM 的转发表项。
- 25 6、根据权利要求 3 所述的系统，其特征在于，所述控制器还用于：

基于所述配置信息管理所述虚拟私有云 VPC 内的资源；所述资源包括 VM 和/或 PM；所述管理包括：增加资源和/或删除资源。

7、根据权利要求 6 所述的系统，其特征在于，所述控制器还用于：

接收对所述 VPC 内的资源的管理操作请求；其中，所述管理操作请求包
5 括待管理的 VPC 对应的隔离标签；

根据所述隔离标签修改所述系统网关及所述交换机中与所述待管理的 VPC 对应的配置信息。

8、根据权利要求 7 所述的系统，其特征在于，所述控制器还用于：

基于资源增加请求增加与资源 IP 地址对应的转发表项；和/或
10 基于资源部分删除请求删除与资源 IP 地址对应的转发表项；和/或
基于资源全部删除请求删除与所述待管理的 VPC 对应的配置信息。

9、根据权利要求 2 所述的系统，其特征在于，所述系统网关用于：

接收所述 VM 的第一报文；所述第一报文包括隔离标签；

基于所述第一报文中的隔离标签找到与所述隔离标签对应的配置信息，
15 并基于找到的配置信息将所述第一报文转发至对应的交换机；

所述系统网关还用于：

接收所述交换机的第二报文；其中，所述第二报文包括隔离标签；

基于所述第二报文中的隔离标签找到与所述隔离标签对应的配置信息，
并基于找到的配置信息将所述第二报文转发至目标 VM。

20 10、根据权利要求 2 所述的系统，其特征在于，所述交换机用于：

接收所述 PM 的第三报文；所述第三报文包括隔离标签；

基于所述第三报文中的隔离标签找到与所述隔离标签对应的配置信息，
并基于找到的配置信息将所述第三报文转发至对应的系统网关；

所述交换机还用于：

25 接收所述系统网关的第四报文；其中，所述第四报文包括隔离标签；

基于所述第四报文中的隔离标签找到与所述隔离标签对应的配置信息，并基于找到的配置信息将所述第四报文转发至目标 PM。

11、根据权利要求 1-10 任一项所述的系统，其特征在于，所述系统网关是通过在服务器中运行相应软件实现的。

5 12、一种虚拟私有云通信系统的系统配置方法，其特征在于，应用于权利要求 1 至 11 任一项所述的系统中的控制器，所述控制器分别与所述系统网关和所述交换机通信连接；所述方法包括：

分别对所述系统网关和所述交换机进行信息配置，生成配置信息；

并将所述配置信息分别发送至所述系统网关和所述交换机；

10 其中所述配置信息包括与所述 VPC 对应的隔离标签；所述配置信息还包括与对应的所述 VPC 包括的资源的转发表项；所述资源包括：VM 和/或 PM。

13、根据权利要求 12 所述的方法，其特征在于，所述生成配置信息的步骤，包括：

基于每个虚拟私有云 VPC 生成与所述 VPC 对应的隔离标签；

15 获取属于同一个虚拟私有云 VPC 的资源的 IP 地址；所述资源包括 VM 和/或 PM；

基于资源的 IP 地址建立转发表项；

根据所述转发表项和所述隔离标签生成与所述 VPC 对应的配置信息。

20 14、根据权利要求 13 所述的方法，其特征在于，所述基于资源的 IP 地址建立转发表项的步骤，包括：

基于所述 VM 的 IP 地址建立所述 VM 的转发表项，和/或

基于所述 PM 的 IP 地址建立所述 PM 的转发表项。

15、根据权利要求 12 所述的方法，其特征在于，还包括：

25 基于所述配置信息管理所述虚拟私有云 VPC 内的资源；所述资源包括 VM 和/或 PM；所述管理包括：增加资源和/或删除资源。

16、根据权利要求 15 所述的方法，其特征在于，还包括：

接收对所述 VPC 内的资源的管理操作请求；其中，所述管理操作请求包括待管理的 VPC 对应的隔离标签；

根据所述隔离标签修改所述系统网关及所述交换机中与所述待管理的 VPC 对应的配置信息。

17、根据权利要求 16 所述的方法，其特征在于，所述管理操作请求包括资源增加请求、资源部分删除请求、资源全部删除请求中的一种或者多种，所述方法还包括：

基于资源增加请求增加与资源 IP 地址对应的转发表项；和/或
10 基于资源部分删除请求删除与资源 IP 地址对应的转发表项；和/或
基于资源全部删除请求删除与所述待管理的 VPC 对应的配置信息。

18、一种控制器，包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现上述权利要求 12 至 17 任一项所述的方法。

15 19、一种计算机可读存储介质，所述存储介质上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求 12 至 17 任一项所述的方法。

20、一种应用程序，其特征在于，用于在运行时执行：权利要求 12-17 任一项所述的方法。