



(12)发明专利

(10)授权公告号 CN 106385365 B

(45)授权公告日 2019.09.06

(21)申请号 201510478224.8

(22)申请日 2015.08.07

(65)同一申请的已公布的文献号

申请公布号 CN 106385365 A

(43)申请公布日 2017.02.08

(73)专利权人 新华三技术有限公司

地址 310052 浙江省杭州市滨江区长河路
466号

(72)发明人 侯叶飞

(74)专利代理机构 北京德琦知识产权代理有限公司

公司 11018

代理人 杨春香 宋志强

(51)Int.Cl.

H04L 12/741(2013.01)

(56)对比文件

CN 104283756 A, 2015.01.14,

CN 104468389 A, 2015.03.25,

CN 104823416 A, 2015.08.05,

CN 104823428 A, 2015.08.05,

审查员 金星

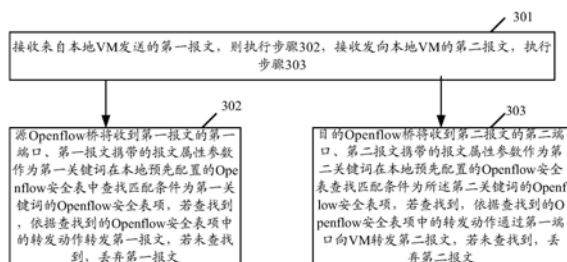
权利要求书2页 说明书9页 附图5页

(54)发明名称

基于开放流Openflow表实现云平台安全的方法和装置

(57)摘要

本申请提供了基于开放流表实现云平台安全的方法和装置。本申请中,云平台中的云服务器上创建用于代替MAC桥的Openflow桥,Openflow桥通过Openflow安全表实现云平台安全,这达到了基于Openflow表实现云平台安全的目的,提高了云平台安全的可控制性能;并且,本发明中,由于Openflow桥采用Openflow类型的流表实现云平台安全,这可以与云服务器上的其他网桥比如BR-Int、BR-Ext(也采用Openflow类型的流表)统一采用相同的流表管理,简化网络配置和管理。



1. 一种基于开放流Openflow表实现云平台安全的方法,其特征在于,该方法应用于在云平台中的云服务器上创建出的用于代替MAC桥的Openflow桥,Openflow桥连接在所述云服务器上的虚拟机VM和内部桥BR-Int之间,该方法包括:

接收来自本地VM发送的第一报文,将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在本地预先配置的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第一报文,若未查找到,丢弃第一报文;

接收发向所述VM的第二报文,将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在本地预先配置的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第二报文,若未查找到,丢弃第二报文。

2. 根据权利要求1所述的方法,其特征在于,所述依据查找到的Openflow安全表项中的转发动作转发第一报文包括:

在所述第一报文为首包时,通过本Openflow桥上第二端口向BR-Int上与所述第二端口互为一对Peer的第三端口发送第一报文;

在所述第一报文不为首包时,在本地Openflow转发表中查找与第一报文匹配的Openflow转发表项,按照查找到的Openflow转发表项中的转发动作转发第一报文。

3. 根据权利要求2所述的方法,其特征在于,在所述第一报文为首包时,该方法进一步包括:

接收云平台中控制器生成并下发的与第一报文匹配的Openflow转发表项,在本地Openflow转发表中存储接收的Openflow转发表项;

其中,当第一报文是所述VM发向目的设备的首包且目的设备为同一云服务器上的其他VM时,与第一报文匹配的Openflow转发表项为所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文 经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由所述目的设备接入的目的Openflow桥时查找到的与第一报文匹配的Openflow安全表项的组合;当第一报文是发向目的设备的首包且目的设备为物理网络上的主机或者不同云服务器上的其他VM时,与第一报文匹配的Openflow转发表项是所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由外部网桥BR-Ext时查找到的与第一报文匹配的Openflow转发表项的组合。

4. 根据权利要求3所述的方法,其特征在于,所述云服务器上的Openflow桥、BR-Int、BR-Ext通过端口类型为Patch的端口联通。

5. 根据权利要求1所述的方法,其特征在于,所述依据查找到的Openflow安全表项中的转发动作转发第二报文包括:

通过所述Openflow桥连接所述VM的第一端口向所述VM发送第二报文。

6. 一种基于开放流Openflow表实现云平台安全的装置,其特征在于,该装置应用于在云平台中云服务器上创建出的用于代替MAC桥的Openflow桥,Openflow桥连接在所述云服务器上的虚拟机VM和内部桥BR-Int之间,该装置包括:

Openflow表项存储单元,用于存储预先配置的Openflow安全表;

出流量控制单元,用于接收来自本地VM发送的第一报文,将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在所述Openflow表项存储单元存储的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第一报文,若未查找到,丢弃第一报文;

入流量控制单元,用于接收发向所述VM的第二报文,将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在所述Openflow表项存储单元存储的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第二 报文,若未查找到,丢弃第二报文。

7. 根据权利要求6所述的装置,其特征在于,所述Openflow表项存储单元进一步存储Openflow转发表;

所述出流量控制单元依据查找到的Openflow安全表项中的转发动作转发第一报文包括:

在所述第一报文为首包时,通过本Openflow桥上第二端口向BR-Int上与所述第二端口互为一对Peer的第三端口发送第一报文;

在所述第一报文不为首包时,在所述Openflow表项存储单元存储的Openflow转发表中查找与第一报文匹配的Openflow转发表项,按照查找到的Openflow转发表项中的转发动作转发第一报文。

8. 根据权利要求7所述的装置,其特征在于,在所述第一报文为首包时,所述Openflow表项存储单元进一步接收云平台中控制器生成并下发的与第一报文匹配的Openflow转发表项,将接收的Openflow转发表项存储至本地Openflow转发表中;

其中,当第一报文是所述VM发向目的设备的首包且目的设备为同一云服务器上的其他VM时,与第一报文匹配的Openflow转发表项为所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由所述目的设备接入的目的Openflow桥时查找到的与第一报文匹配的Openflow安全表项的组合;当第一报文是发向目的设备的首包且目的设备为物理网络上的主机或者不同云服务器上的其他VM时,与第一报文匹配的Openflow转发表项是所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由外部网桥BR-Ext时查找到的与第一报文匹配的Openflow转发表项的组合。

9. 根据权利要求8所述的装置,其特征在于,所述云服务器上的Openflow桥、BR-Int、BR-Ext通过端口类型为Patch的端口联通。

10. 根据权利要求6所述的装置,其特征在于,所述入流量控制单元依据查找到的Openflow安全表项中的转发动作转发第二报文包括:

通过所述Openflow桥连接所述VM的第一端口向所述VM发送第二报文。

基于开放流Openflow表实现云平台安全的方法和装置

技术领域

[0001] 本申请涉及网络通信技术,特别涉及基于开放流 (Openflow) 表实现云平台安全的方法和装置。

背景技术

[0002] 安全一直是各云平台的必选特性,在目前的开源云平台和非开源云平台中,都是通过动态学习的ip表 (iptables) 和二层MAC转发表实现云平台安全的。

[0003] 以开源云平台Openstack为例,非开源云平台原理类似。图1示出了开源云平台Openstack中任一云服务器从逻辑上抽象出的结构图。Linux内核的原生桥 (qbr网桥,也称为MAC桥) 如图1所示的MAC bridge_1、MAC bridge_2、MAC bridge_3是通过动态学习的iptables和二层MAC转发表实现开源云平台Openstack安全,具体为:以如图1所示的虚拟机 (VM:Virtual Machine) 1发送报文至VM2为例,VM1通过本地接口eth0发送报文,MAC桥通过VM1的虚拟网卡 (Veth:Virtual ethernet) 在MAC桥的端口Veth1接收到来自VM1发送的报文,依赖于之前动态学习的iptables对报文进行过滤识别,依赖于动态学习的二层MAC转发表继续转发通过过滤的报文

[0004] 可以看出,目前云平台中云服务器上的MAC桥在实现开源云平台Openstack安全时是基于iptables和二层MAC转发表实现,而iptables和二层MAC转发表,其可控制性比较差,远远不如Openflow表。并且,目前云平台中云服务器上的其他网桥比如内部桥 (BR-Int)、外部桥 ((BR-Ext) 内的表项都是Openflow表,因此,同一云服务器上MAC桥上的iptables和二层MAC转发表会和其他网桥上的Openflow表不统一。

发明内容

[0005] 本申请提供了基于开放流表实现云平台安全的方法和装置,以基于Openflow表实现云平台安全。

[0006] 本申请提供的技术方案包括:

[0007] 一种基于开放流Openflow表实现云平台安全的方法,该方法应用于在云平台中的云服务器上创建出的用于代替MAC桥的Openflow桥,Openflow桥连接在所述云服务器上的虚拟机VM和内部桥BR-Int之间,该方法包括:

[0008] 接收来自本地VM发送的第一报文,将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在本地预先配置的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第一报文,若未查找到,丢弃第一报文;

[0009] 接收发向所述VM的第二报文,将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在本地预先配置的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第二报文,若未查找到,丢弃第二报文。

[0010] 一种基于开放流Openflow表实现云平台安全的装置,该装置应用于在云平台中云服务器上创建出的用于代替MAC桥的Openflow桥,Openflow桥连接在所述云服务器上的虚拟机VM和内部桥BR-Int之间,该装置包括:

[0011] Openflow表项存储单元,用于存储预先配置的Openflow安全表;

[0012] 出流量控制单元,用于接收来自本地VM发送的第一报文,将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在所述Openflow表项存储单元存储的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第一报文,若未查找到,丢弃第一报文;

[0013] 入流量控制单元,用于接收发向所述VM的第二报文,将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在所述Openflow表项存储单元存储的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第二报文,若未查找到,丢弃第二报文。

[0014] 由以上技术方案可以看出,本发明中,在云平台中的云服务器上创建用于代替MAC桥的Openflow桥,Openflow桥通过Openflow安全表实现云平台安全,这达到了基于Openflow表实现云平台安全的目的,提高了云平台安全的可控制性能;

[0015] 进一步地,本发明中,由于云服务器上Openflow桥采用Openflow类型的流表即Openflow安全表实现云平台安全,这可以实现同一云服务器上的Openflow桥和其他网桥比如BR-Int、BR-Ext(也采用Openflow类型的流表)统一采用相同的流表管理,简化网络配置和管理。

附图说明

[0016] 图1示出了开源云平台Openstack中任一云服务器的抽象结构图;

[0017] 图2为本发明提供的云平台中任一云服务器的抽象结构图;

[0018] 图3为本发明提供的方法流程图;

[0019] 图4为本发明实施例1提供的结构示意图;

[0020] 图5为本发明实施例2提供的结构示意图;

[0021] 图6为本发明提供的装置结构图;

[0022] 图7为本发明提供的装置硬件结构图。

具体实施方式

[0023] 为了使本发明的目的、技术方案和优点更加清楚,下面结合附图和具体实施例对本发明进行详细描述。

[0024] 本发明中,为实现基于Openflow表实现云平台安全,在云平台中的云服务器上创建Openflow桥,由Openflow桥替换如背景技术描述的MAC桥来实现云平台安全,图2示出了本发明提供的云平台中任一云服务器从逻辑上抽象出的结构图。如图2所示,Openflow桥的位置与背景技术描述的MAC桥的位置相同,具体是连接在VM和BR-Int之间,但相比于MAC桥通过动态学习的iptables和二层MAC转发表实现云平台安全,本发明中,Openflow桥是基于预先配置的Openflow安全表实现云平台安全。

[0025] 本发明中,Openflow安全表包含多条Openflow安全表项,每一Openflow安全表项

包含以下两部分：匹配条件，转发动作；

[0026] 作为本发明的一个实施例，这里的匹配条件可包含报文接收端口、报文携带的报文属性参数。优选地，本发明中，报文携带的报文属性参数可为报文五元组或者七元组中的至少一个。其中，报文五元组为：目的IP地址、源IP地址、目的端口号、源端口号、协议类型；报文七元组为：目的IP地址、源IP地址、目的MAC地址、源MAC地址、目的端口号、源端口号、协议类型。

[0027] 作为本发明的一个实施例，转发动作可为对匹配Openflow安全表项的报文执行的转发动作，下文具体描述了如何依据Openflow安全表项中的转发动作转发报文，这里暂不赘述。

[0028] 基于上面描述，下面对Openflow桥如何基于预先配置的Openflow安全表实现云平台安全进行描述：

[0029] 参见图3，图3为本发明提供的方法流程图。该流程应用于如上所述的Openflow桥，如图3所示，该流程可包括以下步骤：

[0030] 步骤301，接收来自本地VM发送的第一报文，则执行步骤302，接收发向本地VM的第二报文，执行步骤303。

[0031] 需要说明的是，这里的第一报文、第二报文只是为便于区分VM发送的报文和发向VM的报文，并非限定本发明。

[0032] 这里，为便于描述，当Openflow桥接收来自本地VM发送的第一报文，则称Openflow桥为源Openflow桥，而当Openflow桥接收发向本地VM的第二报文，则称Openflow桥为目的Openflow桥。以下均以Openflow桥细分源Openflow桥和目的Openflow桥描述。

[0033] 步骤302，源Openflow桥将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在本地预先配置的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项，若查找到，依据查找到的Openflow安全表项中的转发动作转发第一报文，若未查找到，丢弃第一报文。

[0034] 步骤303，目的Openflow桥将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在本地预先配置的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项，若查找到，依据查找到的Openflow安全表项中的转发动作通过第一端口向VM转发第二报文，若未查找到，丢弃第二报文。

[0035] 作为一个优选实施例，本步骤303中，依据查找到的Openflow安全表项中的转发动作转发第二报文包括：通过本Openflow桥连接VM的第一端口向VM发送第二报文。

[0036] 至此，完成图3所示的流程。

[0037] 作为本发明的一个实施例，上述步骤302中，源Openflow桥依据查找到的Openflow安全表项中的转发动作转发第一报文包括：

[0038] 步骤a1，源Openflow桥在第一报文为首包时，执行步骤a2，源Openflow桥在第一报文不为首包时，执行步骤a3。

[0039] 这里，第一报文是否为首包的确定方式类似现有确定首包的方式，不再展开描述。

[0040] 步骤a2，源Openflow桥通过本Openflow桥上第二端口向BR-Int上与所述第二端口互为一对Peer的第三端口转发第一报文。结束当前流程。

[0041] 本步骤a2是在第一报文为首包的前提下执行的。

[0042] 本发明中,在第一报文为首包时,当源Openflow桥通过本Openflow桥上第二端口向BR-Int上与第二端口互为一对(Peer)的第三端口发送第一报文后,第一报文会到达BR-Int上的第三端口。当BR-Int通过第三端口收到第一报文后,会在本地Openflow转发表中查找找到与第一报文匹配的Openflow转发表项(记为表项1),按照查找到的表项1中的转发动作继续转发第一报文。

[0043] 当第一报文的目的是设备是同一云服务器上其他VM时,上述BR-Int查找到的表项1中的转发动作就是通过本BR-Int上第四端口发送第一报文至接入目的设备的Openflow桥(即为目的Openflow桥)上与第四端口互为Peer的第五端口,基于此,BR-Int就会通过本BR-Int上第四端口向目的Openflow桥上与第四端口互为Peer的第五端口发送第一报文。当目的Openflow桥通过第五端口收到第一报文时,因为第一报文是发向本地VM的,则目的Openflow桥就会按照类似步骤303的描述,依据收到第一报文的第五端口、第一报文携带的报文属性参数在本地预先配置的Openflow安全表查找匹配的Openflow安全表项(记为表项2),若查找到,依据查找到的表项2中的转发动作通过连接目的设备的出端口发送第一报文至目的设备,最终,第一报文会到达目的设备,若未查找到,丢弃第一报文。

[0044] 当第一报文的目的是设备是物理网络上的主机或者不同云服务器上其他VM时,BR-Int查找到的表项1中的转发动作就是通过本BR-Int上第六端口发送第一报文至BR-Ext上与第六端口互为Peer的第七端口,基于此,BR-Int就会通过本BR-Int上第六端口向BR-Ext上与第六端口互为Peer的第七端口发送第一报文。当BR-Ext收到第一报文后,会在本地Openflow转发表中查找找到与第一报文匹配的Openflow转发表项(记为表项3),依据查找到的表项3中的转发动作继续转发第一报文。这里,查找到的表项3中的转发动作可为对第一报文进行VXLAN封装,并通过BR-Ext上物理端口(到达目的设备的路由出端口)转发VXLAN封装后的第一报文,最终,第一报文会到达目的设备。

[0045] 基于上面描述的第一报文为发向目的设备的首包且目的设备为同一云服务器上其他VM时第一报文在源Openflow桥、BR-Int、目的Openflow桥的转发,或者第一报文为发向目的设备的首包且目的设备为物理网络上的主机或者不同云服务器上的其他VM时第一报文在源Openflow桥、BR-Int、BR-Ext的转发描述,本发明中,云平台上的控制器比如SDN控制器还可进一步动态生成用于转发第一报文的Openflow转发表项(记为表项4)并下发至源Openflow桥进行存储。

[0046] 在本发明中,当第一报文是发向目的设备的首包且目的设备为同一云服务器上其他VM时,表项4就是按照无重复原则对第一报文经由源Openflow桥、BR-Int、目的Openflow桥时查找到的与第一报文匹配的Openflow表项进行组合形成的表项;举例描述,当第一报文是发向目的设备的首包且目的设备为同一云服务器上其他VM时,基于上面描述的第一报文在源Openflow桥、BR-Int、目的Openflow桥的转发,则表项4的匹配条件就是第一报文经由源Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的匹配条件、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项中的匹配条件、第一报文经由目的Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的匹配条件的组合(注意,最终组合的匹配条件需保证没有重复的内容),表项4的转发动作就是第一报文经由源Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的转发动作、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项中的转发动作、第一报文经由目的

Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的转发动作的组合(注意,最终组合的转发动作中可省略掉中间环节的转发操作,即仅保留上面描述的表项2中的转发操作)。

[0047] 而当第一报文是发向目的设备的首包且目的设备为物理网络上的主机或者不同云服务器上的其他VM时,表项4就是按照无重复原则对第一报文经由的源Openflow桥、BR-Int、BR-Ext时查找到的与第一报文匹配的Openflow表项进行组合形成的表项。举例描述,当第一报文是发向目的设备的首包且目的设备为物理网络上的主机或者不同网络节点上的其他VM时,基于上面描述的第一报在源Openflow桥、BR-Int、BR-Ext的转发,则表项4的匹配条件就是第一报文经由源Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的匹配条件、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项中的匹配条件、第一报文经由BR-Ext时与第一报文匹配的Openflow转发表项中的匹配条件的组合(注意,最终组合的匹配条件需保证没有重复的内容),表项4的转发动作就是第一报文经由源Openflow桥时查找到的与第一报文匹配的Openflow安全表项中的转发动作、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项中的转发动作、第一报文经由BR-Ext时与第一报文匹配的Openflow转发表项中的转发动作的组合(注意,最终组合的转发动作中可省略掉中间环节的转发操作,但其他非转发操作比如VXLAN封装等不需要省略)。

[0048] 基于上面描述的表项4可以看出,在第一报文为发向目的设备的首包时,不管目的设备为同一云服务器上其他VM,还是为物理网络上的主机或者不同云服务器上的其他VM,表项4最终汇聚了第一报文经由云服务器上各个网桥时查找到的匹配的Openflow表项,这能够保证后续发向目的设备的非首包直接在源Openflow桥执行一次Openflow转发表项查找,不必再在云服务器中的其他各个网桥查找Openflow表项就能转发至目的设备,提高报文转发效率,具体见步骤a3。

[0049] 步骤a3,源Openflow桥在本地Openflow转发表中查找与第一报文匹配的Openflow转发表项(也即上述的表项4),按照查找到的Openflow转发表项中的转发动作转发第一报文。结束当前流程。

[0050] 本步骤a3是在第一报文为非首包的前提下执行的。

[0051] 基于上面描述的表项4可以看出,表项4汇聚了发向目的设备的首包经由云服务器中各个网桥时查找到的与首包匹配的Openflow表项,基于此,当第一报文为发向目的设备的非首包时,本步骤a3中源Openflow桥在本地Openflow转发表中查找到的与第一报文匹配的Openflow转发表项也即为上述的表项4,因为表项4汇聚了发向目的设备的首包经由云服务器中各个网桥时查找到的与首包匹配的Openflow表项,基于此,本步骤a3中按照查找到的Openflow转发表项中的转发动作转发第一报文,也就意味着第一报文直接穿越云服务器中各个网桥进行转发,实现了只需在源Openflow桥执行一次Openflow转发表,不必再在云服务器中其他各个网桥查找Openflow表项就能转发至第一报文至目的设备,提高报文转发效率。

[0052] 举例描述,以报文a3为发向目的设备(同一云服务器中其他VM)的非首包为例,当源Openflow桥收到报文a3时,发现报文a3为发向目的设备的非首包,则在本地Openflow转发表中查找到与报文a3匹配的Openflow转发表项,按照查找到的Openflow转发表项中的转

发动作转发报文a3。这里与报文a3匹配的Openflow转发表项是对发向目的设备的首包经由源Openflow桥、BR-Int、目的Openflow桥时查找到的匹配的Openflow表项的叠加,如此,按照查找到的Openflow转发表项中的转发动作转发报文a3最终是穿越源Openflow桥、BR-Int、目的Openflow桥将报文a3发向目的Openflow桥上连接目的设备的端口,直接通过该端口转发即可,无需再在BR-Int、目的Openflow桥上查找Openflow表项转发。

[0053] 本发明中,为了保证步骤a1至步骤a3顺利实现,可限定同一云服务器中的各个网桥之间通过端口类型为Patch的端口联通,具体为:源Openflow桥上第二端口、BR-Int上与第二端口互为Peer的第三端口、BR-Int上第四端口、目的Openflow桥上与第四端口互为Peer的第五端口、BR-Int上第六端口、BR-Ext上与第六端口互为Peer的第七端口的端口类型都为Patch。端口类型为Patch,能够保证首包在穿越类型为patch的端口联通的各个Openflow类型的网桥(实质是具有Openflow表项的网桥,即Openflow桥、BR-Int、BR-Ext等)时,会自动组合所有Openflow类型的网桥的Openflow表项,最终生成一条Openflow转发表项(如上述步骤a2中当第一报文为首包时生成的表项4)指导后续非首包的流量转发。

[0054] 以上对步骤202进行了描述。

[0055] 下面通过两个具体实施例对图2所示流程进行描述:

[0056] 实施例1:

[0057] 图4为实施例1的应用组网示意图。图4的应用组网仅以云平台的其中一个服务器的网络为例。如图4所示,VM_11通过本地端口eth_11连接Openflow桥_11上的虚拟网卡Veth_11,VM_12通过本地端口eth_12连接至Openflow桥_12的虚拟网卡Veth_12,依次类推,VM_1n通过本地端口eth_1n连接至Openflow桥_1n的虚拟网卡Veth_1n。在图4中,Openflow桥_11通过端口Patch_VM_11连接至BR-Int的端口Patch_Int_11,Openflow桥_12通过端口Patch_VM_12连接至BR-Int的端口Patch_Int_12,依次类推,Openflow桥_1n通过端口Patch_VM_1n连接至BR-Int的端口Patch_Int_1n,其中,Openflow桥_11上的端口Patch_VM_11与BR-Int上的端口Patch_Int_11互为一对Peer,端口类型为Patch,Openflow桥_12上的端口Patch_VM_12与BR-Int上的端口Patch_Int_12互为一对Peer,端口类型为Patch,依次类推,Openflow桥_1n上的端口Patch_VM_1n与BR-Int上的端口Patch_Int_1n互为一对Peer,端口类型为Patch。在图4中,BR-Int通过端口Patch_40连接至BR-Ext上的端口Patch_41,Patch_40、Patch_41的端口类型为Patch。在图4中的VM_11直至VM_1n、Openflow桥_11直至Openflow桥_1n、BR-Int、BR-Ext处于同一网络节点。

[0058] 在本实施例1中,以VM_11访问VM_12为例,则,

[0059] VM_11通过eth_11发送用于访问VM_12的报文,为便于描述,这里将报文记为报文01;

[0060] Openflow桥_11通过Veth_11收到报文01,发现报文01为本Openflow桥_11首次收到的VM_11访问VM_12的报文(即为首包),则以Veth_11、以及报文01携带的报文属性参数作为关键词在本地预先配置的Openflow安全表中查找匹配条件为该关键词的Openflow安全表项;

[0061] 假如Openflow桥_11未查找到Openflow安全表项,则Openflow桥_11直接丢弃报文01;

[0062] 假如Openflow桥_11查找到Openflow安全表项(将该查找到的Openflow安全表项

记为表项41),则按照表项41中的处理动作继续将报文01通过本Openflow桥_11的端口Patch_VM_11发送出去。

[0063] BR-Int通过Patch_Int_11收到报文01时,在本地的Openflow转发表中查找到与报文01匹配的Openflow转发表项(将该查找到的Openflow转发表项记为表项42),按照表项42中的转发动作将报文01通过端口Patch_Int_12转发。

[0064] Openflow桥_12通过Patch_VM_12接收到报文01,发现报文01是发向VM_12的,则以Patch_VM_12、报文01携带的报文属性参数作为关键词在本地预先配置的Openflow安全表中查找到匹配条件为该关键词的Openflow安全表项,如果查找到,这里将该查找到的Openflow安全表项记为表项43,则按照表项43中的转发动作通过本Openflow桥_12的端口Veth_12发送报文01。最终,VM_11发送的报文01会到达VM_12,即实现了VM_11访问VM_12。

[0065] 云平台上的SDN控制器在报文01从Openflow桥_11、BR-Int、Openflow桥_12三者的转发过程中,进一步将报文01经由Openflow桥_11时查找到的表项41、报文01经由BR-Int时查找到的表项42、以及报文01经由Openflow桥_12时查找到的表项43进行叠加生成一个与报文01匹配的Openflow转发表项(记为表项40)下发至Openflow桥_11的Openflow转发表。该表项40中的匹配条件为表项41至表项43中匹配条件的无重复叠加,该表项40中的转发动作为表项41至表项43中转发动作的无重复叠加,这里以转发动作为通过Openflow桥_12的端口Veth_12转发为例。

[0066] 之后,VM_11再次访问VM_12时,VM_11通过eth_11发送用于访问VM_12的报文,为便于描述,这里将报文记为报文02。

[0067] Openflow桥_11通过Veth_11收到报文02,发现报文02不为本Openflow桥_11首次收到的VM_11访问VM_12的报文(即为非首包),则在本地Openflow转发表中查找与报文02匹配的Openflow转发表项(即上述SDN控制器生成的表项40)。

[0068] Openflow桥_11按照查找到的表项40中的转发动作将报文01透传至Openflow桥_12的Veth_12,触使Openflow桥_12通过Veth_12转发报文02,最终,VM_11发送的报文02会到达VM_12,即实现了VM_11再次访问VM_12。

[0069] 以上对实施例1进行了描述。

[0070] 实施例2:

[0071] 图5为实施例2的应用组网示意图。图5的应用组网仅以云平台的其中一个服务器的网络为例。如图5所示,VM_21通过本地端口eth_21连接至Openflow桥_21的虚拟网卡Veth_21,VM_22通过本地端口eth_22连接至Openflow桥_22的虚拟网卡Veth_22,依次类推,VM_2n通过本地端口eth_2n连接至Openflow桥_2n的虚拟网卡Veth_2n。在图5中,Openflow桥_21通过端口Patch_VM_21连接至BR-Int的端口Patch_Int_21,Openflow桥_22通过端口Patch_VM_22连接至BR-Int的端口Patch_Int_22,依次类推,Openflow桥_2n通过端口Patch_VM_2n连接至BR-Int的端口Patch_Int_2n,其中,Openflow桥_21上的端口Patch_VM_21与BR-Int上的端口Patch_Int_21互为对Peer,端口类型为Patch,Openflow桥_22上的端口Patch_VM_22与BR-Int上的端口Patch_Int_22互为对Peer,端口类型为Patch,依次类推,Openflow桥_2n上的端口Patch_VM_2n与BR-Int上的端口Patch_Int_2n互为对Peer,端口类型为Patch。在图5中,BR-Int通过端口Patch_50连接至BR-Ext上的端口Patch_51,Patch_50、Patch_51的端口类型为Patch。在图5中的VM_21直至VM_2n、Openflow桥_21直

至Openflow桥_2n、BR-Int、BR-Ext处于同一网络节点。

[0072] 在本实施例2中,以VM_21访问物理网络主机PM_21为例,则,

[0073] VM_21通过eth_21发送用于访问PM_21的报文,为便于描述,这里将报文记为报文21。

[0074] Openflow桥_21通过Veth_21收到报文21,发现报文21为本Openflow桥_11首次收到的VM_11访问PM_21的报文(即为首包),则以Veth_21、以及报文21携带的报文属性参数作为关键词在本地预先配置的Openflow安全表中查找匹配条件为该关键词的Openflow安全表项;

[0075] 假如Openflow桥_21未查找到Openflow安全表项,则Openflow桥_21直接丢弃报文21;

[0076] 假如Openflow桥_21查找到Openflow安全表项(将该查找到的Openflow安全表项记为表项51),则按照表项51中的处理动作继续将报文21通过本Openflow桥_21的端口Patch_VM_21发送出去。

[0077] BR-Int通过Patch_Int_21收到报文21时,在本地的Openflow转发表中查找到与报文21匹配的Openflow转发表项(将该查找到的Openflow转发表项记为表项52),按照表项52中的转发动作将报文21通过端口Patch_50转发。

[0078] BR-Ext通过Patch_51接收到报文21,在本地的Openflow转发表中查找到与报文21匹配的Openflow转发表项(这里将该查找到的Openflow安全表项记为表项53),按照查找到的表项53中转发动作中的封装操作将报文21进行VXLAN封装并按照查找到的表项53中转发动作中的转发操作通过物理端口Port_21转发出去。最终,VM_21发送的报文21会到达VM_21,即实现了VM_21访问PM_21。

[0079] 云平台上的SDN控制器在报文21从Openflow桥_21、BR-Int、BR-Ext三者的转发过程中,进一步将报文21经由Openflow桥_21时查找到的表项51、报文21经由BR-Int时查找到的表项52、以及报文01经由BR-Ext时查找到的表项53进行叠加生成一个与报文21匹配的Openflow转发表项(记为表项50)下发至Openflow桥_21的Openflow转发表。该表项50中的匹配条件为表项51至表项53中匹配条件的无重复叠加,该表项50中的转发动作为表项51至表项53中转发动作的无重复叠加,这里以转发动作为进行VXLAN封装并通过物理端口Port_21转发为例。

[0080] 之后,VM_21再次访问PM_21时,VM_21通过eth_21发送用于访问PM_21的报文,为便于描述,这里将报文记为报文22。

[0081] Openflow桥_21通过Veth_21收到报文22,发现报文22不为本Openflow桥_21首次收到的VM_21访问PM_22的报文(即为非首包),则在本地Openflow转发表中查找与报文22匹配的Openflow转发表项(即上述SDN控制器生成的表项50)。

[0082] Openflow桥_21按照查找到的表项50中的转发动作将报文21进行VXLAN封装并透传至BR-Ext的物理端口Port_21,触使BR-Ext通过物理端口Port_21转发VXLAN封装后的报文22,最终,VM_21再次发送的报文22会到达VM_21,即实现了VM_21再次访问PM_21。

[0083] 以上对实施例2进行了描述。

[0084] 至此,完成本发明提供的方法描述。下面对本发明提供的装置进行描述:

[0085] 参见图6,图6为本发明提供的装置结构图。该装置应用于在云平台中云服务器上

创建出的用于代替MAC桥的Openflow桥,Openflow桥连接在云服务器上的VM和BR-Int之间,该装置包括:

[0086] Openflow表项存储单元,用于存储预先配置的Openflow安全表;

[0087] 出流量控制单元,用于接收来自本地VM发送的第一报文,将收到第一报文的第一端口、第一报文携带的报文属性参数作为第一关键词在所述Openflow表项存储单元存储的Openflow安全表中查找匹配条件为第一关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第一报文,若未查找到,丢弃第一报文;

[0088] 入流量控制单元,用于接收发向所述VM的第二报文,将收到第二报文的第二端口、第二报文携带的报文属性参数作为第二关键词在所述Openflow表项存储单元存储的Openflow安全表查找匹配条件为所述第二关键词的Openflow安全表项,若查找到,依据查找到的Openflow安全表项中的转发动作转发第二报文,若未查找到,丢弃第二报文。

[0089] 优选地,Openflow表项存储单元进一步存储Openflow转发表;

[0090] 基于此,所述出流量控制单元依据查找到的Openflow安全表项中的转发动作转发第一报文包括:

[0091] 在所述第一报文为首包时,通过本Openflow桥上第二端口向BR-Int上与所述第二端口互为对Peer的第三端口发送第一报文;

[0092] 在所述第一报文不为首包时,在所述Openflow表项存储单元存储的Openflow转发表中查找与第一报文匹配的Openflow转发表项,按照查找到的Openflow转发表项中的转发动作转发第一报文。

[0093] 优选地,在所述第一报文为首包时,所述Openflow表项存储单元进一步接收云平台中控制器生成并下发的与第一报文匹配的Openflow转发表项,将接收的Openflow转发表项存储至本地Openflow转发表中;

[0094] 其中,当第一报文是所述VM发向目的设备的首包且目的设备为同一云服务器上的其他VM时,与第一报文匹配的Openflow转发表项为所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由所述目的设备接入的目的Openflow桥时查找到的与第一报文匹配的Openflow安全表项的组合;当第一报文是发向目的设备的首包且目的设备为物理网络上的主机或者不同云服务器上的其他VM时,与第一报文匹配的Openflow转发表项是所述第一报文经由本Openflow桥时查找到的与第一报文匹配的Openflow安全表项、第一报文经由BR-Int时查找到的与第一报文匹配的Openflow转发表项、第一报文经由外部网桥BR-Ext时查找到的与第一报文匹配的Openflow转发表项的组合。

[0095] 优选地,云服务器上的Openflow桥、BR-Int、BR-Ext通过端口类型为Patch的端口联通。

[0096] 优选地,所述入流量控制单元依据查找到的Openflow安全表项中的转发动作转发第二报文包括:

[0097] 通过所述Openflow桥连接所述VM的第一端口向所述VM发送第二报文。

[0098] 至此,完成图6所示的装置结构描述。

[0099] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明保护的范围之内。

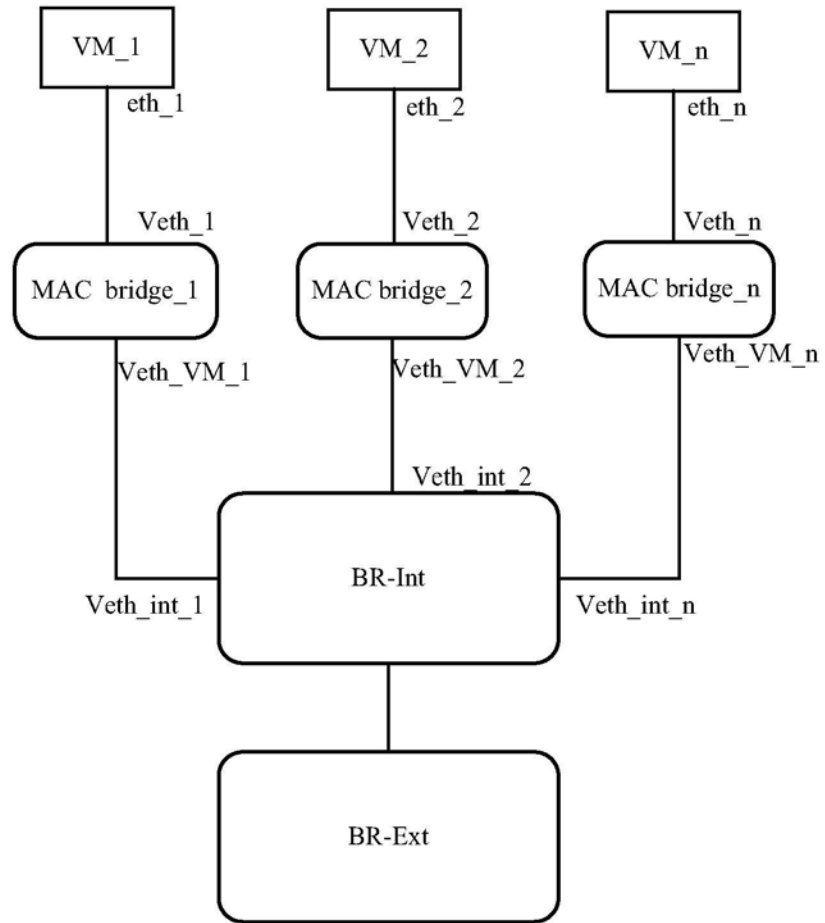


图1

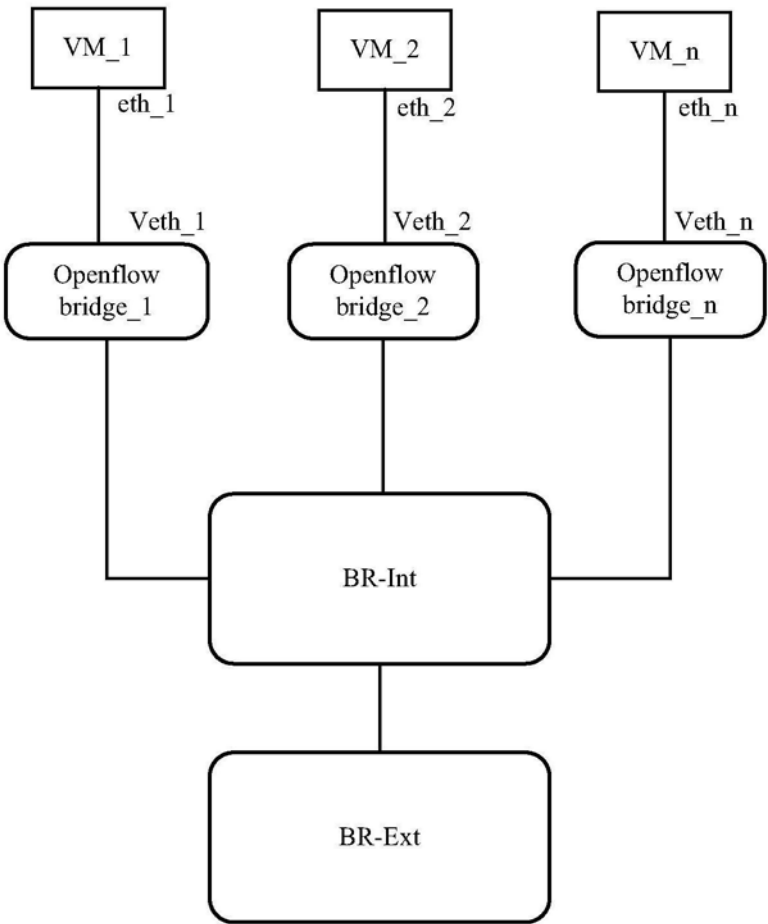


图2

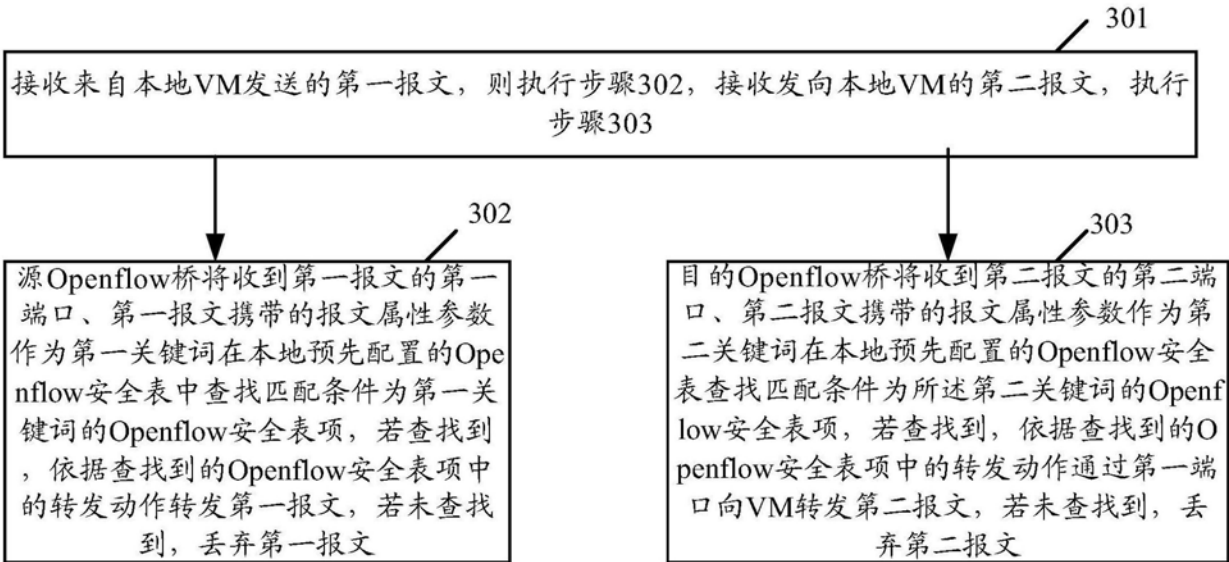


图3

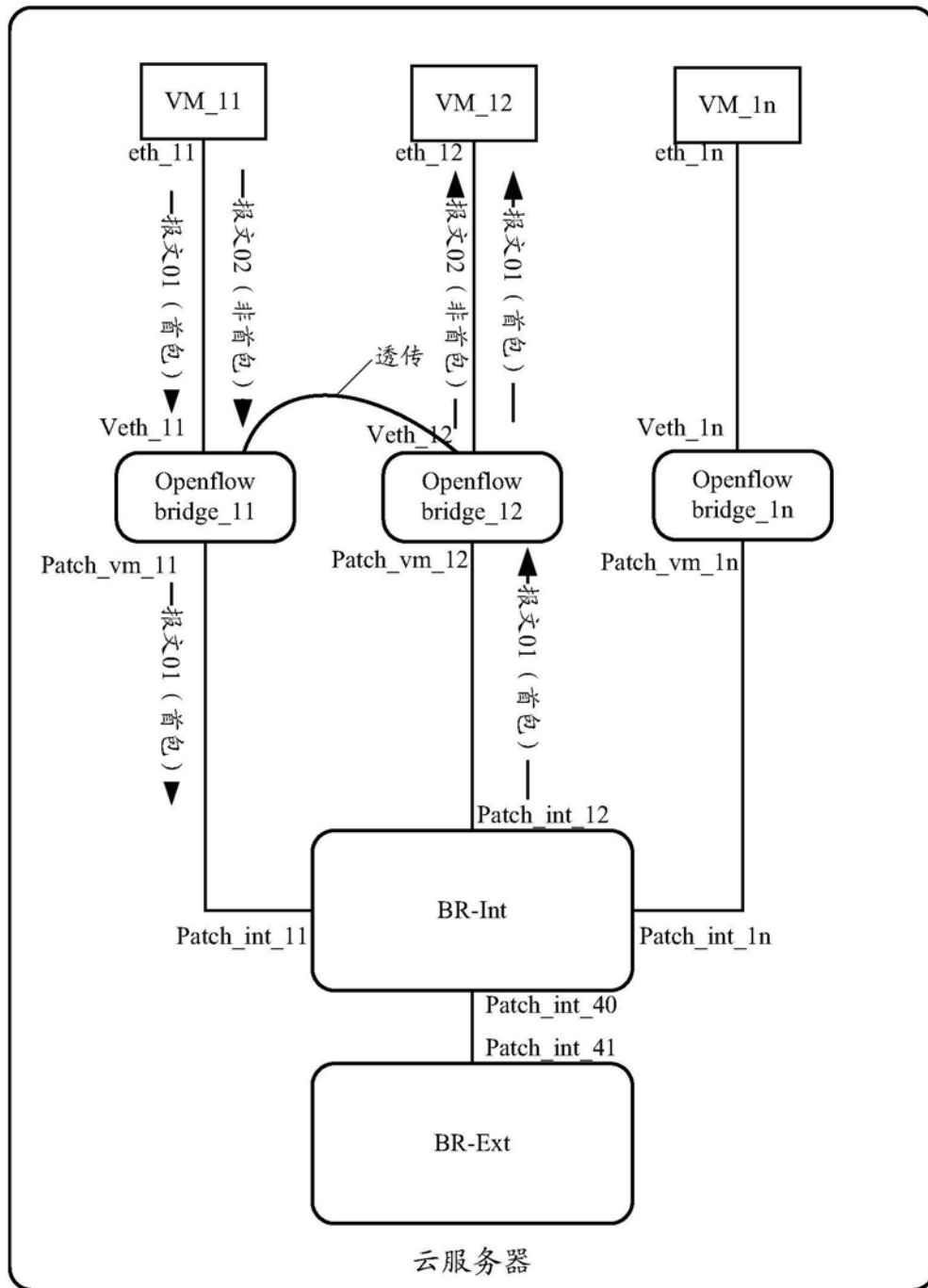


图4

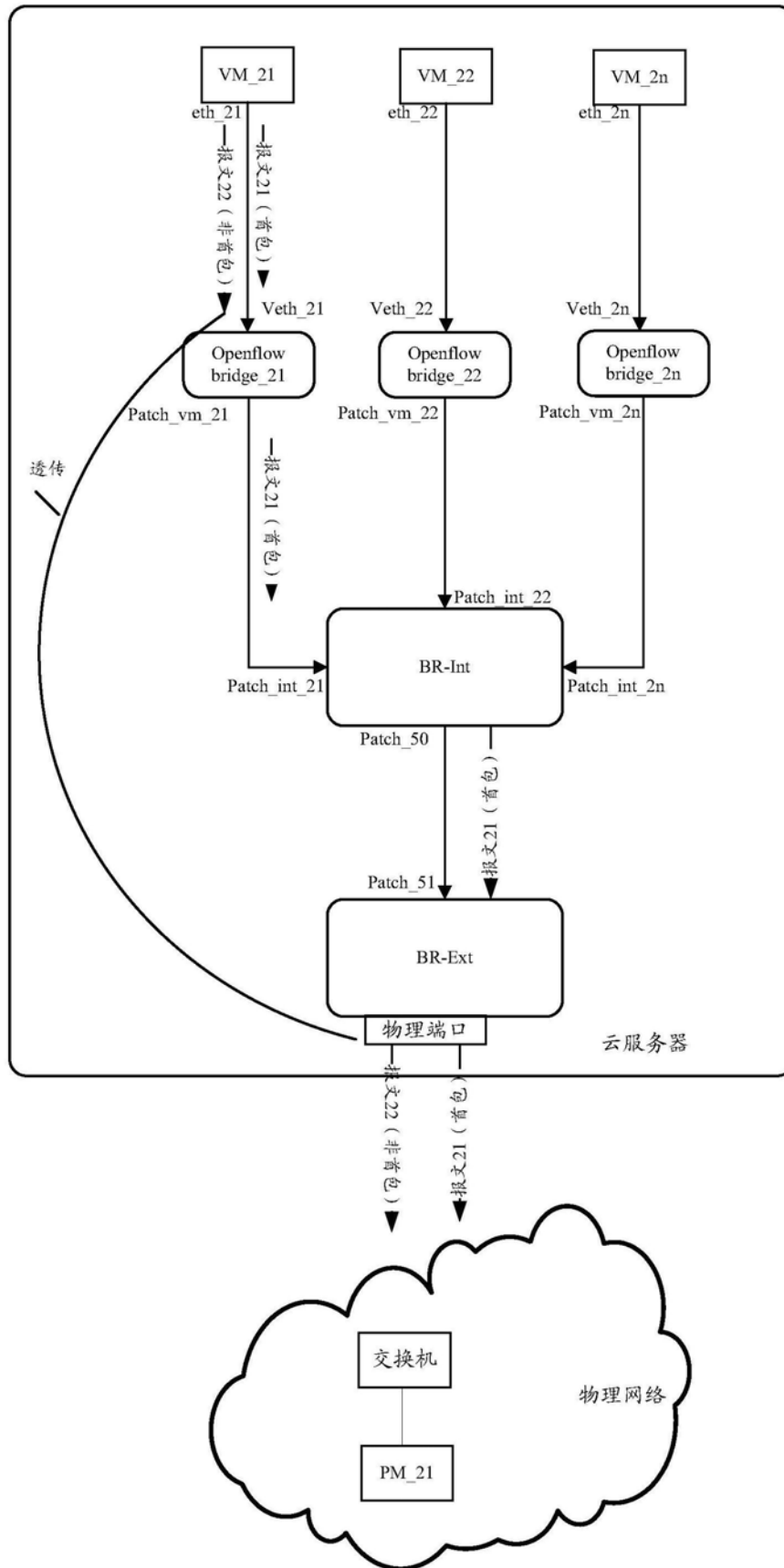


图5

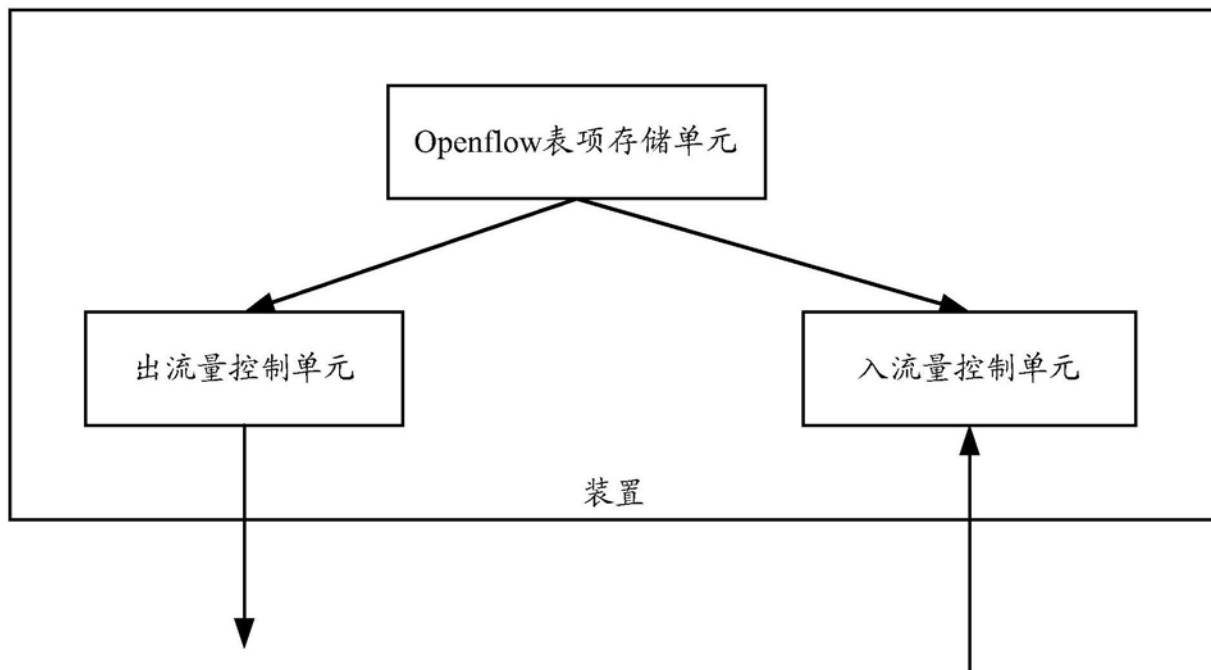


图6

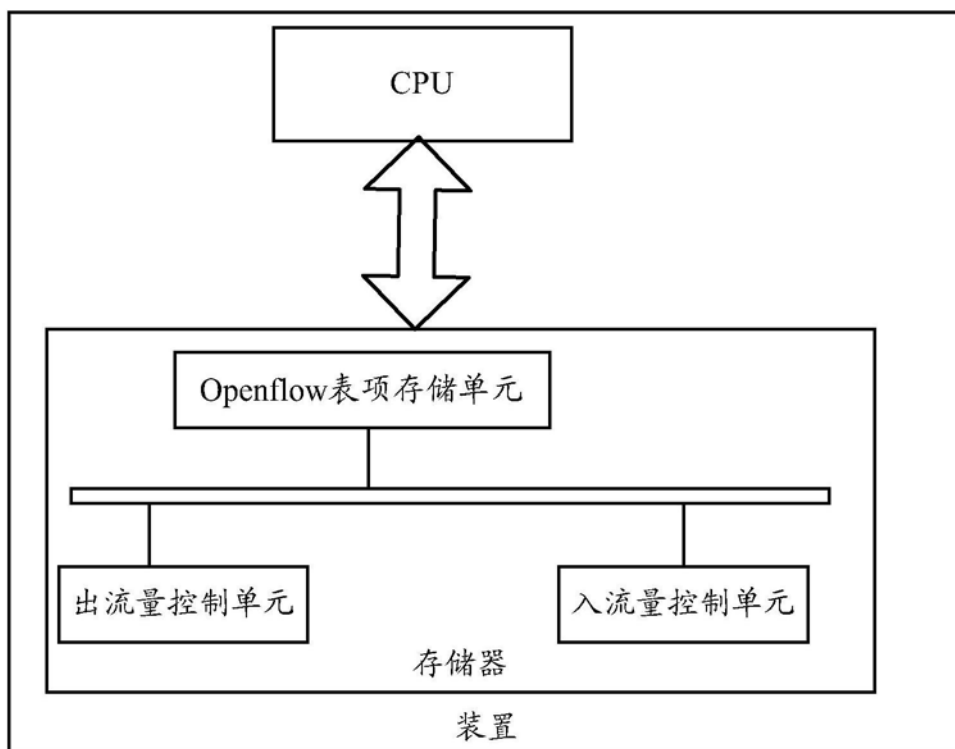


图7