

(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
2020 年 9 月 17 日 (17.09.2020)



(10) 国际公布号
WO 2020/181735 A1

(51) 国际专利分类号:
H04L 29/12 (2006.01)

(21) 国际申请号: PCT/CN2019/103258

(22) 国际申请日: 2019 年 8 月 29 日 (29.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910178099.7 2019 年 3 月 8 日 (08.03.2019) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 贾毫杰(JIA, Haojie); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

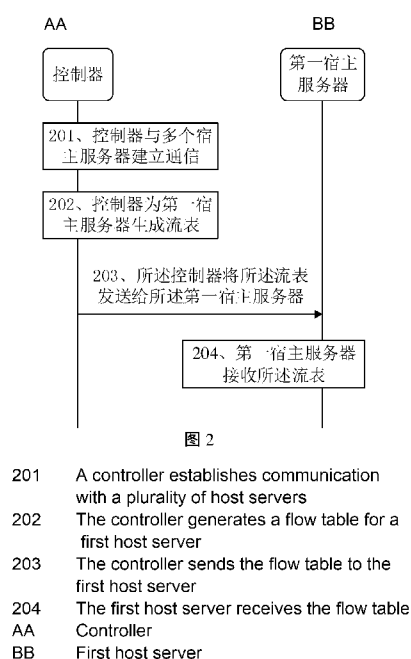
(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

(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,

(54) Title: METHOD FOR PROVIDING NETWORK ADDRESS TRANSLATION (NAT) SERVICE AND CONTROLLER

(54) 发明名称: 一种提供网络地址转换NAT服务的方法及控制器



(57) Abstract: Disclosed are a method for providing a network address translation (NAT) service and a controller. The method comprises: a controller establishing communication with a plurality of host servers; the controller generating a flow table for a first host server, wherein the first host server is any one of the host servers in the plurality of host servers which establish communication with the controller, the flow table comprises a plurality of table items, and each table item in the plurality of table items records an NAT forwarding rule; and the controller sending the flow table to the first host server, wherein the flow table is used by the first host server to provide an NAT service for a cloud host on the first host server. According to the embodiment of the present application, the efficiency of an NAT service is improved, while the bottleneck caused by a performance upper limit of an NAT gateway is also eliminated.

(57) 摘要: 本申请实施例公开了一种提供网络地址转换NAT服务的方法及控制器, 该方法包括: 控制器与多个宿主服务器建立通信, 控制器为第一宿主服务器生成流表, 所述第一宿主服务器为与所述控制器建立通信的多个宿主服务器中的任意一个宿主服务器, 所述流表包括多个表项, 所述多个表项中每个表项记录了一条NAT转发规则; 所述控制器将所述流表发送给所述第一宿主服务器, 所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供NAT服务。本申请实施例提高了NAT服务的效率, 同时也消除了NAT网关的性能上限所造成的瓶颈。

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, 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))。

一种提供网络地址转换 NAT 服务的方法及控制器

本申请要求于 2019 年 03 月 08 日提交中国专利局、申请号为 201910178099.7、申请名称为“一种提供网络地址转换 NAT 服务的方法及控制器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种提供网络地址转换 NAT 服务的方法和控制器。

背景技术

由于实际网络中公网地址资源有限，网关设备通常使用 NAT(Network Address Translation，网络地址转换) 功能来实现内网对 Internet 的访问，NAT 是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程，即 NAT 将数据中的私网地址转换为公网地址，以实现私有网络访问公共网络，且 NAT 通过使用少量的公网地址表示较多的私网地址，从而可减缓可用地址空间的枯竭。

业界通常使用 NAT 网关实例的方式提供 NAT 服务，这种实例可以采用虚拟机的方式部署，也可以用物理机集群的方式进行部署，不论哪种方式，都需要将流量分发到 NAT 网关实例处，对 NAT 网关本身的性能要求较高，一旦流量超过了设计的性能上限，NAT 网关很容易成为瓶颈点。

发明内容

本申请实施例提供了一种提供网络地址转换 NAT 服务的方法和控制器，通过控制器将 NAT 服务分散到各个计算节点上，消除了 NAT 网关的性能上限造成的瓶颈。

第一方面，本申请实施例提供了一种提供网络地址转换 NAT 服务的方法，该方法包括：控制器与多个宿主服务器建立通信；

所述控制器为第一宿主服务器生成流表，所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器，所述流表包括多个表项，所述多个表项中每个表项记录了一条 NAT 转发规则；

所述控制器将所述流表发送给所述第一宿主服务器，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

第二方面，本申请实施例提供了一种控制器，该控制器包括：

配置单元，用于与多个宿主服务器建立通信；

生成单元，用于为第一宿主服务器生成流表，所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器，所述流表包括多个表项，所述多个表项中每个表项记录了一条 NAT 转发规则；

第一发送单元，用于将所述流表发送给所述第一宿主服务器，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

第三方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质

存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行上述第一方面所述的方法。

第四方面，本申请实施例提供了一种服务器，包括处理器、通信接口和计算机可读存储介质，所述处理器、通信接口和计算机可读存储介质相互连接，其中，所述计算机可读存储介质用于存储应用程序代码，所述处理器被配置用于调用所述应用程序代码，执行上述第一方面所述的方法。

综上所述，本申请实施例通过控制器将 NAT 服务分散到各个计算节点上，各个计算节点通过流表的方式提供 NAT 服务，从而提高了 NAT 服务的效率，同时也消除了 NAT 网关的性能上限造成的瓶颈。

附图说明

下面将对本申请实施例中所需要使用的附图作介绍。

图 1 为本申请实施例提供的一种提供 NAT 服务的方法的系统架构示意图；

图 2 为本申请实施例提供的一种提供 NAT 服务的方法的流程示意图；

图 3 为本申请实施例提供的宿主服务器为其承载的云主机发送的报文提供 NAT 服务的示意图；

图 4 为本申请实施例提供一种控制器的结构示意图；

图 5 为本申请实施例提供一种服务器的结构示意图。

具体实施方式

本申请说明书、权利要求书和附图中出现的术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，术语“第一”、“第二”和“第三”等是用于区别不同的对象，而并非用于描述特定的顺序。

为了使本领域技术人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

以下分别进行详细说明。

为了更好的理解本申请实施例提供一种提供网络地址转换 NAT 服务的方法和控制器的，下面先对本申请实施例适用的一种提供网络地址转换 NAT 服务的方法的系统构架进行描述。参阅图 1，图 1 是本方案实施例提供的一种提供网络地址转换 NAT 服务的方法的系统架构示意图。如图 1 所示，系统架构可以包括一个控制器 101、一个或多个宿主服务器 102 以及一个或多个云主机 103。控制器 101 可以和宿主服务器 102 互相通信，各个宿主服务器 102 承载着一个或多个云主机 103，宿主服务器 102 和自身承载的云主机 103 可以互相通信。

需要说明的是，本申请提供的一种提供网络地址转换 NAT 服务的方法的系统构架不限

于图 1 所示系统架构。

基于图 1 给出的一种提供网络地址转换 NAT 服务的方法的系统架构,下面提供一种提供网络地址转换 NAT 服务的方法,一种提供网络地址转换 NAT 服务的方法的流程图如图 2 所示,可以包括以下步骤:

步骤 S201:控制器与多个宿主服务器建立通信。

具体地,该控制器上可以配置该多个宿主服务器的网络地址(可以是互联网中的地址,也可以是局域网中的地址,或者其他同于通信的地址),从而识别来自该多个宿主服务器的数据包,以及针对性地向该多个宿主服务器发送数据包;相应的,该多个宿主服务器上也都可以配置该控制器的网络地址,从而识别来自该控制器的数据包,以及针对性地向该控制器发送数据包。另外,该控制器与该多个宿主服务器之间可以通过有线,或者无线的方式进行数据传输。

S202、控制器为第一宿主服务器生成流表。

具体的,所述第一宿主服务器为与所述控制器建立通信的多个宿主服务器中的任意一个宿主服务器,所述流表包括多个表项,所述多个表项中每个表项记录了一条 NAT 转发规则。

在具体实施方式中,当所述第一宿主服务器与所述控制器第一次建立通信时或者在所述第一宿主服务器发送 NAT 服务请求指令给控制器时,所述控制器为该第一宿主服务器生成对应的流表。该流表中包含多个表项,每个表项都记录了一条 NAT 转发规则。

在其中一种可能的实施方案中,上述 NAT 转发规则可以包括私网信息与公网信息之间的转换规则,其中,所述私网信息包括私网的互联网协议 IP 地址和私网的端口信息,所述公网信息包括公网的 IP 地址和公网的端口信息,所述私网为所述第一宿主服务器上的云主机所属的专用网络。具体的 NAT 转发规则示例可以参考表 1,表 1 给出了 NAT 转发规则包含的信息的示例,主要是私网访问公网的地址和端口映射表。私网 IP 地址为 10.0.0.2,对应的端口号为 1723 的云主机访问公网,需要将该云主机的私网 IP 地址和端口号替换为公网 IP 地址和公网的端口号,根据表 1,可以将云主机的私网 IP 地址为 10.0.0.2 替换为 131.107.0.1,端口号 1723 替换为 4000,替换完成后云主机使用新的 IP 地址和端口号 131.107.0.1/4000 即可访问公网。

表 1 私网访问公网的地址和端口映射表

-	私网 IP 地址	私网端口号	公网 IP 地址	公网端口号
第一表项	10.0.0.2	1723	131.107.0.1	4000
第二表项	10.0.0.3	1723	131.107.0.1	4001
第三表项	10.0.0.4	1724	131.107.0.1	4002

在其中一种可能的实施方式中,所述控制器为第一宿主服务器生成流表之前,还包括:所述控制器接收所述第一宿主服务器发送的 NAT 服务请求指令,所述请求指令用于请求所述控制器为所述第一宿主服务器生成所述流表。

具体的,当第一宿主服务器上的云主机需要访问公网,向该第一宿主服务器发送报文,则第一宿主服务器根据报文信息向控制器发送 NAT 服务请求指令,这个请求指令用于请求

控制器为所述第一宿主服务器生成流表，控制器接收到请求指令后，根据请求指令为第一宿主服务器生成对应的流表，然后将该流表发送给第一宿主服务器。

本实施例通过请求指令请求控制器为宿主服务器生成流表，可以使得控制器的资源优化并及时对宿主服务器的 NAT 服务请求作出相应，进一步提高了 NAT 服务的处理效率。

S203、所述控制器将所述流表发送给所述第一宿主服务器。

具体的，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。在具体的实施方式中，所述控制器为所述第一宿主服务器生成对应的流表后，将该流表发送给第一宿主服务器。

S204、第一宿主服务器接收所述流表。

在具体的实施方式中，第一宿主服务器接收所述控制器发送的流表后，将该流表存储在本地存储器中。当第一宿主服务器上的云主机需要访问公网，向该第一宿主服务器发送报文，则第一宿主服务器调用存储在本地流表，根据该流表为报文匹配流表项，匹配到流表项之后根据流表项将报文的私网 IP 地址和私网端口号替换为公网 IP 地址和公网端口号，然后将替换了 IP 地址和端口的报文转发到公网中。

为了便于理解，图 3 给出了宿主服务器为其承载的云主机发送的报文提供 NAT 服务的示意图。假设云主机要访问目的 IP 地址和端口号分别为 202.99.160.2 和 80 的公网服务器，该云主机的私网 IP 地址和端口号分别为 10.0.0.2 和 1723，该云主机使用私网 IP 地址不能访问外网的服务器，因而需要将其私网 IP 地址替换为外网的 IP 地址，为了外网反馈信息时能准确反馈到对应的云主机上也需要添加上对应的端口信息。所以图 3 中云主机将携带了私网 IP 地址和端口号以及目的 IP 地址和端口号的报文发送到宿主服务器，宿主服务器根据流表为该报文匹配流表项，具体表项可以参考表 1，匹配到流表项后根据流表项将报文的私网 IP 地址和端口号替换为 131.107.0.1/4000，目的 IP 地址和端口号不变，这样报文的源 IP 地址和源端口号属于公网的 IP 地址和端口号，从而使得云主机可以访问目的 IP 地址和端口号分别为 202.99.160.2 和 80 的公网服务器。

在其中一种可能的实施方式中，所述控制器将所述流表发送给所述第一宿主服务器之后，还包括：所述控制器接收所述第一宿主服务器发送的报文；所述控制器根据所述报文确定包含所述报文的 NAT 转发规则的表项；所述控制器将所述包含所述报文的 NAT 转发规则的表项发送给所述第一宿主服务器。

具体的，在所述第一宿主服务器根据上述流表为所述报文匹配流表项失败的情况下，所述第一宿主服务器将该报文发送给控制器，控制器接收该报文，根据该报文为其生成对应的流表项，同样的，该表项包含了所述报文的 NAT 转发规则，用于所述第一宿主服务器对所述报文执行 NAT 操作，然后控制器将其流表项发送给第一宿主服务器，第一宿主服务器接收该流表项之后根据该流表项为所述报文替换 IP 地址和端口号，然后将报文转发到公网中。

采用本申请实施例，当宿主服务器为自身承载的云主机发送的报文根据流表匹配表项失败时，控制器可以为该报文生成或从现有的流表中选择其对应的表项并将该表项发送宿主服务器，从而使得宿主服务器可以成功地为该报文提供 NAT 服务。

或者，在另一种可能的情况下，控制器接收所述第一宿主服务器因匹配表项失败而发

送的报文后，控制器从该控制器维护的流表中为所述报文匹配流表项，确定了流表项之后，将该流表项发送给第一宿主服务器，第一宿主服务器同样地接收该流表项，根据该流表项为所述报文替换 IP 地址和端口号，然后将报文转发到公网中。

或者，在另一种可能的实施方式中，控制器接收所述第一宿主服务器因匹配表项失败而发送的报文后，为所述报文匹配表项失败，所述控制器将为所述报文匹配表项失败的信息返回给第一宿主服务器，第一宿主服务器将所述报文丢弃。

在其中一种可能的实施方式中，在所述第一宿主服务器根据上述流表为所述报文匹配流表项失败的情况下，直接将报文丢弃。

综上所述，该方法通过控制器将 NAT 服务分散到各个计算节点上，各个计算节点通过流表的方式提供 NAT 服务，从而提高了 NAT 服务的效率，同时也消除了 NAT 网关的性能上限所造成的瓶颈。

为了便于更好地实施本申请的上述方案，本申请实施例还对应提供了一种控制器，下面结合附图来进行详细说明：

图 4 所示为一种控制器 400 的结构示意图，所述控制器 400 可以是图 1 所述一种提供网络地址转换 NAT 服务的方法的系统构架中的控制器 101，所述控制器 400 包括：配置单元 401、生成单元 402 和第一发送单元 403，其中：

配置单元 401，用于与多个宿主服务器建立通信；

生成单元 402，用于为第一宿主服务器生成流表，所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器，所述流表包括多个表项，所述多个表项中每个表项记录了一条 NAT 转发规则；

第一发送单元 403，用于将所述流表发送给所述第一宿主服务器，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

在其中一种实施方式中，控制器 400 还包括第一接收单元、确定单元和第二发送单元，其中：

所述第一接收单元，用于在所述第一发送单元将所述流表发送给所述第一宿主服务器之后接收所述第一宿主服务器发送的报文；

所述确定单元，用于根据所述报文确定包含所述报文的 NAT 转发规则的表项；

所述第二发送单元，用于将所述包含所述报文的 NAT 转发规则的表项发送给所述第一宿主服务器，所述包含所述报文的 NAT 转发规则的表项用于所述第一宿主服务器对所述报文执行 NAT 操作。

在其中一种实施方式中，所述接收单元用于接收所述第一宿主服务器发送的报文，具体为：

用于接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文。

在其中一种实施方式中，控制器 400 还包括：

第二接收单元，用于在所述生成单元为第一宿主服务器生成流表之前，接收所述第一宿主服务器发送的 NAT 服务请求指令，所述请求指令用于请求所述控制器为所述第一宿主服务器生成所述流表。

在其中一种实施方式中，所述 NAT 转发规则包括私网信息与公网信息之间的转换规则，

其中,所述私网信息包括私网的互联网协议 IP 地址和私网端口信息,所述公网信息包括公网的 IP 地址和公网端口信息,所述私网为所述第一宿主服务器上的云主机所属的专用网络。

图 4 所示的服务器 400 中各个单元的具体实现及有益效果可以对应参照图 2 所示的方法实施例中的相应描述,此处不再赘述。

请参见图 5,图 5 是本申请实施例提供的一种服务器 500,该服务器 500 包括处理器 501、存储器 502(即计算机可读存储介质)和通信接口 503,所述处理器 501、存储器 502 和通信接口 503 通过总线 504 相互连接。

存储器 502 包括但不限于是随机存储记忆体(random access memory, RAM)、只读存储器(read-only memory, ROM)、可擦除可编程只读存储器(erasable programmable read only memory, EPROM)或便携式只读存储器(compact disc read-only memory, CD-ROM),该存储器 502 用于相关指令及数据的存储。通信接口 503 用于接收和发送数据。

处理器 501 可以是一个或多个中央处理器(central processing unit, CPU),在处理器 501 是一个 CPU 的情况下,该 CPU 可以是单核 CPU,也可以是多核 CPU。

该服务器 500 中的处理器 501 用于读取所述存储器 502 中存储的程序代码,执行以下操作:

处理器 501 与多个宿主服务器建立通信;

处理器 501 为第一宿主服务器生成流表,所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器,所述流表包括多个表项,所述多个表项中每个表项记录了一条 NAT 转发规则;

处理器 501 通过通信接口 503 将所述流表发送给所述第一宿主服务器,所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

在其中一种实施方式中,处理器 501 通过通信接口 503 将所述流表发送给所述第一宿主服务器之后,还包括:

处理器 501 通过通信接口 503 接收所述第一宿主服务器发送的报文;

处理器 501 根据所述报文确定包含所述报文的 NAT 转发规则的表项;

处理器 501 通过通信接口 503 将所述包含所述报文的 NAT 转发规则的表项发送给所述第一宿主服务器,所述包含所述报文的 NAT 转发规则的表项用于所述第一宿主服务器对所述报文执行 NAT 操作。

在其中一种实施方式中,处理器 501 通过通信接口 503 接收所述第一宿主服务器发送的报文,具体为:

处理器 501 通过通信接口 503 接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文。

在其中一种实施方式中,处理器 501 为第一宿主服务器生成流表之前,还包括:

处理器 501 通过通信接口 503 接收所述第一宿主服务器发送的 NAT 服务请求指令,所述请求指令用于请求所述控制器为所述第一宿主服务器生成所述流表。

在其中一种实施方式中,所述 NAT 转发规则包括私网信息与公网信息之间的转换规则,其中,所述私网信息包括私网的互联网协议 IP 地址和私网端口信息,所述公网信息包括公网的 IP 地址和公网端口信息,所述私网为所述第一宿主服务器上的云主机所属的专用网络。

需要说明的是，上述各个操作的实现还可以对应参照图 2 所示的方法实施例的相应描述。

在图 5 所描述的服务器 500 通过控制器将 NAT 服务分散到各个计算节点上，各个计算节点通过流表的方式提供 NAT 服务，从而提高了 NAT 服务的效率，同时也消除了 NAT 网关的瓶颈点。

本申请实施例还提供了一种计算机可读存储介质，所述计算机存储介质存储有计算机程序，所述计算机程序包括程序指令，当所述程序指令被处理器执行时，图 2 所示的方法流程得以实现。

综上所述，本申请实施例提供了一种提供网络地址转换 NAT 服务的方法和控制器，通过控制器将 NAT 服务分散到各个计算节点上，各个计算节点通过流表的方式提供 NAT 服务，从而提高了 NAT 服务的效率，同时也消除了 NAT 网关的性能上限所造成的瓶颈。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，该流程可以由计算机程序来指令相关的硬件完成，该程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法实施例的流程。而前述的存储介质包括：ROM 或随机存储记忆体 RAM、磁碟或者光盘等各种可存储程序代码的介质。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。

最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：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申请各实施例技术方案的范围。

权 利 要 求

1、一种提供网络地址转换 NAT 服务的方法，其特征在于，包括：

控制器与多个宿主服务器建立通信；

所述控制器为第一宿主服务器生成流表，所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器，所述流表包括多个表项，所述多个表项中每个表项记录了一条 NAT 转发规则；

所述控制器将所述流表发送给所述第一宿主服务器，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

2、根据权利要求 1 所述方法，其特征在于，所述控制器将所述流表发送给所述第一宿主服务器之后，还包括：

所述控制器接收所述第一宿主服务器发送的报文；

所述控制器根据所述报文确定包含所述报文的 NAT 转发规则的表项；

所述控制器将所述包含所述报文的 NAT 转发规则的表项发送给所述第一宿主服务器，所述包含所述报文的 NAT 转发规则的表项用于所述第一宿主服务器对所述报文执行 NAT 操作。

3、根据权利要求 2 所述方法，其特征在于，所述控制器接收所述第一宿主服务器发送的报文，包括：

所述控制器接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文。

4、根据权利要求 1-3 任一项所述方法，其特征在于，所述控制器为第一宿主服务器生成流表之前，还包括：

所述控制器接收所述第一宿主服务器发送的 NAT 服务请求指令，所述请求指令用于请求所述控制器为所述第一宿主服务器生成所述流表。

5、根据权利要求 1 所述方法，其特征在于，所述 NAT 转发规则包括私网信息与公网信息之间的转换规则，其中，所述私网信息包括私网的互联网协议 IP 地址和私网端口信息，所述公网信息包括公网的 IP 地址和公网端口信息，所述私网为所述第一宿主服务器上的云主机所属的专用网络。

6、根据权利要求 3 所述的方法，其特征在于，所述控制器接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文之后，还包括：

所述控制器从所述控制器维护的流表中为所述报文匹配流表项，确定了流表项之后，将所述流表项发送给第一宿主服务器。

7、根据权利要求 3 所述的方法，其特征在于，所述控制器接收所述第一宿主服务器在

为报文匹配表项失败后发送的所述报文之后，还包括：

若所述控制器为所述报文匹配表项失败，所述控制器将为所述报文匹配表项失败的信息返回给所述第一宿主服务器，以提示所述第一宿主服务器将所述报文丢弃。

8、根据权利要求 1-3 任一项所述的方法，其特征在于，所述控制器为第一宿主服务器生成流表，包括：

在所述控制器接收到所述第一宿主服务器发送的 NAT 服务请求指令时，所述控制器为所述第一宿主服务器生成对应的流表。

9、根据权利要求 1-3 任一项所述的方法，其特征在于，所述控制器上配置了所述多个宿主服务器的网络地址，以用于识别来自所述多个宿主服务器的数据包，以及用于针对性地向所述多个宿主服务器发送数据包；所述多个宿主服务器上配置了所述控制器的网络地址，以用于识别来自所述控制器的数据包，以及用于针对性地向所述控制器发送数据包。

10、一种控制器，其特征在于，包括：

配置单元，用于与多个宿主服务器建立通信；

生成单元，用于为第一宿主服务器生成流表，所述第一宿主服务器为与所述控制器建立通信的所述多个宿主服务器中的任意一个宿主服务器，所述流表包括多个表项，所述多个表项中每个表项记录了一条 NAT 转发规则；

第一发送单元，用于将所述流表发送给所述第一宿主服务器，所述流表用于所述第一宿主服务器为所述第一宿主服务器上的云主机提供 NAT 服务。

11、根据权利要求 10 所述控制器，其特征在于，还包括第一接收单元、确定单元和第二发送单元，其中：

所述第一接收单元，用于在所述第一发送单元将所述流表发送给所述第一宿主服务器之后接收所述第一宿主服务器发送的报文；

所述确定单元，用于根据所述报文确定包含所述报文的 NAT 转发规则的表项；

所述第二发送单元，用于将所述包含所述报文的 NAT 转发规则的表项发送给所述第一宿主服务器，所述包含所述报文的 NAT 转发规则的表项用于所述第一宿主服务器对所述报文执行 NAT 操作。

12、根据权利要求 11 所述控制器，其特征在于，所述第一接收单元，用于接收所述第一宿主服务器发送的报文，具体为：

用于接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文。

13、根据权利要求 10-12 任一项所述控制器，其特征在于，所述第一接收单元，还用于在所述生成单元为第一宿主服务器生成流表之前，接收所述第一宿主服务器发送的 NAT 服务请求指令，所述请求指令用于请求所述控制器为所述第一宿主服务器生成所述流表。

14、根据权利要求 10 所述控制器，其特征在于，所述 NAT 转发规则包括私网信息与公网信息之间的转换规则，其中，所述私网信息包括私网的互联网协议 IP 地址和私网端口信息，所述公网信息包括公网的 IP 地址和公网端口信息，所述私网为所述第一宿主服务器上的云主机所属的专用网络。

15、根据权利要求 12 所述的控制器，其特征在于，所述第一发送单元，用于在所述第一接收单元接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文之后，从所述控制器维护的流表中为所述报文匹配流表项，确定了流表项之后，将所述流表项发送给所述第一宿主服务器。

16、根据权利要求 12 所述的控制器，其特征在于，所述第一发送单元，用于在所述第一接收单元接收所述第一宿主服务器在为报文匹配表项失败后发送的所述报文之后，若所述控制器为所述报文匹配表项失败，为所述报文匹配表项失败的信息返回给所述第一宿主服务器，以提示所述第一宿主服务器将所述报文丢弃。

17、根据权利要求 10-12 任一项所述的控制器，其特征在于，所述生成单元具体用于：在所述控制器接收到所述第一宿主服务器发送的 NAT 服务请求指令时，为所述第一宿主服务器生成对应的流表。

18、根据权利要求 10-12 任一项所述的控制器，其特征在于，所述控制器上配置了所述多个宿主服务器的网络地址，以用于识别来自所述多个宿主服务器的数据包，以及用于针对性地向所述多个宿主服务器发送数据包；所述多个宿主服务器上配置了所述控制器的网络地址，以用于识别来自所述控制器的数据包，以及用于针对性地向所述控制器发送数据包。

19、一种控制器，其特征在于，所述控制器包括处理器、计算机可读存储介质和通信接口，其中，所述计算机可读存储介质用于存储程序指令，所述通信接口用于在所述处理器的控制下执行数据的接收和发送操作，所述处理器用于调用所述程序指令来执行权利要求 1-9 任一项所述的方法。

20、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质用于存储程序指令，所述程序指令在处理器上运行时，实现权利要求 1-9 任一项所述的方法。

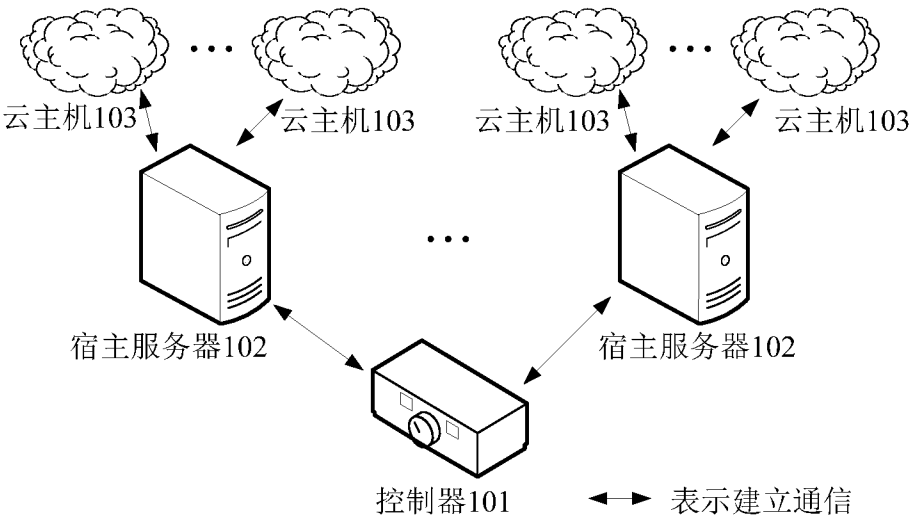


图 1

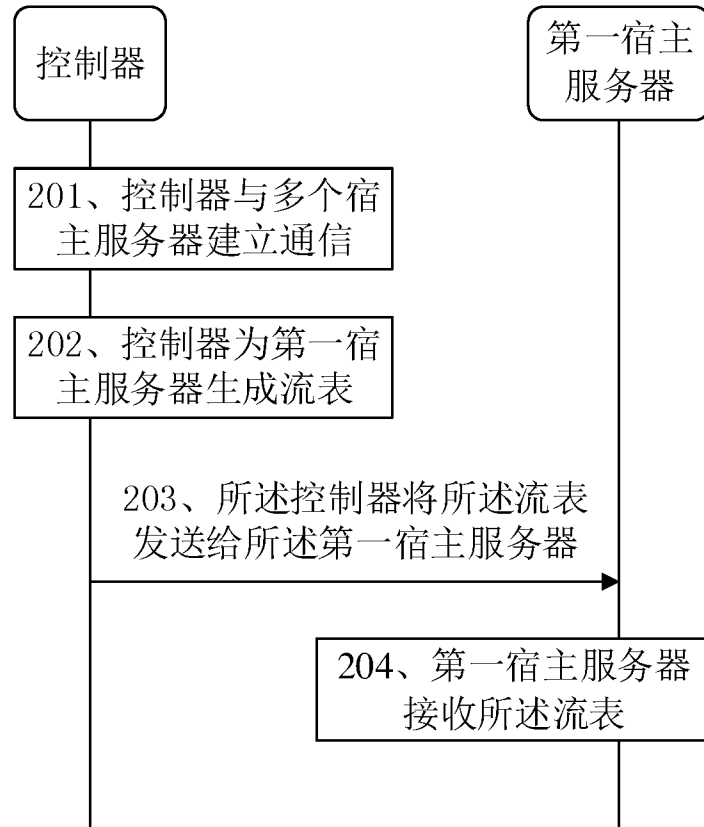


图 2

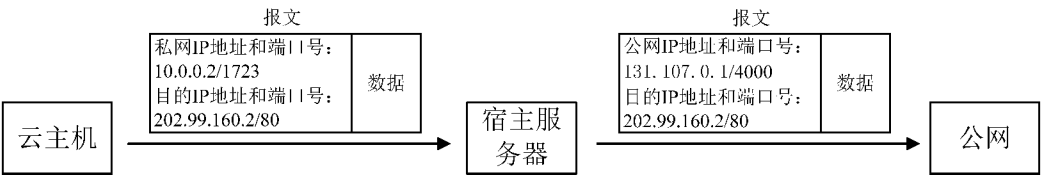


图 3

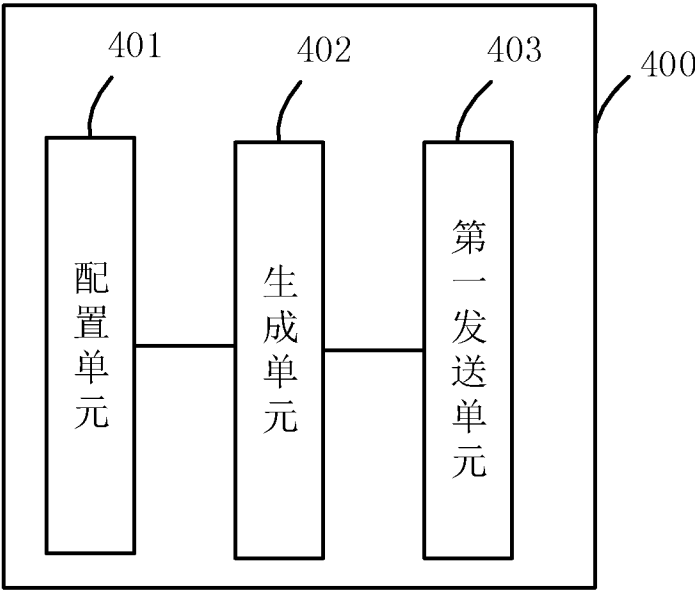


图 4

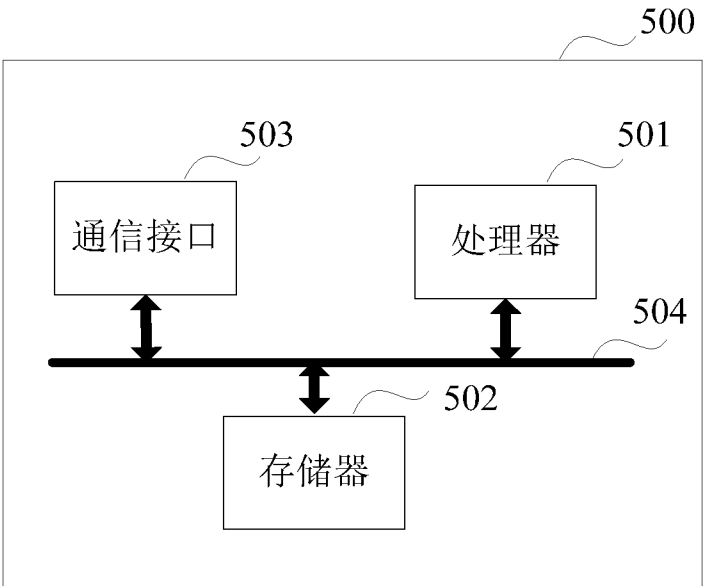


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/103258

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/12(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

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, CNKI: 网络地址转换, 转发, 规则, 流表, 表项, 映射表, 宿主, 云, 主机, 虚拟, network address translation, NAT, flow table, forwarding rule, cloud, host server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110012118 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 12 July 2019 (2019-07-12) description, paragraphs [0004]-[0040]	1-20
X	CN 104601432 A (H3C TECHNOLOGIES CO., LTD.) 06 May 2015 (2015-05-06) description, paragraphs [0063]-[0099]	1-20
X	CN 107172120 A (LENOVO (BEIJING) CO., LTD.) 15 September 2017 (2017-09-15) description, paragraphs [0067]-[0117]	1-20
A	CN 104601738 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER) 06 May 2015 (2015-05-06) entire document	1-20
A	CN 103581324 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 12 February 2014 (2014-02-12) entire document	1-20
A	WO 2017032300 A (HUAWEI TECHNOLOGIES CO., LTD.) 02 March 2017 (2017-03-02) entire document	1-20



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

06 November 2019

Date of mailing of the international search report

28 November 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/103258

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110012118	A	12 July 2019	None	
CN	104601432	A	06 May 2015	None	
CN	107172120	A	15 September 2017	None	
CN	104601738	A	06 May 2015	None	
CN	103581324	A	12 February 2014	None	
WO	2017032300	A	02 March 2017	CN 106487695 A	08 March 2017

国际检索报告

国际申请号

PCT/CN2019/103258

A. 主题的分类 H04L 29/12 (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 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, EPDOC, CNPAT, CNKI: 网络地址转换, 转发, 规则, 流表, 表项, 映射表, 宿主, 云, 主机, 虚拟, network address translation, NAT, flow table, forwarding rule, cloud, host server		
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
PX	CN 110012118 A (平安科技深圳有限公司) 2019年 7月 12日 (2019 - 07 - 12) 说明书第[0004]-[0040]段	1-20
X	CN 104601432 A (杭州华三通信技术有限公司) 2015年 5月 6日 (2015 - 05 - 06) 说明书第[0063]-[0099]段	1-20
X	CN 107172120 A (联想北京有限公司) 2017年 9月 15日 (2017 - 09 - 15) 说明书第[0067]-[0117]段	1-20
A	CN 104601738 A (国家计算机网络与信息安全管理中心) 2015年 5月 6日 (2015 - 05 - 06) 全文	1-20
A	CN 103581324 A (中国联合网络通信集团有限公司) 2014年 2月 12日 (2014 - 02 - 12) 全文	1-20
A	WO 2017032300 A (HUAWEI TECHNOLOGIES CO., LTD.) 2017年 3月 2日 (2017 - 03 - 02) 全文	1-20
☐ 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 2019年 11月 6日		国际检索报告邮寄日期 2019年 11月 28日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 黄欣欣 电话号码 (86-10)53961641

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/103258

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	110012118	A	2019年 7月 12日	无	
CN	104601432	A	2015年 5月 6日	无	
CN	107172120	A	2017年 9月 15日	无	
CN	104601738	A	2015年 5月 6日	无	
CN	103581324	A	2014年 2月 12日	无	
WO	2017032300	A	2017年 3月 2日	CN 106487695 A	2017年 3月 8日