(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108199982 B
(45)授权公告日 2021.10.15

(21)申请号 201810004871.9
(22)申请日 2018.01.03
(65)同一申请的已公布的文献号
申请公布号 CN 108199982 A
(43)申请公布日 2018.06.22
(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市南山区高新区科技中一路腾讯大厦35层
专利权人 腾讯云计算(北京)有限责任公司
(72)发明人 赵罡 裴超 金峰 赵星 刘颖
(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 何平 邓云鹏
(51)Int.Cl.
H04L 12/931(2013.01)
H04L 29/06(2006.01)
(56)对比文件
CN 106656815 A,2017.05.10
CN 105245456 A,2016.01.13
CN 107453992 A,2017.12.08
WO 2015199685 A1,2015.12.30
审查员 王怡轩

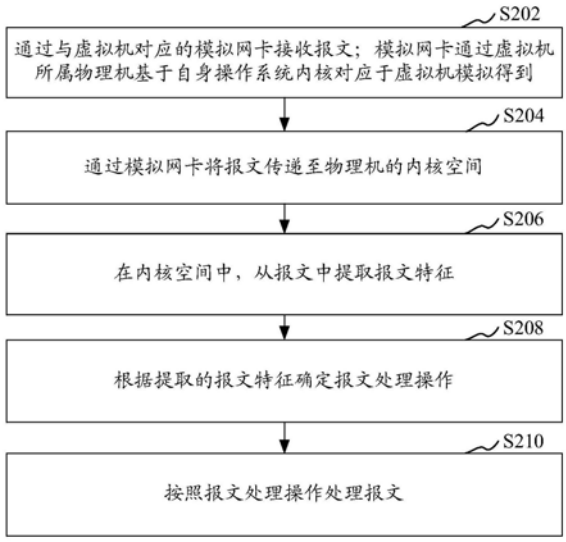
权利要求书3页 说明书18页 附图7页

(54)发明名称

报文处理方法、装置、存储介质和计算机设备

(57)摘要

本发明涉及一种报文处理方法、装置、存储介质和计算机设备，包括：通过与虚拟机对应的模拟网卡接收报文；所述模拟网卡通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机模拟得到；通过所述模拟网卡将所述报文传递至所述物理机的内核空间；在所述内核空间中，从所述报文中提取报文特征；根据提取的所述报文特征确定报文处理操作；按照所述报文处理操作处理所述报文。本申请提供的方案拓宽了报文处理方式的适用范围。



CN 108199982 B

1.一种报文处理方法,包括:

通过与虚拟机对应的模拟网卡,接收所述虚拟机通过为所述虚拟机虚拟得到的虚拟网卡所发送的报文;所述模拟网卡,是通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机为虚拟交换机模拟得到的;

通过所述模拟网卡将所述报文传递至所述物理机的内核空间;

在所述内核空间中,从所述报文中提取报文特征;

根据提取的所述报文特征确定报文处理操作;

按照所述报文处理操作处理所述报文。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述虚拟交换机接收由所述虚拟机对应的虚拟网卡所发送的报文,并根据所述报文的报文特征查找与所述报文对应的通信连接;

当未查找到与所述报文对应的通信连接时,所述虚拟交换机将所述报文上送至与所述虚拟机对应的模拟网卡。

3.根据权利要求2所述的方法,其特征在于,所述根据所述报文的报文特征查找与所述报文对应的通信连接,包括:

从所述报文中提取报文特征;

将所述报文特征映射为哈希值;

查找与所述哈希值匹配的通信连接。

4.根据权利要求2所述的方法,其特征在于,所述方法还包括:

当查找到与所述报文对应的通信连接时,则

查询与所述通信连接对应存储的报文处理操作;

按照查询到的所述报文处理操作处理所述报文。

5.根据权利要求2所述的方法,其特征在于,所述方法还包括:

确定所述报文特征所对应的通信连接及所述通信连接所对应的连接状态;

记录所述通信连接并相应记录所述连接状态;

将所述报文特征和所述报文处理操作对应于所述通信连接存储。

6.根据权利要求1所述方法,其特征在于,所述根据提取的所述报文特征确定报文处理操作,包括:

将提取的所述报文特征与预设的访问控制报文特征比较;

当提取的所述报文特征与所述访问控制报文特征匹配时,则确定报文处理操作为报文丢弃操作;

所述按照所述报文处理操作处理所述报文,包括:

丢弃所述报文。

7.根据权利要求6所述的方法,其特征在于,所述报文特征包括目的网络地址;所述方法还包括:

当提取的所述报文特征与所述访问控制报文特征不匹配、且所述目的网络地址为与虚拟机对应的实体网络地址时,则确定报文处理操作为报文转发操作;

所述按照所述报文处理操作处理所述报文,包括:

转发所述报文。

8.根据权利要求7所述方法，其特征在于，所述报文特征还包括源网络地址、所述源网络地址对应的源虚拟网络标识及所述目的网络地址所对应的目的虚拟网络标识；

当所述源虚拟网络标识与所述目的虚拟网络标识一致时，所述转发所述报文，包括：

通过所述目的网络地址指向的虚拟机所对应的模拟网卡转发所述报文。

9.根据权利要求8所述方法，其特征在于，所述方法还包括：

当所述源虚拟网络标识与所述目的虚拟网络标识不一致时，则

通过虚拟隧道端口查找中间地址；所述中间地址与所述目的网络地址指向的虚拟机所属物理机对应；

将所述中间地址添加到所述报文的头部生成隧道报文；

通过所述虚拟隧道端口转发所述隧道报文。

10.根据权利要求7所述方法，其特征在于，所述方法还包括：

当提取的所述报文特征与所述访问控制报文特征不匹配、且所述目的网络地址为虚拟网络地址时，则确定报文处理操作为报文目的端修改操作；

将所述目的网络地址修改为与所述虚拟网络地址对应的实体网络地址；

所述按照所述报文处理操作处理所述报文，包括：

转发修改后的所述报文。

11.根据权利要求7所述方法，其特征在于，所述方法还包括：

当提取的所述报文特征与所述访问控制报文特征不匹配、且所述目的网络地址为公网网络地址时，则确定报文处理操作为报文源端修改操作；

将所述报文的源网络地址修改为所述公网网络地址对应的实体网络地址；

所述按照所述报文处理操作处理所述报文，包括：

转发修改后的所述报文。

12.根据权利要求1所述的方法，其特征在于，所述方法还包括：

通过虚拟隧道端口接收隧道报文；所述虚拟隧道端口通过所述物理机基于自身操作系统内核对应所述虚拟机所属虚拟网络虚拟得到；

通过所述虚拟隧道端口将所述隧道报文传递至所述物理机的内核空间；

在所述内核空间中，从所述隧道报文中提取报文特征；

根据提取的所述隧道报文特征确定报文处理操作；

按照所述报文处理操作处理所述隧道报文。

13.根据权利要求12所述的方法，其特征在于，所述方法还包括：

从所述隧道报文中提取网络地址；

将与所述网络地址对应的物理地址添加到所述隧道报文的首部，并执行所述通过所述虚拟隧道端口将所述隧道报文传递至所述物理机的内核空间的步骤。

14.根据权利要求12所述的方法，其特征在于，所述方法还包括：

接收由物理网卡所传递的隧道报文；

根据所述隧道报文的报文特征查找与所述隧道报文对应的通信连接；

当未查找到与所述隧道报文对应的通信连接时，将所述隧道报文上送至所述虚拟隧道端口。

15.根据权利要求14所述的方法，其特征在于，所述方法还包括：

当查找到与所述隧道报文对应的通信连接时，则

查询与所述通信连接对应存储的报文处理操作；

按照查询到的所述报文处理操作处理所述隧道报文。

16.一种计算机可读存储介质，所述计算机可读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，使得所述处理器执行如权利要求1至15中任一项所述的方法的步骤。

17.一种计算机设备，包括存储器和处理器，所述存储器中储存有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行如权利要求1至15中任一项所述的方法的步骤。

报文处理方法、装置、存储介质和计算机设备

技术领域

[0001] 本发明涉及计算机技术领域，特别是涉及一种报文处理方法、装置、存储介质和计算机设备。

背景技术

[0002] 随着计算机技术的发展，云计算逐步成为业界的发展热点，国内外各大厂商的云计算服务平台也开始纷纷投入到科学、教育、文化、卫生、政府、高性能计算、电子商务、物联网等多个领域进行使用。

[0003] 在云计算领域，虚拟机间通信所用的报文通常由虚拟交换机来中转处理，传统技术中，在虚拟交换机的架构设计上，报文处理依赖于多个处理路径的相互配合，从而导致传统的虚拟交换机报文处理方式适用范围窄。

发明内容

[0004] 基于此，有必要针对传统的虚拟交换机报文处理方式适用范围窄的问题，提供一种报文处理方法、装置、存储介质和计算机设备。

[0005] 一种报文处理方法，包括：

[0006] 通过与虚拟机对应的模拟网卡接收报文；所述模拟网卡通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机模拟得到；

[0007] 通过所述模拟网卡将所述报文传递至所述物理机的内核空间；

[0008] 在所述内核空间中，从所述报文中提取报文特征；

[0009] 根据提取的所述报文特征确定报文处理操作；

[0010] 按照所述报文处理操作处理所述报文。

[0011] 一种报文处理装置，包括：

[0012] 接收模块，用于通过与虚拟机对应的模拟网卡接收报文；所述模拟网卡通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机模拟得到；

[0013] 传递模块，用于通过所述模拟网卡将所述报文传递至所述物理机的内核空间；

[0014] 提取模块，用于在所述内核空间中，从所述报文中提取报文特征；

[0015] 确定模块，用于根据提取的所述报文特征确定报文处理操作；

[0016] 处理模块，用于按照所述报文处理操作处理所述报文。

[0017] 一种计算机可读存储介质，所述计算机可读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，使得所述处理器执行以下步骤：

[0018] 通过与虚拟机对应的模拟网卡接收报文；所述模拟网卡通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机模拟得到；

[0019] 通过所述模拟网卡将所述报文传递至所述物理机的内核空间；

[0020] 在所述内核空间中，从所述报文中提取报文特征；

[0021] 根据提取的所述报文特征确定报文处理操作；

[0022] 按照所述报文处理操作处理所述报文。

[0023] 一种计算机设备，包括存储器和处理器，所述存储器中储存有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行以下步骤：

[0024] 通过与虚拟机对应的模拟网卡接收报文；所述模拟网卡通过所述虚拟机所属物理机基于自身操作系统内核对应于所述虚拟机模拟得到；

[0025] 通过所述模拟网卡将所述报文传递至所述物理机的内核空间；

[0026] 在所述内核空间中，从所述报文中提取报文特征；

[0027] 根据提取的所述报文特征确定报文处理操作；

[0028] 按照所述报文处理操作处理所述报文。

[0029] 上述报文处理方法、装置、存储介质和计算机设备，由于模拟网卡是通过虚拟机所属物理机，基于该物理机自身的操作系统内核对应于虚拟机模拟得到的，那么该模拟网卡可直接接收报文，并在接收到报文后即可直接将该报文传递至物理机的内核空间，继而在内核空间中从报文中提取报文特征，以根据提取的报文特征来确定报文处理操作，从而即可自动根据确定的报文处理操作来处理报文。这样不需要依赖于多个处理路径的相互配合，从而拓宽了报文处理方式的适用范围，极大程度上满足了报文处理需求。

附图说明

[0030] 图1为一个实施例中报文处理方法的应用环境图；

[0031] 图2为一个实施例中报文处理方法的流程示意图；

[0032] 图3为一个实施例中虚拟机发送报文方向的报文传输逻辑过程图；

[0033] 图4为一个实施例中虚拟机接收报文方向的报文传输逻辑过程图；

[0034] 图5为一个实施例中虚拟交换机的网络拓扑图；

[0035] 图6为另一个实施例中虚拟交换机的网络拓扑图；

[0036] 图7为一个实施例中报文处理装置的模块结构图；

[0037] 图8为另一个实施例中报文处理装置的模块结构图；

[0038] 图9为另一个实施例中报文处理装置的模块结构图；

[0039] 图10为一个实施例中计算机设备的内部结构图。

具体实施方式

[0040] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0041] 图1为一个实施例中报文处理方法的应用环境图。参照图1，该报文处理方法应用于报文处理系统。该报文处理系统包括物理机1000。其中，该物理机1000至少包括第一物理机1100和第二物理机1200。第一物理机1100和第二物理机1200之间通过物理线路连接。物理机可虚拟出多台虚拟机，基于同一台物理机虚拟出的多台虚拟机可属于同一用户，也可以分别属于不同的用户。物理机可为各用户分别虚拟出相应的虚拟交换机，同一个用户在同一台物理机上的虚拟机通过虚拟交换机连接，组成VPC(Virtual Private Cloud虚拟私有网络)。比如，第一物理机1100上的虚拟机1110和虚拟机1120属于用户A，对应虚拟交换机

1101组成属于用户A的VPC网络。第一物理机1100上的虚拟机1130属于用户B，对应虚拟交换机1102组成属于用户B的VPC网络。虚拟机之间进行通信的报文可通过虚拟交换机进行处理。

[0042] 图2为一个实施例中报文处理方法的流程示意图。本实施例主要以该方法应用于上述图1中的物理机1000来举例说明，可以理解基于该物理机1000虚拟出的虚拟交换机用于执行该报文处理方法。参照图2，该报文处理方法具体包括如下步骤：

[0043] S202，通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到。

[0044] 其中，物理机是相对于虚拟机而言对实体计算机的命名。物理机提供给虚拟机以硬件环境，也可称为“寄主”或“宿主”。虚拟机(Virtual Machine，VM)是通过虚拟化技术基于物理机虚拟出的独立且完整的计算机系统，也是逻辑上的一台计算机设备。虚拟化技术是资源管理技术，是将计算机的各自实体资源，如服务器、网络、内存以及存储等，予以抽象或者转换后呈现出来，打破实体结构件的不可切割的障碍。

[0045] 网卡又称网络适配器，是网络中连接计算机设备和数据传输介质的接口。可以理解，物理机在配备网卡后才能实现与物理机以外的设备的通信。那么在基于物理机虚拟得到虚拟机后，也需要为该虚拟机虚拟出属于该虚拟机的虚拟网卡，从而使得该虚拟机可通过该虚拟网卡与该虚拟机以外的设备进行通信。

[0046] 交换机(Switch)是一种用于数据中转的网络设备。交换机可以为接入自身的任意两个网络节点提供的传输通道。可以理解，物理机之间可通过交换机的数据中转进行通信。那么在基于物理机虚拟得到虚拟机后，也需要为该虚拟机虚拟出属于相应的虚拟交换机，从而使得该虚拟机可通过该虚拟交换机与其他虚拟机进行通信。

[0047] 模拟网卡是不同于前述虚拟网卡的网卡，是基于物理机为虚拟交换机虚拟得到的与虚拟机对应的网卡。模拟网卡与虚拟机一一对应，虚拟交换机可通过模拟网卡接收相应虚拟机的虚拟网卡发送的报文。报文是网络中交换与传输的数据单元。待传输的数据在传输过程中会不断的根据网络通信协议封装成分组、包、帧形成报文来传输。网络通信协议比如TCP(Transmission Control Protocol)/IP(Internet Protocol)协议等。

[0048] 可以理解，基于同一台物理机虚拟得到的虚拟机可以分属于不同的用户。属于同一用户的虚拟机对应相同的虚拟交换机。这些虚拟机各自存在一个对应的、属于该虚拟交换机的模拟网卡用于传输报文。

[0049] 具体地，物理机上虚拟得到的虚拟机在需要进行数据传输时，通过该虚拟机的协议栈对待传输的数据进行封装处理得到报文后，通过该虚拟机的虚拟网卡向外发送。此时，与该虚拟机对应的虚拟交换机，可通过物理机(虚拟交换机和虚拟机的宿主机)基于自身操作系统内核对应于该虚拟机模拟得到的模拟网卡接收该报文。

[0050] S204，通过模拟网卡将报文传递至物理机的内核空间。

[0051] 其中，操作系统用于管理计算机硬件与软件，操作系统内核所在的区域为内核空间，内核功能模块运行在内核空间。

[0052] 具体地，模拟网卡在接收到报文后，即将该报文传递至物理机的内核空间。这样该物理机即可通过内核协议栈对该报文进行处理。

[0053] S206，在内核空间中，从报文中提取报文特征。

[0054] 其中，报文特征是反映报文特定特征的数据。报文特征包括信息提取特征和网络行为特征。信息提取特征是直接从报文中提取的特征数据，比如网络通信协议标识、源IP地址或者源端口号等。网络行为特征是根据信息提取特征确定的报文所对应网络行为的特征数据，比如，根据信息提取特征确定的TCP连接请求报文或者TCP连接确认报文等。

[0055] 通常情形下，报文由报文头和数据正文两个部分组成。数据正文部分是实际要传输的数据。报文头部分，则是实际要传输的数据在传输过程中经过各网络层时根据相应网络层的网络通信协议添加的信息段。比如，实际要传输的数据在经过传输层时，可根据传输层的TCP协议，将TCP协议标识、源端口号和目的端口号添加在实际要传输的数据的头部，形成TCP报文后继续传输。可以理解，最后从虚拟机的虚拟网卡发送出的报文可经过多层网络通信协议封装，也就是说可包括多层报文头。

[0056] 具体地，物理机可通过内核协议栈从报文的多层报文头中逐层提取报文特征。网络通信协议标识是报文所包括的各层网络通信协议的标识。报文在生成时，经过数据链路层、网络层和传输层等时，都会在报文上添加相应网络通信协议层的网络通信协议标识。不同类型的数据包中包括的各层网络通信协议的标识不同。比如，报文网络层网络通信协议标识为TCP(Transmission Control Protocol传输控制协议)/UDP(User Datagram Protocol用户数据报协议)，传输层中目的端口为53端口的数据包为域名解析数据包。

[0057] 具体地，物理机的内核协议栈可逐层获取报文中包括的网络通信协议标识，确定获取的网络通信协议标识所对应的网络通信协议，再按照确定的该网络通信协议解析报文头，从而从报文中提取报文特征。

[0058] S208，根据提取的报文特征确定报文处理操作。

[0059] 其中，报文处理操作是根据报文特征确定的应该对该报文进行的操作。报文处理操作比如报文转发操作或者报文丢弃操作等。

[0060] 具体地，物理机通过内核协议栈从报文中提取报文特征后，可将提取的报文特征与预先设置的报文处理策略所对应的特征条件进行匹配，当提取的报文特征满足某一报文处理策略所对应的特征条件时，则将该报文处理策略对应的报文处理操作作为应当对该报文进行的报文处理操作。

[0061] 在一个实施例中，物理机的操作系统可以是Linux操作系统。基于Linux操作系统虚拟出的Bridge(虚拟网桥设备)和Vdev(Virtual net device，虚拟网络设备)可架构得到虚拟交换机。其中，Vdev通过模拟网卡接收报文后上送至Bridge。Linux操作系统内核包括Netfilter内核模块，用于管理报文。Netfilter内核模块提供了一系列钩子函数(Hook函数)，netfilter内核模块在内核协议栈中若干位置设置了钩子点(HOOK)，而在每个钩子点上注册了相应的钩子函数。物理机通过内核协议栈对报文进行处理，当报文经过内核协议栈的某一钩子点时，即根据相应注册的钩子函数检测该报文的报文特征是否满足特征条件，满足则将该钩子函数对应的报文处理操作确定为应当对该报文进行的报文处理操作。

[0062] S210，按照报文处理操作处理报文。

[0063] 具体地，物理机在确定应当对该报文进行的报文处理操作后，即根据该报文处理操作处理该报文。比如，当报文处理操作为报文丢弃操作时，则丢弃该报文；或者，当报文处理操作为报文转发操作时，则转发该报文等。

[0064] 可以理解，上述处理过程中报文的处理经历了通过报文特征确定报文处理操作的

过程，而非仅经历已知的固定的报文处理操作。也就是说，上述报文处理过程是基于虚拟交换机架构的慢速路径处理方式。

[0065] 上述报文处理方法，由于模拟网卡是通过虚拟机所属物理机，基于该物理机自身的操作系统内核对应于虚拟机模拟得到的，那么该模拟网卡可直接接收报文，并在接收到报文后即可直接将该报文传递至物理机的内核空间，继而在内核空间中从报文中提取报文特征，以根据提取的报文特征来确定报文处理操作，从而即可自动根据确定的报文处理操作来处理报文。这样不需要依赖于多个处理路径的相互配合，从而拓宽了报文处理方式的适用范围，极大程度上满足了报文处理需求。

[0066] 在一个实施例中，该报文处理方法还包括：接收由虚拟机对应的虚拟网卡所发送的报文；根据报文的报文特征查找与报文对应的通信连接；当未查找到与报文对应的通信连接时，将报文上送至与虚拟机对应的模拟网卡。可以理解，上述步骤可在S202之前执行。

[0067] 其中，通信连接是意图通信的双方间对应的连接记录。可以理解，虚拟机在协议栈生成报文发起数据传输时，会相应生成该报文对应的通信连接(连接记录)。此后，与该通信连接相应的报文均相应记录在该通信连接下。比如，虚拟机A向虚拟机B发送的请求连接报文，以及虚拟机B针对该请求连接报文向虚拟机A反馈的确认连接报文属于同一通信连接。而且，虚拟机A和虚拟机B在连接建立完成后传输的报文也属于该通信连接。同样的，虚拟交换机在接收到报文后，也会在相应生成该报文对应的通信连接，保证虚拟交换机和虚拟机保持同步的连接记录。

[0068] 可以理解，相对于上述的慢速路径处理方式，虚拟交换机还架构了一种快速路径处理方式。在快速路径处理方式中，仅按照报文特征对报文进行固定的报文处理操作。通常情况下，属于相同通信连接的报文所对应的报文处理操作是相同的。那么，当将属于某一通信连接的第一个报文按照慢速路径处理方式处理后，即可得到属于该通信连接的报文相应的报文特征，以及相应的报文处理操作。虚拟交换机可针对该通信连接对应记录报文特征和报文处理操作，从而确定该通信连接的报文所对应的快速路径处理方式。这样，后续属于该通信连接的报文即可直接按照相应的快速路径处理方式进行处理。

[0069] 在一个实施例中，快速路径处理方式可通过快速路径模块实现。快速路径模块可以通过虚拟软件进程的方式实现，也可通过实体硬件设备的方式实现。比如，物理机可利用DPDK(Data Plane Development Kit数据平面开发工具集)预先配置快速报文处理进程，配置的快速报文处理进程可以直接接收虚拟网卡发送的报文并对接收的报文进程处理。物理机还可通过智能硬件(如智能网卡)等实现快速路径模块。

[0070] 具体地，物理机上虚拟出的虚拟机可通过虚拟网卡，直接与相应虚拟交换机架构的快速路径模块连接，虚拟交换机从而实现直接通过快速路径模块接收由虚拟机对应的虚拟网卡所发送的报文。快速路径模块在接收到报文后，提取该报文的报文特征，查找与该报文特征相应记录的通信连接。当未查找到与报文对应的通信连接时，将报文上送至与发送报文的虚拟机对应的模拟网卡。

[0071] 在一个实施例中，根据报文的报文特征查找与报文对应的通信连接，包括：从报文中提取报文特征；将报文特征映射为哈希值；查找与哈希值匹配的通信连接。

[0072] 具体地，虚拟交换机可预先设置需要从报文中提取报文特征的特征项，以及对这些特征项所对应的特征数据进行哈希计算所通过的哈希函数。这样，虚拟交换机在针对该

通信连接对应记录报文特征和报文处理操作时，可将报文特征按照预设的哈希函数计算得到哈希值，将该哈希值与通信连接相应记录。这样，虚拟交换机在后续处理报文时，则可直接提取预先设置的这些特征项的特征数据，再根据预设的哈希算法计算提取的这些特征数据所对应的哈希值，从而直接查找与该哈希值对应的通信连接，继而获取到对应于该通信连接记录的报文处理操作来处理报文。

[0073] 举例说明，虚拟交换机预先设置的需要特征项可以是七元组特征项。该七元组特征项包括：源IP地址、源端口、目的IP地址、目的端口、传输层协议、报文入端口和虚拟网络标识。其中，报文入端口是接收报文所通过的端口。比如，模拟网卡标识或者快速路径模块标识等。虚拟网络标识是发送报文的虚拟机所属虚拟网络的标识。这样，每个报文都是解析这七个字段来计算哈希值，此时哈希查找是O(1)的复杂度。而在允许随意组合流表的报文特征时，最坏情况下是需要遍历所有流表才能匹配到流表项，此时的复杂度为O(n)。

[0074] 在本实施例中，在快速路径处理方式中，采用哈希匹配方式查找报文相应的通信连接，这样在数据量较大的场景下查找，哈希查找的复杂度可得到极大的降低，大大提高了查找效率。

[0075] 在一个实施例中，当查找到与报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理报文。

[0076] 具体地，快速路径模块在查找到与报文对应的通信连接时，则查询与该通信连接对应存储的报文处理操作，进而按照查询到的报文处理操作处理报文。

[0077] 在本实施例中，在能够通过快速路径处理方式处理报文时，优先通过快速路径处理方式处理报文，提高了报文处理效率。

[0078] 上述实施例中，优先通过快速路径处理方式处理报文，在不存在于当前接收到的报文相应的通信连接，使得无法通过快速路径处理方式处理报文时，再将报文上送，通过慢速路径处理方式来处理。

[0079] 在一个实施例中，该报文处理方法还包括：确定报文特征所对应的通信连接及通信连接所对应的连接状态；记录通信连接并相应记录连接状态；将报文特征和报文处理操作对应于通信连接存储。可以理解，确定报文特征所对应的通信连接及通信连接所对应的连接状态，及记录通信连接并相应记录连接状态的步骤可以在按照快速路径处理方式处理报文时进行，也可在按照慢速路径处理方式处理报文时进行。这样可以保证虚拟交换机中记录的各通信连接所对应的连接状态与真实的数据传输连接状态一致。

[0080] 通常情况下，通信双方在通信过程中所建立的通信连接会经历一系列的状态变化。比如，一条TCP连接会经历建立连接状态、数据通信状态以及断开连接状态等状态变化。可以理解，每个连接状态都对应有各自的超时时间。不同的连接状态对应的超时时间不同。其中，超时时间是实现设置的可处于相应连接状态的时长。比如，建立连接状态的超时时间较短，可以理解为建立连接的双方不可能将大量时间花费在等待对方应答连接的过程中。数据通信状态的超时时间较长，可以理解为防止通信双方之间需要传输的数据量较大时，需要频繁的建立连接导致耗时，而通过设置较长的超时时间使得双方之间保持有长连接。

[0081] 在Linux操作系统下，Linux内核可通过conntrack记录通信连接并相应记录连接状态。

[0082] 具体地，虚拟交换机在按照慢速路径处理方式处理报文时，确定报文特征所对应

的通信连接，并根据报文特征确定该通信连接当前所对应的连接状态。此后，虚拟交换机进而记录通信连接及连接状态，并将超时时间更新为当前记录的连接状态所对应的超时时间。再将报文特征和报文处理操作对应于通信连接存储。

[0083] 虚拟交换机在按照快速路径处理方式处理报文时，也可确定报文特征所对应的通信连接，并根据报文特征确定该通信连接当前所对应的连接状态。此后，虚拟交换机进而转换对应该通信连接记录的连接状态为当前确定的连接状态，并将超时时间更新为当前记录的连接状态所对应的超时时间。

[0084] 在本实施例中，虚拟交换机上记录的各通信连接的连接状态基本能够与虚拟机上相应通信连接的连接状态一致。从而避免了虚拟交换机上记录的连接状态与实际连接状态不一致，而导致通信连接失效需要重新建立通信连接的情形，继而导致无谓的快速路径处理方式与慢速路径处理方式的交换，提高报文处理效率。

[0085] 在一个实施例中，S208包括：将提取的报文特征与预设的访问控制报文特征比较；当提取的报文特征与访问控制报文特征匹配时，则确定报文处理操作为报文丢弃操作。S210包括：丢弃报文。

[0086] 其中，访问控制报文特征表示需要被控制访问的报文的特征。可以理解，当报文的特征与访问控制报文特征匹配时，则表示该报文需要被控制。访问控制报文特征可以是网络地址特征、通信端口特征或者通信协议特征等中的至少一种。

[0087] 具体地，虚拟交换机可事先配置访问控制策略，并预先根据该访问控制策略确定访问控制报文特征。这样虚拟交换机在实际接收到报文时，即可在提取该报文的报文特征后，将提取的报文特征与预设的访问控制报文特征进行比较。在虚拟交换机确定提取的报文特征与预设的访问控制报文特征匹配时，即判定该报文属于应当被控制的报文，进而确定报文处理操作为报文丢弃操作，从而丢弃该报文。

[0088] 在一个实施例中，虚拟交换机可通过访问控制列表来实现访问控制策略。访问控制列表(Access Control List，ACL)是虚拟交换机的指令列表，用来控制进出虚拟交换机的报文。

[0089] 具体地，在本实施例中，虚拟交换机通过模拟网卡或快速路径模块接收虚拟虚拟机发送的报文并进行报文处理的过程可以理解为虚拟机发包方向的处理流程。在该场景下，虚拟交换机可事先对虚拟机的通信对象进行控制。

[0090] 虚拟交换机可事先配置访问控制列表，访问控制列表中记录是不允许访问的报文的特征(访问控制报文特征)。当虚拟交换机判定报文的特征记录于访问控制列表中时，则判定此项访问不被允许，即确定该报文对应的报文处理操作为报文丢弃操作，继而丢弃该报文。

[0091] 在本实施例中，通过预设访问控制特征来进行过滤报文，提高了网络安全性。

[0092] 在一个实施例中，访问控制列表中记录的也可以是允许访问的报文的特征。当虚拟交换机判定报文的特征未记录于访问控制列表中时，则判定此项访问不被允许，即确定该报文对应的报文处理操作为报文丢弃操作，继而丢弃该报文。

[0093] 在一个实施例中，报文特征包括目的网络地址。该报文处理方法还包括：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为与虚拟机对应的实体网络地址时，则确定报文处理操作为报文转发操作。S210包括：转发报文。

[0094] 其中，目的网络地址是通信目的端所对应的网络地址。目的网络地址具体可以是目的IP地址。实体网络地址是真实可访问的网络地址。当目的网络地址为与虚拟机对应的实体网络地址时，表示意图访问的对象是可唯一确定的虚拟机，此时虚拟交换机即可对报文进行转发以使得该报文到达目的端。

[0095] 在一个实施例中，报文特征还包括源网络地址、源网络地址对应的源虚拟网络标识及目的网络地址所对应的目的虚拟网络标识。当源虚拟网络标识与目的虚拟网络标识一致时，转发报文，包括：通过目的网络地址指向的虚拟机所对应的模拟网卡转发报文。

[0096] 其中，源网络地址是通信发起端所对应的网络地址。源网络地址具体可以是源IP地址。源虚拟网络标识是通信发起端所在虚拟网络的标识。目的虚拟网络标识是通信目的端所在虚拟网络的标识。可以理解，一个虚拟网络对应一个虚拟交换机，一个虚拟网络可对应多个虚拟机。

[0097] 当源虚拟网络标识与目的虚拟网络标识一致时，表示通信发起端(发送报文的虚拟机)与通信目的端(接收报文的虚拟机)是基于相同的物理机虚拟出的虚拟机、且属于相同的虚拟网络。对于属于相同的虚拟网络的通信双方间，通过该虚拟网络对应的虚拟交换机和通信双方间各自对应的模拟网卡即可完成报文转发。

[0098] 具体地，虚拟交换机在判定源虚拟网络标识与目的虚拟网络标识一致时，则查询目的网络地址指向的虚拟机所对应的模拟网卡，通过查询到的该模拟网卡转发报文。

[0099] 举例说明，虚拟机A和虚拟机B同属虚拟网络1，虚拟网络1对应虚拟交换机1。虚拟机A意图与虚拟机B通信，即通过虚拟机A的虚拟网卡A发送报文，虚拟交换机1继而通过与虚拟机A对应的模拟网卡A接收该报文，在确定该报文是发送至虚拟机B的报文时，则通过虚拟机B对应的模拟网卡B转发至虚拟机B的虚拟网卡B，从而将虚拟机A发送的报文转发给虚拟机B。

[0100] 在本实施例中，提供了属于同一虚拟网络下的虚拟机之间报文转发的途径，实现了同一虚拟网络下的虚拟机之间报文转发。

[0101] 在一个实施例中，虚拟交换机还可将报文，通过目的网络地址指向的虚拟机所对应的模拟网卡下发至快速路径模块，再由快速路径模块转发至目的虚拟机。虚拟交换机若通过快速路径模块接收报文，可直接通过该快速路径模块转发该报文至目的虚拟机。

[0102] 在一个实施例中，该报文处理方法还包括：当源虚拟网络标识与目的虚拟网络标识不一致时，则通过虚拟隧道端口查找中间地址；中间地址与目的网络地址指向的虚拟机所属物理机对应；将中间地址添加到报文的头部生成隧道报文；通过虚拟隧道端口转发隧道报文。

[0103] 可以理解，一个虚拟网络对应一个虚拟隧道端口(tun port)。属于不同的虚拟网络的虚拟交换机之间通过虚拟隧道端口传输报文。虚拟交换机可通过虚拟隧道端口将报文强制传输到特定的地址。

[0104] 当源虚拟网络标识与目的虚拟网络标识不一致时，表示通信发起端(发送报文的虚拟机)与通信目的端(接收报文的虚拟机)是属于不同的虚拟网络。对于属于不同的虚拟网络的通信双方间，通过通信双方所在虚拟网络所对应的虚拟交换机、通信双方所在虚拟网络所对应的虚拟隧道端口，以及通信双方间各自对应的模拟网卡完成报文转发。

[0105] 具体地，虚拟交换机在判定源虚拟网络标识与目的虚拟网络标识不一致时，则查

询目的网络地址指向的虚拟机所属物理机对应中间地址，将该中间地址添加到报文的头部生成隧道报文，再通过虚拟隧道端口转发隧道报文。其中，中间地址具体可以是物理机对应的MAC(Media Access Control，媒体访问控制)地址或者IP地址中的至少一个。在一个实施例中，虚拟交换机可将报文自身携带的MAC地址去除后再将查询到的MAC地址添加至报文的头部。

[0106] 举例说明，物理机1虚拟出的虚拟机A属虚拟网络1，虚拟网络1对应虚拟交换机1和虚拟隧道端口1。物理机2虚拟出的虚拟机B属虚拟网络2，虚拟网络2对应虚拟交换机2和虚拟隧道端口2。虚拟机A意图与虚拟机B通信，即通过虚拟机A的虚拟网卡A发送报文，虚拟交换机1继而通过与虚拟机A对应的模拟网卡A接收该报文，在确定该报文是发送至虚拟机B的报文时，则查询虚拟机B所属物理机2的MAC地址和/或IP地址，将该MAC地址和/或IP地址添加到报文的头部生成隧道报文，再通过虚拟隧道端口1转发隧道报文。虚拟隧道端口1与虚拟隧道端口2直接可通过物理线路连接。

[0107] 在本实施例中，提供了属于不同虚拟网络下的虚拟机之间报文转发的途径，实现了不同虚拟网络下的虚拟机之间报文转发。

[0108] 在一个实施例中，虚拟交换机还可将报文，通过虚拟隧道端口下发至快速路径模块，再由快速路径模块转发至目的虚拟机。

[0109] 上述实施例中，提供了多种虚拟网络场景下的报文转发途径，实现了各种虚拟网络场景下的报文转发。

[0110] 在一个实施例中，该报文处理方法还包括：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为虚拟网络地址时，则确定报文处理操作为报文目的端修改操作；将目的网络地址修改为与虚拟网络地址对应的实体网络地址。S210包括：转发修改后的报文。

[0111] 其中，虚拟网络地址是未分配至具体虚拟机的网络地址。虚拟机通过虚拟网络地址访问的目的端不是唯一确定的。虚拟交换机在负载均衡处理时，通常会为提供相同服务的虚拟机配置共同的虚拟网络地址，并将该虚拟网络地址对外提供给其他虚拟机供访问。

[0112] 具体地，虚拟交换机在提取的报文特征与访问控制报文特征不匹配、且目的网络地址为虚拟网络地址时，则判定事先进行了负载均衡处理。此时，虚拟交换机可查找与该虚拟网络地址对应的实体网络地址，从查找到的实体网络地址中随机选取一个作为目的网络地址，将报文中原来的目的网络地址修改为新确定的目的网络地址。虚拟交换机也可选择负载量低的虚拟机所对应的实体网络地址作为目的网络地址。

[0113] 在本实施例中，通过将虚拟网络地址与多个实体网络地址对应，在实际访问时，通过虚拟网络地址访问其中一个实体网络地址对应的虚拟机，从而将访问分摊到多个虚拟机上，实现了负载均衡。

[0114] 在一个实施例中，该报文处理方法还包括：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为公网网络地址时，则确定报文处理操作为报文源端修改操作；将报文的源网络地址修改为公网网络地址对应的实体网络地址。S210包括：转发修改后的报文。

[0115] 其中，公网网络地址是用于访问公共资源的网络地址。虚拟机在访问外部公共网络时，需要通过具有访问权限的网络地址进行访问。

[0116] 具体地，虚拟交换机在提取的报文特征与访问控制报文特征不匹配、且目的网络地址为公网网络地址时，则判定虚拟机意图网络外部公共网络。此时，虚拟交换机可查找与该公网网络地址对应的实体网络地址，进而将报文的源网络地址修改该实体网络地址。

[0117] 在本实施例中，提供了虚拟机访问外部公共网络时的报文处理方式，实现了虚拟机访问外部公共网络。

[0118] 在一个实施例中，虚拟机还可被配置为支持预设设置的网络安全策略。网络安全策略一般支持按连接方向区分，需要实现精确的连接记录和管理。比如：可以设置网络安全策略为拒绝一切外部主动访问，但是允许虚拟机主动访问外部。那么，每个主动向外访问的通信连接需要记录下来。收到外部进入虚拟机的报文时，如果该报文属于已存在的通信连接，则进行相应处理；否则需要丢弃该报文。

[0119] 可以理解，上述实施例中涉及的报文传输方向可以是通信发起端发送报文时的报文传输方向；或者是相同虚拟网络内部通信时，通信目的端接收报文时的报文传输方向。参考图3，在一个实施例中，提供了虚拟机发送报文方向的报文传输逻辑过程图。

[0120] 具体地，源虚拟机可通过虚拟网卡发送报文。当虚拟交换机存在快速路径模块时，可通过快速路径模块直接接收报文，并继续通过快速路径模块根据该报文的报文特征查找与该报文对应的通信连接。当虚拟交换机通过快速路径模块当查找到与该报文对应的通信连接时，则继续查询与该通信连接对应存储的报文处理操作，进而通过快速路径模块按照查询到的报文处理操作处理报文。

[0121] 当虚拟交换机未通过快速路径模块查找到与该报文对应的通信连接时，则将该报文上送至与源虚拟机对应的模拟网卡，通过模拟网卡再将报文传递至物理机的内核空间，进而在物理机的内核空间中，根据该报文的报文特征确定报文处理操作，按照该报文处理操作处理报文。

[0122] 当虚拟交换机不存在快速路径模块时，可通过与源虚拟机对应的模拟网卡直接接收报文，进而通过模拟网卡再将报文传递至物理机的内核空间，进而在物理机的内核空间中，根据该报文的报文特征确定报文处理操作，按照该报文处理操作处理报文。

[0123] 当报文需要被继续传输时，若目的虚拟机与源虚拟机属于相同虚拟网络时，虚拟交换机可将报文传递至目的虚拟机所对应的模拟网卡，该模拟网卡可在存在快速路径模块时，将报文下发至快速路径模块，由快速路径处理模块转发至目的虚拟机。该模拟网卡也可直接将报文转发至目的虚拟机。

[0124] 若目的虚拟机与源虚拟机属于不同虚拟网络时，虚拟交换机可将报文传递至虚拟隧道端口，该虚拟隧道端口可在存在快速路径模块时，将报文下发至快速路径模块，由快速路径处理模块转发该报文。该虚拟隧道端口也可直接转发该报文。

[0125] 在一个实施例中，该报文处理方法还包括：通过虚拟隧道端口接收隧道报文；虚拟隧道端口通过物理机基于自身操作系统内核对应虚拟机所属虚拟网络虚拟得到；通过虚拟隧道端口将隧道报文传递至物理机的内核空间；在内核空间中，从隧道报文中提取报文特征；根据提取的隧道报文特征确定报文处理操作；按照报文处理操作处理隧道报文。

[0126] 可以理解，该实施例中涉及的报文传输方向可以是通信目的端接收报文时的报文传输方向。此时通信发起端和通信目的端处于不同的虚拟网络中，不同虚拟网络间通过虚拟隧道端口传递报文。

[0127] 具体地，发报文的虚拟机(通信发起端)通过自身所属虚拟网络所对应的虚拟交换机通过虚拟隧道端口将报文封装为隧道报文后转发，接收报文的虚拟机(通信目的端)通过自身所属虚拟网络所对应的虚拟交换机通过虚拟隧道端口接收隧道报文。其中，隧道报文是根据隧道协议封装后，由虚拟隧道端口转发或接收的报文。隧道协议比如GRE(Generic Routing Encapsulation,通用路由封装)协议。

[0128] 在一个实施例中，该报文处理方法还包括：从隧道报文中提取网络地址；将与网络地址对应的物理地址添加到隧道报文的首部，并执行通过虚拟隧道端口将隧道报文传递至物理机的内核空间的步骤。

[0129] 具体地，虚拟交换机在通过虚拟隧道端口接收到隧道报文后，根据隧道协议解析该隧道报文，从该隧道报文中提取网络地址。虚拟交换机继而查找与该网络地址对应的物理地址，将查找到的物理地址添加到隧道报文的首部后传递至物理机的内核空间。该网络地址具体可以是目的IP地址，也就是接收报文的虚拟机的IP地址。该物理地址具体可以是目的MAC地址，也就是接收报文的虚拟机的MAC地址。

[0130] 在本实施例中，根据隧道报文中的网络地址，查找实际应当接收报文的虚拟机的物理地址，再将物理地址添加到报文头，这样即可根据网络地址和物理地址准确地将报文发送至目的地。

[0131] 具体地，在内核空间中对隧道报文的处理过程与上述实施例中的处理过程类似。物理机在确定应当对该报文进行的报文处理操作后，即根据该报文处理操作处理该报文。比如，当报文处理操作为报文丢弃操作时，则丢弃该报文；或者，当报文处理操作为报文转发操作时，则转发该报文等。

[0132] 对于转发报文的场景，可以理解，此时虚拟交换机是需要将报文转发至自身所对应虚拟网络下的虚拟机，则可通过与应当接收报文的虚拟机所对应的模拟网卡将报文转发至该虚拟机。

[0133] 可以理解，上述处理过程中报文的处理经历了通过报文特征确定报文处理操作的过程，而非仅经历已知的固定的报文处理操作。也就是说，上述报文处理过程是基于虚拟交换机架构的慢速路径处理方式。

[0134] 上述实施例中，通过虚拟隧道端口可直接接收隧道报文，并在接收到隧道报文后即可直接将该隧道报文传递至物理机的内核空间，继而在内核空间中从隧道报文中提取报文特征，以根据提取的报文特征来确定报文处理操作，从而即可自动根据确定的报文处理操作来处理隧道报文。这样不需要依赖于多个处理路径的相互配合，从而拓宽了报文处理方式的适用范围，极大程度上满足了报文处理需求。

[0135] 在一个实施例中，该报文处理方法还包括：接收由物理网卡所传递的隧道报文；根据隧道报文的报文特征查找与隧道报文对应的通信连接；当未查找到与隧道报文对应的通信连接时，将隧道报文上送至虚拟隧道端口。

[0136] 可以理解，类似于上述实施例，隧道报文也可在存在快速路径处理方式时，优先通过快速路径处理方式进行处理。在快速路径处理方式中，仅按照报文特征对报文进行固定的报文处理操作。通常情况下，属于相同通信连接的报文所对应的报文处理操作是相同的。那么，当将属于某一通信连接的第一个报文按照慢速路径处理方式处理后，即可得到属于该通信连接的报文相应的报文特征，以及相应的报文处理操作。虚拟交换机可针对该通信

连接对应记录报文特征和报文处理操作，从而确定该通信连接的报文所对应的快速路径处理方式。这样，后续属于该通信连接的报文即可直接按照相应的快速路径处理方式进行处理。

[0137] 在一个实施例中，快速路径处理方式可通过快速路径模块实现。快速路径模块可以通过虚拟软件进程的方式实现，也可通过实体硬件设备的方式实现。比如，物理机可利用DPDK(Data Plane Development Kit数据平面开发工具集)预先配置快速报文处理进程，配置的快速报文处理进程可以直接接收虚拟网卡发送的报文并对接收的报文进程处理。物理机还可通过智能硬件(如智能网卡)等实现快速路径模块。

[0138] 具体地，物理机的物理网卡可与快速路径模块连接，虚拟隧道端口则与快速路径模块连接，虚拟交换机从而实现直接通过快速路径模块接收由物理网卡所发送的报文。快速路径模块在接收到报文后，提取该报文的报文特征，查找与该报文特征相应记录的通信连接。当未查找到与报文对应的通信连接时，将报文上送至虚拟隧道端口。

[0139] 在一个实施例中，该报文处理方法还包括：当查找到与隧道报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理隧道报文。

[0140] 具体地，快速路径模块在查找到与报文对应的通信连接时，则查询与该通信连接对应存储的报文处理操作，进而按照查询到的报文处理操作处理报文。

[0141] 在本实施例中，在能够通过快速路径处理方式处理报文时，优先通过快速路径处理方式处理报文，提高了报文处理效率。

[0142] 上述实施例中，优先通过快速路径处理方式处理报文，在不存在于当前接收到的报文相应的通信连接，使得无法通过快速路径处理方式处理报文时，再将报文上送，通过慢速路径处理方式来处理。

[0143] 可以理解，上述实施例中涉及的报文传输方向可以是通信目的端接收报文时的报文传输方向，此时通信发起端和通信目的端属于不同的虚拟网络。参考图4，在一个实施例中，提供了虚拟机接收报文方向的报文传输逻辑过程图。

[0144] 具体地，目的虚拟机所属物理机可通过物理网卡(物理线路)接收源虚拟机所对应的虚拟交换机转发的报文。当虚拟交换机存在快速路径模块时，可通过快速路径模块直接接收报文，并继续通过快速路径模块根据该报文的报文特征查找与该报文对应的通信连接。当虚拟交换机通过快速路径模块当查找到与该报文对应的通信连接时，则继续查询与该通信连接对应存储的报文处理操作，进而通过快速路径模块按照查询到的报文处理操作处理报文。

[0145] 当虚拟交换机未通过快速路径模块查找到与该报文对应的通信连接时，则将该报文上送至与虚拟隧道端口，从隧道报文中提取网络地址；将与网络地址对应的物理地址添加到隧道报文的首部后，通过虚拟隧道端口再将报文传递至物理机的内核空间，进而在物理机的内核空间中，根据该报文的报文特征确定报文处理操作，按照该报文处理操作处理报文。

[0146] 当报文需要被继续传输时，虚拟交换机可将报文传递至目的虚拟机所对应的模拟网卡，该模拟网卡可在存在快速路径模块时，将报文下发至快速路径模块，由快速路径处理模块转发至目的虚拟机。该模拟网卡也可直接将报文转发至目的虚拟机。

[0147] 当虚拟交换机不存在快速路径模块时，可通过虚拟隧道端口直接接收报文，从隧道报文中提取网络地址；将与网络地址对应的物理地址添加到隧道报文的首部后，进而通过虚拟隧道端口再将报文传递至物理机的内核空间，进而在物理机的内核空间中，根据该报文的报文特征确定报文处理操作，按照该报文处理操作处理报文。当报文需要被继续传输时，虚拟交换机可将报文传递至目的虚拟机所对应的模拟网卡，由模拟网卡直接将报文转发至目的虚拟机。

[0148] 图5示出了一个实施例中虚拟交换机的网络拓扑图。参考图5，在linux操作系统环境下，基于Linux操作系统虚拟出的Bridge(虚拟网桥设备)、Vdev(Virtual net device，虚拟网络设备)和Tun Port(虚拟隧道)可架构得到虚拟交换机。在本实施例中，快速路径处理方式和慢速路径处理方式并存。Vdev与Tun Port通过通用的快慢速路径通信接口(Netlink/Driver API)与快速路径模块连接。再参考图6，图6示出了另一个实施例中虚拟交换机的网络拓扑图。在本实施例中，仅存在慢速路径处理方式，此时，Vdev则可直接通过模拟网卡与虚拟机的虚拟网卡连接，Tun Port则直接与物理机的物理网卡连接。其中，通过虚拟交换机可实现NAT、ACL、QoS和LB。

[0149] 应该理解的是，虽然上述各实施例的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，上述各实施例中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0150] 如图7所示，在一个实施例中，提供了一种报文处理装置700。参照图7，该报文处理装置700包括：接收模块701、传递模块702、提取模块703、确定模块704和处理模块705。

[0151] 接收模块701，用于通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到。

[0152] 传递模块702，用于通过模拟网卡将报文传递至物理机的内核空间。

[0153] 提取模块703，用于在内核空间中，从报文中提取报文特征。

[0154] 确定模块704，用于根据提取的报文特征确定报文处理操作。

[0155] 处理模块705，用于按照报文处理操作处理报文。

[0156] 上述报文处理装置700，由于模拟网卡是通过虚拟机所属物理机，基于该物理机自身的操作系统内核对应于虚拟机模拟得到的，那么该模拟网卡可直接接收报文，并在接收到报文后即可直接将该报文传递至物理机的内核空间，继而在内核空间中从报文中提取报文特征，以根据提取的报文特征来确定报文处理操作，从而即可自动根据确定的报文处理操作来处理报文。这样不需要依赖于多个处理路径的相互配合，从而拓宽了报文处理方式的适用范围，极大程度上满足了报文处理需求。

[0157] 如图8所示，报文处理装置700还包括：快速处理模块706和上送模块707。

[0158] 快速处理模块706，用于接收由虚拟机对应的虚拟网卡所发送的报文；根据报文的报文特征查找与报文对应的通信连接；

[0159] 上送模块707，用于当未查找到与报文对应的通信连接时，将报文上送至与虚拟机

对应的模拟网卡。

[0160] 在一个实施例中，快速处理模块706还用于从报文中提取报文特征；将报文特征映射为哈希值；查找与哈希值匹配的通信连接。

[0161] 在一个实施例中，快速处理模块706还用于当查找到与报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理报文。

[0162] 如图9所示，报文处理装置700还包括：记录模块708。

[0163] 记录模块708，用于确定报文特征所对应的通信连接及通信连接所对应的连接状态；记录通信连接并相应记录连接状态；将报文特征和报文处理操作对应于通信连接存储。

[0164] 在一个实施例中，确定模块704还用于将提取的报文特征与预设的访问控制报文特征比较；当提取的报文特征与访问控制报文特征匹配时，则确定报文处理操作为报文丢弃操作。处理模块705还用于丢弃报文。

[0165] 在一个实施例中，报文特征包括目的网络地址。确定模块704还用于当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为与虚拟机对应的实体网络地址时，则确定报文处理操作为报文转发操作。处理模块705还用于转发报文。

[0166] 在一个实施例中，报文特征还包括源网络地址、源网络地址对应的源虚拟网络标识及目的网络地址所对应的目的虚拟网络标识。当源虚拟网络标识与目的虚拟网络标识一致时，处理模块705还用于通过目的网络地址指向的虚拟机所对应的模拟网卡转发报文。

[0167] 在一个实施例中，当源虚拟网络标识与目的虚拟网络标识不一致时，处理模块705还用于通过虚拟隧道端口查找中间地址；中间地址与目的网络地址指向的虚拟机所属物理机对应；将中间地址添加到报文的头部生成隧道报文；通过虚拟隧道端口转发隧道报文。

[0168] 在一个实施例中，确定模块704还用于当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为虚拟网络地址时，则确定报文处理操作为报文目的端修改操作；将目的网络地址修改为与虚拟网络地址对应的实体网络地址。处理模块705还用于转发修改后的报文。

[0169] 在一个实施例中，确定模块704还用于当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为公网网络地址时，则确定报文处理操作为报文源端修改操作；将报文的源网络地址修改为公网网络地址对应的实体网络地址。处理模块705还用于转发修改后的报文。

[0170] 在一个实施例中，接收模块701还用于通过虚拟隧道端口接收隧道报文；虚拟隧道端口通过物理机基于自身操作系统内核对应虚拟机所属虚拟网络虚拟得到。传递模块702还用于通过虚拟隧道端口将隧道报文传递至物理机的内核空间。提取模块703还用于在内核空间中，从隧道报文中提取报文特征。确定模块704还用于根据提取的隧道报文特征确定报文处理操作。处理模块705还用于按照报文处理操作处理隧道报文。

[0171] 在一个实施例中，接收模块701还用于从隧道报文中提取网络地址；将与网络地址对应的物理地址添加到隧道报文的首部。

[0172] 在一个实施例中，快速处理模块706还用于接收由物理网卡所传递的隧道报文；根据隧道报文的报文特征查找与隧道报文对应的通信连接。上送模块707还用于当未查找到与隧道报文对应的通信连接时，将隧道报文上送至虚拟隧道端口。

[0173] 在一个实施例中，快速处理模块706还用于当查找到与隧道报文对应的通信连接

时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理隧道报文。

[0174] 图10示出了一个实施例中计算机设备的内部结构图。该计算机设备具体可以是图1中的物理机1000。如图10所示，该计算机设备包括通过系统总线连接的处理器、存储器和网络接口。其中，存储器包括非易失性存储介质和内存储器。该计算机设备的非易失性存储介质存储有操作系统，还可存储有计算机程序，该计算机程序被处理器执行时，可使得处理器实现报文处理方法。该内存储器中也可储存有计算机程序，该计算机程序被处理器执行时，可使得处理器执行报文处理方法。计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏等，输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，也可以是外接的键盘、触控板或鼠标等。本领域技术人员可以理解，图10中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0175] 在一个实施例中，本申请提供的报文处理装置可以实现为一种计算机程序的形式，计算机程序可在如图10所示的计算机设备上运行，计算机设备的非易失性存储介质可存储组成该报文处理装置的各个程序模块，比如，图7所示的接收模块701、传递模块702、提取模块703、确定模块704和处理模块705等。各个程序模块组成的计算机程序使得处理器执行本说明书中描述的本申请各个实施例的报文处理方法中的步骤。

[0176] 例如，图10所示的计算机设备可以通过如图7所示的报文处理装置700中的接收模块701通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到。传递模块702通过模拟网卡将报文传递至物理机的内核空间。提取模块703在内核空间中，从报文中提取报文特征。确定模块704根据提取的报文特征确定报文处理操作。处理模块705按照报文处理操作处理报文。

[0177] 在一个实施例中，提供了一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时，使得处理器执行以下步骤：通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到；通过模拟网卡将报文传递至物理机的内核空间；在内核空间中，从报文中提取报文特征；根据提取的报文特征确定报文处理操作；按照报文处理操作处理报文。

[0178] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：接收由虚拟机对应的虚拟网卡所发送的报文；根据报文的报文特征查找与报文对应的通信连接；当未查找到与报文对应的通信连接时，将报文上送至与虚拟机对应的模拟网卡。

[0179] 在一个实施例中，根据报文的报文特征查找与报文对应的通信连接，包括：从报文中提取报文特征；将报文特征映射为哈希值；查找与哈希值匹配的通信连接。

[0180] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当查找到与报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理报文。

[0181] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：确定报文特征所对应的通信连接及通信连接所对应的连接状态；记录通信连接并相应记录连接状态；将报文特征和报文处理操作对应于通信连接存储。

[0182] 在一个实施例中，根据提取的报文特征确定报文处理操作，包括：将提取的报文特征与预设的访问控制报文特征比较；当提取的报文特征与访问控制报文特征匹配时，则确定报文处理操作为报文丢弃操作。按照报文处理操作处理报文，包括：丢弃报文。

[0183] 在一个实施例中，报文特征包括目的网络地址。该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为与虚拟机对应的实体网络地址时，则确定报文处理操作为报文转发操作。按照报文处理操作处理报文，包括：转发报文。

[0184] 在一个实施例中，报文特征还包括源网络地址、源网络地址对应的源虚拟网络标识及目的网络地址所对应的目的虚拟网络标识。当源虚拟网络标识与目的虚拟网络标识一致时，转发报文，包括：通过目的网络地址指向的虚拟机所对应的模拟网卡转发报文。

[0185] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当源虚拟网络标识与目的虚拟网络标识不一致时，则通过虚拟隧道端口查找中间地址；中间地址与目的网络地址指向的虚拟机所属物理机对应；将中间地址添加到报文的头部生成隧道报文；通过虚拟隧道端口转发隧道报文。

[0186] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为虚拟网络地址时，则确定报文处理操作为报文目的端修改操作；将目的网络地址修改为与虚拟网络地址对应的实体网络地址。按照报文处理操作处理报文，包括：转发修改后的报文。

[0187] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为公网网络地址时，则确定报文处理操作为报文源端修改操作；将报文的源网络地址修改为公网网络地址对应的实体网络地址。按照报文处理操作处理报文，包括：转发修改后的报文。

[0188] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：通过虚拟隧道端口接收隧道报文；虚拟隧道端口通过物理机基于自身操作系统内核对应虚拟机所属虚拟网络虚拟得到；通过虚拟隧道端口将隧道报文传递至物理机的内核空间；在内核空间中，从隧道报文中提取报文特征；根据提取的隧道报文特征确定报文处理操作；按照报文处理操作处理隧道报文。

[0189] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：从隧道报文中提取网络地址；将与网络地址对应的物理地址添加到隧道报文的首部，并执行通过虚拟隧道端口将隧道报文传递至物理机的内核空间的步骤。

[0190] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：接收由物理网卡所传递的隧道报文；根据隧道报文的报文特征查找与隧道报文对应的通信连接；当未查找到与隧道报文对应的通信连接时，将隧道报文上送至虚拟隧道端口。

[0191] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当查找到与隧道报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理隧道报文。

[0192] 上述存储介质，由于模拟网卡是通过虚拟机所属物理机，基于该物理机自身的操作系统内核对应于虚拟机模拟得到的，那么该模拟网卡可直接接收报文，并在接收到报文后即可直接将该报文传递至物理机的内核空间，继而在内核空间中从报文中提取报文特

征，以根据提取的报文特征来确定报文处理操作，从而即可自动根据确定的报文处理操作来处理报文。这样不需要依赖于多个处理路径的相互配合，从而拓宽了报文处理方式的适用范围，极大程度上满足了报文处理需求。

[0193] 在一个实施例中，提供了一种计算机设备，包括存储器和处理器，存储器中储存有计算机程序，计算机程序被处理器执行时，使得处理器执行以下步骤：通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到；通过模拟网卡将报文传递至物理机的内核空间；在内核空间中，从报文中提取报文特征；根据提取的报文特征确定报文处理操作；按照报文处理操作处理报文。

[0194] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：接收由虚拟机对应的虚拟网卡所发送的报文；根据报文的报文特征查找与报文对应的通信连接；当未查找到与报文对应的通信连接时，将报文上送至与虚拟机对应的模拟网卡。

[0195] 在一个实施例中，根据报文的报文特征查找与报文对应的通信连接，包括：从报文中提取报文特征；将报文特征映射为哈希值；查找与哈希值匹配的通信连接。

[0196] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当查找到与报文对应的通信连接时，则查询与通信连接对应存储的报文处理操作；按照查询到的报文处理操作处理报文。

[0197] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：确定报文特征所对应的通信连接及通信连接所对应的连接状态；记录通信连接并相应记录连接状态；将报文特征和报文处理操作对应于通信连接存储。

[0198] 在一个实施例中，根据提取的报文特征确定报文处理操作，包括：将提取的报文特征与预设的访问控制报文特征比较；当提取的报文特征与访问控制报文特征匹配时，则确定报文处理操作为报文丢弃操作。按照报文处理操作处理报文，包括：丢弃报文。

[0199] 在一个实施例中，报文特征包括目的网络地址。该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为与虚拟机对应的实体网络地址时，则确定报文处理操作为报文转发操作。按照报文处理操作处理报文，包括：转发报文。

[0200] 在一个实施例中，报文特征还包括源网络地址、源网络地址对应的源虚拟网络标识及目的网络地址所对应的目的虚拟网络标识。当源虚拟网络标识与目的虚拟网络标识一致时，转发报文，包括：通过目的网络地址指向的虚拟机所对应的模拟网卡转发报文。

[0201] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当源虚拟网络标识与目的虚拟网络标识不一致时，则通过虚拟隧道端口查找中间地址；中间地址与目的网络地址指向的虚拟机所属物理机对应；将中间地址添加到报文的头部生成隧道报文；通过虚拟隧道端口转发隧道报文。

[0202] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为虚拟网络地址时，则确定报文处理操作为报文目的端修改操作；将目的网络地址修改为与虚拟网络地址对应的实体网络地址。按照报文处理操作处理报文，包括：转发修改后的报文。

[0203] 在一个实施例中，该计算机程序被处理器执行时，还使得处理器执行以下步骤：当提取的报文特征与访问控制报文特征不匹配、且目的网络地址为公网网络地址时，则确定

报文处理操作为报文源端修改操作;将报文的源网络地址修改为公网网络地址对应的实体网络地址。按照报文处理操作处理报文,包括:转发修改后的报文。

[0204] 在一个实施例中,该计算机程序被处理器执行时,还使得处理器执行以下步骤:通过虚拟隧道端口接收隧道报文;虚拟隧道端口通过物理机基于自身操作系统内核对应虚拟机所属虚拟网络虚拟得到;通过虚拟隧道端口将隧道报文传递至物理机的内核空间;在内核空间中,从隧道报文中提取报文特征;根据提取的隧道报文特征确定报文处理操作;按照报文处理操作处理隧道报文。

[0205] 在一个实施例中,该计算机程序被处理器执行时,还使得处理器执行以下步骤:从隧道报文中提取网络地址;将与网络地址对应的物理地址添加到隧道报文的首部,并执行通过虚拟隧道端口将隧道报文传递至物理机的内核空间的步骤。

[0206] 在一个实施例中,该计算机程序被处理器执行时,还使得处理器执行以下步骤:接收由物理网卡所传递的隧道报文;根据隧道报文的报文特征查找与隧道报文对应的通信连接;当未查找到与隧道报文对应的通信连接时,将隧道报文上送至虚拟隧道端口。

[0207] 在一个实施例中,该计算机程序被处理器执行时,还使得处理器执行以下步骤:当查找到与隧道报文对应的通信连接时,则查询与通信连接对应存储的报文处理操作;按照查询到的报文处理操作处理隧道报文。

[0208] 上述计算机设备,由于模拟网卡是通过虚拟机所属物理机,基于该物理机自身的操作系统内核对应于虚拟机模拟得到的,那么该模拟网卡可直接接收报文,并在接收到报文后即可直接将该报文传递至物理机的内核空间,继而在内核空间中从报文中提取报文特征,以根据提取的报文特征来确定报文处理操作,从而即可自动根据确定的报文处理操作来处理报文。这样不需要依赖于多个处理路径的相互配合,从而拓宽了报文处理方式的适用范围,极大程度上满足了报文处理需求。

[0209] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一非易失性计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0210] 以上实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0211] 以上实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对本发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明专利的保护范围应以所附权利要求为准。

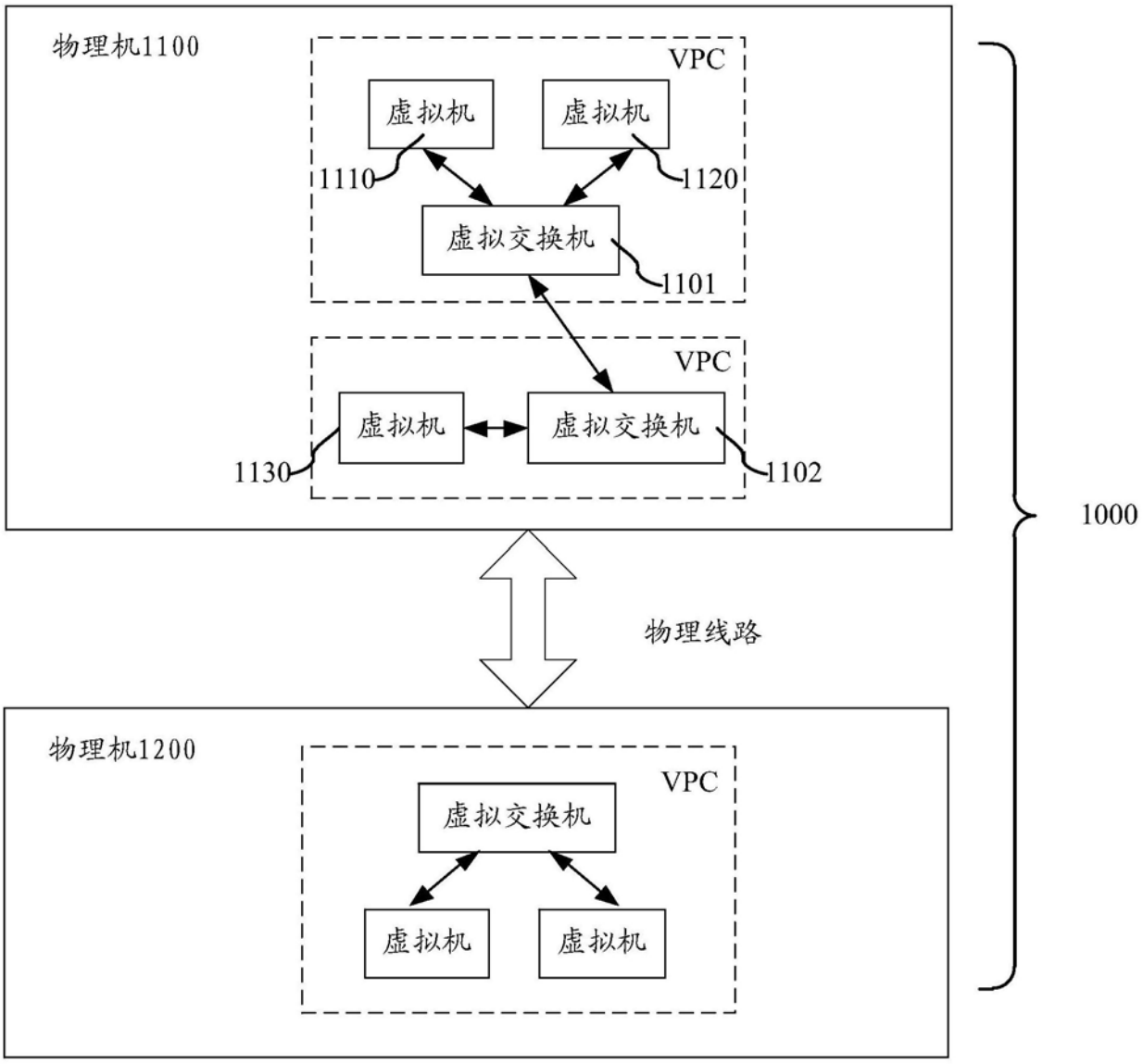

物理机1100
VPC
虚拟机
虚拟机
1110
1120
虚拟交换机
1101
VPC
虚拟机
虚拟交换机
1130
1102
1000
物理线路
物理机1200
VPC
虚拟交换机
虚拟机
虚拟机

图1

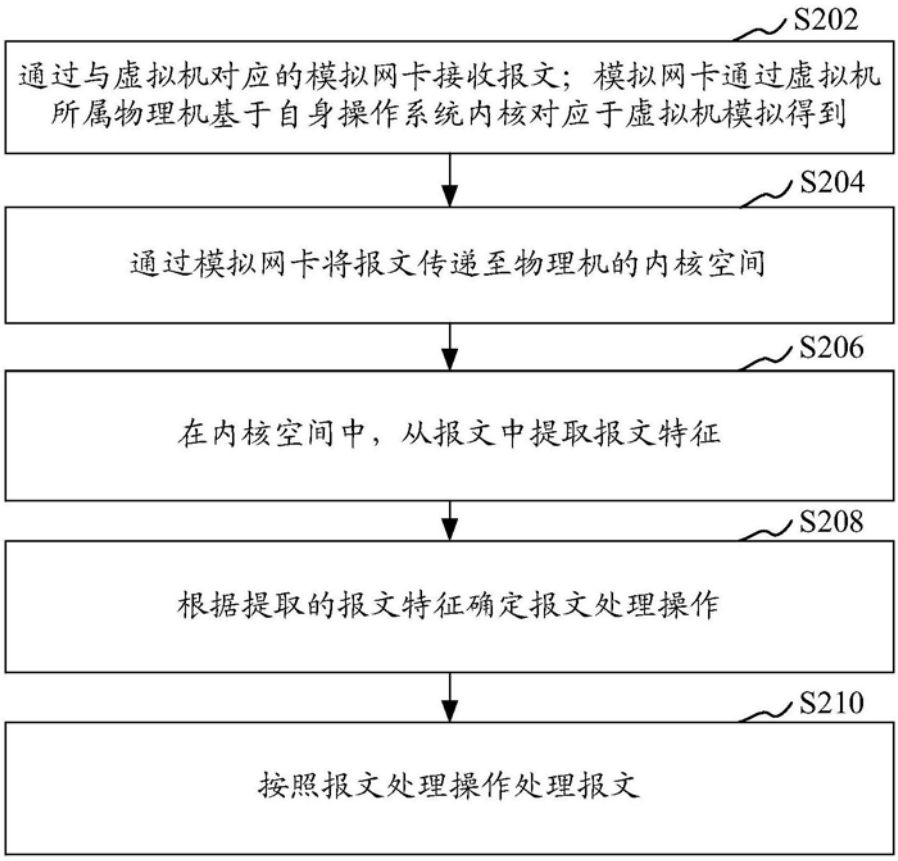

S202
通过与虚拟机对应的模拟网卡接收报文；模拟网卡通过虚拟机所属物理机基于自身操作系统内核对应于虚拟机模拟得到
S204
通过模拟网卡将报文传递至物理机的内核空间
S206
在内核空间中，从报文中提取报文特征
S208
根据提取的报文特征确定报文处理操作
S210
按照报文处理操作处理报文

图2

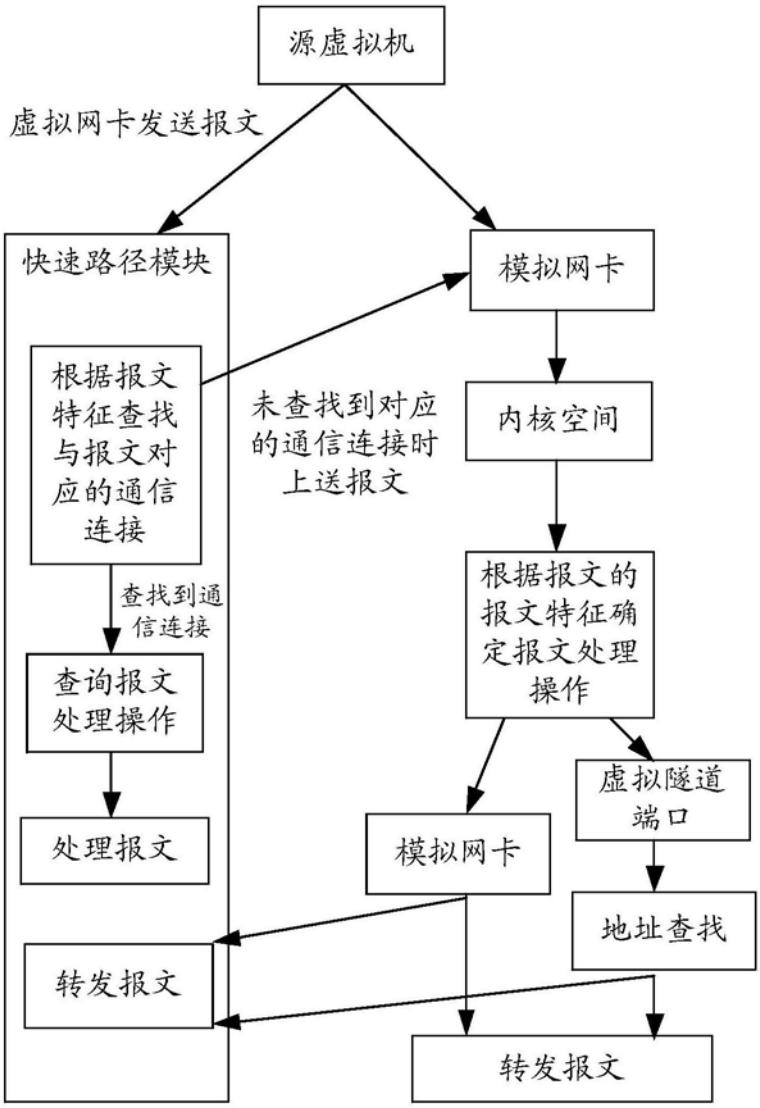

源虚拟机
虚拟网卡发送报文
快速路径模块
模拟网卡
根据报文特征查找与报文对应的通信连接
未查找到对应的通信连接时上送报文
内核空间
查找到通信连接
根据报文的报文特征确定报文处理操作
查询报文处理操作
虚拟隧道端口
处理报文
模拟网卡
地址查找
转发报文
转发报文

图3

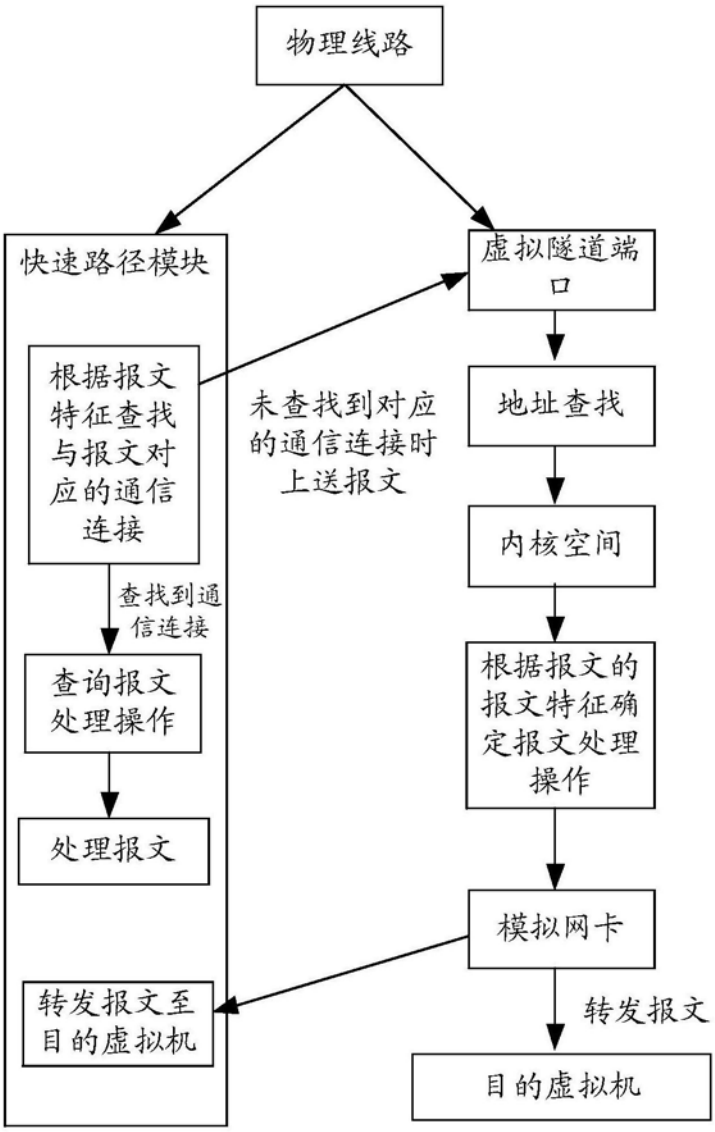

物理线路
快速路径模块
虚拟隧道端口
根据报文特征查找与报文对应的通信连接
未查找到对应的通信连接时上送报文
地址查找
内核空间
查找到通信连接
查询报文处理操作
根据报文的报文特征确定报文处理操作
处理报文
模拟网卡
转发报文至目的虚拟机
转发报文
目的虚拟机

图4

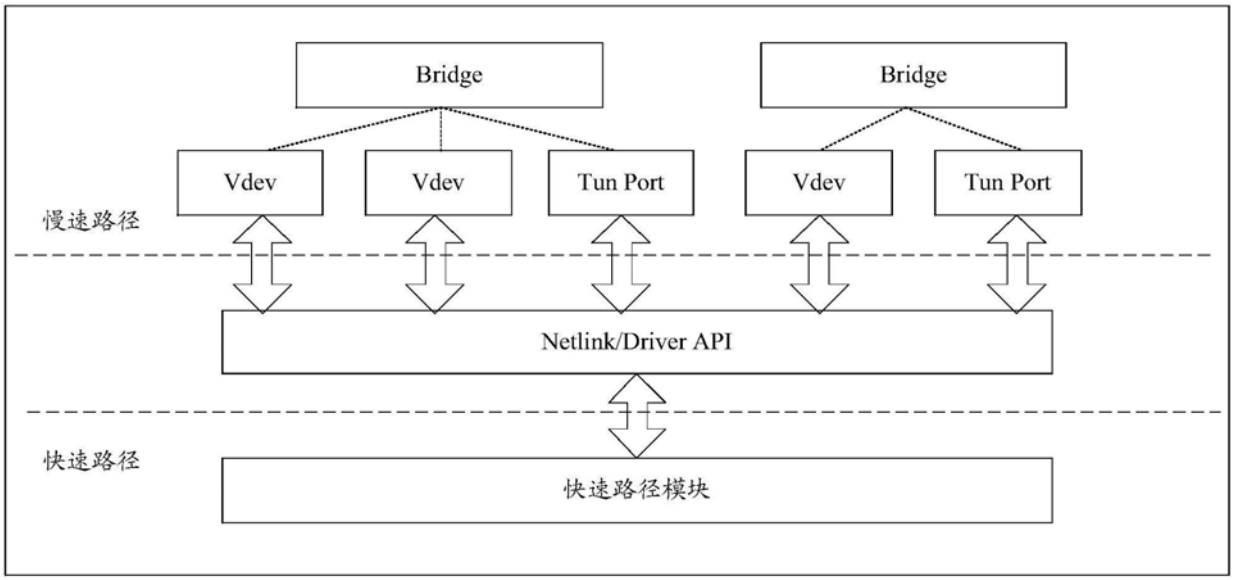

Bridge
Bridge
Vdev
Vdev
Tun Port
Vdev
Tun Port
慢速路径
Netlink/Driver API
快速路径
快速路径模块

图5

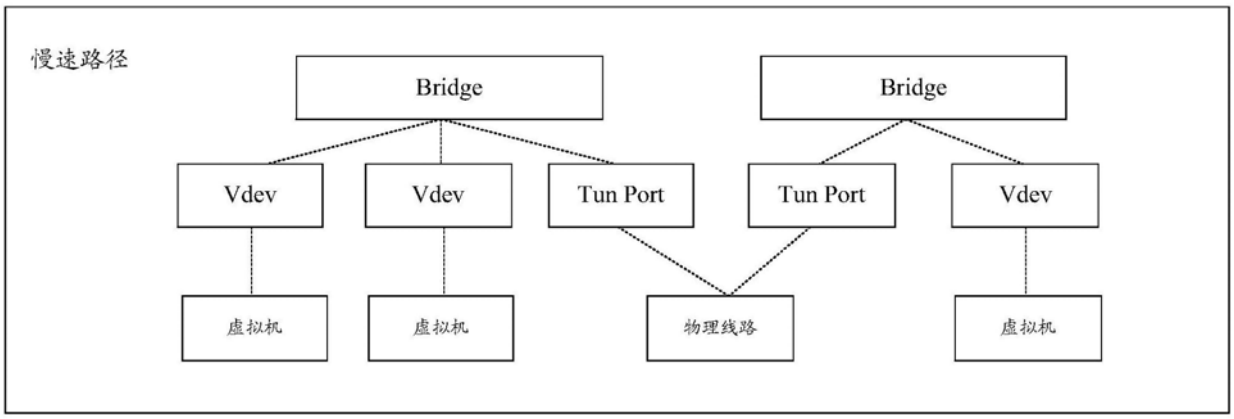

慢速路径
Bridge
Bridge
Vdev
Vdev
Tun Port
Tun Port
Vdev
虚拟机
虚拟机
物理线路
虚拟机

图6

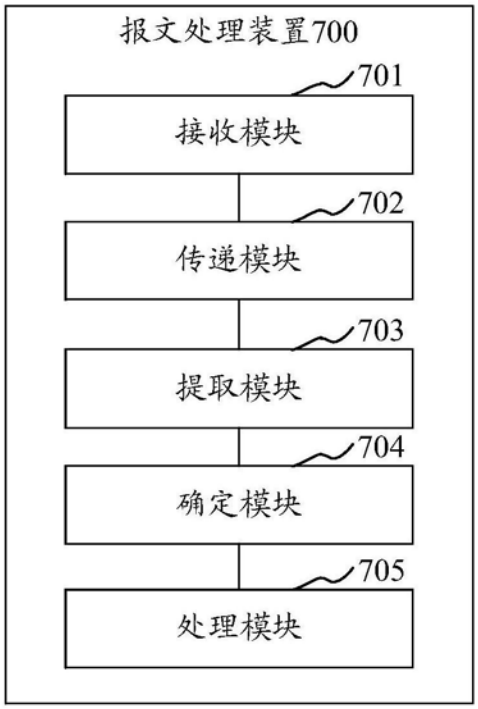

报文处理装置700
701
接收模块
702
传递模块
703
提取模块
704
确定模块
705
处理模块

图7

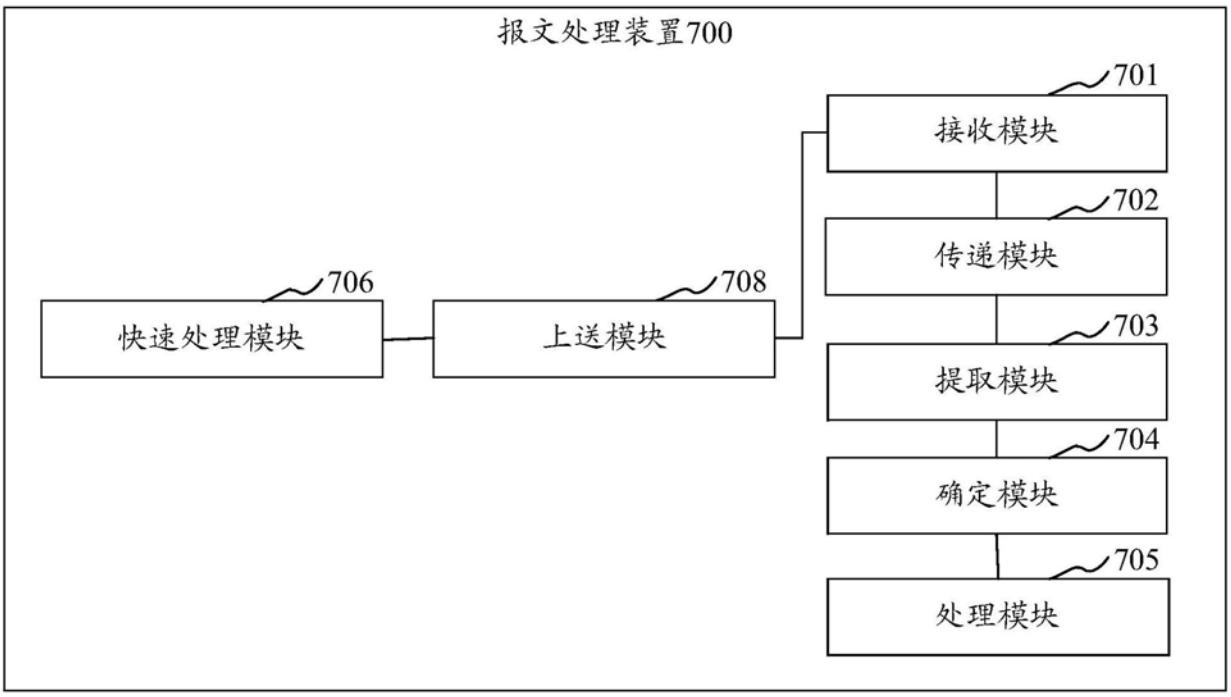

报文处理装置700
701
接收模块
702
传递模块
703
提取模块
704
确定模块
705
处理模块
706
快速处理模块
708
上送模块

图8

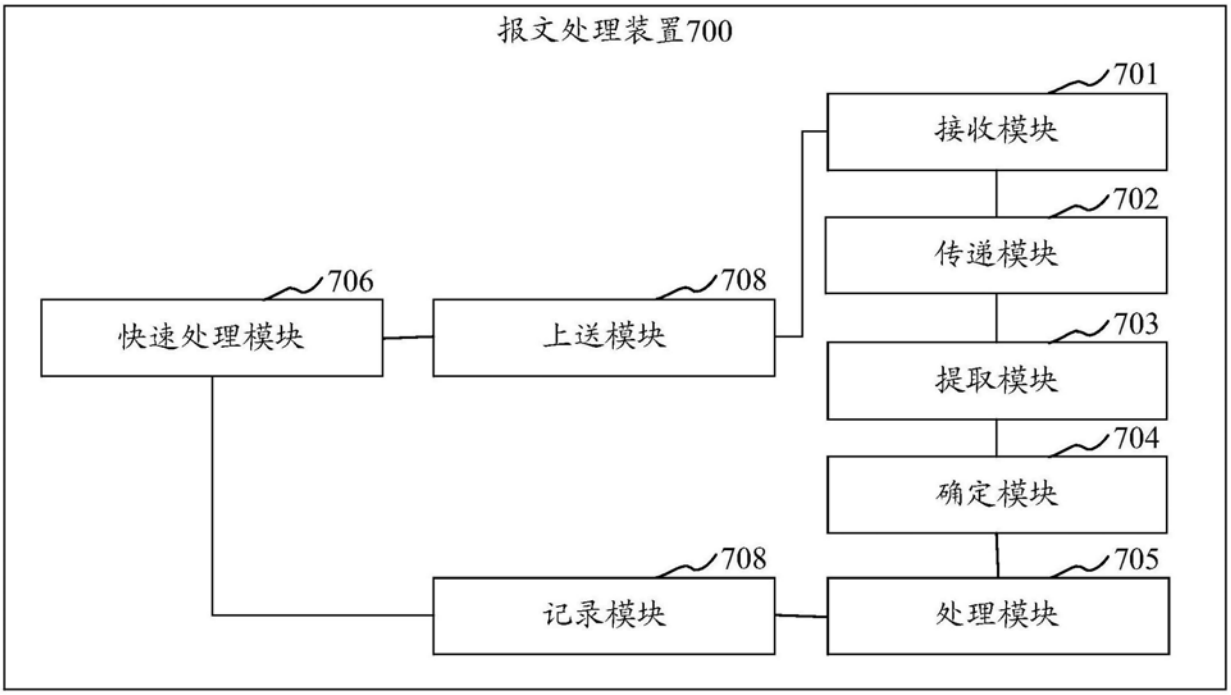

报文处理装置700
701
接收模块
702
传递模块
703
提取模块
704
确定模块
705
处理模块
706
快速处理模块
708
上送模块
708
记录模块

图9

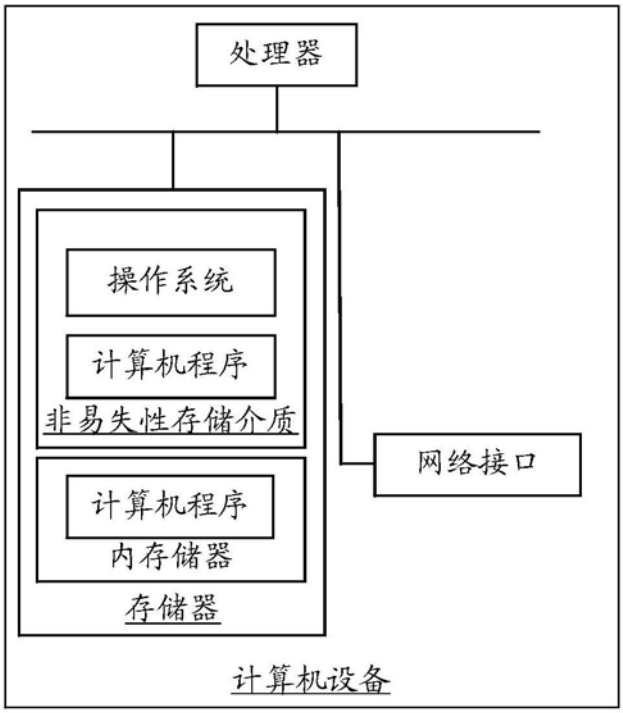

处理器
操作系统
计算机程序
非易失性存储介质
计算机程序
内存储器
存储器
网络接口
计算机设备

图10