(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
2019 年 1 月 3 日 (03.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/000434 A1

(51) 国际专利分类号:
H04L 12/741 (2013.01) *G06F 9/48* (2006.01)

(21) 国际申请号: PCT/CN2017/091278

(22) 国际申请日: 2017 年 6 月 30 日 (30.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 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: 卢 胜 文 (LU, Shengwen); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, 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,

(54) **Title:** DATA PROCESSING METHOD, NETWORK INTERFACE CARD AND SERVER

(54) 发明名称: 一种数据处理方法、网络接口卡及服务器

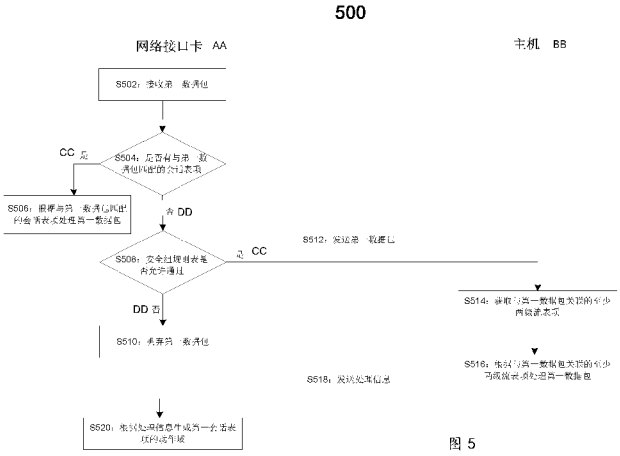

图 5

S502 RECEIVE A FIRST DATA PACKET
S504 IS THERE A SESSION ENTRY MATCHING THE FIRST DATA PACKET
S506 PROCESS THE FIRST DATA PACKET ACCORDING TO THE SESSION ENTRY MATCHING THE FIRST DATA PACKET
S508 DOES A SECURITY GROUP RULE TABLE ALLOW SAME TO PASS
S510 DISCARD THE FIRST DATA PACKET
S512 SEND THE FIRST DATA PACKET
S514 ACQUIRE AT LEAST TWO STAGES OF FLOW ENTRIES ASSOCIATED WITH THE FIRST DATA PACKET
S516 PROCESS THE FIRST DATA PACKET ACCORDING TO AT LEAST TWO STAGES OF FLOW ENTRIES ASSOCIATED WITH THE FIRST DATA PACKET
S518 SEND PROCESSING INFORMATION
S520 GENERATE AN ACTION FIELD OF A FIRST SESSION ENTRY ACCORDING TO THE PROCESSING INFORMATION
AA NETWORK INTERFACE CARD
BB HOST
CC YES
DD NO

(57) **Abstract:** Provided are a data processing method, a network interface card and a server. The method comprises: a host receiving a first data packet sent by a network interface card, acquiring at least two flow entries associated with the first data packet, generating processing information according to the at least two flow entries, and sending the processing information to the network interface card. The network interface card generates an action field of a first session entry according to the processing information, and also generates a matching field of the first session entry according to matching information about the first data packet, wherein the first session entry

WO 2019/000434 A1

[见续页]

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, KM, 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))。

is used for recording a rule for the network interface card to process the data packet matching the first session entry. According to the action fields of multiple flow entries associated with the data packet, an action field of one session entry is obtained by means of combination, and the processing function for the data packet is offloaded onto the network interface card for implementation, thereby saving on the hardware resources of a server and simplifying the processing flow for the data packet.

(57) 摘要: 本发明实施例提供了一种数据处理方法、网络接口卡及服务器。该方法包括：主机接收网络接口卡发送的第一数据包，获取与第一数据包关联的至少两个流表项，根据至少两个流表项生成处理信息，并向网络接口卡发送处理信息。网络接口卡根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域。第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。根据与数据包关联的多个流表项的动作域，合并一个会话表项的动作域，并将对数据包的处理功能卸载到网络接口卡实现，从而节约了服务器的硬件资源，且简化了对数据包的处理流程。

一种数据处理方法、网络接口卡及服务器

技术领域

本申请涉及计算机领域，尤其涉及一种数据处理方法、网络接口卡（英文全称：network interface card，缩写：网络接口卡）及服务器。

背景技术

云计算环境中，需要对数量较高的用户提供服务，用于提供云服务的数据中心中的服务器的数量往往较多。每个服务器上运行多个虚拟机（英文全称：virtual machine，缩写：VM），租户租借的虚拟机需要能够对外通信，并且与其它的虚拟机隔离。虚拟机与其他服务器上运行的虚拟机或同一服务器上的虚拟机之间通过虚拟交换机（英文全称：virtual switch，缩写：VS）通信，当前常见的虚拟交换机包括 open vSwitch（OVS）。软件定义网络（英文全称：software defined networking，缩写：SDN）控制器通常通过 OpenFlow 协议定义的流表（英文全称：flow table）对各个虚拟交换机进行控制。

每个服务器上的硬件资源至少需要支持运行多个 VM、虚拟交换机以及虚拟机监视器（英文全称：virtual machine monitor，缩写：VMM），虚拟机监视器又称为虚拟机管理器（英文全称：virtual machine manager，缩写：VMM）或管理程序（英文全称：hypervisor）。每台服务器的硬件资源有限，如果负担了数据交换任务的虚拟交换机占用的硬件资源太多，则容易影响服务器上 VM 的运行，降低工作效率。

发明内容

有鉴于此，本申请公开了一种数据处理方法、网络接口卡及服务器。根据与数据包关联的多个流表项的动作域，生成一个会话表项的动作域，并将对数据包的处理功能卸载到网络接口卡实现。

第一方面，本申请提供了一种服务器，服务器包含主机和网络接口卡，主机上运行有虚拟机和虚拟交换机。网络接口卡通过主机接口与主机相连，通过网络接口与外部网络相连。主机用于接收网络接口卡发送的第一数据包，根据第一数据包携带的匹配信息获取与第一数据包关联的至少两个流表项。主机还用于根据该至少两个流表项生成处理信息，并通过主机接口向网络接口卡发送该处理信息，该处理信息用于指示虚拟交换机根据该至少两个流表项对第一数据包的处理操作。网络接口卡用于根据处理信息生成第一会话表项的动作域，还用于根据第一数据包的匹配信息生成第一会话表项的匹配域，其中，第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。

其中第一数据包可以为网络接口卡通过主机接口从虚拟机接收的数据包或通过网络接口从外部网络接收的数据包。

服务器根据与数据包关联的至少两个流表项的动作域，生成一个会话表项的动作域，并将对数据包的处理功能卸载到网络接口卡实现，从而节省了主机的硬件资源。

根据第一方面，在第一方面第一种可能的实现方式中，网络接口卡还用于接收第二数据包，根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。其中，第二数据包与第一数据包属于相同的数据流，具有相同的匹配信息。

网络接口卡只需要查询与数据包匹配的一个会话表项，就可以实现对数据包的处理操作，从而简化了数据包处理流程。

根据第一方面或第一方面第一种可能的实现方式，在第一方面第二种可能的实现方式中，主机接收网络接口卡发送的第一数据包之前，网络接口卡还用于接收第一数据包，根据匹配信息查询记录的会话表项，并在没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

网络接口卡维护有一个会话表。不同的数据流具有不同的匹配信息，且不同的数据流可能有不同的处理方式，每一个会话表项对应一个数据流。网络接口卡接收到数据包后，会根据数据包携带的匹配信息查询会话表。如果找到了与数据包匹配的会话表项，则根据会话表项动作域记载的信息处理该数据包。如果没有查询到与数据包对应的会话表项，则该第一数据包为该第一数据包所在的数据流的首个数据包，或该第一数据包不是该数据流的首个数据包，但该数据流对应的会话表项在会话表中已经被删除，数据接口卡将第一数据包上报给主机上运行的虚拟交换机处理。

根据第一方面或第一方面以上任一种可能的实现方式，在第一方面第三种可能的实现方式中，网络接口卡还用于查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。

安全组规则用于实现安全过滤规则，将安全组规则也卸载到网络接口卡上，网络接口卡可以根据该第一会话表项对匹配的数据包进行多项处理，从而简化了数据包的处理流程。

根据第一方面第三种可能的实现方式，在第一方面第四种可能的实现方式中，主机配置有安全组功能；主机还用于查询与第一数据包匹配的安全组规则，并向网络接口卡发送第一数据包匹配的安全组规则。

如果安全组规则配置在主机上，则主机可以根据第一数据包的匹配信息查询第一数据包的安全组规则，并将第一数据包的安全组规则通过主机接口传递给网络接口卡。

根据第一方面第三种或第四种可能的实现方式，在第一方面第五种可能的实现方式中，如果安全组规则包含正反向允许通过的防火墙规则，网络接口卡还用于创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

第二会话表项的动作域可以设置为上传主机或者设置为空，后续会根据虚拟交换机对反向数据包的实际处理更新第二会话表的动作域，第一会话表项和第二会话表项也可以合并成一条记录，动作域区分正向和反向 2 个域，例如可以设定 VM 发出方向为正向，网络侧过来的方向为反向，查反向表时交换源节点信息和目的节点信息。

根据第一方面或第一方面以上任一种可能的实现方式，在第一方面第六种可能的实现方式中，主机还用于在修改至少两个流表项中的一个流表项后，向网络接口卡发送修改指令，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作；网络接口卡还用于根据修改指令修改第一会话表项。

服务器可以根据链表技术把会话表项链接到虚拟交换机的流表项，当虚拟交换机的

的表项删除或修改的时候，主机会通知网络接口卡去同步删除或者修改会话表。

根据第一方面或第一方面以上任一种可能的实现方式，在第一方面第七种可能的实现方式中，若第一会话表项在超过预设时间阈值的时间段内未被访问，网络接口卡还用于删除第一会话表项。

因为网络接口卡的存储空间有限，或者分配给会话表的存储空间有限，当一个会话表项长时间未被访问时，则启动老化机制，即将一段时间未被访问的会话表项删除，从而节省存储空间。

根据第一方面第七种可能的实现方式，在第一方面第八种可能的实现方式中，网络接口卡删除第一会话表项后，还用于向主机发送删除指令；主机还用于根据删除指令删除至少两个流表项。

根据流表的老化机制，长时间不访问的流表项将会自动老化，流表项老化后，会话表项就会跟着删除，这样的话，会话表就不断的要重新创建、删除。主机可以对流表的老化进行设置，可以设置很长的老化时间或者不老化。当会话表项老化（即被删除）后，就可以通知主机将与会话表项对应的流表项进行老化。

第二方面，本申请提供了一种数据处理方法，服务器包含运行有虚拟交换机的主机和网络接口卡，该方法包括：主机接收网络接口卡发送的第一数据包，获取与第一数据包关联的至少两个流表项，根据至少两个流表项生成处理信息，并向网络接口卡发送处理信息。网络接口卡根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域。第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。

根据第二方面，在第二方面第一种可能的实现方式中，该方法还包括：网络接口卡接收第二数据包，第二数据包与第一数据包具有相同的匹配信息。网络接口卡根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

根据第二方面或第二方面第一种可能的实现方式，在第二方面第二种可能的实现方式中，主机接收网络接口卡发送的第一数据包之前，该方法还包括：网络接口卡接收第一数据包，根据匹配信息查询记录的会话表项，并在没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

根据第二方面或第二方面以上任一种可能的实现方式，在第二方面第三种可能的实现方式中，该方法还包括：网络接口卡查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。

根据第二方面第三种可能的实现方式，在第二方面第四种可能的实现方式中，主机配置有安全组功能；该方法还包括：主机查询与第一数据包匹配的安全组规则，并向网络接口卡发送第一数据包匹配的安全组规则。

根据第二方面第三种或第四种可能的实现方式，在第二方面第五种可能的实现方式中，如果安全组规则包含正反向允许通过的防火墙规则，该方法还包括：网络接口卡创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

根据第二方面或第二方面以上任一种可能的实现方式，在第二方面第六种可能的实现方式中，该方法还包括：主机在修改至少两个流表项中的一个流表项后，向网络接口卡发送修

改指令。修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作。网络接口卡根据修改指令修改第一会话表项。

根据第二方面或第二方面以上任一种可能的实现方式，在第二方面第七种可能的实现方式中，该方法还包括：若第一会话表项在超过预设时间阈值的时间段内未被访问，网络接口卡删除第一会话表项。

根据第二方面第七种可能的实现方式，在第二方面第八种可能的实现方式中，网络接口卡删除第一会话表项后，方法还包括：网络接口卡向主机发送删除指令；主机根据删除指令删除至少两个流表项。

第二方面或第二方面任一种可能的实现方式为第一方面或第一方面任一种可能的服务器实现方式对应的方法，第一方面或第一方面任一种可能的实现方式中的描述对应适用于第二方面或第二方面任一种可能的实现方式，在此不再赘述。

第三方面，本发明提供了一种数据处理方法，该方法包括：网络接口卡向主机发送第一数据包。网络接口卡接收来自主机的处理信息，处理信息用于指示主机根据与第一数据包匹配的至少两个流表项对第一数据包的处理操作。网络接口卡根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域。第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。

根据第三方面，在第三方面第一种可能的实现方式中，该方法还包括：网络接口卡接收第二数据包，第二数据包与第一数据包具有相同的匹配信息。网络接口卡根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

根据第三方面或第三方面第一种可能的实现方式，在第三方面第二种可能的实现方式中，该方法包括：网络接口卡接收第一数据包，根据匹配信息查询记录的会话表项，并在没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

根据第三方面或第三方面以上任一种可能的实现方式，在第三方面第三种可能的实现方式中，该方法还包括：网络接口卡查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。

根据第三方面第三种可能的实现方式，在第三方面的第四种可能的实现中，如果安全组规则包含正反向允许通过的防火墙规则，该方法还包括：网络接口卡创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

根据第三方面或第三方面以上任一种可能的实现方式，在第三方面第五种可能的实现方式中，该方法还包括：网络接口卡接口卡接收来自主机的修改指令，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作；网络接口卡根据修改指令修改第一会话表项。

根据第三方面或第三方面以上任一种可能的实现方式，在第三方面第六种可能的实现方式中，该方法还包括：若第一会话表项在超过预设时间阈值的时间段内未被访问，网络接口卡删除第一会话表项。

根据第三方面第六种可能的实现方式，在第三方面的第七种可能的实现中，网络接口卡删除第一会话表项后，方法还包括：网络接口卡向主机发送删除指令，删除指令用于指示主机删除至少两个流表项。

第三方面或第三方面任一种可能的实现方式为第一方面或第一方面任一种可能的服务器

实现方式对应的网络接口卡侧方法，第一方面或第一方面任一种可能的实现方式中的描述对应适用于第三方面或第三方面任一种可能的实现方式，在此不再赘述。

第四方面，本发明提供了一种网络接口卡，该网络接口卡包括：发送单元，用于向主机发送第一数据包；接收单元，用于接收来自主机的处理信息，处理信息用于指示主机根据与第一数据包匹配的至少两个流表项对第一数据包的处理操作；处理单元，用于根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域，第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。

根据第四方面，在第四方面第一种可能的实现方式中，接收单元还用于接收第二数据包，第二数据包与第一数据包具有相同的匹配信息；处理单元还用于根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

根据第四方面或第四方面第一种可能的实现方式，在第四方面第二种可能的实现方式中，发送单元向主机发送第一数据包之前，接收单元还用于接收第一数据包；处理单元还用于根据匹配信息查询记录的会话表项；发送单元还用于在处理单元没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

根据第四方面或第四方面以上任一种可能的实现方式，在第四方面第三种可能的实现方式中，处理单元还用于查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。

根据第四方面第三种可能的实现方式，在第四方面的第四种可能的实现中，如果安全组规则包含正反向允许通过的防火墙规则，处理单元还用于创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

根据第四方面或第四方面以上任一种可能的实现方式，在第四方面第五种可能的实现方式中，接收单元还用于接收来自主机的修改指令，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作；处理单元还用于根据修改指令修改第一会话表项。

根据第四方面或第四方面以上任一种可能的实现方式，在第四方面第六种可能的实现方式中，若第一会话表项在超过预设时间阈值的时间段内未被访问，处理单元还用于删除第一会话表项。

根据第四方面第六种可能的实现方式，在第四方面的第七种可能的实现中，处理单元删除第一会话表项后，还用于向主机发送删除指令，删除指令用于指示主机删除至少两个流表项。

第四方面或第四方面任一种可能的实现方式为第一方面或第一方面任一种可能的服务器实现方式对应的网络接口卡，第一方面或第一方面任一种可能的实现方式中的描述对应适用于第四方面或第四方面任一种可能的实现方式，在此不再赘述。

第五方面，本发明提供了一种网络接口卡，包括：主机接口、处理器、存储器；主机接口用于连接主机；处理器用于通过主机接口向主机发送第一数据包；主机接口还用于通过主机接口接收来自主机的处理信息，处理信息用于指示主机根据与第一数据包匹配的至少两个流表项对第一数据包的处理操作；处理器还用于根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域，第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则；存储器用于存储第一会话表项。

根据第五方面，在第五方面第一种可能的实现方式中，网络接口卡还包括网络接口，网络接口用于连接外部网络；处理器还用于通过主机接口或网络接口接收第二数据包，第二数据包与第一数据包具有相同的匹配信息；处理器还用于根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

根据第五方面或第五方面第一种可能的实现方式，在第五方面第二种可能的实现方式中，网络接口卡还包括网络接口，网络接口用于连接外部网络；处理器通过主机接口向主机发送第一数据包之前，还用于通过主机接口或网络接口接收第一数据包，根据匹配信息查询记录的会话表项，并在没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

根据第五方面或第五方面以上任一种可能的实现方式，在第五方面第三种可能的实现方式中，处理器还用于查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。

根据第五方面第三种可能的实现方式，在第五方面的第四种可能的实现中，如果安全组规则包含正反向允许通过的防火墙规则，处理器还用于创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

根据第五方面或第五方面以上任一种可能的实现方式，在第五方面第五种可能的实现方式中，处理器还用于通过主机接口接收来自主机的修改指令，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作；处理器还用于根据修改指令修改第一会话表项。

根据第五方面或第五方面以上任一种可能的实现方式，在第五方面第六种可能的实现方式中，若第一会话表项在超过预设时间阈值的时间段内未被访问，处理器还用于删除第一会话表项。

根据第五方面第六种可能的实现方式，在第五方面的第七种可能的实现中，处理器删除第一会话表项后，还用于通过主机接口向主机发送删除指令，删除指令用于指示主机删除至少两个流表项。

第五方面或第五方面任一种可能的实现方式为第一方面或第一方面任一种可能的服务器实现方式对应的网络接口卡，第一方面或第一方面任一种可能的实现方式中的描述对应适用于第五方面或第五方面任一种可能的实现方式，在此不再赘述。

根据本申请公开的技术方案，数据包的处理过程中的一部分运行压力被转移到了网络接口卡上，而网络接口卡作为一个硬件设备，不仅处理效率高，并且其运行无需占用硬件层的其他资源。且本申请将虚拟交换机根据多个流表项对数据处理的处理信息记录在一个会话表项中，网络接口卡只需要一个会话表项就可以实现对匹配数据包的处理，简化了处理流程。

附图说明

图 1 为一种数据中心架构的示意图；

图 2 为一种服务器的组织结构示意图；

图 3 为依据本发明一实施例的服务器的组织结构示意图；

图 4 为依据本发明一实施例的服务器的硬件结构示意图；

图 5 为为依据本发明一实施例的数据包处理方法的流程示意图

图 6 为依据本发明一实施例的服务器的组织结构示意图；

图 7 为依据本发明一实施例的数据包处理方法的流程示意图；

图 8 为依据本发明一实施例的网络接口卡的逻辑结构示意图；

图 9 为依据本发明一实施例的网络接口卡的硬件结构示意图。

具体实施方式

下面将结合附图，对本发明实施例进行描述。

本发明实施例采用术语第一和第二等来区分各个对象，例如第一数据包和第二数据包等，但各个“第一”和“第二”之间不具有逻辑或时序上的依赖关系。

在本发明实施例中，数据包由匹配信息和载荷（英文全称：payload）构成。其中，匹配信息用于与流表或者会话表的匹配域进行匹配。

在本发明实施例中，服务器上的硬件层设置有网络接口卡，处理器，输入/输出设备以及存储设备。服务器除网络接口卡之外的部分称之为主机。

在本发明实施例中，虚拟交换机为运行在服务器的主机上的，通过软件实现的交换设备，常用于SDN中。常见的虚拟交换机包括OVS。

在本发明实施例中，流表用于在SDN中控制数据流，也可以称为SDN流表，具体可以采用符合OpenFlow协议的流表或符合其他协议的流表。流表的流表项包括匹配域和动作域，该匹配域用于与数据包进行匹配，该动作域用于指示虚拟交换机根据匹配结果对数据包进行处理。动作域可以包含对匹配数据包的处理信息，例如转发、丢弃、上送SDN控制器等，还可以包含数据包的路由信息，例如数据包的目的端口标识等。在本发明实施例中，流表的动作域可以包含OpenFlow协议支持的任意动作，本发明对此不进行限定。

在本发明实施例中，虚拟交换机可访问的流表集合包含至少两个流表，虚拟交换机使用根据流表集合中的流表对数据包进行处理。具体的，一个数据包可能与多个流表中的多个流表项关联，虚拟交换机接收到网络接口卡发送的数据包后，可以查询与该数据包关联的多个流表项，并根据该多个流表项依次对该数据包进行处理。

在本发明实施例中，会话表用于网络接口卡（英文全称：network interface card，缩写：NIC）控制数据流。会话表的会话表项包括匹配域和动作域，匹配域用于匹配数据包，动作域用于指示网络接口卡对匹配上的数据包进行处理。会话表项的动作域是根据与数据包关联的多个流表项的动作域生成的。

在本发明实施例中，流表集合一般存储于服务器的存储设备中，会话表可以存储于服务器的存储设备中，也可以存储于网络接口卡内部的存储设备中。若流表集合和会话表均存储于服务器的存储设备中，服务器在其存储设备中为流表集合和会话表分别开辟一块存储空间。本发明实施例中，以会话表存储于网络接口卡内部为例进行介绍，本领域技术人员可以直接推导出会话表存储于服务器的存储设备的情况。

在本发明实施例中，数据流（英文全称：data flow）指示携带相同的匹配信息的一系列数据包。具体的，同一数据流中的数据包的匹配信息，均可以匹配上该数据流对应的流表项的匹配域或会话表项的匹配域。

在本发明实施例中，示例性的采用了SR-IOV（英文全称：single-root I/O virtualization）的网络接口卡与VM直连的技术，在实际使用中也可以采用其他支持网络接口卡与VM直连的技术。

在本发明实施例中，与数据包关联的流表项是指虚拟交换机对该数据包处理的流程中需要使用的流表项。该流表项可以具体为 OVS 转发流表项。例如，虚拟交换机首先根据数据包 1 的匹配信息在流表 1 中查询与该数据包 1 匹配的流表项 1，并根据流表项 1 动作域记录的信息对该数据包 1 进行处理操作得到数据包 2，然后再根据数据包 2 的匹配信息在流表 2 中查询与该数据包 2 匹配的流表项 2，并根据流表项 2 动作域记录的信息对该数据包 2 进行处理操作，则流表项 1 和流表项 2 都是与数据包 1 关联的数据包。其中，如果虚拟交换机根据流表项 1 动作域记录的信息对数据包 1 进行了修改操作，则数据包 2 与数据包 1 是不同的，如果虚拟交换机没有根据流表项 1 对数据包 1 进行修改操作，则数据包 2 与数据包 1 是相同的。

数据中心中每个服务器上的硬件资源需要支持运行多个虚拟机、虚拟交换机以及虚拟机监视器。每台服务器的硬件资源有限，如果负担了数据交换任务的虚拟交换机占用的硬件资源太多，则容易影响服务器上虚拟机的运行，降低工作效率。为了减轻服务器硬件的负担，可以将虚拟交换机的业务卸载到网络接口卡上来实现。

在 OpenFlow 协议中，虚拟交换机的功能非常灵活，对数据包的不同处理操作被记录在不同的流表项中，虚拟交换机维护有与数据包关联的多个流表项。由于硬件很难实现大规模的支持掩码匹配的流表，并且多个流表的查找也很影响性能。如果将虚拟交换机上的业务直接卸载到网络接口卡上，例如将虚拟交换机的流表直接复制到网络接口卡，则大量的流表会导致网络接口卡负载过大，达不到优化的目的。

本发明实施例中，根据与数据包关联的多个流表项的动作域，合并一个会话表项的动作域，并将对数据包的处理功能卸载到网络接口卡实现。网络接口卡只需要查询与数据包匹配的一个会话表项，就可以实现对数据包的处理操作，从而节约了服务器的硬件资源，且简化了对数据包的处理流程。

图 1 为依据本发明一实施例的 SDN 架构的示意图，图 1 中示意性的采用了集中式的 SDN 控制器，实际中 SDN 控制器也可以分布式的部署于各个服务器。

每个主机运行时，其硬件层支持软件层内的虚拟交换机以及多个虚拟机的运行。每个服务器内的主机和网络接口卡建立通信连接，主机通过网络接口卡与外部网络通信，例如，首先由网络接口卡从外部网络获取数据包，然后发送至主机上运行的 VM，而该主机上运行的 VM 发往外部网络的数据包也会发送至网络接口卡，通过网络接口卡发送至外部网络。

下面以服务器 200 和服务器 300 为例，展示虚拟交换机的功能是否卸载到网络接口卡对数据处理流程的影响。

如图 2，如果不将虚拟交换机的功能卸载到网络接口卡，服务器 200 内的网络接口卡从外部网络接收到数据包后，如果判断该数据包的目的地属于服务器 200，则将该数据包发送至虚拟交换机，则由虚拟交换机将该数据包与流表集合中的流表进行匹配，并根据匹配上的流表项的指示，将该数据处理后发送至与该虚拟交换机相连的目的 VM。

由以上数据包的处理流程可见，数据处理过程中主要的运行压力集中在虚拟交换机上，而虚拟交换机的运行依赖于服务器上的硬件层的资源，虚拟交换机占用的处理器和存储设备资源越多，服务器上能够用于 VM 运行的资源就越少，而如果限定虚拟交换机能够占用的硬件层的资源的上限，那么随着数据包流量的增大，虚拟交换机的性能将难以保证。

如图 3，本发明实施例提供的数据处理流程中，服务器 300 内的网络接口卡从外部网络

接收到数据包后，如果判断该数据包的目的VM运行于服务器300上，则在会话表中查找与该数据包匹配的会话表项，并根据该数据包匹配的会话表项的指示，将该数据处理后发送至与该网络接口卡相连的目的VM。

会话表项的动作域来源于与数据包匹配的多个流表项的动作域的结合。如果网络接口卡未查询到与接收到的数据包匹配的会话表项，就会将该数据包发送至虚拟交换机，虚拟交换机查询与该数据包匹配的多个流表项，根据查询到的多个流表项处理该数据包，并向网络接口卡发送根据与该数据包匹配的流表项生成的处理信息。

如果虚拟交换机查询不到与该数据包匹配的流表项，则向SDN控制器请求获取该数据包对应的流表项，并根据从SDN控制器获取到的多个流表项处理该数据包，并向网络接口卡发送根据获取的流表项生成的处理信息。

网络接口卡根据该处理信息生成与该数据包的匹配信息匹配的一个会话表项的动作域，以供后续的使用。

由以上数据包的处理流程可见，在本申请提供的数据处理流程中，数据包的处理过程中的一部分运行压力被转移到了网络接口卡上，而网络接口卡作为一个硬件设备，不仅处理效率高，并且其运行无需占用硬件层的其他资源。且本申请将虚拟交换机根据多个流表项对数据处理的处理信息记录在一个会话表项中，简化了处理流程，网络接口卡只需要一个会话表项就可以实现对匹配数据包的处理。

需要说明的是，示意性的，图3中的服务器300上的所有VM都可以与网络接口卡相连，实际上也可以只有部分VM与网络接口卡相连，其他部分VM与虚拟交换机相连，具体VM的配置方式并不限定于必须全部都与网络接口卡相连。

图4为依据本发明一实施例的的服务器300的硬件结构示意图，服务器300上运行有虚拟机和虚拟交换机。

如图4所示，服务器300包括处理器301，处理器301与系统内存308连接。处理器301可以为中央处理器（CPU），图像处理器（英文全称：graphics processing unit，缩写：GPU），数字信号处理器（英文全称：digital signal processor，缩写：DSP）或其他形式的集成电路。

服务器300还包括网络接口卡303，网络接口卡303用于实现服务器300上虚拟机与外部网络的通信。

总线307用于在服务器300的各部件之间传递信息，总线307可以使用有线的连接方式或采用无线的通讯方式，本申请并不对此进行限定。总线307还可以连接有输入/输出接口304，辅助存储器（英文：secondary storage）305和通信接口306。

输入/输出接口304连接有输入/输出设备，用于接收输入的信息，输出操作结果。输入/输出设备可以为鼠标、键盘、显示器、或者光驱等。

辅助存储器305的存储介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如光盘)、或者半导体介质（例如固态硬盘（英文全称：solid state disk，缩写：SSD））等。

通信接口306使用例如但不限于收发器一类的收发装置，来实现与其他设备或通信网络之间的通信，通信接口306可以通过有线或者无线的形式与通信网络互连。该通信网络可以是因特网，内联网(英文:intranet)，局域网（英文全称：local area network，缩写：LAN），广域网络（英文全称：wide area network，缩写：WAN），存储区域网络（英文全称：storage

area network，缩写：SAN）等，或者以上网络的任意组合。

本发明实施例的一些特征可以由处理器 301 执行系统内存 302 中的软件代码来完成/支持。系统内存 108 可以包括一些软件，例如，操作系统（例如 Darwin、RTXC、LINUX、UNIX、OS X、WINDOWS 或嵌入式操作系统（例如 Vxworks）），应用程序和数据处理模块。

工作状态下，服务器运行了至少一个 VM 以及虚拟交换机。用于实现本发明实施例提供的数据处理方法中主机侧的方法的程序代码保存在系统内存 302 中，并由处理器 301 执行。工作状态下，网络接口卡执行本发明实施例提供的数据处理方法中网络接口卡侧的方法。

本申请还提供了一种数据处理方法，前述 SDN 架构中的服务器运行时执行该方法，其流程示意图如图 5 所示。

图 5 为依据本发明一实施例的一种数据处理方法 500 的流程图，前述服务器 300 运行时执行方法 500，如图 5 所示，方法 500 包括：

S502：网络接口卡接收第一数据包。

其中，第一数据包携带第一数据包的匹配信息和载荷。该第一数据包可以为服务器上运行的虚拟机向外部网络发送的数据包或由外部网络发送给该服务器上运行的虚拟机的数据包。

可选的，在步骤 S502 之前，方法 500 还包括配置虚拟机与网络接口卡互联的端口。本发明实施例中，网络接口卡通过网络接口卡端口与虚拟机互联，一个网络接口卡端口可以通过 SR-I/OV 技术与主机上运行的一个 VM 连接，网络接口卡端口可以为 SR-I/OV 技术定义的虚拟功能（英文全称：virtual function，缩写：VF）的端口。在本发明实施例中，网络接口卡还可以使用其他技术与虚拟机互联，本发明实施例不对网络接口卡与虚拟机互联的技术进行限定。网络接口卡还可以为支持虚拟机设备队列(英文全称：Virtual Machine Device Queues，缩写：VMDq)功能的网络接口卡。服务器配置虚拟机与网络接口卡互联的端口可以包括：

S5001：服务器的主机根据虚拟交换机端口的配置信息，在虚拟交换机上建立至少一个虚拟交换机端口，每个虚拟交换机端口对应该主机上运行的一个 VM。

S5002：该主机生成网络接口卡端口的配置信息，并将该网络接口卡端口的配置信息发送至服务器的网络接口卡。

具体的，该主机获取该虚拟交换机端口的配置信息，将该虚拟交换机端口的配置信息发送至该主机上运行的网络接口卡驱动，该网络接口卡驱动根据该虚拟交换机端口的配置信息，生成网络接口卡端口的配置信息，并发送至该网络接口卡。该虚拟交换机端口的配置信息与该网络接口卡端口的配置信息的功能类似，该网络接口卡驱动将虚拟交换机端口的配置信息转换为网络接口卡端口的配置信息主要为了符合网络接口卡驱动与网络接口卡通信的规范。

S5003：该网络接口卡根据该网络接口卡端口的配置信息，在该网络接口卡上配置至少一个网络接口卡端口，每个网络接口卡端口与该主机上运行的一个 VM 连接。

网络接口卡端口具体可以为 SR-I/OV 技术定义的虚拟功能（英文全称：virtual function，缩写：VF）的端口。

具体的架构图如图 6 所示，虚拟交换机的每一个端口与网络接口卡的一个 VF 相对应，网络接口卡通过 VF 与虚拟机互联。

S5001-S5003 为可选步骤，且 S5001-S5003 为该虚拟交换机和该网络接口卡的配置过程，无须每次执行 S5001-S5003 的后续步骤前都执行一次 S5001-S5003。通过该配置过程，主机上运行的 VM 通过网络接口卡端口与网络接口卡连接。

由于 VS 端口与 VM 一一对应，同时 VM 与网络接口卡端口一一对应，因此 VS 端口与网络接口卡端口一一对应。在 S5001-S5003 的执行过程中将 VS 端口与网络接口卡端口的对应关系存入该虚拟交换机和/或将 VS 端口与网络接口卡端口的对应关系存入该网络接口卡。

可选的，方法 500 还包括配置该虚拟交换机与该网络接口卡通信的至少一个队列，用于该虚拟交换机将从网络接口卡接收到的数据包返回给该网络接口卡。队列的配置有多种形式，例如，该虚拟交换机与该网络接口卡通过一个队列通信，该虚拟交换机将需要发往该网络接口卡的全部数据包发送至该队列，再例如，该虚拟交换机与该网络接口卡通过 n 个队列通信，n 为该主机上运行的 VM 的数量，每一个队列与一个 VM 对应。本发明实施例并不限定队列的配置形式。

S504：网络接口卡根据第一数据包的匹配信息在会话表中查找是否有与该第一数据包匹配的会话表项。如果存在与第一数据包匹配的会话表项，则执行步骤 S506；如果不存在与第一数据包匹配的会话表项，则执行步骤 S508。

会话表项包括匹配域和动作域，匹配域用于与数据包的匹配信息进行匹配，动作域记录的信息用于指示网络接口卡对与该会话表项匹配的数据包进行处理。数据包的匹配信息可以包含数据包的源信息和/或数据包的目的信息。其中源信息和目的信息可以包含互联网协议（英文全称：Internet Protocol，缩写：IP）地址，媒体接入控制地址(英文全称：Media Access Control，缩写：MAC)，端口编号（例如，传输控制协议（英文全称：Transmission Control Protocol，缩写 TCP）端口，用户数据报协议（英文全称：User Datagram Protocol，缩写：UDP）端口），或者其他类似的用来标识数据的源和目的的信息。

通常可以使用 IP 五元组（源 IP+源端口+协议类型+目的 IP+目的端口），或者 IP 三元组（源 IP+目的 IP+协议类型）来标识一个数据包的匹配信息，匹配信息也可以包含 IP 报文所属的其它特征项，例如入接口、虚拟局域网（英文全称：Virtual Local Area Network，缩写：VLAN）、租户 ID、甚至 MAC 地址等。

在本发明的一个实施例中，当系统里面同时存在多种协议的情况下，不同类型的协议配置的地址可能相同，比如 VM1 属于 IPV4 协议，VM2 属于 IPV6 协议，这时候他们两个可能存在 IP 地址相同的情况，就需要增加协议类型信息来区分 IP 地址是属于 VM1 还是 VM2，即数据报文是什么协议传输过来的。例如，可以通过添加 IP 协议（IPV4，IPV6）或 TCP 协议等来标识一个会话。

在本发明施例的实现过程中，当配置网络接口卡只做交换功能，会话表构建时可以使用 MAC 信息。当配置网络接口卡做路由功能，那么会话表构建时可以使用 MAC 信息、IP 信息和三层协议类型。当配置网络接口卡做更高层网络功能（防火墙、网络地址转换（英文全称：Network Address Translation，缩写：NAT）等），则会话表构建时可以使用 MAC，IP，端口和三、四层协议类型。

在本发明实施例中，会话表项的匹配域记录的信息可以为与该会话表项匹配的数据包携带的匹配信息的字段或部分字段。会话表项的匹配域记录的信息也可以为根据数据包携带的匹配信息的字段或部分字段处理之后的信息，例如，会话表项的匹配域记录的信息可以为该会话表项匹配的数据包携带的匹配信息的哈希运算结果。本发明实施例不对会话表项的匹配域与数据包携带的匹配信息之间的对应关系进行限定。

当网络接口卡收到数据包之后，会根据数据包携带的匹配信息去查询会话表，具体可以根据匹配信息中携带的字段去查询会话表项，或者根据匹配信息携带的字段处理之后的结果（例如，哈希运算）去查询会话表项。

如果该第一数据包的匹配信息无法匹配会话表的任何一个会话表项，则该第一数据包为该第一数据包所在的数据流的首个数据包，或该第一数据包不是该数据流的首个数据包，但该数据流对应的会话表项在会话表中已经被删除。

S506：网络接口卡根据与第一数据包匹配的会话表项处理第一数据包。

更具体的，网络接口卡根据与第一数据包匹配的会话表项的动作域记录的信息处理该第一数据包。

如果会话表中存在与第一数据包匹配的会话表项，则网络接口卡接收到数据包后可以直接根据会话表项的动作域对数据包进行处理，不需要将数据包上报给虚拟交换机处理，从而简化了数据处理流程，且减小了虚拟交换机对服务器硬件资源的占用。

S508：网络接口卡查询安全组规则是否允许第一数据包通过。如果安全组规则允许第一数据包通过，则执行步骤 S512；如果安全组规则不允许第一数据包通过，则执行步骤 S510。

在 S508 之前，方法 500 还可以包括：网络接口卡创建与第一数据包匹配的第一会话表项，并根据第一数据包的匹配信息创建与第一数据包匹配的第一会话表项的匹配域，网络接口卡可以将第一数据包的匹配信息的部分或全部字段写入第一会话表项的匹配域，网络接口卡也可以将第一数据包的匹配信息的部分或全部字段的处理结果写入第一会话表项的匹配域，本发明实施例不对第一会话表项的匹配域的形式进行限定。第一会话表项的动作域的信息可以先为空或者为上报虚拟交换机。

具体实现过程中，可以将安全组规则建立在网络接口卡芯片内部或服务器的主机上。如果安全组规则建立在主机上，则主机查找第一数据包匹配的安全组规则后，向网络接口卡发送该第一数据包匹配的安全组规则。安全组规则用于实现安全过滤规则，从而实现主机或 VM 间的访问隔离。

S510：网络接口卡丢弃第一数据包。

如果安全组规则不允许第一数据包通过，则网络接口卡丢弃第一数据包。方法 500 还可以包括：将创建的第一会话表项删除，或者将第一会话表的老化时间设置为较短时间，让其快速老化。

S512：网络接口卡将第一数据包发送给主机。

具体的，网络接口卡将第一数据包发送给主机上运行的虚拟交换机。第一数据包在会话表中没有匹配的会话表项，而且安全组规则允许第一数据包通过，网络接口卡将第

一数据包发送给主机上运行的虚拟交换机处理。

S514：主机获取与第一数据包关联的至少两个流表项。

具体的，可以由主机上运行的虚拟交换机获取与第一数据包关联的至少两个流表项。

在 OpenFlow 协议中，虚拟交换机的功能非常灵活，对数据包的不同处理操作被记录在不同的流表项中，一般情况下，虚拟交换机维护有与一个数据包关联的多个流表项。在本发明实施例中，与数据包关联的流表项是指虚拟交换机对该数据处理的过程中需要使用的流表项。在本发明实施例中，从源出发到目的的传输过程中，数据包可能发生变化，但为了描述方便，本发明实施例使用第一数据包或第二数据包等术语来表述一个数据包的整个生命周期。例如，虚拟交换机根据流表项 1 动作域对数据包 1 进行了修改操作，得到了数据包 2，数据包 2 与数据包 1 是不同的，在本发明实施例的描述中，仍然将数据包 1 和数据包 2 都叫做第一数据包或第二数据包。

如果不存在与第一数据包匹配的流表项，则第一数据包为该第一数据包所在的数据流的首个数据包，或该第一数据包不是该数据流的首个数据包，但该数据流对应的流表项已经被删除，则该虚拟交换机获取该第一数据包后，可以将该第一数据包或者第一数据包的匹配信息发送至 SDN 控制器，并接收 SDN 控制器根据该第一数据包生成的该数据流对应的流表项。

S516：主机根据获取的第一数据包关联的至少两个流表项处理第一数据包。

更具体的，可以由主机上运行的虚拟交换机根据获取的第一数据包关联的至少两个流表项处理第一数据包。虚拟交换机根据第一数据包关联的至少两个流表项处理第一数据包后，将处理后的数据包和处理结果转发给网络接口卡，由网络接口卡转发出去。

S518：主机向网络接口卡发送处理信息。

更具体的，可以由主机上运行的虚拟交换机向网络接口卡发送处理信息。

主机获取与所述第一数据包关联的至少两个流表项之后，根据该至少两个流表项生成处理信息，该处理信息处理信息用于指示虚拟交换机根据该至少两个流表项对第一数据包的处理操作。在本发明实施例中，如果该至少两个流表项的动作域记录的信息都是对第一数据包本身进行处理操作，则该处理信息可以为该至少两个流表项的动作域记录的信息，如果该至少两个流表项中的第一流表项的动作域记录的信息不是对第一数据包本身进行处理，例如，该第一流表项的动作域记录的信息为查找下一级流表，则处理信息中可以不携带第一流表项的动作域记录的信息。在具体实现中，处理信息可以包含该至少两个流表项的动作域记录的信息，或者为该至少两个流表项的动作域记录的信息综合后的信息。

S520：网络接口卡根据主机发送的处理信息生成第一会话表项的动作域。

该第一流会话表项包含匹配域和动作域，匹配域用于匹配第一数据包的匹配信息。第一会话表项用于指示网络接口卡处理与该第一会话表项匹配的数据包，即用于指示网络接口卡处理第一数据包所在数据流的其他数据包。

步骤 S520 之后，如果网络接口卡接收到第二数据包，该第二数据包与第一数据包属于同一个数据流，即第二数据包携带与第一数据包相同的匹配信息，则网络接口卡根据第二数据包携带的匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项处理第二数据包。更具体的，网络接口卡根据第一会话表项的动作域处理第二数据包。

可选的，方法500还包括：网络接口卡将第一数据包匹配的安全组规则写入第一会话表项的动作域。网络接口卡可以根据该第一会话表项对匹配的数据包进行多项处理，从而简化了数据包的处理流程。安全组模块如果对第一数据包的安全组规则进行了修改，还可以向网络接口卡发送修改指令，该指令用于指示安全组模块对第一数据包的安全组规则的修改，网络接口卡根据该修改指令修改第一会话表项的动作域关于安全组规则的记录。

方法500还可以包括：当安全组规则用于实现状态防火墙功能时，在该防火墙功能的处理结果是对第一数据包的源和目的正反向数据包都允许通过的情况下，网络接口卡根据第一数据包的匹配信息创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项，表明第一数据包的目的地址发起到源地址的报文的安全动作也是通过。

网络接口卡可以根据第一数据包的匹配信息得出第一数据包的目的到第一数据包的源的反向数据包的匹配信息，第一数据包的反向数据流的的源信息和目的信息分别为第一数据包的目的信息和源信息。第二会话表项的匹配域可以根据第一会话表项类似的方法进行配置，在此不再赘述。

第二会话表项的动作域可以设置为上传主机或者设置为空，后续会根据虚拟交换机对反向数据包的实际处理更新第二会话表的动作域，具体方案流程与下文描述中第一会话表项的动作域的配置流程类似。

第一会话表项和第二会话表项也可以合并成一条记录，动作域区分正向和反向2个域，例如可以设定VM发出方向为正向，网络侧过来的方向为反向，查反向表时交换源节点信息和目的节点信息。

可选的，方法500还包括：虚拟机虚拟交换机修改与第一数据包的匹配信息匹配的至少两个流表项中的任意一个流表项后，虚拟交换机向网络接口卡发送修改指令，该修改指令用于指示虚拟交换机对流表项的修改操作，网络接口卡根据该修改指令修改第一会话表项。

服务器可以根据链表技术把会话表项链接到虚拟交换机的流表项，当虚拟交换机的的表项删除或修改的时候，主机通知网络接口卡去同步删除或者修改会话表。

在另外一种实现方式中，每一个流表项和会话表项都有一个索引ID，主机建立流表项索引ID与会话表项索引ID的映射关系，主机监控虚拟交换机流表更新情况，当发现流表项发生了更新，就会通知网络接口卡，网络接口卡根据流表项的更新操作，对会话表项进行更新。

安全组规则的更新与流表项信息更新管理方式类似，在此不再赘述。

可选的，方法500还包括：第一会话表项在超过预设时间阈值的时间段内未被访问时，网络接口卡删除所述第一会话表项，并向所述虚拟交换机发送删除指令，虚拟交换机根据删除指令删除与第一数据包的匹配信息匹配的至少两个流表项。

因为OVS流表有老化机制，长时间不访问的流表项将会自动老化，流表项老化后，会话表项就会跟着删除，这样的话，会话表就不断的要重新创建、删除。本发明实施例中，主机可以对OVS流表的老化进行设置，可以设置很长的老化时间或者不老化。会话表项可以设置老化机制，当会话表项老化后，就可以通知OVS也将与会话表项对应的流

表项进行老化。

在本发明实施例中，为了防止 TCP 的 SYN（英文全称：synchronous）攻击（指拼命发送建链请求的攻击），针对 TCP 的建链请求，网络接口卡可以从 TCP 请求中识别出这是建链请求，针对这类请求先设置很短的老化时间（比如小于 5 秒），表项短时间没有访问将会老化删除，让这条记录尽快删除，避免会话表被攻击。SYN 攻击利用 TCP 协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。一旦有新报文，会话表就会创建新的会话记录，如果不删除的话，空间会被占满，从而无法创建新的记录。

其中，SYN 是 TCP/IP 建立连接时使用的握手信号，在客户机和服务器之间建立正常的 TCP 网络连接时，客户机首先发出一个 SYN 消息，服务器使用 SYN+ACK 应答表示接收到了这个消息，最后客户机再以 ACK 消息响应，这样在客户机和服务器之间才能建立起可靠的 TCP 连接，数据才可以在客户机和服务器之间传递。TCP 连接完成了三次握手，连接建立状态进入稳态后，老化时间可以设置为长的老化时间（比如 30 分钟）。

针对 UDP 应用，单向报文建立会话表时设置短的老化时间，收到回应报文时改为长的老化时间。

另外，针对 TCP 删除链路的请求，一旦发现是删除请求，则网络接口卡可以删除会话表项，避免占用空间。

图 7 为依据本发明一实施例的一种数据处理方法 700 的流程图，前述服务器 300 运行时执行方法 700,在方法 700 中网络接口卡需要根据虚拟交换机的处理信息查询第一数据包的安全组规则，如图 7 所示，方法 700 包括：

S702：网络接口卡接收第一数据包。

S704：网络接口卡根据第一数据包的匹配信息在会话表中查找是否有与该第一数据包匹配的会话表项。如果存在与第一数据包匹配的会话表项，则执行步骤 S706；如果不存在与第一数据包匹配的会话表项，则执行步骤 S708。

S706：网络接口卡根据与第一数据包匹配的会话表项处理第一数据包。

步骤 S702-S706 的具体描述参照步骤 S502-S506，在此不再赘述。

S708：网络接口卡将第一数据包发送给主机。

在 S708 之前，方法 700 还可以包括：网络接口卡创建与第一数据包匹配的第一会话表项，并根据第一数据包的匹配信息创建与第一数据包匹配的第一会话表项的匹配域，网络接口卡可以将第一数据包的匹配信息的部分或全部字段写入第一会话表项的匹配域，网络接口卡也可以将第一数据包的匹配信息的部分或全部字段的处理结果写入第一会话表项的匹配域，本发明实施例不对第一会话表项的匹配域的形式进行限定。第一会话表项的动作域可以先为空或者为上报虚拟交换机。

S710：主机获取与第一数据包关联的至少两个流表项。

S712：主机根据获取的第一数据包关联的至少两个流表项处理第一数据包。

S714：主机向网络接口卡发送处理信息。

步骤 S708-S714 的具体描述参照步骤 S512-S518，在此不再赘述。

S716：网络接口卡查询安全组规则是否允许第一数据包通过。如果安全组规则允许

第一数据包通过，则执行步骤 S718；如果安全组规则不允许第一数据包通过，则执行步骤 S720。

网络接口卡根据虚拟交换机发送的处理信息，查询第一数据包的安全组规则。具体实现过程中，可以将安全组规则建立在网络接口卡芯片内部或服务器的主机上。

S718：网络接口卡根据主机发送的处理信息生成第一会话表项的动作域。

步骤 S718 的具体描述参照步骤 S520，在此不再赘述。

S720：网络接口卡丢弃第一数据包。

如果安全组规则不允许第一数据包通过，则网络接口卡丢弃第一数据包。

如果安全组规则不允许第一数据包通过，方法 700 还可以包括：将创建的第一会话表项删除。

方法 700 中，网络接口卡需要根据虚拟交换机发送的处理信息来查询第一数据包的处理信息，方法 700 的部分具体描述参照方法 500。

参照图 6 的架构进行举例说明，假设数据包的匹配信息为 IP 五元组，VM-1 的 IP 地址为 12.5.3.1，通过 VF1 与网络接口卡连接，VM-1 通过端口 2351 访问 IP 地址为 52.5.13.5 的外部服务器时。其访问流程如下：

VM 的首先发起 TCP 的 SYN 报文，报文通过网络接口卡的 VF1 直接发到网络接口卡。

网络接口卡以 IP 五元组 12.5.3.1：2351+TCP+52.5.13.5:80 查找会话表项。对于数据流的首个数据包，网络接口卡查询不到会话表项。

网络接口卡查询安全组表，假设安全组配置规则允许 12.5.3.1 访问 52.5.13.5。

网络接口卡将数据包发给主机，虚拟交换机查询与数据包匹配的至少两个流表项，根据至少两个流表项的处理结果是转发到外部端口 NET1。

主机向网络接口卡发送处理信息，网络接口卡创建一个匹配域为 12.5.3.1：2351+TCP+52.5.13.5:80 的正向会话表项，正向会话表项的动作域为将数据包转发到外部网口 NET1。

如果安全组规则为正反向都允许通过，网络接口卡还可以创建一个匹配域为 52.5.13.5:80+TCP+12.5.3.1：2351 的反向会话表项，反向会话表项的动作域为空（为空上送主机）。正向会话表项和反向会话表项也可以是一个表项，动作域区分正向区和反向区，正向为转发到外部网口，反向为空，反向查找时交换源、目的的 IP 地址和端口号。

为了进一步提高安全性和防攻击性，跟踪 TCP 状态，会话表记录 SYN 状态和序号（每一个 TCP 请求都有序号），老化时间为短老化时间，例如 3 秒。同时将会话表项链接到 OVS 命中的流表项和安全组命中的安全组表项中，并限制 OVS 流表表项老化（设置为不老化，或者老化时间很长），具体可以通过在 OVS 和安全组中分别建立会话表项与流表项之间的映射关系，以及会话表项与安全组表项之间的映射关系。

主机将数据包重新发给网络接口卡，网络接口卡从网络端口 NET1 中将数据包发送出去。

外部服务器回应 SYN+ACK 报文，数据包进入网络接口卡后，网络接口卡查询会话表，

命中反向会话表项，但动作域为空，网络接口卡将数据包发送给 OVS 进行转发处理，OVS 查询流表项，确定要将数据包转发给端口 1，然后网络接口卡驱动查询端口与 VF 的映射关系，得知端口 1 对应 VF1，则转发结果为转发到 VF1，则主机向网络接口卡发送处理信息，处理信息指示转发结果为将数据包转发到 VF1，网络接口卡根据处理信息更新反向会话表项的动作域，并通过 VF1 将报文发给 VM-1。

VM-1 收到报文之后，再回一个 ACK 报文，带着 TCP 序号，然后网络接口卡判断会话表项的 SYN 状态和序号，如果序号匹配，则进入建立状态，将会话表项修改为长老化时间，例如 30 分钟。后续的 TCP 数据报文查询会话表都能直接得到转发结果，不再需要上送主机进行 OVS 转发。如果会话表项对应的流表项或者安全组规则修改或删除，则根据关联的索引关系修改或删除会话表项。如果 VM-1 或外部服务器发起 TCP 关闭操作，完成 TCP 的结束状态处理后，网络接口卡删除会话表 12.5.3.1：2351+TCP+52.5.13.5:80 的正反向表项，并通知 OVS 和安全组中分别删除会话表项与流表项之间的映射关系，以及会话表项与安全组表项之间的映射关系，并重新允许该 OVS 流表表项老化。

实现过程中，网络接口卡接收到数据包后，如果没有查找到对应的会话表项，也可以先将数据包上报给 OVS，然后根据 OVS 发送的处理信息查找安全表规则，例如，如果处理结果为将数据包转发 VF1，网络接口卡查询 VF1 下配置的安全组规则，发现是禁止通过，则丢弃报文，删除所建的会话表项。如果不需要针对 VM 接口来进行安全组检查，则可以先查安全组表，如果不通过直接丢弃，不再上送主机进行 OVS 转发。

图 8 为依据本发明一实施例的网络接口卡 800 的硬件结构示意图，如 8 所示，网络接口卡 800 包括：处理器 802，存储器 804，网络接口 806，主机接口 808 和总线 8100。

主机接口 808 用于连接主机。

处理器 802 用于通过主机接口 808 向主机发送第一数据包，通过主机接口 808 接收来自主机的处理信息，处理信息用于指示主机根据与第一数据包匹配的至少两个流表项对第一数据包的处理操作，并根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域，第一会话表项用于记录网络接口卡处理与第一会话表项匹配的数据包的规则。

本发明实施例中的处理器 802 可以为任意形式的处理逻辑，例如，处理器 802 可以为可以为中央处理器，图像处理器，数字信号处理器（英文全称：digital signal processor，缩写：DSP）或其他形式的集成电路。

处理器 802 的功能可以由硬件的集成电路来实现，也可以由处理器执行存储器 804 中存储的代码来实现，本发明对此不进行限定。

存储器 804 用于存储第一会话表项。

网络接口卡还包括网络接口 806，网络接口 806 用于连接外部网络，处理器 802 还用于通过主机接口 808 或网络接口 806 接收第二数据包，第二数据包与第一数据包具有相同的匹配信息，802 还用于根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

处理器 802 通过主机接口 808 向主机发送第一数据包之前，还用于通过主机接口 808 或网络接口 806 接收第一数据包，根据匹配信息查询记录的会话表项，并在没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

可选的，处理器 802 还用于查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。如果安全组规则包含正反向允许通过的防火墙规则，处理器 802 还用于创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

可选的，处理器 802 还用于通过主机接口 808 接收来自主机的修改指令，并根据修改指令修改第一会话表项，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作。

可选的，若第一会话表项在超过预设时间阈值的时间段内未被访问，处理器 802 还用于删除第一会话表项。处理器 802 删除第一会话表项后，还用于通过主机接口 808 向主机发送删除指令，删除指令用于指示主机删除至少两个流表项。

本发明实施例是网络接口卡的装置实施例，本发明其他实施例部分的特征描述，适用于本发明实施例，在此不再赘述。

图 9 为依据本发明一实施例的网络接口卡 900 的逻辑结构示意图，如图 9 所示，网络接口卡 900 包括：发送单元 902，接收单元 904 和处理单元 906。

发送单元 904 用于向主机发送第一数据包；接收单元 902 用于接收来自主机的处理信息，处理信息用于指示主机根据与第一数据包匹配的至少两个流表项对第一数据包的处理操作；处理单元 906 用于根据处理信息生成第一会话表项的动作域，并根据第一数据包的匹配信息生成第一会话表项的匹配域，第一会话表项用于记录网络接口卡 900 处理与第一会话表项匹配的数据包的规则。

接收单元 902 还用于接收第二数据包，第二数据包与第一数据包具有相同的匹配信息；处理单元 906 还用于根据匹配信息查询与第二数据包匹配的第一会话表项，并根据第一会话表项的动作域处理第二数据包。

发送单元 904 向主机发送第一数据包之前，接收单元 902 还用于接收第一数据包；处理单元 906 还用于根据匹配信息查询记录的会话表项；发送单元 904 还用于在处理单元 906 没有查询到与第一数据包匹配的会话表项时，将第一数据包发送给主机。

可选的，处理单元 906 还用于查询与第一数据包匹配的安全组规则，并将安全组规则写入第一会话表项的动作域。如果安全组规则包含正反向允许通过的防火墙规则，处理单元 906 还用于创建第二会话表项，并根据第一数据包的匹配信息生成第二会话表项的匹配域，第二会话表项为与第一数据包的反方向数据流匹配的会话表项。

可选的，接收单元 902 还用于接收来自主机的修改指令，修改指令用于指示主机对至少两个流表项中的一个流表项的修改操作；处理单元 906 还用于根据修改指令修改第一会话表项。

可选的，若第一会话表项在超过预设时间阈值的时间段内未被访问，处理单元 906 还用于删除第一会话表项。处理单元 906 删除第一会话表项后，还用于向主机发送删除指令，删除指令用于指示主机删除至少两个流表项。

本发明实施例是网络接口卡的装置实施例，本发明其他实施例部分的特征描述，适用于本发明实施例，在此不再赘述。

本发明实施例部分的发送单元 902 和接收单元 904 的功能可以由图 8 实施例中的处理器 802 和主机接口 808 来实现，或者由处理器 802，存储器 804 和主机接口 808 来实现。

本发明实施例部分的发送单元 904 的部分功能还可以由图 8 实施例中的处理器 802

和网络接口 806 来实现，或者由处理器 802，存储器 804 和网络接口 806 来实现。

本发明实施例部分的处理单元 904 的功能可以由图 8 实施例中的处理器 802 来实现，或者由处理器 802 执行存储器 804 中的代码来实现。

以上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，或者替换其中部分技术特征；而这些修改或者替换，并不使相应技术方案脱离权利要求的保护范围。

权 利 要 求

1、一种服务器，其特征在于，所述服务器包含主机和网络接口卡，所述网络接口卡通过主机接口与所述主机相连；

所述主机用于接收所述网络接口卡发送的第一数据包，获取与所述第一数据包关联的至少两个流表项，根据所述至少两个流表项生成处理信息，并向所述网络接口卡发送所述处理信息；

所述网络接口卡用于根据所述处理信息生成第一会话表项的动作域；

所述网络接口卡还用于根据所述第一数据包的匹配信息生成所述第一会话表项的匹配域；

所述第一会话表项用于记录所述网络接口卡处理与所述第一会话表项匹配的数据包的规则。

2、根据权利要求 1 所述的服务器，其特征在于，所述网络接口卡还用于接收第二数据包，所述第二数据包与所述第一数据包具有相同的匹配信息，根据所述匹配信息查询与所述第二数据包匹配的所述第一会话表项，并根据所述第一会话表项的动作域处理所述第二数据包。

3、根据权利要求 1 或 2 所述的服务器，其特征在于，所述主机接收所述网络接口卡发送的所述第一数据包之前，所述网络接口卡还用于接收所述第一数据包，根据所述匹配信息查询记录的会话表项，并在没有查询到与所述第一数据包匹配的会话表项时，将所述第一数据包发送给所述主机。

4、根据权利要求 1-3 任一项所述的服务器，其特征在于，所述网络接口卡还用于查询与所述第一数据包匹配的安全组规则，并将所述安全组规则写入所述第一会话表项的动作域。

5、根据权利要求 4 所述的服务器，其特征在于，所述主机配置有安全组功能；

所述主机还用于查询与所述第一数据包匹配的安全组规则，并向所述网络接口卡发送所述第一数据包匹配的安全组规则。

6、根据权利要求 4 或 5 所述的服务器，其特征在于，如果所述安全组规则包含正反向允许通过的防火墙规则，所述网络接口卡还用于创建第二会话表项，并根据所述第一数据包的匹配信息生成所述第二会话表项的匹配域，所述第二会话表项为与所述第一数据包的反方向数据流匹配的会话表项。

7、根据权利要求 1-6 任一项所述的服务器，其特征在于，所述主机还用于在修改所述至少两个流表项中的一个流表项后，向所述网络接口卡发送修改指令，所述修改指令用于指示所述主机对所述至少两个流表项中的一个流表项的修改操作；

所述网络接口卡还用于根据所述修改指令修改所述第一会话表项。

8、根据权利要求 1-7 任一项所述的服务器，其特征在于，若所述第一会话表项在超过预设时间阈值的时间段内未被访问，所述网络接口卡还用于删除所述第一会话表项。

9、根据权利要求 8 所述的服务器，其特征在于，所述网络接口卡删除所述第一会话表项后，还用于向所述主机发送删除指令；

所述主机还用于根据所述删除指令删除所述至少两个流表项。

10、一种数据处理方法，其特征在于，服务器包含运行有虚拟交换机的主机和网络接口卡，所述方法包括：

所述主机接收所述网络接口卡发送的第一数据包，获取与所述第一数据包关联的至少两个流表项，根据所述至少两个流表项生成处理信息，并向所述网络接口卡发送所述处理信息；

所述网络接口卡根据所述处理信息生成第一会话表项的动作域；

所述网络接口卡根据所述第一数据包的匹配信息生成所述第一会话表项的匹配域；

所述第一会话表项用于记录所述网络接口卡处理与所述第一会话表项匹配的数据包的规则。

11、根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

所述网络接口卡接收第二数据包，所述第二数据包与所述第一数据包具有相同的匹配信息；

所述网络接口卡根据所述匹配信息查询与所述第二数据包匹配的所述第一会话表项，并根据所述第一会话表项的动作域处理所述第二数据包。

12、根据权利要求 10 或 11 所述的方法，其特征在于，所述主机接收所述网络接口卡发送的所述第一数据包之前，所述方法还包括：

所述网络接口卡接收所述第一数据包，根据所述匹配信息查询记录的会话表项，并在没有查询到与所述第一数据包匹配的会话表项时，将所述第一数据包发送给所述主机。

13、根据权利要求 10-12 任一项所述的方法，其特征在于，所述方法还包括：

所述网络接口卡查询与所述第一数据包匹配的安全组规则，并将所述安全组规则写入所述第一会话表项的动作域。

14、根据权利要求 13 所述的方法，其特征在于，所述主机配置有安全组功能；

所述方法还包括：

所述主机查询与所述第一数据包匹配的安全组规则，并向所述网络接口卡发送所述第一数据包匹配的安全组规则。

15、根据权利要求 13 或 14 所述的方法，其特征在于，如果所述安全组规则包含正反向允许通过的防火墙规则，所述方法还包括：

所述网络接口卡创建第二会话表项，并根据所述第一数据包的匹配信息生成所述第二会话表项的匹配域，所述第二会话表项为与所述第一数据包的反方向数据流匹配的会话表项。

16、根据权利要求 10-15 任一项所述的方法，其特征在于，所述方法还包括：

所述主机在修改所述至少两个流表项中的一个流表项后，向所述网络接口卡发送修改指令，所述修改指令用于指示所述主机对所述至少两个流表项中的一个流表项的修改操作；

所述网络接口卡根据所述修改指令修改所述第一会话表项。

17、根据权利要求 10-16 任一项所述的方法，其特征在于，所述方法还包括：

若所述第一会话表项在超过预设时间阈值的时间段内未被访问，所述网络接口卡删除所述第一会话表项。

18、根据权利要求 17 所述的方法，其特征在于，所述网络接口卡删除所述第一会话表项后，所述方法还包括：

所述网络接口卡向所述主机发送删除指令；

所述主机根据所述删除指令删除所述至少两个流表项。

19、一种数据处理方法，其特征在于，所述方法包括：

网络接口卡向主机发送第一数据包；

所述网络接口卡接收来自所述主机的处理信息，所述处理信息用于指示所述主机根据与所述第一数据包匹配的至少两个流表项对所述第一数据包的处理操作；

所述网络接口卡根据所述处理信息生成第一会话表项的动作域，并根据所述第一数据包的匹配信息生成所述第一会话表项的匹配域，所述第一会话表项用于记录所述网络接口卡处理与所述第一会话表项匹配的数据包的规则。

20、根据权利要求 19 所述的方法，其特征在于，所述方法还包括：

所述网络接口卡接收第二数据包，所述第二数据包与所述第一数据包具有相同的匹配信息；

所述网络接口卡根据所述匹配信息查询与所述第二数据包匹配的所述第一会话表项，并根据所述第一会话表项的动作域处理所述第二数据包。

21、根据权利要求 19 或 20 所述的方法，其特征在于，所述网络接口卡向主机发送第一数据包之前，所述方法包括：

所述网络接口卡接收所述第一数据包，根据所述匹配信息查询记录的会话表项，并在没有查询到与所述第一数据包匹配的会话表项时，将所述第一数据包发送给所述主机。

22、根据权利要求 19-21 任一项所述的方法，其特征在于，所述方法还包括：

所述网络接口卡查询与所述第一数据包匹配的安全组规则，并将所述安全组规则写入所述第一会话表项的动作域。

23、根据权利要求 22 所述的方法，其特征在于，如果所述安全组规则包含正反向允许通过的防火墙规则，所述方法还包括：

所述网络接口卡创建第二会话表项，并根据所述第一数据包的匹配信息生成所述第二会话表项的匹配域，所述第二会话表项为与所述第一数据包的反方向数据流匹配的会话表项。

24、根据权利要求 19-23 任一项所述的方法，其特征在于，所述方法还包括：

所述网络接口卡接口卡接收来自所述主机的修改指令，所述修改指令用于指示所述主机对所述至少两个流表项中的一个流表项的修改操作；

所述网络接口卡根据所述修改指令修改所述第一会话表项。

25、根据权利要求 19-24 任一项所述的方法，其特征在于，所述方法还包括：

若所述第一会话表项在超过预设时间阈值的时间段内未被访问，所述网络接口卡删除所述第一会话表项。

26、根据权利要求 25 所述的方法，其特征在于，所述网络接口卡删除所述第一会话表项后，所述方法还包括：

所述网络接口卡向所述主机发送删除指令，所述删除指令用于指示所述主机删除所述至少两个流表项。

27、一种网络接口卡，其特征在于，所述网络接口卡包括：

发送单元，用于向主机发送第一数据包；

接收单元，用于接收来自所述主机的处理信息，所述处理信息用于指示所述主机

根据与所述第一数据包匹配的至少两个流表项对所述第一数据包的处理操作；

处理单元，用于根据所述处理信息生成第一会话表项的动作域，并根据所述第一数据包的匹配信息生成所述第一会话表项的匹配域，所述第一会话表项用于记录所述网络接口卡处理与所述第一会话表项匹配的数据包的规则。

28、根据权利要求 27 所述的网络接口卡，其特征在于，所述接收单元还用于接收第二数据包，所述第二数据包与所述第一数据包具有相同的匹配信息；

所述处理单元还用于根据所述匹配信息查询与所述第二数据包匹配的所述第一会话表项，并根据所述第一会话表项的动作域处理所述第二数据包。

29、根据权利要求 27 或 28 所述的网络接口卡，其特征在于，所述发送单元向主机发送第一数据包之前，所述接收单元还用于接收所述第一数据包；所述处理单元还用于根据所述匹配信息查询记录的会话表项；所述发送单元还用于在所述处理单元没有查询到与所述第一数据包匹配的会话表项时，将所述第一数据包发送给所述主机。

30、根据权利要求 27-29 任一项所述的网络接口卡，其特征在于，所述处理单元还用于查询与所述第一数据包匹配的安全组规则，并将所述安全组规则写入所述第一会话表项的动作域。

31、根据权利要求 30 所述的网络接口卡，其特征在于，如果所述安全组规则包含正反向允许通过的防火墙规则，处理单元还用于创建第二会话表项，并根据所述第一数据包的匹配信息生成所述第二会话表项的匹配域，所述第二会话表项为与所述第一数据包的反方向数据流匹配的会话表项。

32、根据权利要求 27-31 任一项所述的网络接口卡，其特征在于，所述接收单元还用于接收来自所述主机的修改指令，所述修改指令用于指示所述主机对所述至少两个流表项中的一个流表项的修改操作；

所述处理单元还用于根据所述修改指令修改所述第一会话表项。

33、根据权利要求 27-32 任一项所述的网络接口卡，其特征在于，若所述第一会话表项在超过预设时间阈值的时间段内未被访问，所述处理单元还用于删除所述第一会话表项。

34、根据权利要求 33 所述的网络接口卡，其特征在于，所述处理单元删除所述第一会话表项后，还用于向所述主机发送删除指令，所述删除指令用于指示所述主机删除所述至少两个流表项。

35、一种网络接口卡，其特征在于，包括：主机接口、处理器、存储器；

所述主机接口用于连接所述主机；

所述处理器用于通过所述主机接口向所述主机发送第一数据包；

所述主机接口还用于通过所述主机接口接收来自所述主机的处理信息，所述处理信息用于指示所述主机根据与所述第一数据包匹配的至少两个流表项对所述第一数据包的处理操作；

所述处理器还用于根据所述处理信息生成第一会话表项的动作域，并根据所述第一数据包的匹配信息生成所述第一会话表项的匹配域，所述第一会话表项用于记录所述网络接口卡处理与所述第一会话表项匹配的数据包的规则；

所述存储器用于存储所述第一会话表项。

36、根据权利要求 35 所述的网络接口卡，其特征在于，所述网络接口卡还包括网络

接口，所述网络接口用于连接外部网络；

所述处理器还用于通过所述主机接口或所述网络接口接收第二数据包，所述第二数据包与所述第一数据包具有相同的匹配信息；

所述处理器还用于根据所述匹配信息查询与所述第二数据包匹配的所述第一会话表项，并根据所述第一会话表项的动作域处理所述第二数据包。

37、根据权利要求 35 或 36 所述的网络接口卡，其特征在于，所述网络接口卡还包括网络接口，所述网络接口用于连接外部网络；

所述处理器通过主机接口向主机发送第一数据包之前，还用于通过所述主机接口或所述网络接口接收所述第一数据包，根据所述匹配信息查询记录的会话表项，并在没有查询到与所述第一数据包匹配的会话表项时，将所述第一数据包发送给所述主机。

38、根据权利要求 35-37 任一项所述的网络接口卡，其特征在于，所述处理器还用于查询与所述第一数据包匹配的安全组规则，并将所述安全组规则写入所述第一会话表项的动作域。

39、根据权利要求 38 所述的网络接口卡，其特征在于，如果所述安全组规则包含正反向允许通过的防火墙规则，处理器还用于创建第二会话表项，并根据所述第一数据包的匹配信息生成所述第二会话表项的匹配域，所述第二会话表项为与所述第一数据包的反方向数据流匹配的会话表项。

40、根据权利要求 35-39 任一项所述的网络接口卡，其特征在于，所述处理器还用于通过所述主机接口接收来自所述主机的修改指令，所述修改指令用于指示所述主机对所述至少两个流表项中的一个流表项的修改操作；

所述处理器还用于根据所述修改指令修改所述第一会话表项。

41、根据权利要求 35-40 任一项所述的网络接口卡，其特征在于，若所述第一会话表项在超过预设时间阈值的时间段内未被访问，所述处理器还用于删除所述第一会话表项。

42、根据权利要求 41 所述的网络接口卡，其特征在于，所述处理器删除所述第一会话表项后，还用于通过所述主机接口向所述主机发送删除指令，所述删除指令用于指示所述主机删除所述至少两个流表项。

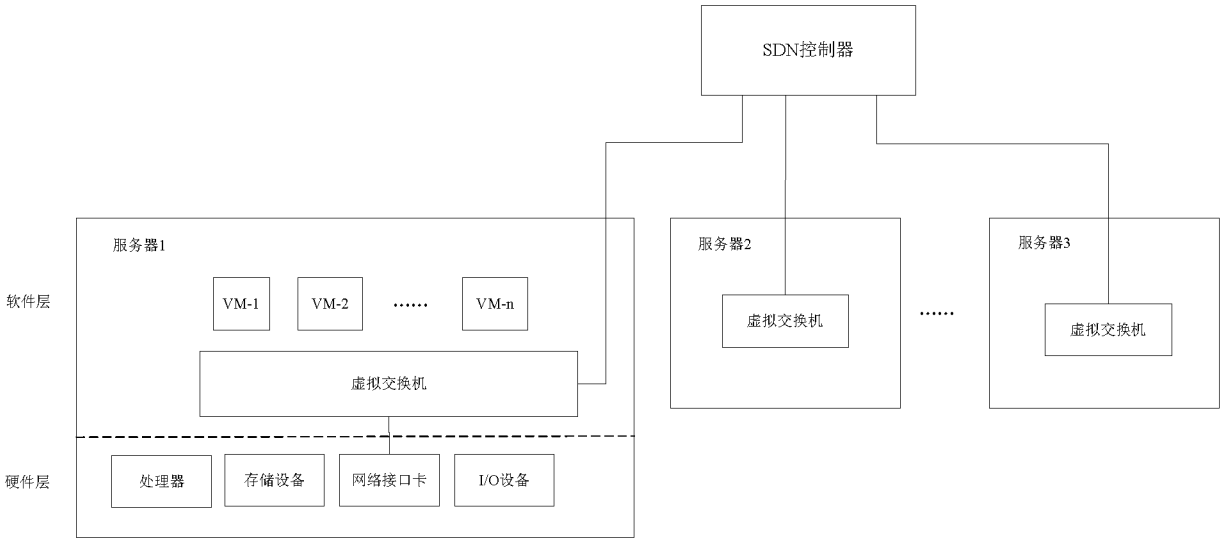
SDN控制器
服务器1
软件层
VM-1
VM-2
……
VM-n
虚拟交换机
硬件层
处理器
存储设备
网络接口卡
I/O设备
服务器2
虚拟交换机
……
服务器3
虚拟交换机

图 1

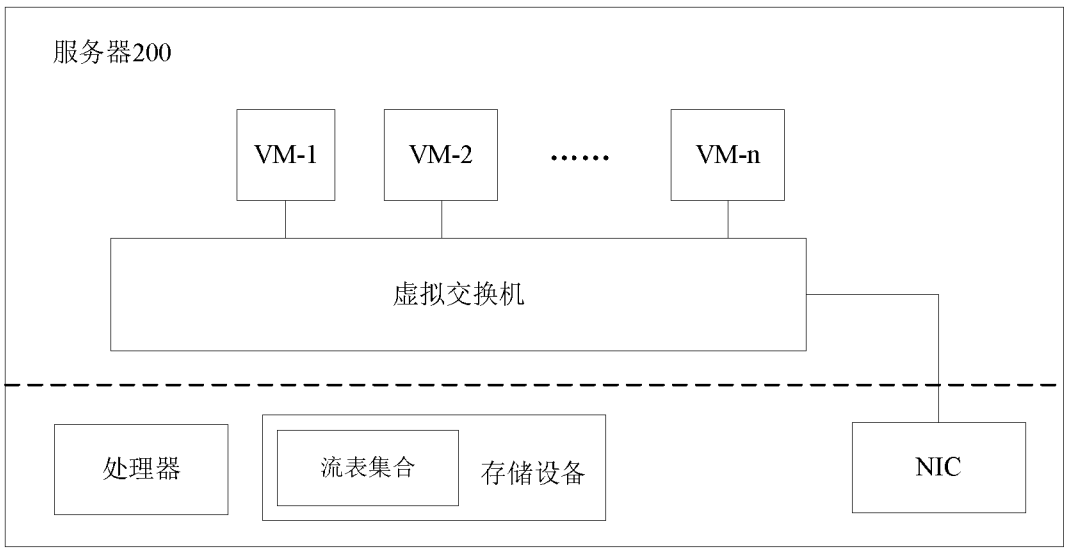
服务器200
VM-1
VM-2
……
VM-n
虚拟交换机
处理器
流表集合
存储设备
NIC

图 2

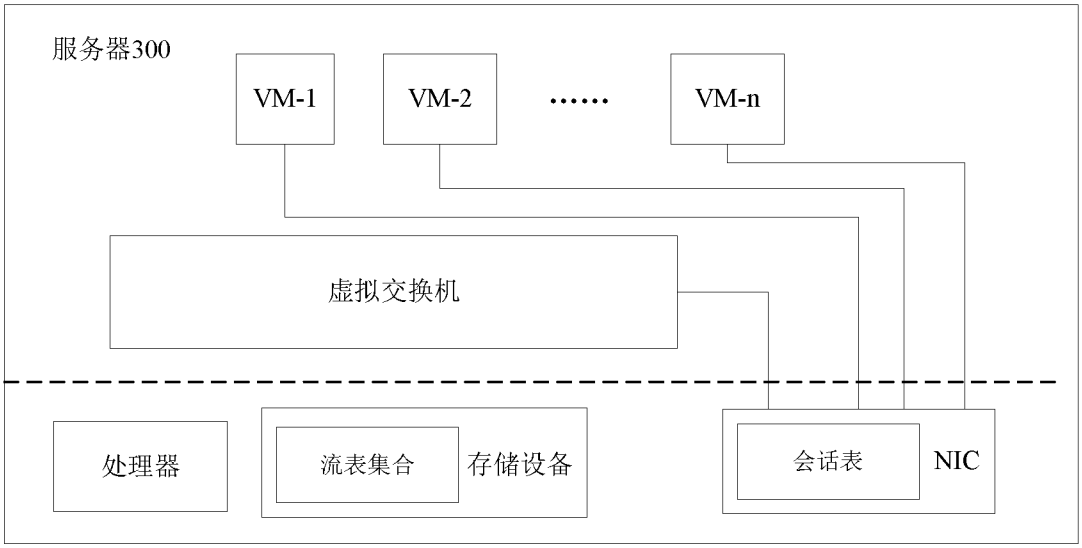
服务器300
VM-1
VM-2
……
VM-n
虚拟交换机
处理器
流表集合
存储设备
会话表
NIC

图 3

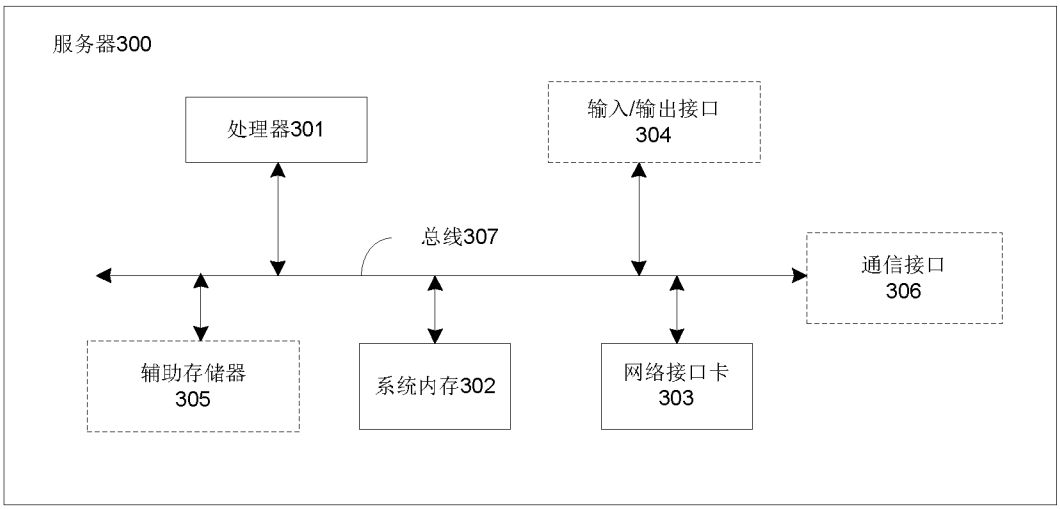
服务器300
处理器301
输入/输出接口
304
总线307
通信接口
306
辅助存储器
305
系统内存302
网络接口卡
303

图 4

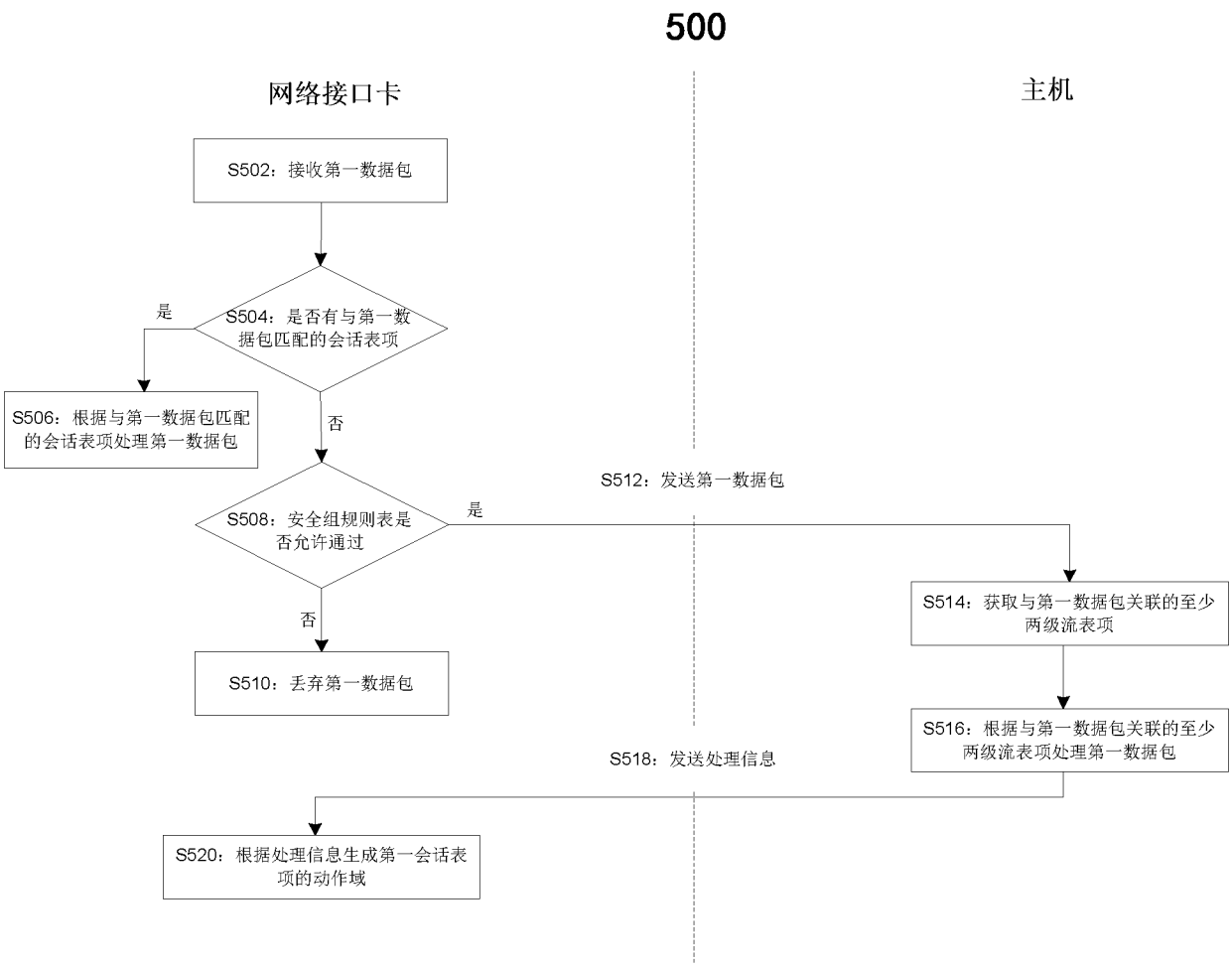
500
网络接口卡
主机
S502：接收第一数据包
S504：是否有与第一数据包匹配的会话表项
是
否
S506：根据与第一数据包匹配的会话表项处理第一数据包
S508：安全组规则表是否允许通过
是
否
S510：丢弃第一数据包
S512：发送第一数据包
S514：获取与第一数据包关联的至少两级流表项
S516：根据与第一数据包关联的至少两级流表项处理第一数据包
S518：发送处理信息
S520：根据处理信息生成第一会话表项的动作域

图 5

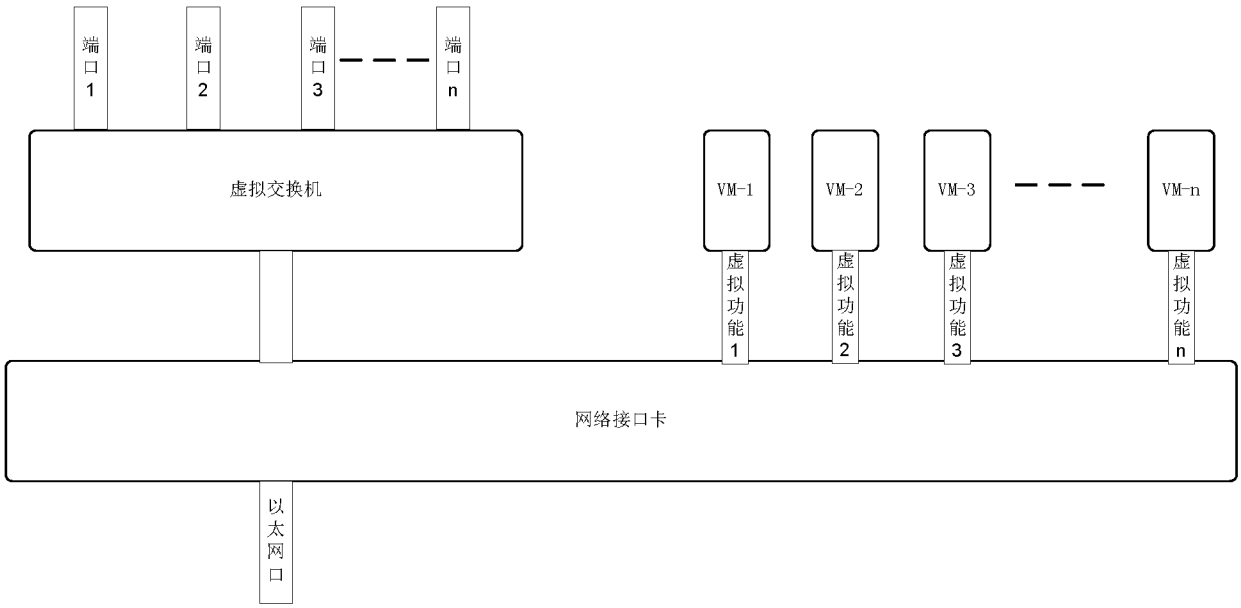
端口1
端口2
端口3
端口n
虚拟交换机
VM-1
VM-2
VM-3
VM-n
虚拟功能1
虚拟功能2
虚拟功能3
虚拟功能n
网络接口卡
以太网口

图 6

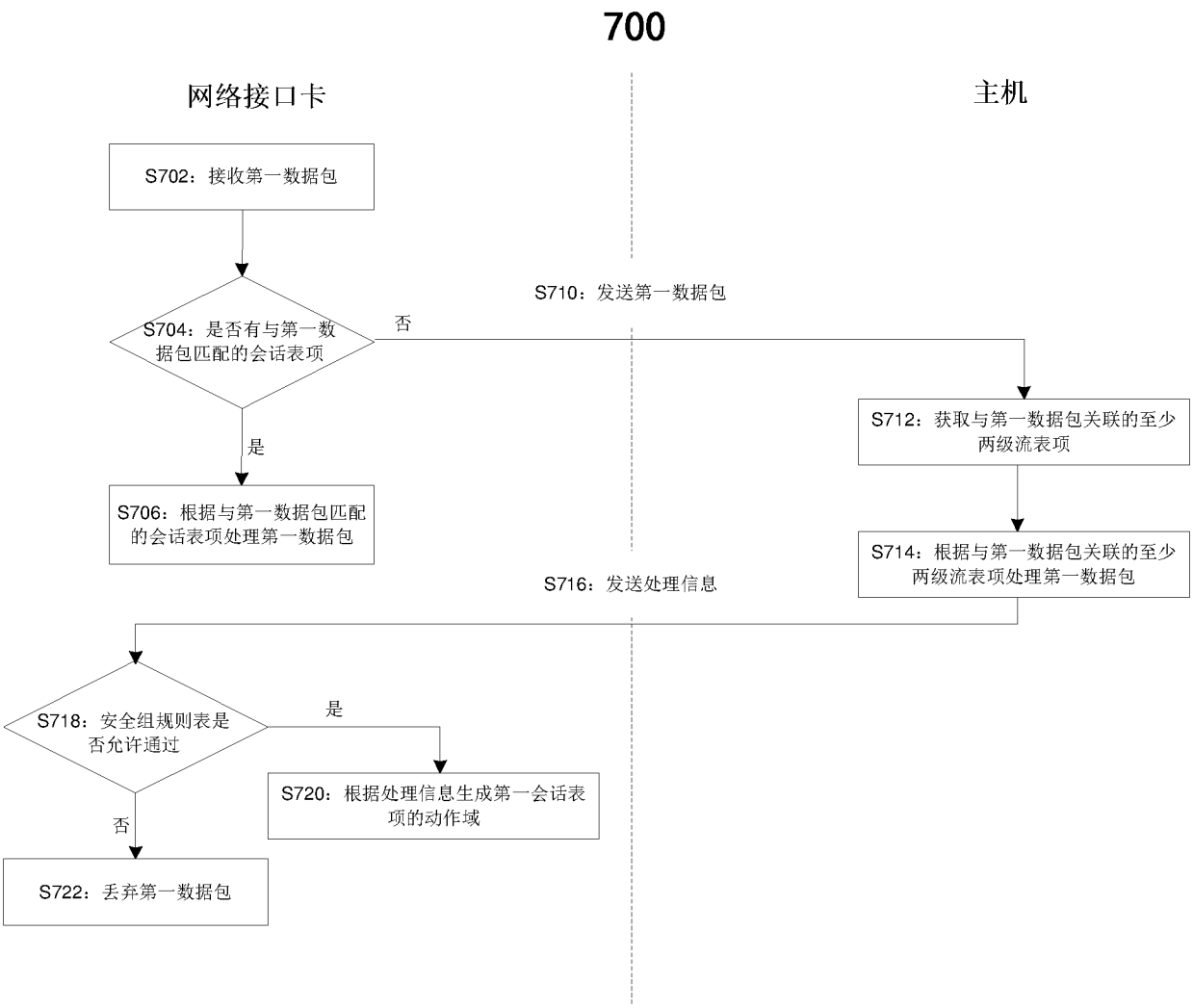
700
网络接口卡
主机
S702：接收第一数据包
S704：是否有与第一数据包匹配的会话表项
否
是
S706：根据与第一数据包匹配的会话表项处理第一数据包
S710：发送第一数据包
S712：获取与第一数据包关联的至少两级流表项
S714：根据与第一数据包关联的至少两级流表项处理第一数据包
S716：发送处理信息
S718：安全组规则表是否允许通过
是
否
S720：根据处理信息生成第一会话表项的动作域
S722：丢弃第一数据包

图 7

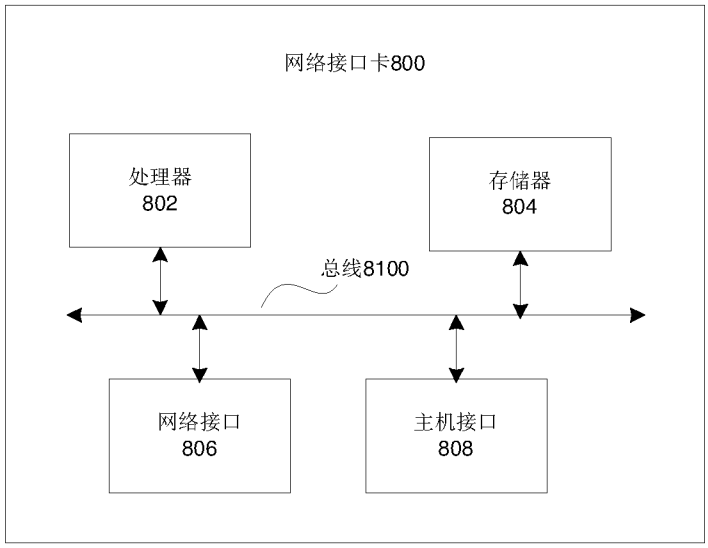
网络接口卡800
处理器
802
存储器
804
总线8100
网络接口
806
主机接口
808

图 8

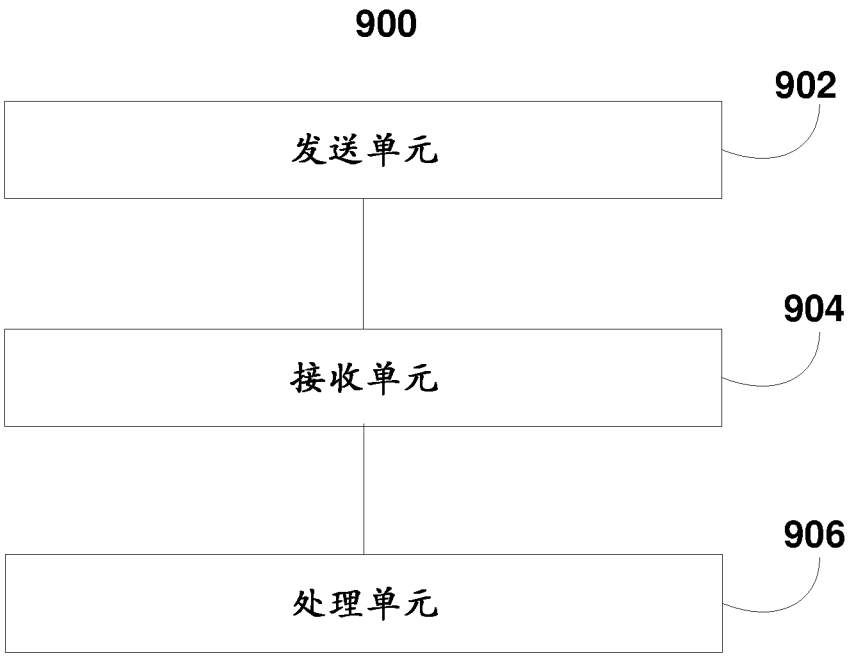

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/091278

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/741 (2013.01) i; G06F 9/48 (2006.01) 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)

H04L 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)

WPI, EPODOC, CNPAT: 虚拟机, 网卡, 网络适配器, NIC, 匹配, 转发, 流表, VM, virtual machine, network interface card, match, forward, transmit, flowtable

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 105245456 A (INSPUR (BEIJING) ELECTRONIC INFORMATION INDUSTRY CO., LTD), 13 January 2016 (13.01.2016), description, paragraphs 0112 and 0116, and figure 1	1-42
Y	CN 106302225 A (SHANGHAI UCLOUD INFORMATION TECHNOLOGY CO., LTD.), 04 January 2017 (04.01.2017), claim 2	1-42
A	CN 105939291 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.), 14 September 2016 (14.09.2016), entire document	1-42
A	CN 106815067 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 09 June 2017 (09.06.2017), entire document	1-42
A	CN 104883302 A (HUAWEI TECHNOLOGIES CO., LTD.), 02 September 2015 (02.09.2015), entire document	1-42
A	CN 104426816 A (HUAWEI TECHNOLOGIES CO., LTD.), 18 March 2015 (18.03.2015), entire document	1-42
A	CN 103401797 A (H3C TECHNOLOGIES CO., LIMITED), 20 November 2013 (20.11.2013), entire document	1-42
A	CN 106533942 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 22 March 2017 (22.03.2017), entire document	1-42

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 February 2018	26 February 2018
Name and mailing address of the ISA 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 HE, Xiulian Telephone No. (86-10) 62413423

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/091278

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105245456 A	13 January 2016	None	
CN 106302225 A	04 January 2017	None	
CN 105939291 A	14 September 2016	None	
CN 106815067 A	09 June 2017	None	
CN 104883302 A	02 September 2015	None	
CN 104426816 A	18 March 2015	WO 2015024373 A1	26 February 2015
CN 103401797 A	20 November 2013	None	
CN 106533942 A	22 March 2017	None	

国际检索报告

国际申请号 PCT/CN2017/091278

A. 主题的分类

H04L 12/741(2013.01)i; G06F 9/48(2006.01)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)

H04L 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）)

WPI, EPODOC, CNPAT: 虚拟机，网卡，网络适配器，NIC，匹配，转发，流表，VM, virtual machine, network interface card, match, forward, transmit, flowtable

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
Y	CN 105245456 A (浪潮北京电子信息产业有限公司) 2016年 1月 13日 (2016-01-13) 说明书第0112，0116段、图1	1-42
Y	CN 106302225 A (上海优刻得信息科技有限公司) 2017年 1月 4日 (2017-01-04) 权利要求2	1-42
A	CN 105939291 A (杭州迪普科技有限公司) 2016年 9月 14日 (2016-09-14) 全文	1-42
A	CN 106815067 A (中国移动通信集团公司) 2017年 6月 9日 (2017-06-09) 全文	1-42
A	CN 104883302 A (华为技术有限公司) 2015年 9月 2日 (2015-09-02) 全文	1-42
A	CN 104426816 A (华为技术有限公司) 2015年 3月 18日 (2015-03-18) 全文	1-42
A	CN 103401797 A (杭州华三通信技术有限公司) 2013年 11月 20日 (2013-11-20) 全文	1-42
A	CN 106533942 A (北京邮电大学) 2017年 3月 22日 (2017-03-22) 全文	1-42

☐ 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	国际检索报告邮寄日期
2018年 2月 9日	2018年 2月 26日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	贺秀莲
传真号 (86-10)62019451	电话号码 (86-10)62413423

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/091278

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 105245456 A	2016年 1月 13日	无	
CN 106302225 A	2017年 1月 4日	无	
CN 105939291 A	2016年 9月 14日	无	
CN 106815067 A	2017年 6月 9日	无	
CN 104883302 A	2015年 9月 2日	无	
CN 104426816 A	2015年 3月 18日	WO 2015024373 A1	2015年 2月 26日
CN 103401797 A	2013年 11月 20日	无	
CN 106533942 A	2017年 3月 22日	无	