

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2013 年 12 月 27 日 (27.12.2013)



(10) 国际公布号
WO 2013/189059 A1

- (51) 国际专利分类号:
H04L 12/70 (2013.01)
- (21) 国际申请号: PCT/CN2012/077304
- (22) 国际申请日: 2012 年 6 月 21 日 (21.06.2012)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人 (对除美国外的所有指定国): 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): 王雨晨 (WANG, Yuchen) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 武雪平 (WU, Xueping) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京同立钧成知识产权代理有限公司 (LEADER PATENT & TRADEMARK FIRM); 中国北京市海淀区西直门北大街 32 号枫蓝国际 A 座 8F-6, Beijing 100082 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

(54) Title: PACKET PROCESSING METHOD, APPARATUS, HOST AND NETWORK SYSTEM

(54) 发明名称: 报文处理方法、装置、主机和网络系统

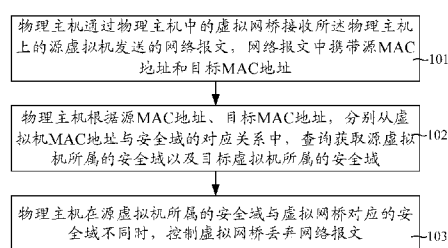


图 1b / Fig. 1b

101 A physical host receives, through a virtual network bridge in the physical host, a network packet sent by a source virtual machine on the physical host, wherein the network packet carries a source MAC address and a destination MAC address
102 The physical host queries, according to the source MAC address and the destination MAC address, a security domain of the source virtual machine and a security domain of a destination virtual machine from correspondence between the MAC address and the security domain of each virtual machine
103 The physical host controls the virtual network bridge to discard the network packet when the security domain of the source virtual machine is different from a security domain corresponding to the virtual network bridge

(57) Abstract: Embodiments of the present invention provide a packet processing method, apparatus, host and network system. The method comprises: a physical host receiving, through a virtual network bridge in the physical host, a network packet sent by a source virtual machine on the physical host, wherein the network packet carries a source MAC address and a destination MAC address; the physical host querying, according to the source MAC address and the destination MAC address, a security domain of the source virtual machine and a security domain of a destination virtual machine from correspondence between the MAC address and the security domain of each virtual machine; and the physical host controlling the virtual network bridge to discard the network packet when the security domain of the source virtual machine is different from a security domain corresponding to the virtual network bridge. Embodiments of the present invention further provide another packet processing method, apparatus, host and network system. The embodiments of the present invention greatly decrease the load of a physical switch, and improve the communication efficiency of a virtual network.

(57) 摘要:

[见续页]

WO 2013/189059 A1



本发明实施例提供一种报文处理方法、装置、主机和网络系统，方法包括：物理主机通过所述物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；所述物理主机根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。本发明实施例还提供另一种报文处理方法、装置、主机和网络系统。本发明实施例大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

报文处理方法、装置、主机和网络系统

技术领域

- 5 本发明涉及通信技术，尤其涉及一种报文处理方法、装置、主机和网络系统。

背景技术

在数据中心中，不同用户的业务系统都有自己的计算机、网络等基础设施，且不同业务系统的基础设施之间相互独立，因此可以通过网络物理隔离手段来保证业务系统之间的信息隔离，防止业务系统的信息泄露。比如，财务系统的计算机和网络与其他业务系统相隔离，这样可以保证其他业务系统的用户无法通过网络窃取财务系统内的数据。

虚拟化是指计算机元件在虚拟的基础上而不是真实的基础上运行，CPU
15 的虚拟化技术可以单 CPU 模拟多 CPU 并行，允许一个平台同时运行多个操作系统，且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。由于虚拟化技术在提升工作效率方面的优势，在数据中心上应用虚拟化技术成为当前技术研究热点，但在数据中心虚拟化之后，运行用户业务的不再是物理计算机而是安装在物理计算机上的虚拟机，属于
20 不同租户的不同虚拟机可能运行在同一物理主机上，由虚拟机组成的不同业务系统会共享相同的网络基础设施。此时难以实现信息系统的隔离，如财务系统和研发系统使用不同的虚拟机，但不同的虚拟机运行在同一物理主机上或者同处于同一网络内，则用户可以通过研发系统内的虚拟机通过地址欺骗、网络监听等手段窃取财务系统的数据。因此，在出现不同的租户共享物理基
25 础设施时，如何跨越物理边界将虚拟机划分为不同的虚拟网络，并保证虚拟网络之间的信息隔离成为保证虚拟化数据中心多租户安全的一项基本要求。

在现有技术中，为了保证虚拟网络之间的信息隔离，通常通过使虚拟机的网络流量经过交换机，即将物理主机上虚拟机生成的所有流量均发送到物理主机之外的交换机上，通过交换机对流量进行过滤控制处理，交换机会像
30 处理普通主机的流量一样对来自于虚拟机的流量进行处理，从而使用现有的

虚拟局域网（Virtual Local Area Network；以下简称：VLAN）技术对虚拟机进行隔离。

然而，现有技术中虚拟机之间通信的所有流量均引到交换机进行处理，极大地加重了交换机的负担。

5

发明内容

本发明提供一种报文处理方法、装置、主机和网络系统，减轻物理交换机的负担，提高虚拟网络通信效率。

第一方面提供了一种报文处理方法，包括：

10 物理主机通过所述物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

所述物理主机根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

15 所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

在第一方面的第一种可能的实现方式中，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文包括：

20 当所述目标 MAC 地址为非广播地址时：

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同、且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；

25 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

结合第一方面的第一种可能的实现方式，在第二种可能的实现方式中，所述控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文包括：

30 当所述目标虚拟机与所述源虚拟机位于同一个物理主机时，控制所述虚拟网桥根据所述目标 MAC 地址，将所述网络报文直接发送到所述物理主机

上的目标虚拟机上;

当所述目标虚拟机与所述源虚拟机不在同一个物理主机上时, 控制所述虚拟网桥将所述网络报文发送至物理交换机, 由所述物理交换机进行转发。

在第一方面的第三种可能的实现方式中, 所述物理主机在所述源虚拟机
5 所属的安全域与所述虚拟网桥对应的安全域不同时, 控制所述虚拟网桥丢弃
所述网络报文包括:

当所述目标 MAC 地址为广播地址时:

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同, 控制
所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播;

10 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同, 控制
所述虚拟网桥丢弃所述网络报文。

结合第一方面、第一方面的第一种可能的实现方式、第一方面的第二种
可能的实现方式, 或第一方面的第三种可能的实现方式, 在第一方面的第四
种实现方式中, 在所述分别从各虚拟机 MAC 地址与安全域的对应关系中,
15 查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域之前, 还包括:

所述物理主机将本机的 MAC 分组策略上报给策略服务器, 所述 MAC 分
组策略包括所述物理主机上的虚拟机 MAC 地址与安全域的对应关系;

所述物理主机从所在网络中的策略服务器中获取到局域网中的 MAC 分
组策略, 所述局域网中的 MAC 分组策略中包括各虚拟机 MAC 地址与安全域
20 的对应关系。

结合第一方面的第四种实现方式, 在第一方面的第五种实现方式中, 在
所述物理主机将本机的 MAC 分组策略上报给策略服务器后, 还包括:

当所述物理主机检测到本机的 MAC 分组策略发生变化时, 将变化后的
MAC 分组策略上报给所述策略服务器, 以使所述策略服务器更新局域网中的
25 MAC 分组策略。

第二方面提供了另一种报文处理方法, 包括:

物理主机通过该物理主机中的虚拟网桥接收物理交换机转发的网络报
文, 所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚
拟机发送的, 所述网络报文中携带源 MAC 地址和目标 MAC 地址;

30 所述物理主机根据所述源 MAC 地址、所述目标 MAC 地址, 分别从各虚

拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

- 5 在第二方面的第一种可能的实现方式中，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文包括：

当所述目标 MAC 地址为非广播地址时：

- 10 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同、且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上；

- 15 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

在第二方面的第二种可能的实现方式中，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文包括：

当所述目标 MAC 地址为广播地址时：

- 20 若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；

若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制所述虚拟网桥丢弃所述网络报文。

第三方面提供了一种报文处理装置，包括：

- 25 第一策略获取模块，用于获取各虚拟机 MAC 地址与安全域的对应关系；
第一接收模块，用于通过物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

- 30 第一获取模块，用于根据所述第一接收模块接收的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址，分别从所述第一策略获取模块获取到

的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

第一发送控制模块，用于在所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

在第三方面的第一种可能的实现方式中，所述第一发送控制模块包括：

第一发送单元，用于当所述目标 MAC 地址为非广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；

第一丢弃单元，用于当所述目标 MAC 地址为非广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

结合第三方面的第一种可能的实现方式，在第三方面的第二种实现方式中，所述第一发送单元包括：

发送子单元，用于当所述目标 MAC 地址为非广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目标虚拟机与所述源虚拟机位于同一物理主机时，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上；

转发子单元，用于当所述目标虚拟机与所述源虚拟机不在同一个物理主机上时，控制所述虚拟网桥将所述网络报文发送至物理交换机，由所述物理交换机进行转发。

在第三方面的第三种可能的实现方式中，所述第一发送控制模块包括：

第一广播单元，用于当所述目标 MAC 地址为广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同时，控制所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播；

第二丢弃单元，用于当所述目标 MAC 地址为广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

第四方面提供了一种报文处理装置，包括：

5 第二策略获取模块，用于获取各虚拟机 MAC 地址与安全域的对应关系；

第二接收模块，用于通过物理主机中的虚拟网桥接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

10 第二获取模块，用于根据所述第二接收模块接收到的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址，分别从所述第二策略获取模块获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

15 第二发送控制模块，用于在所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

在第四方面的第一种可能的实现方式中，所述第二发送控制模块包括：

20 第二发送单元，用于当所述目标 MAC 地址为非广播地址时，若所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述第二获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上；

25 第三丢弃单元，用于当所述目标 MAC 地址为非广播地址时，若所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述第二获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

在第四方面的第二种可能的实现方式中，所述第二发送控制模块包括：

30 第二广播单元，用于当所述目标 MAC 地址为广播地址时，若所述第二获取模块获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；

第四丢弃单元，用于当所述目标 MAC 地址为广播地址时，若所述第二获取模块获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制所述虚拟网桥丢弃所述网络报文。

第五方面提供了一种源主机，包括处理器，还包括虚拟网桥和策略控制器，其中：

所述策略控制器被配置用于从所处网络中的策略服务器中获取各虚拟机 MAC 地址与安全域的对应关系；

所述虚拟网桥被配置用于接收所述主机中的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

所述处理器被配置用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

在第五方面的第一种可能的实现方式中，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

在第五方面的第二种可能的实现方式中，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同时，控制所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网

络报文。

第六方面提供了一种目标主机，包括处理器，还包括虚拟网桥和策略控制器，其中：

所述策略控制器被配置用于从所处网络中的策略服务器中获取各虚拟机

5 MAC 地址与安全域的对应关系；

所述虚拟网桥被配置用于接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

10 所述处理器被配置用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

15 在第六方面的第一种可能的实现方式中，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述
20 网络报文发送到目标虚拟机上；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

25 在第六方面的第二种可能的实现方式中，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制所述虚拟网桥丢弃所述网络报文。

30 第七方面提供了一种网络系统，包括上述源主机，目标主机，以及策略

服务器，所述策略服务器被配置用于向所述主机中的策略控制器提供各虚拟机 MAC 地址与安全域的对应关系。。

在第七方面的第一种实现方式中，所述策略服务器还用于接收所述主机通过策略控制器上报的本机的 MAC 分组策略，所述 MAC 分组策略包括虚拟机 MAC 地址与安全域的对应关系；根据所述 MAC 分组策略更新本地的各虚拟机 MAC 地址与安全域的对应关系。

本发明实施例的技术效果是：物理主机通过虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，分别从虚拟机 MAC 地址与安全域的对应关系中查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1a 为本发明报文处理方法实施例一的应用示意图；

图 1b 为本发明报文处理方法实施例一的流程图；

图 2 为本发明报文处理方法实施例二的流程图；

图 3 为本发明报文处理方法实施例三的流程图；

图 4 为本发明报文处理方法实施例三中虚拟局域网的应用场景示意图；

图 5 为本发明报文处理方法实施例四的流程图；

图 6 为本发明报文处理方法实施例五的流程图；

图 7 为本发明报文处理方法实施例五中迁移前的虚拟局域网的应用场景示意图；

图 8 为本发明报文处理方法实施例五中迁移后的虚拟局域网的应用场景示意图；

图 9 为本发明报文处理装置实施例一的结构示意图；

图 10 为本发明报文处理装置实施例二的结构示意图；

图 11 为本发明报文处理装置实施例三的结构示意图；

图 12 为本发明报文处理装置实施例四的结构示意图；

5 图 13 为本发明主机实施例一的结构示意图；

图 14 为本发明主机实施例二的结构示意图；

图 15 为本发明网络系统实施例的结构示意图。

具体实施方式

10 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

15 为了便于理解，图 1a 为本发明报文处理方法实施例一的应用示意图。该图中的物理主机既可以是发送网络报文的源虚拟机所在的物理主机（即源主机），也可以是网络报文的目的虚拟机所在的物理主机（即目标主机）。后面将结合该示意图介绍本发明报文处理方法实施例。

图 1b 为本发明报文处理方法实施例一的流程图，如图 1b 所示，本实施例
20 提供了一种报文处理方法，本实施例从源虚拟机所在的物理主机一侧对本发明的方案进行具体说明，本实施例提供的报文处理方法可以具体包括如下步骤：

步骤 101，物理主机通过所述物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标
25 MAC 地址。

所述网络报文的接收方可以是所述物理主机中的另一虚拟机，也可以是另一物理主机中的虚拟机。

可选地，本实施例的一种具体实现方式为在安装虚拟机的物理主机（HOST）的操作系统（Operation System；以下简称：OS）或者运行虚拟机的
30 的虚拟机管理器（Hypervisor）内设置一个通信隔离器，该通信隔离器可以采

用软件方式来实现，如网络通信隔离软件。通过该网络通信隔离软件设置并管理一个策略控制器和至少一个虚拟网桥（Virtual Bridge；以下简称：VB）。虚拟网桥用软件的方式，实现类似于物理网桥的功能（即在链路层实现中继，对网络报文转发，并可以隔离碰撞等）。在本实施例中，一个虚拟网桥与一个安全域相对应，安装在物理主机上的虚拟机的虚拟网卡分别映射到该物理主机上的一个虚拟网桥上，其中虚拟机所属的安全域与所映射的虚拟网桥对应的安全域相同，从而建立虚拟机 MAC 地址与安全域的对应关系。其中，安全域是指相互信任，可以互相通信的计算机（即可以是物理主机，也可以是虚拟机）的集合。具体地，在物理主机中安装虚拟机时，上述网络通信隔离软件向用户提供一个选项列表，其中的每个选项都对应一个安全域，接收用户的选择结果，从而将所安装的虚拟机的 MAC 地址映射在选中的安全域对应的虚拟网桥上。

可选地，物理主机在建立了本物理主机上的虚拟机 MAC 地址与安全域的对应关系之后，上述通信隔离器将包含本机中的虚拟机 MAC 地址与安全域的对应关系的 MAC 分组策略，通过策略控制器上报到所处网络中的策略服务器，也可以通过策略控制器获取其他物理主机的虚拟机 MAC 地址与安全域的对应关系。通过上述机制，各物理主机上的策略控制器能够分享各虚拟机 MAC 地址与安全域的对应关系，以便后续确认如何发送报文。在本实施例中，当源虚拟机向目标虚拟机发送网络报文时，由于虚拟局域网中的各虚拟机的虚拟网卡分别映射在虚拟机所在物理主机上，各虚拟机所属的安全域对应的虚拟网桥上，因此虚拟机向外发送的报文均先被其对应的虚拟网桥截获。本步骤为物理主机通过物理主机中的虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文，此处的物理主机具体为源虚拟机所在的物理主机，源虚拟机向目标虚拟机发送网络报文时，该网络报文中携带所述网络报文的源 MAC 地址和目标 MAC 地址。其中，源虚拟机对应的虚拟网桥即为源虚拟机所属的安全域对应的虚拟网桥，源 MAC 地址为源虚拟机的 MAC 地址，目标 MAC 地址为目标虚拟机的 MAC 地址。

步骤 102，物理主机根据源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域。

在本实施例中，可以在策略服务器上存储局域网的 MAC 分组策略，策略控制器可以从策略服务器上获取该 MAC 分组策略。该 MAC 分组策略可以具体为局域网中各虚拟机 MAC 地址与安全域的对应关系。通过设置 MAC 分组策略，可以将局域网划分为多个安全域，同属于一个安全域的虚拟机的虚拟网卡映射在该安全域对应的虚拟网桥上。其中，策略服务器可以设置在二层网络上独立的一个服务器设备上。当物理主机通过虚拟网桥接收到网络报文时，通信隔离器需要决定发送或丢弃该网络报文，本步骤为物理主机中的通信隔离器通过策略控制器从策略服务器获取包含各虚拟机 MAC 地址与安全域的对应关系的虚拟局域网的 MAC 分组策略，根据所属网络报文中的源 MAC 地址、目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中，分别查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域。具体地，物理主机在接收到网络报文后，先根据所述源 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中，查询获取源虚拟机所属的安全域；并根据目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中，查询获取目标虚拟机所属的安全域。

步骤 103，物理主机在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文。

当获取到源虚拟机所属的安全域和目标虚拟机所属的安全域后，物理主机会根据源虚拟机所属的安全域、目标虚拟机所属的安全域，以及虚拟网桥自身对应的安全域，控制虚拟网桥对接收到的网络报文进行具体的发送控制处理，此处的发送控制处理为将该网络报文向目标虚拟机或物理交换机转发，或者不再发送该网络报文，即阻断此报文，将该报文进行丢弃处理。具体地，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，通信隔离器控制虚拟网桥丢弃网络报文。其中，可以根据预设的该物理主机中虚拟网桥与安全域的对应关系来获取虚拟网桥自身对应的安全域。由此可见，本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，即使转发到物理交换机的网络报文也只需经过转发，无需过滤控制，从而大大减轻物理交换机的负担。

本实施例提供了一种报文处理方法，物理主机通过虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，分别

从虚拟机 MAC 地址与安全域的对应关系中查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 2 为本发明报文处理方法实施例二的流程图，如图 2 所示，本实施例提供了一种报文处理方法，本实施例从目标虚拟机所在的物理主机一侧对本发明的方案进行具体说明，本实施例提供的报文处理方法可以具体包括如下步骤：

步骤 201，物理主机通过虚拟网桥接收物理交换机转发的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址。

本实施例为当源虚拟机与目标虚拟机不在同一物理主机上时，源虚拟机对应的虚拟网桥在经过过滤控制后，通过物理交换机将网络报文发送到目标虚拟机所在的物理主机上。本步骤具体为物理主机通过虚拟网桥接收物理交换机转发的网络报文，该网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，此处的物理主机为目标虚拟机所在的物理主机，虚拟网桥为目标虚拟机所属的安全域对应的虚拟网桥，在该虚拟报文中携带所述网络报文的源 MAC 地址和目标 MAC 地址。其中，源 MAC 地址为源虚拟机的 MAC 地址，目标 MAC 地址为目标虚拟机的 MAC 地址。

步骤 202，物理主机根据源 MAC 地址、目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。

当目标虚拟机所在的物理主机接收到网络报文时，也需要对该网络报文进行转发控制处理。本步骤为目标虚拟机所在的物理主机根据源 MAC 地址、目标 MAC 地址，以及通过策略控制器获取到的虚拟机 MAC 地址与安全域的对应关系中，分别查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。具体地，目标虚拟机所在的物理主机在接收到网络报文后，通信隔离器先根据源 MAC 地址，从各 MAC 地址与安全域的对应关系中，查询获取源虚拟机所属的安全域；并根据目标 MAC 地址，从各 MAC 地址与安全域的对应关系中，获取目标虚拟机所属的安全域。

可选地，与实施例一相类似，物理主机通过策略控制器从所处网络中的策略控制器获取虚拟局域网的 MAC 分组策略，所述虚拟局域网的 MAC 分组策略中包括各 MAC 地址与安全域的对应关系。

步骤 203，物理主机在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文。

当获取到源虚拟机所属的安全域和目标虚拟机所属的安全域后，物理主机根据源虚拟机所属的安全域、目标虚拟机所属的安全域，以及接收到所述网络报文的虚拟网桥对应的安全域，控制所述虚拟网桥对接收到的网络报文进行具体的发送控制处理；此处的发送控制处理为将该网络报文向映射在该虚拟网桥上的虚拟机发送，或者不再发送该网络报文，即阻断此报文，将该报文进行丢弃处理。具体地，本步骤为在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，物理主机中的通信隔离器控制虚拟网桥丢弃所述网络报文，从而实现对网络报文的双重过滤，保证了虚拟局域网的安全性。

本实施例提供了一种报文处理方法，物理主机通过目标虚拟机对应的虚拟网桥接收物理交换机转发的由源虚拟机向目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中查询分别获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 3 为本发明报文处理方法实施例三流程图，如图 3 所示，本实施例提供了一种报文处理方法，本实施例具体针对网络报文的的目标 MAC 地址为非广播地址的情况，本实施例可以具体包括如下步骤：

步骤 301，物理主机通过策略控制器从策略服务器获取各虚拟机 MAC 地址与安全域的对应关系。

在本实施例中，物理主机先通过策略控制器从策略服务器获取各虚拟机 MAC 地址与安全域的对应关系，用于对网络报文进行过滤控制，通过虚拟机 MAC 地址与安全域的对应关系将虚拟局域网划分为多个安全域。具体地，策略服务器上保存的各虚拟机 MAC 地址与安全域的对应关系，是由用户在各

物理主机上配置，并通过各物理主机上的策略控制器向策略服务器上报的，以使得各物理主机的 MAC 分组策略可以在不同物理主机之间共享。本实施例可以在 HOST OS 或者运行虚拟机的虚拟机管理器（Hypervisor）内设置一个通信隔离器，在该通信隔离器中设置一个策略控制器和至少一个虚拟网桥；

5 由于虚拟机 MAC 地址可以标识虚拟机，而一个虚拟机对应一个虚拟网卡，则可以由通信隔离器根据虚拟机 MAC 地址与安全域的对应关系，将各虚拟机的虚拟网卡分别映射到各虚拟机所属的安全域对应的虚拟网桥上。

图 4 为本发明报文处理方法实施例三中虚拟局域网的应用场景示意图，为了简明起见，在附图 4 中仅以虚拟网络中有两个物理主机、两个安全域的情况进行说明，在包含更多物理主机和更多安全域的情况下的处理方案类似。

10 如图 4 所示，假设 VM1、VM2、VM5、VM6 属于安全域 1，VM3、VM4、VM7、VM8 属于安全域 2，安全域 1 对应物理主机 1 中的虚拟网桥 11 和物理主机 2 中的虚拟网桥 21，安全域 2 对应物理主机 2 中的虚拟网桥 12 和物理主机 2 中的虚拟网桥 22，VM1、VM2、VM5、VM6 的 MAC 地址分别为

15 MAC1、MAC2、MAC5、MAC6，VM3、VM4、VM7、VM8 的 MAC 地址分别为 MAC3、MAC4、MAC7、MAC8，VM1、VM2 的虚拟网卡均映射在虚拟网桥 11 上，VM5、VM6 的虚拟网卡均映射在虚拟网桥 21 上，MAC3、MAC4 的虚拟网卡均映射在虚拟网桥 12 上，MAC7、MAC8 的虚拟网卡均映射在虚拟网桥 22 上。

20 步骤 302，源虚拟机所在的物理主机中的虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文。

本步骤为源虚拟机所在的物理主机接收源虚拟机向目标虚拟机发送的网络报文，该物理主机具体通过源虚拟机所属的安全域对应的虚拟网桥接收该网络报文，该网络报文中携带所述网络报文的源 MAC 地址和目标 MAC 地址。

25 以图 4 为例，VM1、VM2 发送的网络报文被对应的虚拟网桥 11 截获，VM3、VM4 发送的网络报文被对应的虚拟网桥 12 截获。当 VM1 向 VM2 发送网络报文时，物理主机 1 通过虚拟网桥 11 接收到该网络报文，该网络报文中可以携带源 MAC 地址 MAC1 和目标 MAC 地址 MAC2。具体地，物理主机在接收到该网络报文后，通过该网络报文的目标 MAC 地址可以识别该网络报文

30 是否为广播报文，当其目标 MAC 地址为“全 FF”时，该网络报文为广播报

文，本实施例具体以网络报文为非广播报文为例进行说明，后续实施例四中将对广播报文的处理过程进行说明。

步骤 303，源虚拟机所在的物理主机根据源 MAC 地址、目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。

源虚拟机所在的物理主机接收到网络报文后，源虚拟机所在的物理主机中的通信隔离器根据源 MAC 地址、目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。以图 4 为例，当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM2 的网络报文后，根据虚拟机 MAC 地址与安全域的对应关系可以获取到 MAC1 和 MAC2 对应的安全域均为安全域 1，即获取到源虚拟机所属的安全域和目标虚拟机所属的安全域均为安全域 1。

步骤 304，源虚拟机所在的物理主机判断源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域是否相同，如果是，则执行步骤 305，否则执行步骤 314。

源虚拟机所在的物理主机中的通信隔离器先判断源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域是否相同，如果是，则执行步骤 305，否则执行步骤 314。以上述图 4 为例，当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM2 的网络报文后，获取到源虚拟机所属的安全域为安全域 1，其与虚拟网桥 11 对应的安全域相同，则执行步骤 305 进行继续判断。

步骤 305，源虚拟机所在的物理主机判断目标虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域是否相同，如果是，则执行步骤 306，否则执行步骤 314。

当源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同时，源虚拟机所在的物理主机中的通信隔离器继续判断目标虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域是否相同，如果是，则执行步骤 306，否则执行步骤 314。以上述图 4 为例，当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM2 的网络报文后，获取到 VM1、VM2 所属的安全域均与虚拟网桥 11 对应的安全域相同，则执行步骤 306 对报文进行转发处理。当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM3 的网络报文后，

获取到 VM3 所属的安全域与虚拟网桥 11 对应的安全域不同，则执行步骤 314，直接将该网络报文进行丢弃处理。

步骤 306，源虚拟机所在的物理主机判断目标虚拟机所在的物理主机与源虚拟机所在的物理主机是否相同，如果是，则执行步骤 307，否则执行步骤 308。

当源虚拟机所属的安全域和目标虚拟机所属的安全域均与接收网络报文的虚拟网桥对应的安全域相同时，源虚拟机所在的物理主机中的通信隔离器继续判断目标虚拟机所在的物理主机与源虚拟机所在的物理主机是否相同，如果是，则执行步骤 307，否则执行步骤 308。具体地，物理主机根据虚拟机在安装时选择的安全域，可以建立并保存虚拟机 MAC 地址和虚拟网桥的映射关系。此时可以根据上述映射关系确认源虚拟机和目标虚拟机是否映射在同一个虚拟网桥上，如果源虚拟机和目标虚拟机是映射在同一个虚拟网桥上的，则显然源虚拟机和目标虚拟机所在的物理主机相同。

以上述图 4 为例，当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM2 的网络报文后，获取到 VM1 与虚拟网桥 11 对应的安全域相同，且 VM2 所属的安全域与虚拟网桥 11 对应的安全域相同，且 VM1 和 VM2 均位于物理主机 1 上，则执行步骤 307，直接控制虚拟网桥 11 将该网络报文直接发送到 VM2 上。当物理主机 1 通过虚拟网桥 11 接收到 VM1 发送到 VM5 的网络报文后，获取到 VM1 所属的安全域与虚拟网桥 11 对应的安全域相同，且 VM5 所属的安全域与虚拟网桥 11 对应的安全域相同，但 VM1 和 VM5 分别位于物理主机 1 和物理主机 2 上，则执行步骤 308，将该网络报文通过物理交换机进行转发。

步骤 307，源虚拟机所在的物理主机控制虚拟网桥根据目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上。

当源虚拟机所属的安全域与接收网络报文的虚拟网桥对应的安全域相同，且目标虚拟机所属的安全域与接收网络报文的虚拟网桥对应的安全域相同，且源虚拟机所在的物理主机中的通信隔离器继续判断目标虚拟机所在的物理主机与源虚拟机所在的物理主机也相同时，源虚拟机所属安全域对应的虚拟网桥可以根据目标 MAC 地址将网络报文直接发送到其所在的物理主机上的目标虚拟机上。例如图 4 中的 VM1 和 VM2 同属于安全域 1，且在同一

物理主机上，则虚拟网桥 11 可以将 VM1 的网络报文直接发送到 VM2，无需经过物理交换机的处理，降低了物理交换机的负担。

步骤 308，源虚拟机所在的物理主机控制虚拟网桥将网络报文发送至物理交换机，以便所述物理交换机后续将所述网络报文发送至目标虚拟机所在的物理主机中。

当源虚拟机所属的安全域与接收网络报文的虚拟网桥对应的安全域相同、且目标虚拟机所属的安全域与接收网络报文的虚拟网桥对应的安全域相同、但目标虚拟机所在的物理主机与源虚拟机所在的物理主机不同时，由于两个虚拟机不在同一物理主机上，则需要物理交换机的转发，通信隔离器可以控制源虚拟机所在的物理主机上的、源虚拟机所属的安全域对应的虚拟网桥将网络报文先发送到物理交换机上，由物理交换机将该网络报文转发到目标虚拟机所在的物理主机中目标虚拟机对应的虚拟网桥上。例如图 4 中的 VM1 和 VM5 同属于安全域 1，但二者不在同一物理主机上，则虚拟网桥 11 可以将 VM1 的网络报文通过物理交换机先转发到 VM5 所在的物理主机中其对应的虚拟网桥 21 上，网络过滤功能的实现无需依赖物理交换机的过滤控制处理，物理交换机只需转发，同样也可以降低物理交换机的负担。

步骤 309，目标虚拟机所在物理主机中的虚拟网桥接收到物理交换机发送的网络报文。

物理交换机对来自于虚拟机的网络报文和来自于物理主机的报文不区分地执行相同的转发处理。具体地，物理交换机中保存有各 MAC 地址（即包括虚拟机的 MAC 地址，也包括物理主机的 MAC 地址）与交换机端口的映射关系，接收到网络报文后，查询其目标 MAC 地址对应的交换机端口，然后通过查询到的交换机端口将该网络报文转发出去。例如，MAC5、MAC6、MAC7、MAC8 以及物理主机 2 的 MAC 地址都映射在同一个交换机端口上，物理交换机将目标 MAC 地址为 MAC5、MAC6、MAC7、MAC8、或物理主机 2 的 MAC 地址的网络报文都发送给物理主机 2 的网络接口中，具体该网络报文应该发送给 VM5、WM6、WM7、VM8 还是物理主机 2 的操作系统，则需要根据虚拟机 MAC 与虚拟网桥的映射关系，由虚拟网桥进行进一步的转发。本实施例中仅描述一个虚拟机向另一个虚拟机发送的网络报文的处理过程。例如物理主机 2 根据该物理主机上虚拟机 MAC 地址和虚拟网桥的映

射关系，控制目的虚拟机 WM5 映射的虚拟网桥 21 进行进一步转发。

步骤 310，目标虚拟机所在的物理主机根据所述网络报文的源 MAC 地址、目标 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。

- 5 可选地，与实施例一相类似，物理主机 2 通过策略控制器从所处网络中的策略控制器获取虚拟局域网的 MAC 分组策略，所述虚拟局域网的 MAC 分组策略中包括各 MAC 地址与安全域的对应关系。

步骤 311，目标虚拟机所在的物理主机判断源虚拟机所属的安全域与虚拟网桥对应的安全域是否相同，如果是，则执行步骤 312，否则执行步骤 314。

- 10 本步骤为目标虚拟机所在的物理主机上，目标虚拟机所属的安全域对应的虚拟网桥接收到物理交换机转发的网络报文后，该目标虚拟机所在的物理主机中的通信隔离器判断源虚拟机所属的安全域与接收到网络报文的该虚拟网桥对应的安全域是否相同，如果是，则执行步骤 312，否则执行步骤 314。其中，由于源虚拟机和目标虚拟机同属于一个安全域，则目标虚拟机所属的安全域与源虚拟机所属的安全域相同，例如图 4 中的 VM1 和 VM5 同属于安全域 1，但二者不在同一物理主机上，VM5 对应的虚拟网桥为物理主机 2 上的虚拟网桥 21，则物理主机 2 在通过虚拟网桥 21 接收到物理交换机转发的网络报文后，同样先判断 VM1 所属的安全域是否与虚拟网桥 21 对应的安全域是否相同，通过判断可知二者均为安全域 1，则可以继续后续判断步骤。
- 15

- 20 步骤 312，目标虚拟机所在的物理主机判断目标虚拟机所属的安全域与虚拟网桥对应的安全域是否相同，如果是，则执行步骤 313，否则执行步骤 314。

- 当目标虚拟机所在的物理主机中的通信隔离器获知源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同时，此处的虚拟网桥具体为目标虚拟机所属的安全域对应的虚拟网桥，继续判断目标虚拟机所属的安全域与接收到网络报文的该虚拟网桥对应的安全域是否相同，如果是，则执行步骤 313，否则执行步骤 314。仍以图 4 中的 VM1-VM5 为例，物理主机 2 上的虚拟网桥 21 获知 VM1 所属的安全域与虚拟网桥 21 对应的安全域相同，继续判断 VM5 所属的安全域是否与虚拟网桥 21 对应的安全域是否相同，通过判断可知二者均为安全域 1，则可以执行步骤 313，直接将该网络报文转发
- 25
- 30

到 VM5 上。

步骤 313, 目标虚拟机所在的物理主机, 根据目标 MAC 地址, 控制虚拟网桥将网络报文发送到目标虚拟机上。

当目标虚拟机所在的物理主机获知源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同, 且目标虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同, 目标虚拟机所在的物理主机根据目标 MAC 地址将网络报文发送到物理主机上的目标虚拟机上, 则实现了在源虚拟机和目标虚拟机所对应的虚拟网桥上均对网络报文进行过滤控制, 进一步提高了虚拟局域网的安全性。

步骤 314, 目标虚拟机所在的物理主机控制虚拟网桥丢弃所述网络报文。

当目标虚拟机对应的虚拟网桥获知源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同, 但目标虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域不同, 则目标虚拟机所在的物理主机中的通信隔离器控制目标虚拟机所属的安全域对应的虚拟网桥对网络报文进行丢弃处理, 阻断源虚拟机与目标虚拟机之间的通信, 则实现了在源虚拟机和目标虚拟机所对应的虚拟网桥上均对网络报文进行过滤控制, 进一步提高了虚拟局域网的安全性。

需要指出的是, 本实施例中的上述部分步骤之间没有严格的执行顺序的限制, 如步骤 304 和步骤 305 可以互换, 步骤 311 和步骤 312 可以互换。

另外, 本实施例还可以防止 MAC 欺骗攻击, 即防止用户通过恶意篡改虚拟机的 MAC 地址来进行欺骗攻击。仍以上述图 4 为例, 假设 VM2 的用户希望与安全域 2 中的计算机进行通信, 则其将自身的 MAC 地址篡改为 VM3 的 MAC 地址, 即将 MAC2 改为 MAC3, 并试图使用篡改后的 MAC 地址与 VM4 进行通信; 此时网络报文的源 MAC 地址为 MAC3, 目标地址为 MAC4。当 VM2 使用 MAC3 向 VM4 发送网络报文时, 此前 VM2 所映射的安全域 1 中的虚拟网桥 1 接收到该网络报文时, 会发现源 MAC 地址 MAC3 不属于安全域 1, 因此虚拟网桥 1 会阻断该网络报文的发送, 从而使得 VM2 无法冒充 VM3 对外通信。

本实施例提供了一种报文处理方法, 物理主机通过虚拟网桥接收物理交换机转发的由源虚拟机向目标虚拟机发送的网络报文, 根据 MAC 分组策略、

源 MAC 地址和目标 MAC 地址, 分别获取源虚拟机所属的安全域以及目标虚拟机所属的安全域, 根据源虚拟机所属的安全域和目标虚拟机所属的安全域对网络报文进行发送控制处理; 本实施例通过虚拟网桥实现了对网络报文的过滤控制, 无需将虚拟机之间的所有流量均发送到物理交换机来处理, 从而大大减轻了物理交换机的负担, 提高虚拟网络的通信效率。

图 5 为本发明报文处理方法实施例四的流程图, 如图 5 所示, 本实施例提供了一种报文处理方法, 本实施例具体针对网络报文的目标 MAC 地址为广播地址的情况, 本实施例可以具体包括如下步骤:

步骤 501, 物理主机通过策略控制器从策略服务器获取各虚拟机 MAC 地址与安全域的对应关系, 本步骤可以与上述步骤 301 类似, 此处不再赘述。

步骤 502, 源虚拟机所在的物理主机中的虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文。

本步骤为源虚拟机所在的物理主机通过虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文, 该虚拟网桥可以具体为源虚拟机所属的安全域对应的虚拟网桥, 该网络报文中携带所述网络报文的源 MAC 地址、目标 MAC 地址。本实施例针对的是以太网广播报文的处理过程, 因此网络报文中携带的目标 MAC 地址是以太网广播地址, 即该网络报文的目标为局域网中的所有计算机。具体地, 物理主机在接收到该网络报文后, 通过该网络报文的目标 MAC 地址可以识别该网络报文是否为广播报文, 当其目标 MAC 地址为“全 FF”时, 该网络报文为广播报文, 本实施例具体以网络报文为广播报文为例进行说明。

步骤 503, 源虚拟机所在的物理主机根据源 MAC 地址, 从各虚拟机 MAC 地址与安全域的对应关系中, 查询获得源虚拟机所属的安全域。

由于目标虚拟机并不是一个特定的虚拟机, 则源虚拟机对应的虚拟机网桥只获取源虚拟机所属的安全域, 具体获取方法与上述步骤 303 中类似, 此处不再赘述。

步骤 504, 源虚拟机所在的物理主机判断源虚拟机所属的安全域与虚拟网桥对应的安全域是否相同, 如果是, 则执行步骤 505, 否则执行步骤 509。

本步骤为源虚拟机所在的物理主机中的通信隔离器判断源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域是否相同, 如果是, 则执

行步骤 505，直接将该网络报文在局域网中进行广播，否则执行步骤 509，将该网络报文进行丢弃处理。

步骤 505，源虚拟机所在的物理主机将网络报文通过物理交换机在所述局域网内广播。

- 5 当源虚拟机所属的安全域与接收到网络报文的虚拟网桥对应的安全域相同时，源虚拟机所在的物理主机将网络报文通过物理交换机在局域网内广播。以上述图 4 为例，假设 VM1 希望与 VM5 通信，但此时 VM1 并不知道 VM5 的 MAC 地址，则 VM1 会首先通过发送广播报文的方式向局域网中的所有计算机机发送一个 ARP Request 网络报文，由于 VM1 属于安全域 1，则该网络
10 报文会被虚拟网桥 11 获取到，物理主机 1 中的通信隔离器通过判断获知 VM1 所属的安全域与虚拟网桥 11 相同时，控制虚拟网桥 11 将网络报文通过物理交换机在该局域网内广播。

物理交换机对网络报文的转发过程请参照附图 3 步骤 309 中的描述，在这里不再赘述。

- 15 步骤 506，局域网中接收到此网络报文的物理主机根据所述网络报文的源 MAC 地址，从各虚拟机 MAC 地址与安全域的对应关系中查询获得源虚拟机所属的安全域。

- 20 步骤 507，局域网中接收到此网络报文的物理主机，针对该物理主机中的每个虚拟网桥，判断源虚拟机所属的安全域与该虚拟网桥对应的安全域是否相同，如果是，则执行步骤 508，否则执行步骤 509。

- 25 当源虚拟机所在的物理交换机在局域网内广播该网络报文后，局域网内的所有虚拟网桥均会接收到该网络报文，即局域网内的所有物理主机均通过各自的虚拟网桥接收到该网络报文。本步骤为局域网中接收到此网络报文的物理主机中的通信隔离器，判断源虚拟机所属的安全域与该虚拟网桥对应的
30 安全域是否相同，如果是，则执行步骤 508，否则执行步骤 509。仍以上述图 4 为例，当 VM1 希望与 VM5 通信，VM1 通过广播报文的方式向局域网发送网络报文，虚拟网桥 11 将此网络报文通过物理交换机在局域网内广播。局域网内的所有虚拟网桥都会通过物理交换机接收到上述广播报文，并会根据广播报文的源 MAC 地址获得此源虚拟机所属的安全域，各物理主机中的通信
30 隔离器判断此源虚拟机所属的安全域与局域网中接收到此报文的虚拟网桥对

应的安全域是否相同，如果是，则执行步骤 508，否则执行步骤 509。即当在局域网中广播该网络报文后，虚拟网桥 11、虚拟网桥 12、虚拟网桥 21 和虚拟网桥 22 均会接收到该网络报文，则物理主机 1 通过虚拟网桥 11 和虚拟网桥 12 接收到该网络报文，物理主机 2 通过虚拟网桥 21 和虚拟网桥 22 接收到该网络报文，物理主机 1 分别判断虚拟网桥 11、虚拟网桥 12 对应的安全域与源虚拟机所属的安全域是否相同物理主机 2 分别判断虚拟网桥 21、虚拟网桥 22 对应的安全域与源虚拟机所属的安全域是否相同；通过判断，虚拟网桥 11 和虚拟网桥 21 对应的安全域与之相同，则虚拟网桥 11 将该网络报文转发给映射在其上的所有虚拟机，即图中的 VM5、VM6；而虚拟网桥 12 和虚拟网桥 22 对应的安全域与之不同，则虚拟网桥 12 和 22 将该网络报文进行丢弃处理。

步骤 508，局域网中接收到此网络报文的物理主机，控制对应的安全域与源虚拟机所属的安全域相同的虚拟网桥，将该网络报文转发给映射在其上的所有虚拟机。

当与该网络报文的源虚拟机属于同一个安全域的虚拟网桥接收到网络报文后，该虚拟网桥会将该网络报文转发给映射在其上的所有虚拟机。如图 4 所示，此时如果 VM5 开机，VM5 将会接收虚拟网桥 22 转发的这个 ARP Request 报文。

步骤 509，局域网中接收到此网络报文的物理主机，控制对应的安全域与源虚拟机所属的安全域不同的虚拟网桥丢弃所述网络报文。

如果局域网内接收到此网络报文的虚拟网桥对应的安全域与源虚拟机所属的安全域不相同时，虚拟网桥会丢弃此报文。

本实施例提供了一种报文处理方法，通过目标虚拟机对应的虚拟网桥接收物理交换机转发的由源虚拟机发送的网络报文，根据虚拟机 MAC 地址与安全域的对应关系和源 MAC 地址，获取源虚拟机所属的安全域，根据源虚拟机所属的安全域，以及虚拟网桥对应的安全域，对网络报文进行发送控制处理；本实施例通过虚拟网桥实现了对不同安全域中广播报文的隔离，在此过程中物理交换机中无需进行额外的过滤控制处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 6 为本发明报文处理方法实施例五的流程图，如图 6 所示，本实施例

提供了一种报文处理方法，本实施例具体应用于虚拟机迁移场景中，虚拟机迁移是指原本基于一个物理主机的硬件资源和处理资源实现的虚拟机，转而从另一个物理主机的硬件资源和处理资源来实现，本实施例不对虚拟机迁移的实现原理进行探讨，只对在发生虚拟机迁移前后，如何对不同安全域中的网络报文实现隔离的方法进行介绍。

本实施例在上述实施例三或实施例四的基础之上，还可以具体包括如下步骤：

步骤 601，物理主机获取本机的 MAC 分组策略。

在本实施例中，在进行报文处理之前，局域网中的各物理主机可以先获取本机的 MAC 分组策略，该 MAC 分组策略可以包括虚拟机 MAC 地址与安全域的对应关系。MAC 分组策略可以由用户根据实际情况自行设定，其中，虚拟网桥与安全域之间的对应关系也可以由用户根据实际情况来设定。从用户角度来说，在物理主机上安装虚拟机时，物理主机中的网络通信隔离软件会弹出一个选项列表，其中的每个选项都对应一个安全域。由于一个虚拟机对应一个虚拟机 MAC 地址，在虚拟机安装在物理主机上之后，物理主机便可以自动获取到该虚拟机的 MAC 地址；当接收到用户根据上述选项列表选中的选项后，在虚拟机安装完成后，物理主机中的网络通信隔离软件便将该虚拟机的虚拟网卡映射在选中的安全域对应的那个虚拟网桥上之后，从而建立了该虚拟机 MAC 地址与该虚拟机网桥所属的安全域之间的对应关系，物理主机便可以获取到该虚拟机 MAC 地址与安全域之间的对应关系。对于每个虚拟机来说，物理主机均可以通过上述过程获取到本机中的虚拟机 MAC 地址与安全域之间的对应关系。同时，物理主机还可以获取到用户设定的虚拟网桥与安全域之间的对应关系。

步骤 602，物理主机将本机的 MAC 分组策略上报到策略服务器。

物理主机在获取到本机的 MAC 分组策略后，通过该物理主机中的策略控制器，将本机的 MAC 分组策略，即将本机中的虚拟机 MAC 地址与安全域的对应关系上报到策略服务器。局域网中的各物理主机分别通过各自的策略控制器，将各自的 MAC 分组策略上报到策略服务器，策略服务器在本地保存整个局域网中的 MAC 分组策略，后续，一个物理主机通过其中的策略控制器便可以从该策略服务器上获取其他物理主机的 MAC 分组策略。

图 7 为本发明报文处理方法实施例五中迁移前的虚拟局域网的应用场景示意图, 如图 7 所示, VM1-VM6 的 MAC 地址分别为 MAC1-MAC6, 防火墙的 MAC 地址为 MAC-F, 在虚拟机迁移之前, VM1、VM2、VM3、VM4 安装在物理主机 1 上, VM5 安装在物理主机 2 上, VM6 安装在物理主机 3 上, 物理主机 1 中设置有虚拟网桥 11 和虚拟网桥 12, 物理主机 2 中设置有虚拟网桥 21 和虚拟网桥 22, 物理主机 3 中设置有虚拟网桥 31 和虚拟网桥 32。用户根据实际情况, 将 VM1、VM2 的虚拟网卡映射在虚拟网桥 11 上, 将 VM3、VM4 的虚拟网卡映射在虚拟网桥 12 上, 将 VM5 的虚拟网卡映射在虚拟网桥 22 上, 将 VM6 的虚拟网卡映射在虚拟网桥 32 上, 同时设置虚拟网桥 11、虚拟网桥 21 和虚拟网桥 31 均属于安全域 1, 虚拟网桥 12、虚拟网桥 22 和虚拟网桥 32 均属于安全域 2。物理主机 1 可以获取到本机的 MAC 分组策略为: VM1、VM2 与安全域 1 具有对应关系, VM3、VM4 与安全域 2 具有对应关系, 此外还可以获知虚拟网桥 11 与安全域 1 具有对应关系, 虚拟网桥 12 与安全域 2 具有对应关系; 物理主机 2 可以获取到本机的 MAC 分组策略为: VM5 与安全域 2 具有对应关系, 此外还可以获知虚拟网桥 21 与安全域 1 具有对应关系, 虚拟网桥 22 与安全域 2 具有对应关系; 物理主机 3 可以获取到本机的 MAC 分组策略为: VM6 与安全域 2 具有对应关系, 此外还可以获知虚拟网桥 31 与安全域 1 具有对应关系, 虚拟网桥 32 与安全域 2 具有对应关系。然后物理主机 1 通过策略控制器 1 将本机的 MAC 分组策略上报给策略服务器, 物理主机 2 通过策略控制器 2 将本机的 MAC 分组策略上报给策略服务器, 物理主机 3 通过策略控制器 3 将本机的 MAC 分组策略上报给策略服务器。

步骤 603, 若物理主机检测到本机的 MAC 分组策略发生变化, 物理主机将变化后的 MAC 分组策略通过策略控制器上报到策略服务器。

在本实施例中, 物理主机还对本机的 MAC 分组策略进行定期检测, 判断该 MAC 分组策略是否发生变化; 当本机的 MAC 分组策略发生变化时, 物理主机将变化后的 MAC 分组策略通过策略控制器上报到策略服务器。

步骤 604, 策略服务器根据变化后的 MAC 分组策略, 更新本地保存的局域网的 MAC 分组策略。

策略服务器接收各物理主机中的策略控制器发送的变化后的 MAC 分组

策略,并根据变化后的 MAC 分组策略更新本地保存的局域网的 MAC 分组策略,以使其他物理主机能够从策略服务器同步获取到更新后的局域网的 MAC 分组策略。需要指出的时,虚拟机迁移前后的报文处理过程可以与上述实施例三或实施例四中描述的一致,此处不再赘述。可选地,为了保证各物理主机上 MAC 分组策略的一致性,策略服务器可以在每次发生更新后,主动向各物理主机中的策略控制器发送更新后的局域网的 MAC 分组策略;策略服务器也可以按照设定的同步周期,定期向各物理主机中的策略控制器发送更新后的局域网的 MAC 分组策略。

当虚拟机发生迁移时,对应的 MAC 分组策略可能会发生变化。图 8 为本发明报文处理方法实施例五中迁移后的虚拟局域网的应用场景示意图,如图 8 所示,当虚拟机发生迁移后,VM1 从物理主机 1 迁移到物理主机 2 上,VM2 从物理主机 1 迁移到物理主机 3 上,具体地,VM1 的虚拟网卡被映射到虚拟网桥 21 上,VM2 的虚拟网卡被映射到虚拟网桥 31 上。在虚拟机迁移之后,各物理主机检测到各自的 MAC 分组策略发生变化,则各物理主机将各自变化后的 MAC 分组策略上报到策略服务器。由于虚拟网桥 21 与虚拟网桥 11 同属于安全域 1,但虚拟网桥 31 与虚拟网桥 12 不属于同一个安全域。当 VM1 从物理主机 1 迁移到物理主机 2 上之后,物理主机 2 上的虚拟网桥 1 会从策略服务器获取 MAC 分组策略,从而实现对 VM1 的流量控制,可见,VM1 在迁移之后仍可以与其他 VM 正常通信,并不会出现由于迁移而导致的通信中断的现象。

本领域普通技术人员可以理解:实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时,执行包括上述各方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

图 9 为本发明报文处理装置实施例一的结构示意图,如图 9 所示,本实施例提供了一种报文处理装置,可以具体执行上述方法实施例一中的各个步骤,此处不再赘述。本实施例提供的报文处理装置可以具体包括第一策略获取模块 901、第一接收模块 902、第一获取模块 903 和第一发送控制模块 904。其中,第一策略获取模块 901 用于获取各虚拟机 MAC 地址与安全域的对应

关系。第一接收模块 902 用于通过物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址。第一获取模块 903 用于根据第一接收模块 902 接收的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址，分别从第一策略获取模块 901 获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。第一发送控制模块 904 用于在第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

图 10 为本发明报文处理装置实施例二的结构示意图，如图 10 所示，本实施例提供了一种报文处理装置，可以具体执行上述方法实施例三或实施例四中的各个步骤，此处不再赘述。本实施例提供的报文处理装置在上述图 9 所示的基础之上，第一发送控制模块 904 可以具体包括第一发送单元 914 和第一丢弃单元 924。其中，第一发送单元 914 用于当目标 MAC 地址为非广播地址时，若第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且第一获取模块 903 获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文。第一丢弃单元 924 用于当目标 MAC 地址为非广播地址时，述第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或第一获取模块 903 获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

进一步地，本实施例中的第一发送单元 914 可以具体包括发送子单元 9141 和转发子单元 9142。其中，发送子单元 9141 用于当所述目标 MAC 地址为非广播地址时，若第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且第一获取模块 903 获取到的所述目标虚拟机所属的安全域与虚拟网桥对应的安全域均相同时，且所述目标虚拟机所在的物理主机与所述源虚拟机所在的物理主机相同时，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上。转发子单元 9142 用于当所述目标虚拟机与所述源虚拟机不在同一个物理主机上时，控制所述虚拟网桥将所述网络报文发送至物理交换机，由所

述物理交换机进行转发。

在本实施例中，第一发送控制模块 904 可以包括第一广播单元 934 和第二丢弃单元 944。其中，第一广播单元 934 用于当所述目标 MAC 地址为广播地址时，若第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同时，控制所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播。第二丢弃单元 944 用于当所述目标 MAC 地址为广播地址时，若第一获取模块 903 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

本实施例提供了一种报文处理装置，物理主机通过虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，分别从虚拟机 MAC 地址与安全域的对应关系中查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 11 为本发明报文处理装置实施例三的结构示意图，如图 11 所示，本实施例提供了一种报文处理装置，可以具体执行上述方法实施例二中的各个步骤，此处不再赘述。本实施例提供的报文处理装置可以具体包括第二策略获取模块 1101、第二接收模块 1102、第二获取模块 1103 和第二发送控制模块 1104。其中，第二策略获取模块 1101 用于获取各虚拟机 MAC 地址与安全域的对应关系。第二接收模块 1102 用于通过物理主机中的虚拟网桥接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址。第二获取模块 1103 用于根据第二接收模块 1102 接收到的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址，分别从第二策略获取模块 1101 获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域。第二发送控制模块 1104 用于在第二获取模块 1103 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

图 12 为本发明报文处理装置实施例四的结构示意图，如图 12 所示，本

实施例提供了一种报文处理装置，可以具体执行上述方法实施例三或实施例四中的各个步骤，此处不再赘述。本实施例提供的报文处理装置在上述图 11 所示的基础之上，第二发送控制模块 1104 可以包括第二发送单元 1114 和第三丢弃单元 1124。其中，第二发送单元 1114 用于当所述目标 MAC 地址为非广播地址时，若第二获取模块 1103 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且第二获取模块 1103 获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上。第三丢弃单元 1124 用于当所述目标 MAC 地址为非广播地址时，若第二获取模块 1103 获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或第二获取模块 1103 获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

或者，第二发送控制模块 1104 可以包括第二广播单元 1134 和第四丢弃单元 1144。其中，第二广播单元 1134 用于当所述目标 MAC 地址为广播地址时，若第二获取模块 1103 获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机。第四丢弃单元 1144 用于当所述目标 MAC 地址为广播地址时，若第二获取模块 1103 获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制所述虚拟网桥丢弃所述网络报文。

本实施例提供了一种报文处理装置，物理主机通过虚拟网桥接收物理交换机转发的由源虚拟机向目标虚拟机发送的网络报文，根据 MAC 分组策略、源 MAC 地址和目标 MAC 地址，分别获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，根据源虚拟机所属的安全域和目标虚拟机所属的安全域对网络报文进行发送控制处理；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 13 为本发明主机实施例一的结构示意图，如图 13 所示，本实施例提供了一种源主机，该源主机可以具体执行上述方法实施例三或四中的各个步骤，此处不再赘述。该源主机可以具体包括处理器 1301，源主机还可以包括虚拟网桥 1302 和策略控制器 1303。其中，策略控制器 1303 被配置用于从所

处网络中的策略服务器中获取各虚拟机 MAC 地址与安全域的对应关系。虚拟网桥 1302 被配置用于接收所述主机中的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址。处理器 1301 被配置用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从策略控制器 1303 获取到的
5 各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与虚拟网桥 1302 对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

具体地，本实施例中的处理器 1301 具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从策略控制器 1303 获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与虚拟网桥 1302 对应的安全域相同，且所述目标虚拟机所属的安全域与虚拟网桥 1302 对应的安全域相同，控制虚拟网桥 1302 根据所述目标 MAC
10 地址发送所述网络报文；若所述源虚拟机所属的安全域与虚拟网桥 1302 对应的安全域不同，或所述目标虚拟机所属的安全域与虚拟网桥 1302 对应的安全域不同，控制虚拟网桥 1302 丢弃所述网络报文。

具体地，本实施例中的处理器 1301 具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从策略控制器 1303 获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若所述源虚拟机所属的安全域与虚拟网桥 1302 对应的安全域相同时，控制虚拟网桥 1302 将所述网络
20 报文通过物理交换机在局域网内广播；若所述源虚拟机所属的安全域与虚拟网桥 1302 对应的安全域不同时，控制虚拟网桥 1302 丢弃所述网络报文。

本实施例提供了一种源主机，源主机通过虚拟网桥接收源虚拟机向目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，分别从虚拟机
25 MAC 地址与安全域的对应关系中查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，
30 从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 14 为本发明主机实施例二的结构示意图，如图 14 所示，本实施例提供了一种目标主机，该目标主机可以具体执行上述方法实施例三或四中的各个步骤，此处不再赘述。该目标主机可以具体包括处理器 1401，目标主机还可以包括虚拟网桥 1402 和策略控制器 1403。策略控制器 1403 被配置用于从
5 所处网络中的策略服务器中获取各虚拟机 MAC 地址与安全域的对应关系。虚拟网桥 1402 被配置用于接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址。处理器 1401 被配置用于根据
10 所述源 MAC 地址、所述目标 MAC 地址，分别从策略控制器 1403 获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与虚拟网桥 1402 对应的安全域不同时，控制虚拟网桥 1402 丢弃所述网络报文。

具体地，本实施例中的处理器 1401 具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询
15 获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与虚拟网桥 1402 对应的安全域相同，且所述目标虚拟机所属的安全域与虚拟网桥 1402 对应的安全域相同，控制虚拟网桥 1402 根据所述目标 MAC 地址将所述网络报文发送到目标虚拟机上；若所述源虚拟机所属的安全域与虚拟网桥 1402 对应的安全域不同，或所述目标虚拟机所属的安全域与虚拟网桥 1402 对应的安全域不同，控
20 制虚拟网桥 1402 丢弃所述网络报文。

具体地，本实施例中的处理器 1401 具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询
25 获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若虚拟网桥 1402 对应的安全域与所述源虚拟机所属的安全域相同，控制虚拟网桥 1402 将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；若虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制虚拟网桥 1402 丢弃所述网络报文。

本实施例提供了一种目标主机，目标主机通过虚拟网桥接收源虚拟机向
30 目标虚拟机发送的网络报文，根据源 MAC 地址和目标 MAC 地址，分别从虚

拟机 MAC 地址与安全域的对应关系中查询获取源虚拟机所属的安全域以及目标虚拟机所属的安全域，在源虚拟机所属的安全域与虚拟网桥对应的安全域不同时，控制虚拟网桥丢弃网络报文；本实施例通过虚拟网桥实现了对网络报文的过滤控制，无需将虚拟机之间的所有流量均发送到物理交换机来处理，从而大大减轻了物理交换机的负担，提高虚拟网络的通信效率。

图 15 为本发明网络系统实施例的结构示意图，如图 15 所示，本实施例还提供了一种网络系统，该网络系统可以具体包括源主机 1501、目标主机 1503 以及策略服务器 1502，源主机 1501 可以具体如上述图 13 所示、目标主机 1503 如上述图 14 所示，策略服务器 1502 被配置用于向源主机 1501、或目标主机 1503 中的策略控制器提供各虚拟机 MAC 地址与安全域的对应关系。该策略服务器 1502 可以通过各源主机 1501、或目标主机 1503 中的策略控制器接收各主机上报的 MAC 分组策略，并在需要时使一个主机可以通过策略控制器共享其他主机上的 MAC 分组策略。

具体地，本实施例中的策略服务器 1502 还用于接收主机 1501、或目标主机 1503 通过策略控制器上报的本机的 MAC 分组策略，所述 MAC 分组策略包括虚拟机 MAC 地址与安全域的对应关系；根据 MAC 分组策略更新本地的局域网中各虚拟机 MAC 地址与安全域的对应关系。

最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权利要求书

1、一种报文处理方法，其特征在于，包括：

物理主机通过所述物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

5 所述物理主机根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

10 2、根据权利要求 1 所述的方法，其特征在于，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文，包括：

当所述目标 MAC 地址为非广播地址时：

15 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同、且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

20 3、根据权利要求 2 所述的方法，其特征在于，所述控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文包括：

当所述目标虚拟机与所述源虚拟机位于同一个物理主机时，控制所述虚拟网桥根据所述目标 MAC 地址，将所述网络报文直接发送到所述物理主机上的目标虚拟机上；

25 当所述目标虚拟机与所述源虚拟机不在同一个物理主机上时，控制所述虚拟网桥将所述网络报文发送至物理交换机，由所述物理交换机进行转发。

4、根据权利要求 1 所述的方法，其特征在于，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文，包括：

30 当所述目标 MAC 地址为广播地址时：

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播；

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

- 5 5、根据权利要求 1 至 4 中任一所述的方法，其特征在于，在所述分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域之前，还包括：

所述物理主机将本机的 MAC 分组策略上报给策略服务器，所述 MAC 分组策略包括所述物理主机上的虚拟机 MAC 地址与安全域的对应关系；

- 10 所述物理主机从所在网络中的策略服务器中获取到局域网中的 MAC 分组策略，所述局域网中的 MAC 分组策略中包括各虚拟机 MAC 地址与安全域的对应关系。

6、根据权利要求 5 所述的方法，其特征在于，在所述物理主机将本机的 MAC 分组策略上报给策略服务器后，还包括：

- 15 当所述物理主机检测到本机的 MAC 分组策略发生变化时，将变化后的 MAC 分组策略上报给所述策略服务器，以使所述策略服务器更新局域网中的 MAC 分组策略。

7、一种报文处理方法，其特征在于，包括：

- 20 物理主机通过该物理主机中的虚拟网桥接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

所述物理主机根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

- 25 所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

8、根据权利要求 7 所述的方法，其特征在于，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文，包括：

- 30 当所述目标 MAC 地址为非广播地址时：

若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同、且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上；

- 5 若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

- 9、根据权利要求 7 所述的方法，其特征在于，所述物理主机在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥
10 丢弃所述网络报文，包括：

当所述目标 MAC 地址为广播地址时：

若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；

- 若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制
15 所述虚拟网桥丢弃所述网络报文。

10、一种报文处理装置，其特征在于，包括：

第一策略获取模块，用于获取各虚拟机 MAC 地址与安全域的对应关系；

- 第一接收模块，用于通过物理主机中的虚拟网桥接收所述物理主机上的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地
20 址；

第一获取模块，用于根据所述第一接收模块接收的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址，分别从所述第一策略获取模块获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；

- 25 第一发送控制模块，用于在所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

11、根据权利要求 10 所述的装置，其特征在于，所述第一发送控制模块包括：

- 30 第一发送单元，用于当所述目标 MAC 地址为非广播地址时，若所述第

一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；

- 5 第一丢弃单元，用于当所述目标 MAC 地址为非广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

12、根据权利要求 11 所述的装置，其特征在于，所述第一发送单元包括：

- 10 发送子单元，用于当所述目标 MAC 地址为非广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述第一获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目标虚拟机与所述源虚拟机位于同一物理主机时，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到
15 所述物理主机上的目标虚拟机上；

转发子单元，用于当所述目标虚拟机与所述源虚拟机不在同一个物理主机上时，控制所述虚拟网桥将所述网络报文发送至物理交换机，由所述物理交换机进行转发。

- 13、根据权利要求 10 所述的装置，其特征在于，所述第一发送控制模块
20 包括：

第一广播单元，用于当所述目标 MAC 地址为广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同时，控制所述虚拟网桥将所述网络报文通过物理交换机在局域网内广播；

- 25 第二丢弃单元，用于当所述目标 MAC 地址为广播地址时，若所述第一获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

14、一种报文处理装置，其特征在于，包括：

第二策略获取模块，用于获取各虚拟机 MAC 地址与安全域的对应关系；

- 30 第二接收模块，用于通过物理主机中的虚拟网桥接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的

目标虚拟机发送的, 所述网络报文中携带源 MAC 地址和目标 MAC 地址;

第二获取模块, 用于根据所述第二接收模块接收到的网络报文中携带的所述源 MAC 地址、所述目标 MAC 地址, 分别从所述第二策略获取模块获取到的各虚拟机 MAC 地址与安全域的对应关系中, 查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域;

第二发送控制模块, 用于在所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时, 控制所述虚拟网桥丢弃所述网络报文。

15、根据权利要求 14 所述的装置, 其特征在于, 所述第二发送控制模块包括:

第二发送单元, 用于当所述目标 MAC 地址为非广播地址时, 若所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同, 且所述第二获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同, 控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到所述物理主机上的目标虚拟机上;

第三丢弃单元, 用于当所述目标 MAC 地址为非广播地址时, 若所述第二获取模块获取到的所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同, 或所述第二获取模块获取到的所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同, 控制所述虚拟网桥丢弃所述网络报文。

16、根据权利要求 14 所述的装置, 其特征在于, 所述第二发送控制模块包括:

第二广播单元, 用于当所述目标 MAC 地址为广播地址时, 若所述第二获取模块获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同, 控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机;

第四丢弃单元, 用于当所述目标 MAC 地址为广播地址时, 若所述第二获取模块获取到的所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同, 控制所述虚拟网桥丢弃所述网络报文。

17、一种源主机, 包括处理器, 其特征在于, 还包括虚拟网桥和策略控制器, 其中:

所述策略控制器被配置用于从所处网络中的策略服务器中获取各虚拟机 MAC 地址与安全域的对应关系；

所述虚拟网桥被配置用于接收所述主机中的源虚拟机发送的网络报文，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

5 所述处理器被配置用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

10 18、根据权利要求 17 所述的源主机，其特征在于，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目
15 标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址发送所述网络报文；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

20 19、根据权利要求 17 所述的源主机，其特征在于，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同时，控制所
25 述虚拟网桥将所述网络报文通过物理交换机在局域网内广播；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

20、一种目标主机，包括处理器，其特征在于，还包括虚拟网桥和策略控制器，其中：

30 所述策略控制器被配置用于从所处网络中的策略服务器中获取各虚拟机 MAC 地址与安全域的对应关系；

所述虚拟网桥被配置用于接收物理交换机转发的网络报文，所述网络报文是另一物理主机中的源虚拟机向所述物理主机中的目标虚拟机发送的，所述网络报文中携带源 MAC 地址和目标 MAC 地址；

所述处理器被配置用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从所述策略控制器获取到的各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；在所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同时，控制所述虚拟网桥丢弃所述网络报文。

21、根据权利要求 20 所述的目标主机，其特征在于，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为非广播地址时，若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，且所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域相同，控制所述虚拟网桥根据所述目标 MAC 地址将所述网络报文发送到目标虚拟机上；若所述源虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，或所述目标虚拟机所属的安全域与所述虚拟网桥对应的安全域不同，控制所述虚拟网桥丢弃所述网络报文。

22、根据权利要求 20 所述的目标主机，其特征在于，所述处理器具体用于根据所述源 MAC 地址、所述目标 MAC 地址，分别从各虚拟机 MAC 地址与安全域的对应关系中，查询获得源虚拟机所属的安全域以及目标虚拟机所属的安全域；当所述目标 MAC 地址为广播地址时，若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域相同，控制所述虚拟网桥将所述网络报文转发给映射在所述虚拟网桥上的所有虚拟机；若所述虚拟网桥对应的安全域与所述源虚拟机所属的安全域不相同，控制所述虚拟网桥丢弃所述网络报文。

23、一种网络系统，包括权利要求 17-19 中任一项所述的源主机，权利要求 20-22 中任一项所述的目标主机，以及策略服务器，所述策略服务器被配置用于向所述源主机或所述目标主机中的策略控制器提供各虚拟机 MAC 地址与安全域的对应关系。

24、根据权利要求 23 所述的网络系统，其特征在于，所述策略服务器还

用于接收所述源主机或目标主机通过策略控制器上报的本机的 MAC 分组策略, 所述 MAC 分组策略包括虚拟机 MAC 地址与安全域的对应关系; 根据所述 MAC 分组策略更新本地的各虚拟机 MAC 地址与安全域的对应关系。

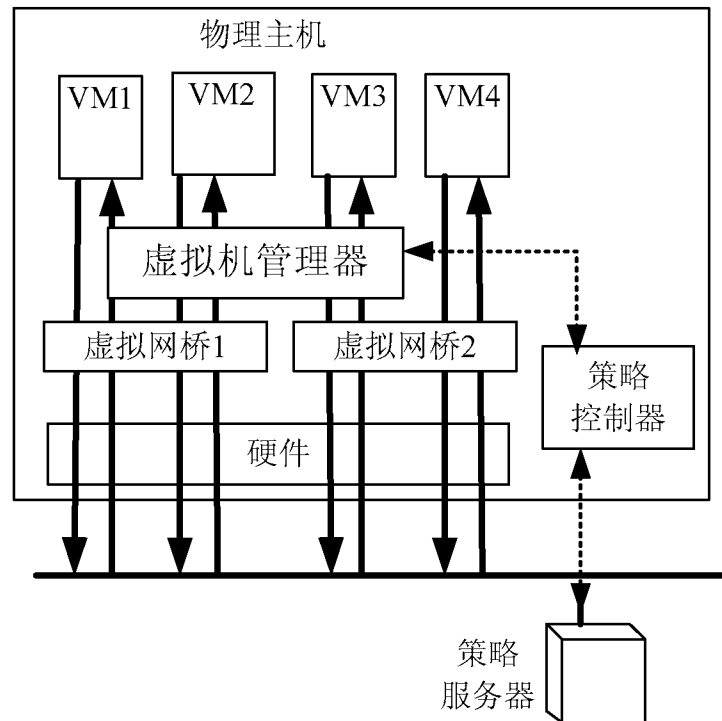


图 1a

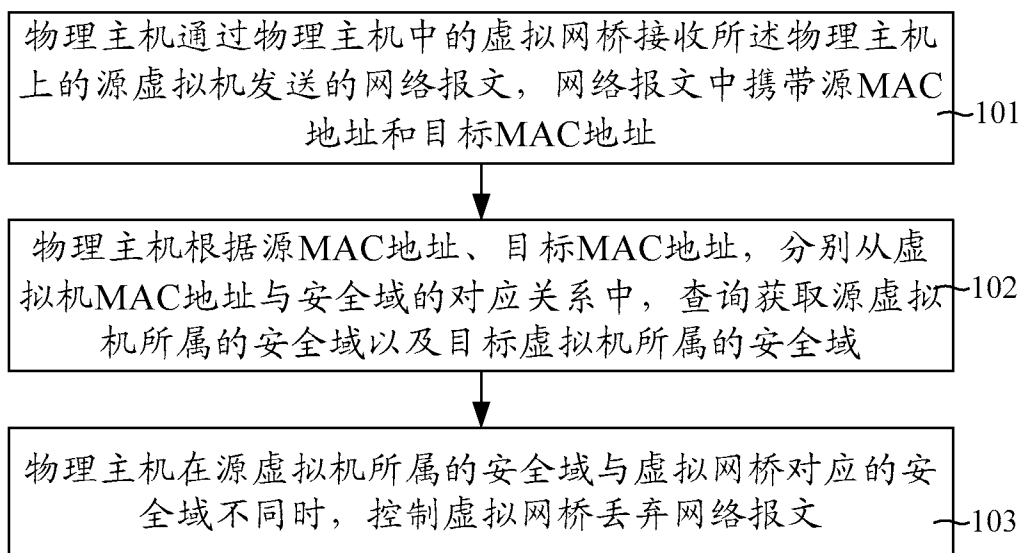


图 1b

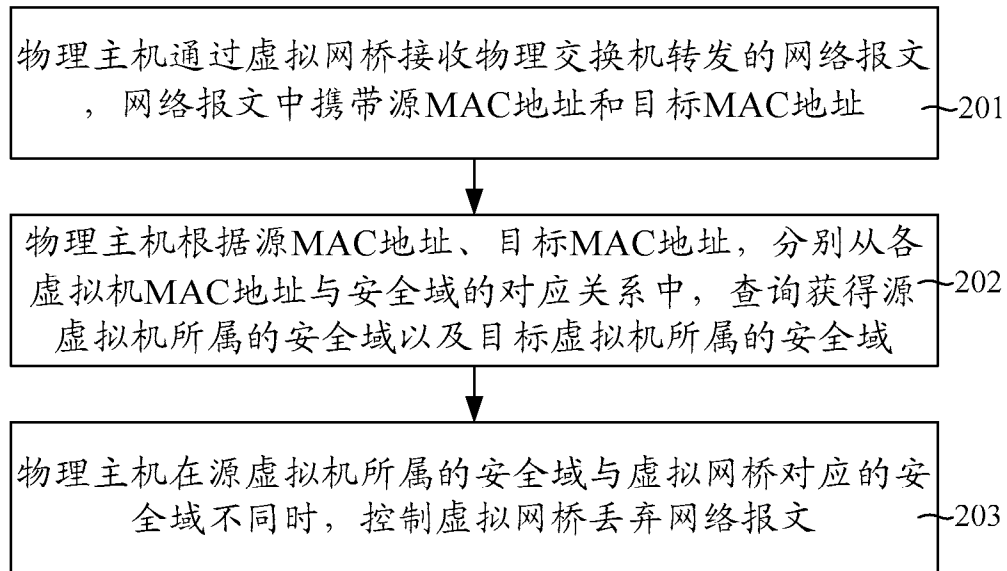


图 2

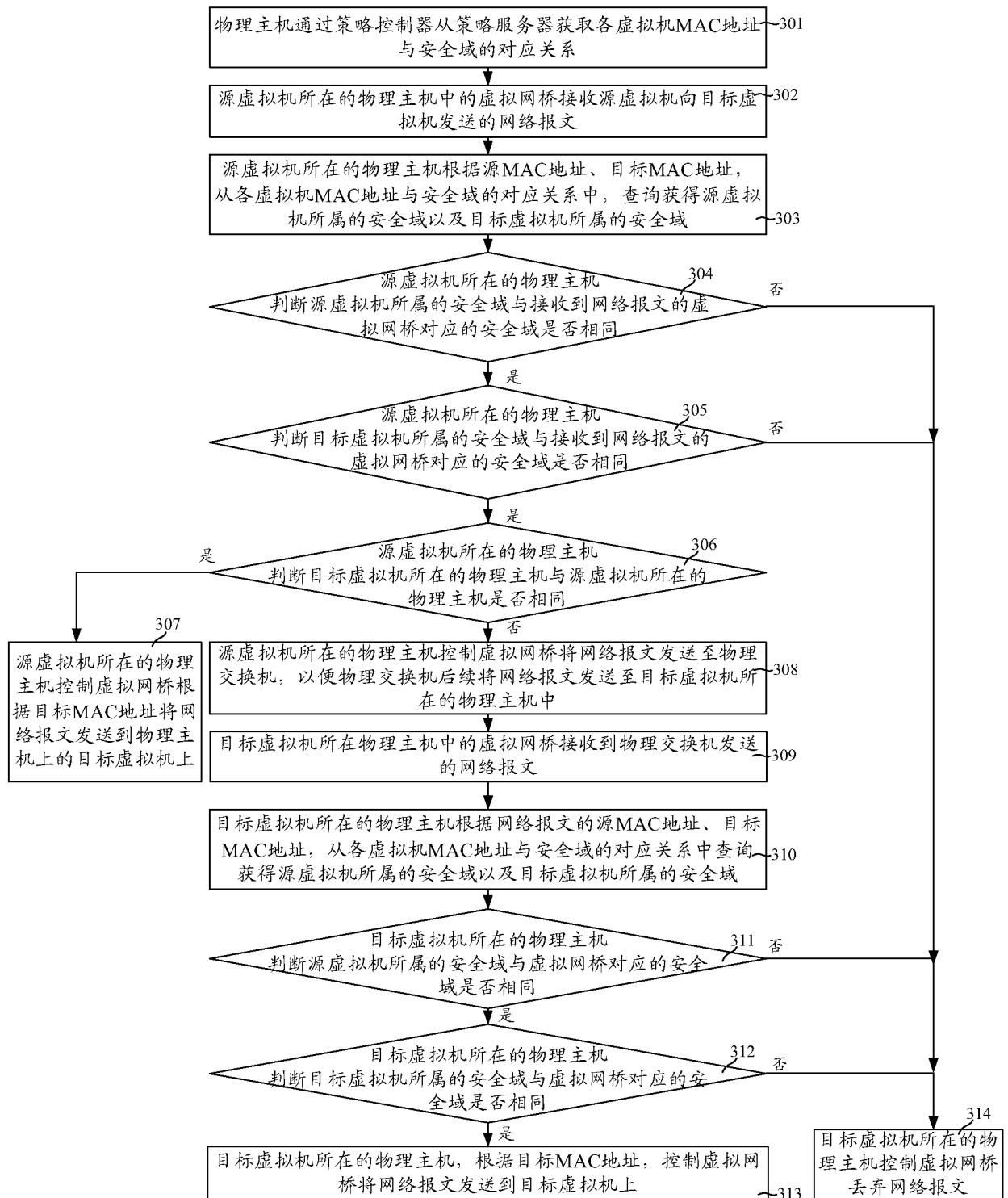


图 3

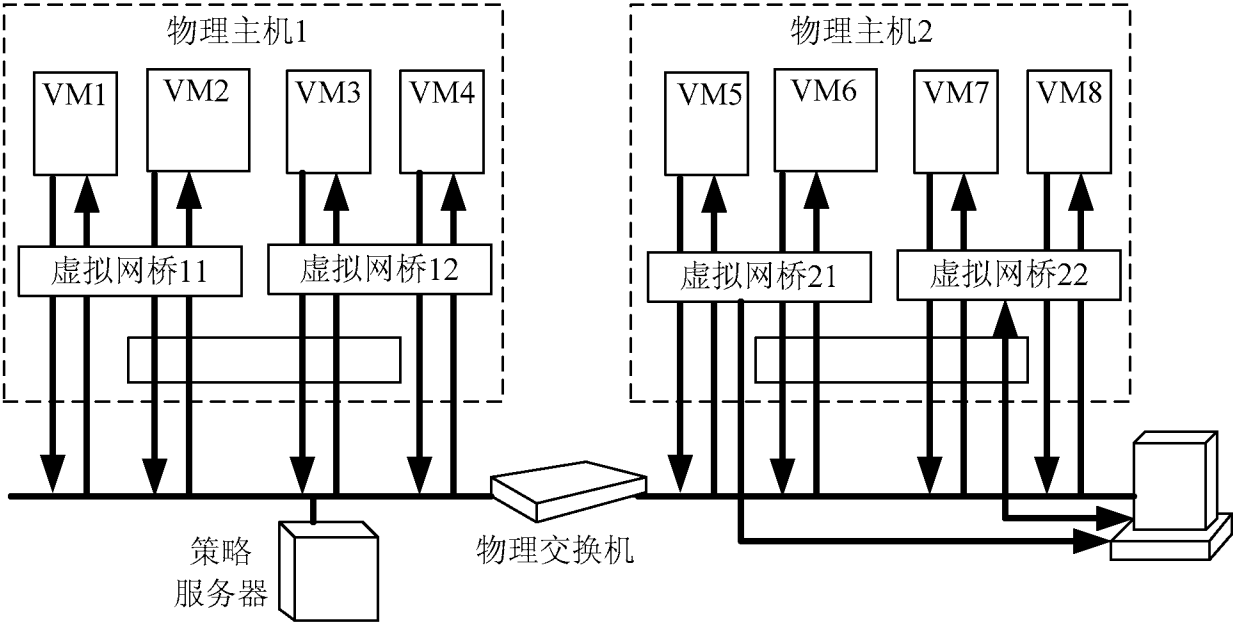


图 4

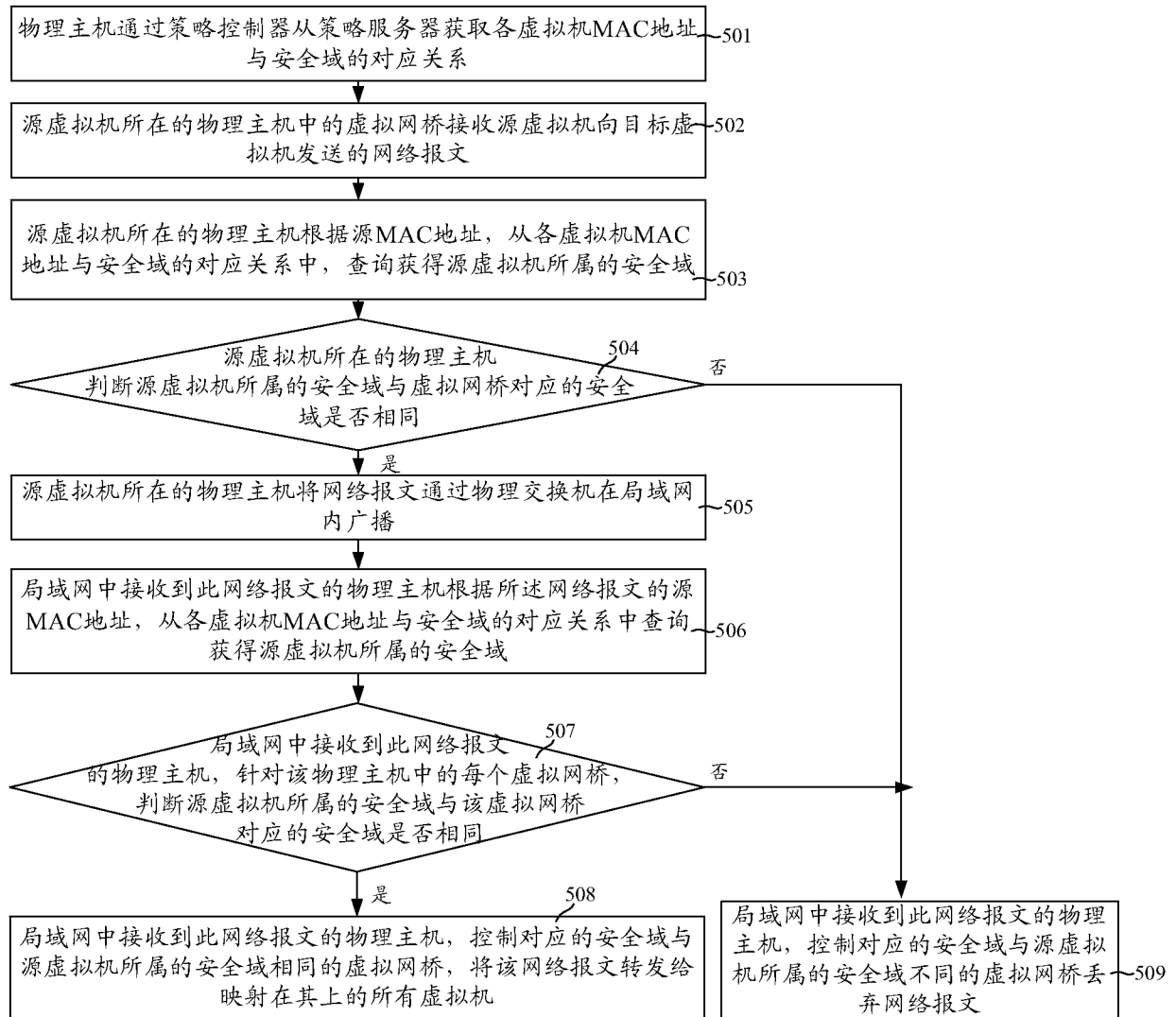


图 5

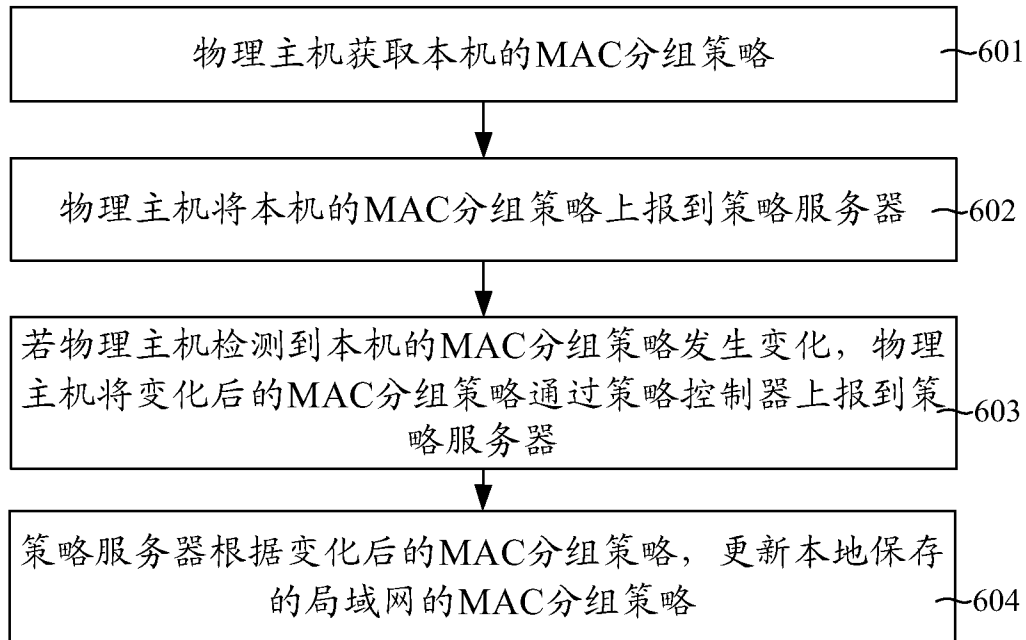


图 6

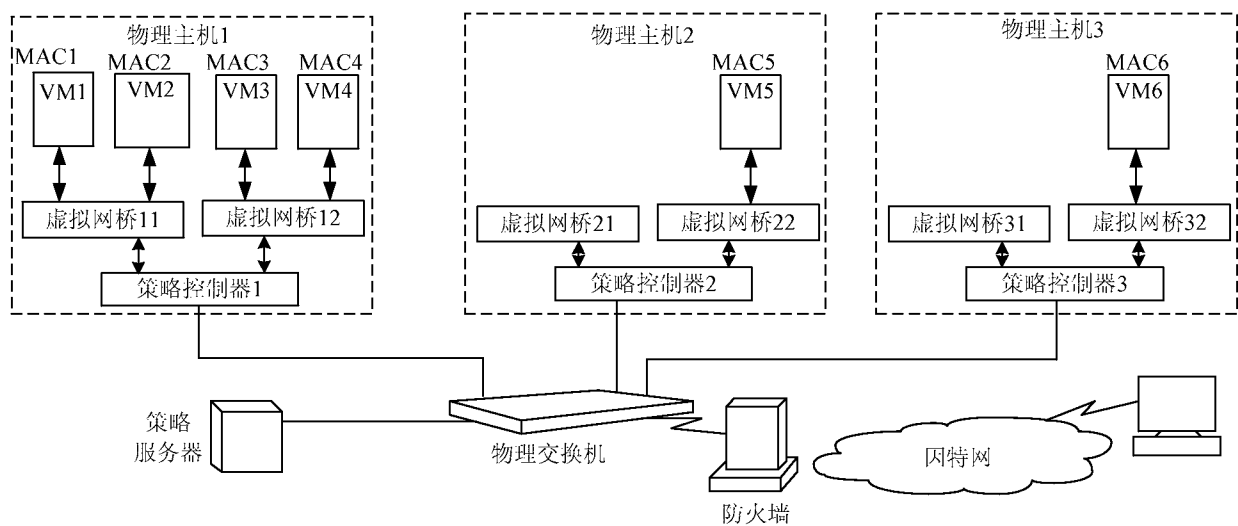


图 7

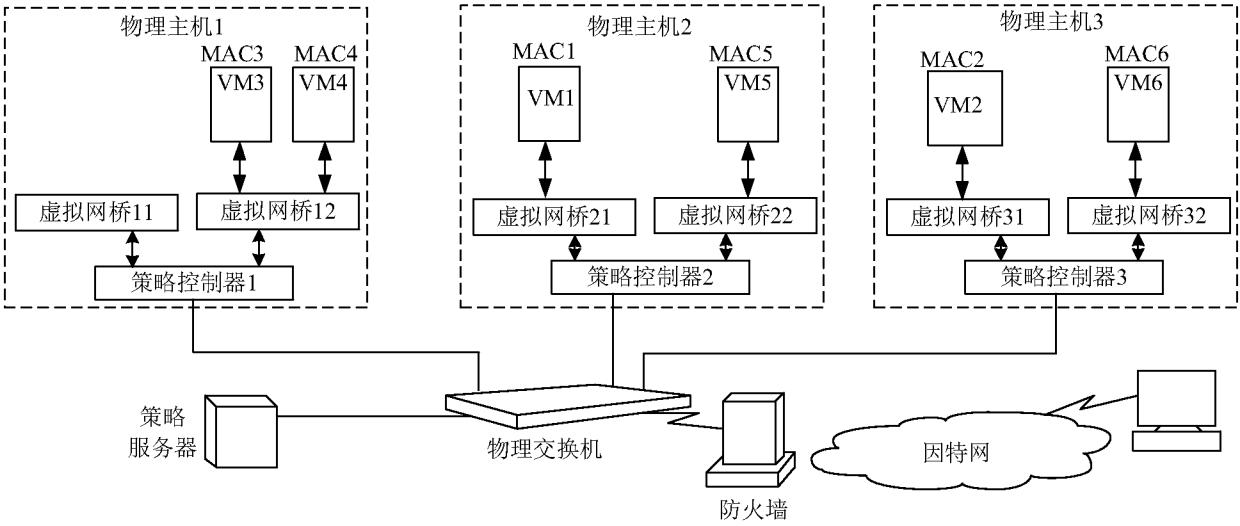


图 8

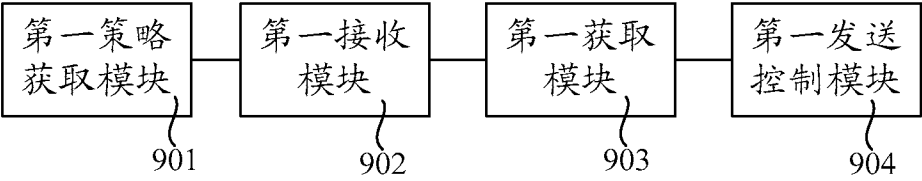


图 9

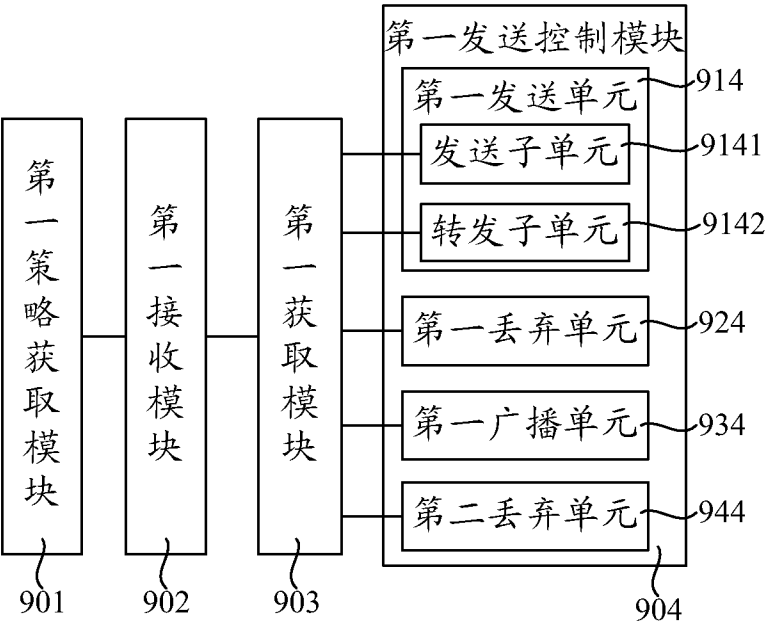


图 10

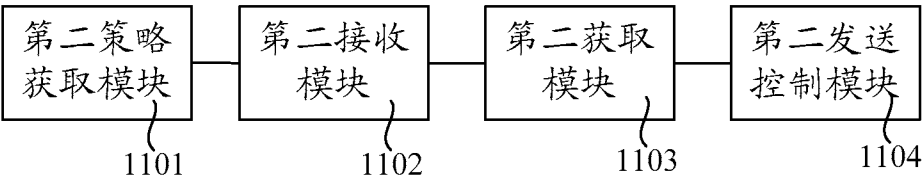


图 11

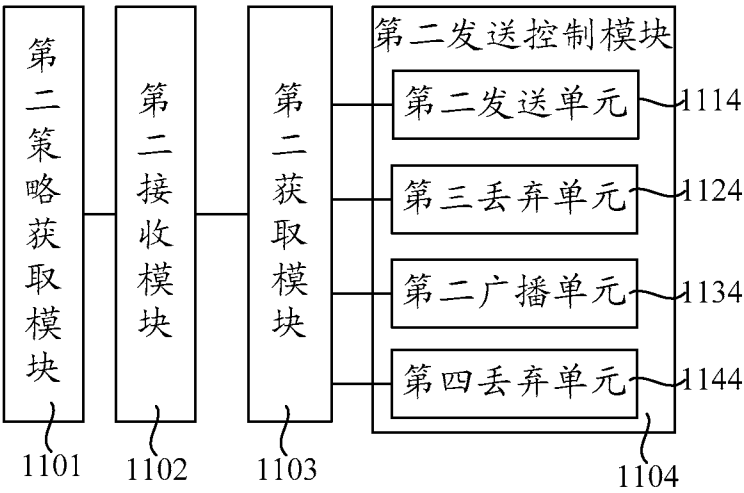


图 12

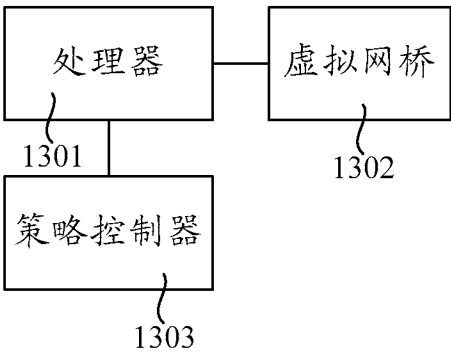


图 13

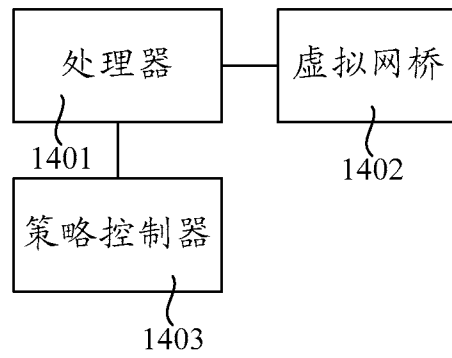


图 14

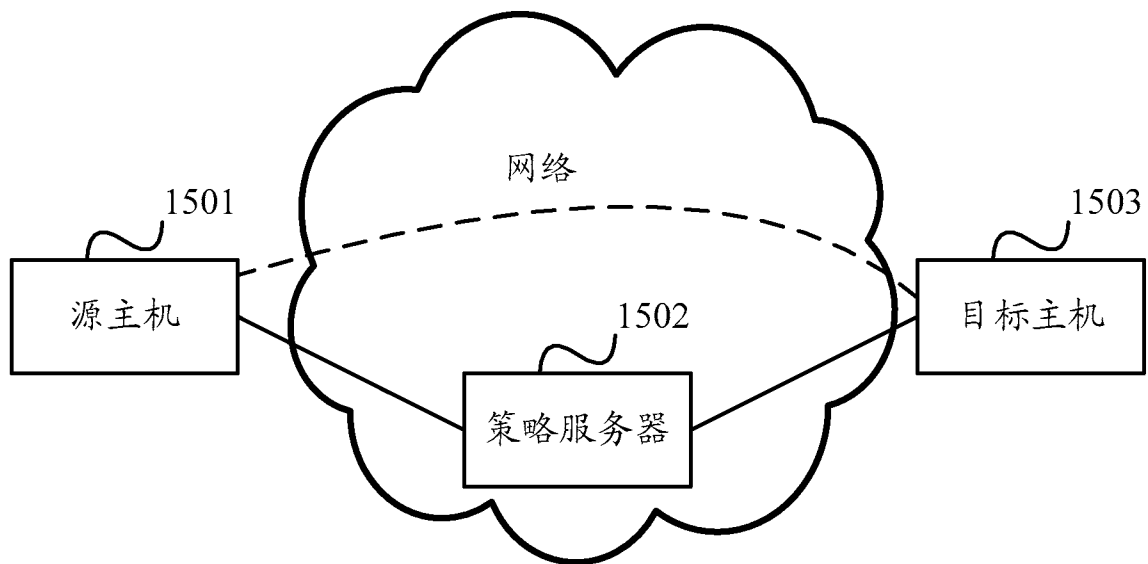


图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/077304

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; H04W; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS, CNKI, CNTXT, VEN: virtual bridge, MAC, security domain, mov+, roam+, virtual machine

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102150399 A (CISCO TECH INC.) 10 August 2011 (10.08.2011) , the whole document	1-24
A	CN 101951384 A (UNIV NANJING INFORMATION SCI&TECHNOLOG) 19 January 2011 (19.01.2011) , the whole document	1-24
A	CN 101739282 A (HUAWEI TECHNOLOGIES CO., LTD., SCHOOL OF SOFTWARE AND MICROEL) 16 June 2010 (16.06.2010) , the whole document	1-24
A	US 7447203 B2 (AT & T INTELLECTUAL PROPERTY I, L.P.) 14 November 2008 (14.11.2008) , the whole document	1-24

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 04 March 2013 (04.03.2013)	Date of mailing of the international search report 21 March 2013 (21.03.2013)
Name and mailing address of the ISA/CN State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer YANG, Hongli Telephone No. (86-10) 62411277

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/077304

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102150399 A	10.08.2011	WO 2010030877 A1	18.03.2010
		US 2010067374 A1	18.03.2010
		US 8134922 B2	13.03.2012
		CA 2733824 A1	18.03.2010
		EP 2324602 A1	25.05.2011
CN 101951384 A	19.01.2011	None	
CN 101739282 A	16.06.2010	None	
US 7447203 B2	04.11.2008	US 2005025143 A1	03.02.2005

国际检索报告

国际申请号
PCT/CN2012/077304

A. 主题的分类

H04L12/70(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L,H04W,G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS,CNKI ,CNTXT:虚拟网桥, MAC, 安全域, 虚拟机, 迁移, VEN: virtual bridge, MAC, security domain, mov+, roam+, virtual machine

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN102150399A (思科技术公司) 10.8 月 2011 (10.08.2011) 全文	1-24
A	CN101951384A (南京信息工程大学) 19.1 月 2011 (19.01.2011) 全文	1-24
A	CN101739282A (华为技术有限公司、北京大学软件与微电子学院) 16.6 月 2010 (16.06.2010) 全文	1-24
A	US7447203B2 (AT & T INTELLECTUAL PROPERTY I, L.,P.) 04.11 月 2008 (04.11.2008) 全文	1-24

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期
04.3 月 2013 (04.03.2013)

国际检索报告邮寄日期
21.3 月 2013 (21.03.2013)

ISA/CN 的名称和邮寄地址:
中华人民共和国国家知识产权局
中国北京市海淀区蓟门桥西土城路 6 号 100088
传真号: (86-10)62019451

受权官员

杨红丽
电话号码: (86-10) **62411277**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/077304

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN102150399A	10.08.2011	WO2010030877A1	18.03.2010
		US2010067374A1	18.03.2010
		US8134922B2	13.03.2012
		CA2733824A1	18.03.2010
		EP2324602A1	25.05.2011
CN101951384A	19.01.2011	无	
CN101739282A	16.06.2010	无	
US7447203B2	04.11.2008	US2005025143A1	03.02.2005