

(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
2018 年 4 月 5 日 (05.04.2018)



(10) 国际公布号
WO 2018/059284 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) **H04L 12/46** (2006.01)
- (21) 国际申请号: PCT/CN2017/102386
- (22) 国际申请日: 2017 年 9 月 20 日 (20.09.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610854615.X 2016 年 9 月 27 日 (27.09.2016) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人; 及
- (71) 申请人 (仅对 US): 肖寒 (XIAO, Han) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。 孙成浩 (SUN, Chenghao) [CN/CN]; 中国浙

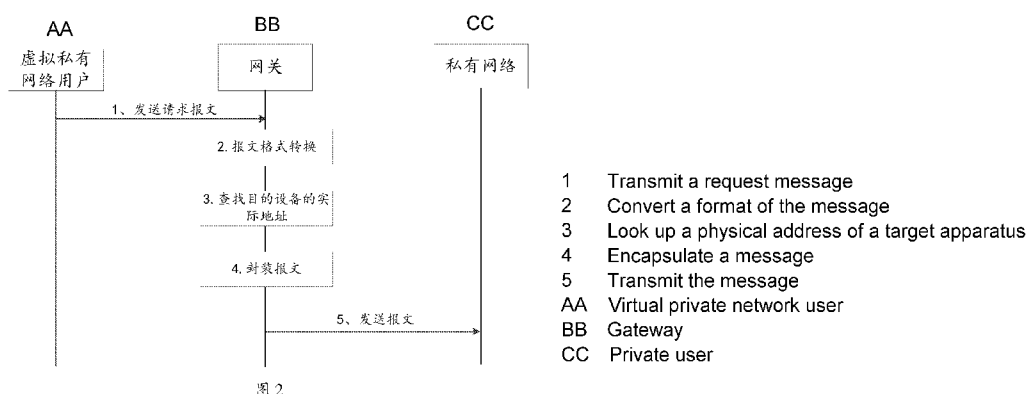
江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。
梁军 (LIANG, Jun) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号 渔阳置业大厦 B 座 605, Beijing 100029 (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,

(54) Title: DATA TRANSMISSION METHOD AND NETWORK EQUIPMENT

(54) 发明名称: 一种数据传输的方法及网络设备



(57) Abstract: The embodiments of the invention relate to the field of telecommunication, and in particular, to a data transmission method. The method comprises: providing a specific configuration of a server address, to enable a user in a virtual private network to obtain, using only a private network capable of providing a service, various services provided by corresponding servers. The embodiment is utilized to enable a user in a virtual private network to obtain services without employing another network other than the private network, thereby reducing, for the user, network traffic.

(57) 摘要: 本方案实施例提供了一种数据传输的方法, 应用于通信技术领域。该方法通过对提供服务的服务器地址进行特定设置, 使得虚拟私有网络内的用户只需能够提供业务服务的私有网络, 就能够获取各项由相应服务器提供的服务, 使得虚拟私有网络内部的用户不需要通过访问除私有网络外的其它网络来获取服务, 从而为用户节省了流量。

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,
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))。

一种数据传输的方法及网络设备

技术领域

本方案涉及通信领域，尤其涉及一种数据传输的方法及网络设备。

背景技术

在 VPC (virtual private cloud, 虚拟私有云) 网络中，每个用户的在网内的地址是可以在相关规范内的地址范围进行自定义设置。由于 VPC 内的地址空间由用户自由规划、地址资源由用户自由控制，因此，云服务提供商都会避免通过占用 VPC 内的网络地址来随便侵入用户在 VPC 内的地址空间。这样的话，云服务提供商无法通过在 VPC 网络内部设置一个统一的 IP 地址为用户提供某种服务，特别是基础服务如 NTP (Network Time Protocol, 网络时间协议)。

目前为了提供前述各个基础服务时，服务器提供商一般会要求用户通过访问指定的公网地址来获取各项基础服务。这种方案存在如下问题：需要用户自行购买公网地址，同时承担各项公网流量的费用。

发明内容

本方案的目的在于提供一种数据传输的方法及网络设备，能够在一定程度上避免用户使用公网流量获取私有网络提供的服务。

第一方面，本方案实施例提供了一种数据传输的方法，包括：

接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

对所述第一目的地址进行地址转换，得到第二目的地址；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述对所述第一目的地址进行地址转换，得到第二目的地址包括：

对所述第一报文进行解析，得到内部目的地址和虚拟网络标识；

根据所述内部目的地址，确定所述第一目的地址，以及，根据所述虚拟网络标识确定所述虚拟私有网络用户所在虚拟私有网络的网络标识信息；

在预配置的地址映射表中查找与所述第一目的地址以及所述网络标识信息共同对应的目的地址；

当查找到与所述第一目的地址以及所述网络标识信息共同对应的目的地址时，则将查找到的目的地址确定为所述第二目的地址。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述根据所述第二目的地址以及所述第一报文，生成第二报文包括：

当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式；

按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式包括：

将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；所述第二包头信息至少包括源地址和目的地址；

则所述按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文包括：

将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送包括：

根据所述第二目的地址以及路由表，确定下一跳设备，所述下一跳设备位于所述虚拟私有网络用户所在虚拟私有网络外部；

将所述第二报文向所述下一跳设备发送。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述指定地址不属于指定网络已配置的地址范围。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述虚拟私有网络为 VPC 网络。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，

所述第一格式为 VXLAN 格式，所述第二格式为 VLAN 格式。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述第一目的地址和所述第二目的地址对应于同一服务器。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述服务器为 NTP 服务器或加密服务器。

第二方面，本方案实施例还提供了一种数据传输的方法，包括：

接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；

对所述第一目的地址进行地址转换，得到第二目的地址；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向与第二类网络发送。

第三方面，本方案实施例还提供了一种数据传输的方法，包括：

接收网络设备发送的第一报文，所述第一报文携带有第一源地址；

对所述第一源地址进行地址转换，得到第二源地址；所述第二源地址为指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

根据所述第二源地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述对所述第一源地址进行地址转换，得到第二源地址包括：

对所述第一报文进行解析，得到所述第一源地址；

在预配置的地址映射表中查找与所述第一源地址对应的源地址；

当查找到与所述第一源地址对应的源地址时，则将查找到的源地址确定为所述第二源地址。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述根据所述第二源地址以及所述第一报文，生成第二报文包括：

当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式；

按照所述第二格式，将所述第一报文携带的报文信息和所述第二源地址进行封装，得到所述第二报文。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式包括：

将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一包头信息至少包括源地址和目的地址；所述第二报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；

则所述按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文包括：

将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述指定地址不属于指定网络已配置的地址范围。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述虚拟私有网络为 VPC 网络。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述第一格式为 VLAN 格式，所述第二格式为 VXLAN 格式。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述第一源地址和所述第二源地址对应于同一服务器。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述服务器为 NTP 服务器或加密服务器。

第四方面，本方案实施例还提供了一种数据传输的方法，包括：

接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址；

对所述第一目的地址进行地址转换，得到第二源地址；所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

第五方面，本方案实施例还提供了一种网络设备，包括：

接收单元，用于接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

转换单元，用于对所述第一目的地址进行地址转换，得到第二目的地址；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

第六方面，本方案实施例还提供了一种网络设备，包括：

接收单元，用于接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；

转换单元，用于对所述第一目的地址进行地址转换，得到第二目的地址；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与第二类网络发送。

第七方面，本方案实施例还提供了一种网络设备，包括：

接收单元，用于接收网络设备发送的第一报文，所述第一报文携带有第一源地址；

转换单元，用于对所述第一源地址进行地址转换，得到第二源地址；
所述第二源地址为指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

生成单元，用于根据所述第二源地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

第八方面，本方案实施例还提供了一种网络设备，包括：

接收单元，用于接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址；

转换单元，用于对所述第一目的地址进行地址转换，得到第二源地址；
所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

本方案实施例所提供的数据传输的方法及网络设备，使得虚拟私有网络内的用户只需能够提供业务服务的私有网络，就能够获取各项由相应服务器提供的服务，使得虚拟私有网络内部的用户不需要通过访问除私有网络外的其它网络来获取服务，从而为用户节省了流量。

附图说明

为了更清楚地说明本方案实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本方案的一些实施例，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它的附图。

图 1 为本方案实施例提供的一种网络架构示意图；

图 2 为本方案实施例提供的一种数据传输的基本原理图；

图 3 为本方案实施例提供的一种数据传输的方法流程图；

图 4 为本方案实施例提供的另一种数据传输的方法流程图；

图 5 为本方案实施例提供的另一种数据传输的方法流程图；

图 6 为本方案实施例提供的另一种数据传输的方法流程图；

图 7 为本方案实施例提供的另一种数据传输的方法流程图；

图 8 为本方案实施例提供的另一种数据传输的方法流程图；

图 9 为本方案实施例提供的另一种数据传输的方法流程图；

图 10 为本方案实施例提供的另一种数据传输的方法流程图；

图 11 为本方案实施例提供的另一种数据传输的方法流程图；

图 12 为本方案实施例提供的在具体场景下进行数据传输的方法流程示意图；

图 13 为本方案实施例提供的在具体场景下进行数据传输的方法流程示意图；

图 14 为本方案实施例提供的一种数据传输的基本原理图；

图 15 为本方案实施例提供的另一种数据传输的基本原理图；

图 16 为本方案实施例提供的一种数据传输的流程示意图；

图 17 为本方案实施例提供的基于加密服务实现的一种数据传输的流程图示意图；

图 18 为本方案实施例提供的一种用于数据传输的网络设备的组成框图；

图 19 为本方案实施例提供的一种用于数据传输的网络设备的组成框图；

图 20 为本方案实施例提供的一种用于数据传输的网络设备的组成框图；

图 21 为本方案实施例提供的一种用于数据传输的网络设备的组成框图；

图 22 为本方案实施例提供的一种用于数据传输的网络设备的组成框图。

具体实施方式

以下结合附图对本方案的原理和特征进行描述，所举实施例只用于解释本方案，并非用于限定本方案的范围。对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，根据本方案精神所获得的所有实施例，都属于本方案的保护范围。

本方案实施例适用于多种类型网络共同组建的系统架构中。在该系统架构中，各类型网络搭建时没有明确的干预关系，可以独立设置其内部的网络地址。每种类型的网络之间可通过地址转换设备衔接。

由虚拟私有网络（例如，VPC 等）、私有网络（例如，按照覆盖范围可以分为局域网和广域网等，按照实际搭建场景可以分为机房、服务器群

组、企业级内网等)及公用网络(例如, Internet 等)三类网络搭建的系统架构如图 1 所示, 各个类型网络之间通过网关进行通信, 各个网关一般配置有地址转换及路由转发等功能。基于前述如图 1 所示架构, 其可实现的基本通信流程可如图 2 所示, 包括:

步骤 1: 虚拟私有网络内部的用户发起初始的请求报文, 并将该请求报文发送至该虚拟私有网络的网关。

值得说明的是, 在虚拟私用网络内部, 根据实际网络配置需要, 还可以为用户提供用于报文转发、封装与解封装等功能的转发设备, 例如 VTEP (VXLAN 隧道终端, VXLAN Tunneling End Point)。由该转发设备代理用户与虚拟私用网络外部进行通信。

步骤 2: 该在网关所连接的虚拟私有网络和前述私有网络之间使用不同的报文格式时, 网关需要对接收到的请求报文进行格式转换, 以适应私有网络中的传输格式。

步骤 3: 该网关进行格式转换的同时, 还需要根据请求报文中的目的地址查找目的设备在私有网络中的实际地址。

步骤 4: 该网关依据实际地址和请求报文的请求内容, 按照适合私有网络中的传输格式进行封装。

步骤 5: 该网关将封装后的报文按照路由中规划的路径进行转发。

私有网络中的目的设备在接收到该请求报文后会根据请求内容进行相应处理, 同时将处理结果返回给该用户。该返回流程属于前述步骤 1 至 5 的逆过程, 在此不再赘述了。

基于前述描述, 本方案实施例提供了一种数据传输的方法, 适用于虚

拟私有网络与私有网络之间的网络设备上，该网络设备可以是网关、SLB（Server Load Balancing，服务器负载均衡）等，该方法流程如图3所示，包括：

101、接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址。

其中，第一目的地址为根据实际情况配置给虚拟私有网络内用户的服务器地址，一般与服务器在私有网络中的实际网络地址不相同。

其中，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围。此处提到的指定地址可理解为是归属于前述私有网络中的网络地址，为避免需要用户自行购买包括公网在内的除私有网络外的其它网络中的地址，同时承担各项网络流量的费用的问题出现，可将该指定地址配置为提供相应基础性服务（例如，NTP，加密服务等）的服务器（例如，NTP服务器或加密服务器）地址。进一步补充说明的是，若业务网络还连接于其它私有网络且可以与其它私有网络进行通信，则需要避免用户的对于前述各类基础性服务的访问流量流向其它私有网络，因此，此时也可以同时要求指定地址不属于其它私有网络某一或多个指定网络已配置的地址范围。

相应的，第一报文可以理解为是用于获取基础性服务的请求报文。由于该报文内携带的目的地址不属于虚拟私有网络内部的地址范围，因此，该报文会经由网关流向虚拟私有网络外部的网络中（在图1所示的架构中，第一报文会由虚拟私有网络流向私有网络中）。

当然，本方案实施例对于第一报文和指定地址的用途不作限定，二者

的用途也可以是为用户提供其它业务服务。

102、对所述第一目的地址进行地址转换，得到第二目的地址。

第二目的地址为与第一目的地址相对应，用于指示服务器在私有网络中的实际网络地址，因此第二目的地址和第一目的地址对应于同一服务器。

103、根据所述第二目的地址以及所述第一报文，生成第二报文。

由于目的地址发生变化，因此需要对第一报文的内容重新进行格式转换或重新打包等操作，以生成第二报文。

104、将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

本方案实施例所提供的数据传输的方法，使得虚拟私有网络内的用户只需能够提供业务服务的私有网络，就能够获取各项由相应服务器提供的服务，使得虚拟私有网络内部的用户不需要通过访问除私有网络外的其它网络来获取服务，从而为用户节省了流量。

由于本发明实施例中对于指定地址的独立设置，因此需要在前述网络设备中配置地址映射表，以存储指定地址和该指定地址所指向的服务器在私有网络中的实际地址之间的对应关系。结合该地址映射表的配置，本发明实施例针对如何从第一目的地址到第二目的地址进行转换提供了相应的实现流程，即前述步骤 102 的具体实现流程，如图 4 所示，包括：

1021、对所述第一报文进行解析，得到内部目的地址和虚拟网络标识。

其中，虚拟网络标识即用户所在的虚拟私有网络的标识信息，用于区分不同的虚拟私有网络。

1022、根据所述内部目的地址，确定所述第一目的地址，以及，根据

所述虚拟网络标识确定所述虚拟私有网络用户所在虚拟私有网络的网络标识信息。

1023、在预配置的地址映射表中查找与所述第一目的地址以及所述网络标识信息共同对应的目的地址。

由于并不是所有用户都有权使用基础性服务，因此，在查找该目的地址的过程中引入虚拟网络标识，其目的是为了区分不同类型的用户。当然这只是一个示例，在其它可能的实现方式中也可以处于其它目的来引入该虚拟网络标识，本方案实施例对此不作限定。

1024、当查找到与所述第一目的地址以及所述网络标识信息共同对应的目的地址时，则将查找到的目的地址确定为所述第二目的地址。

目前，私有网络中常用的IPv4地址范围包括10.0.0.0至10.255.255.255，172.16.0.0至172.31.255.255以及192.168.0.0至192.168.255.255。因此，此处提到的第二目的地址可以从这三段中选择。而针对目前IPv4地址范围的分配情况来说，在本方案实施例中，指定地址可以从100.64.0.0至100.64.0.10的地址范围中选择。该地址范围通常使用在私有网络中，同时一般不会被配置在除私有网络的其它网络上。

因此，第一目的地址（即指定地址）和第二目的地址可以被分别配置为100.64.10.10和10.10.10.101。这样就需要在地址映射表中添加一条映射关系100.64.10.10和VNI<—>10.10.10.101。

由于在不同类型的网络可能会基于不同的通信协议进行配置，因此前文提到的第一报文和第二报文可能具有不同的报文格式。本方案实施例针对这样的情况提供了相应的解决方案，即前述步骤103的一种可能的实现

方式，可参照图 5 所示内容，包括：

1031、当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式。

1032、按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

此处描述的第一格式是指用户所在的虚拟私有网络所支持的报文格式，第二格式是指私有网络所支持的报文格式。例如，当虚拟私有网络为 VPC 时，则对应的第一格式一般应符合 VXLANVXLAN (Virtual Extensible LAN 虚拟可扩展局域网)。当私有网络为虚拟局域网时，则对应的第二格式一般应符合 VLAN(Virtual LAN, 虚拟局域网)。当不同网络类型存在不同报文格式的时候，可以配置相应的格式转换方法，本方案实施例对于不同网络是使用的报文格式不作具体限定。

VXLAN 报文格式主要内容如下表 1 所示。

外部源 IP	外部目的 IP	虚拟网络标识	内部源 IP	外部源 IP	报文信息
--------	---------	--------	--------	--------	------

例如，

10.10.10.11	10.10.10.100	1111111	192.168.1.100	100.64.10.10	abc
-------------	--------------	---------	---------------	--------------	-----

VLAN 报文格式主要内容如下表 2 所示。

源地址	目的地址	报文信息
-----	------	------

例如，

10.10.10.11	10.10.10.101	abc
-------------	--------------	-----

以上示出的内容仅为相应报文的一部分内容，根据实际传输需要还可能设置有 MAC 地址等其它必要信息。

以前述 VXLAN 和 VLAN 报文格式为例，本方案实施例将在此具体描

述前述步骤 1031 和 1032 的实现过程，相关方法流程如图 6 所示，包括：

10311、将所述第一报文中符合第一格式（VXLAN）的第一报头信息替换为符合第二格式（VLAN）的第二包头信息。

由于所述第一报头信息会携带内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址，而所述第二包头信息只需要包括源地址和目的地址即可，因此在该格式转变的过程中，将保留 VXLAN 报文内携带的内部源 IP 作为 VLAN 报文的源 IP，同时保留 VXLAN 报文内携带的内部目的 IP 作为 VLAN 报文的目的 IP。而 VXLAN 报文内的其它 IP 地址和虚拟网络标识则在格式转换的过程中不予保留。

10321、将所述第二包头信息和所述报文信息进行封装，得到所述第二报文。

在依照第二格式进行封装时，由于格式转换后得到的 VLAN 报文携带的源 IP 和目的 IP 只是配置给虚拟私有网络内部用户进行使用的地址，因此还需要将所述第二包头信息中携带的目的地址为所述第二目的地址，以便能够将报文传输至正确的目标设备，而携带的源地址为所述网络设备的地址，以便反馈报文可以由该网络设备正确接收到。

另外，为了实现对于前述第二报文正确且快速的转发，需要预先在虚拟私有网络与私有网络之间的网关上配置与前述第二目的地址相关的路由表，以便接收到向第二目的地址发送的报文时，可以直接进行转发，本方案实施例针对这样的情况提供了相应的解决方案，即前述步骤 104 的一种可能的实现方式，可参照图 7 所示内容，包括：

1041、根据所述第二目的地址以及路由表，确定下一跳设备。

由于第二目的地址为私有网络中的服务器地址，因此所述下一跳设备会位于所述虚拟私有网络用户所在虚拟私有网络外部。

此处提及的路由表一般需要进行预先配置，或由网关通过自学习完成配置。

1042、将所述第二报文向所述下一跳设备发送。

以上为流量从虚拟私有网络中的用户侧流向私有网络侧的步骤说明，以下将会描述从私有网络侧流向虚拟私有网络中的用户侧的步骤。

本方案实施例还提供了一种数据传输的方法，也可以适用于如图 8 所示架构中，该方法包括：

201、接收私有网络中的网络设备发送的第一报文，所述第一报文携带有第一源地址。

202、对所述第一源地址进行地址转换，得到第二源地址。

203、根据所述第二源地址以及所述第一报文，生成第二报文。

204、将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

步骤 201 至步骤 204 的实现流程可以理解为是与步骤 101 至步骤 104 所描述流程的逆向流程，例如，若步骤 101 至步骤 104 实现了用户向私有网络服务器请求基础性服务，那么步骤 201 至步骤 204 就实现了服务器对用户请求的答复流程。

因此，第一源地址与前述第二目的地址实际上是相同的，都用于表示服务器在私有网络中的实际网络地址，而第二源地址与前述第一目的地址（即前述指定地址）是相同的，都用于表示提供给虚拟私有网络内用户的

服务器地址。

此处需要补充说明的是，此处描述的第一报文和第二报文均为服务器侧下发至用户侧的报文，与前文描述的第一报文和第二报文并不相同。

由于本发明实施例中对于指定地址的独立设置，因此需要在前述网络设备中配置地址映射表，以存储指定地址和该指定地址所指向的服务器在私有网络中的实际地址之间的对应关系。结合该地址映射表的配置，本发明实施例针对如何从第一目的地址到第二目的地址进行转换提供了相应的实现流程，即前述步骤 202 的具体实现流程，如图 9 所示，包括：

2021、对所述第一报文进行解析，得到所述第一源地址。

2022、在预配置的地址映射表中查找与所述第一源地址对应的源地址。

2023、当查找到与所述第一源地址对应的源地址时，则将查找到的源地址确定为所述第二源地址。

与前述步骤 1021 至 1024 是互为逆向过程，其详细实现可参照于前，本方案实施例在此不再赘述。

由于在不同类型的网络可能会基于不同的通信协议进行配置，因此前文提到的第一报文和第二报文可能具有不同的报文格式。本方案实施例针对这样的情况提供了相应的解决方案，即前述步骤 203 的一种可能的实现方式，可参照图 10 所示内容，包括：

2031、当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式。

2032、按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

此处描述的第一格式是指私有网络所支持的报文格式，第二格式是指用户所在的虚拟私有网络所支持的报文格式。例如，当私有网络为虚拟局域网时，则对应的第一格式一般应符合 VLAN。当虚拟私有网络为 VPC 时，则对应的第二格式一般应符合。

以前述 VXLAN 和 VLAN 报文格式为例，结合前述表 1 及表 2，本方案实施例将在此具体描述前述步骤 2031 和 2032 的实现过程，相关方法流程如图 11 所示，包括：

20311、将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息。

其中，所述第一包头信息至少包括源地址和目的地址；所述第二报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址。

20321、将所述第二包头信息和所述报文信息进行封装，得到所述第二报文。

所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

步骤 20311 及 20321 其实现的流程可以理解为是步骤 10311 和 10321 的逆向过程，即将报文由 VLAN 格式向 VXLAN 格式进行转换和再封装。

以上为流量从私有网络侧流向虚拟私有网络中的用户侧的步骤描述，其实现流程可以理解为是流量从虚拟私有网络中的用户侧流向私有网络侧的步骤相对应的逆过程，因此对于网络类型、各类网络内的报文格式、指定地址限定、报文转发方法等内容可互相参照理解，在此就不作过多陈

述。

下文将结合示例来直观阐述前述流量从私有网络侧流向虚拟私有网络中的用户侧相关方法的实现过程，以及，流量从虚拟私有网络中的用户侧流向私有网络侧相关方法的实现过程。

在该示例中，存在两个不同的 VPC，均支持 VXLAN，VPC1111111 和 VPC2222222，VPC1111111 内存在用户 A，VPC2222222 内存在用户 B。

用户 A 在 VPC1111111 内的源地址为 192.168.1.100，对外源地址为 10.10.10.11，虚拟网络标识为 1111111。

用户 A 在 VPC2222222 内的源地址为 192.168.1.100，对外源地址为 10.10.10.10，虚拟网络标识为 2222222。

VPC 与私有网络（支持 VLAN）之间的网关 VPC-GW 的网关地址为 10.10.10.100。

NTP 服务器通知给用户 A 和用户 B 的地址为 100.64.10.10，在私有网络中的实际地址为 10.10.10.101。

基于前述限定，流量从私有网络侧流向虚拟私有网络中的用户侧相关方法的实现过程参照图 12 所示报文转发流程，该流程包括：

301、用户 A 向 VPC-GW 发送的报文 1 和用户 B 向 VPC-GW 发送的报文 2。

报文 1 的包头携带有外部源地址 10.10.10.11，外部目的地址 10.10.10.100，虚拟网络标识 1111111，内部源地址 192.168.1.100，内部目的地址 100.64.10.10。

报文 2 的包头携带有外部源地址 10.10.10.10，外部目的地址

10.10.10.100, 虚拟网络标识 222222, 内部源地址 192.168.1.100, 内部目的地址 100.64.10.10。

302、VPC-GW 分别将接收到的报文 1 和报文 2 进行 VXLAN 格式到 VLAN 格式的转换, 得到报文 3 和报文 4。

报文 3 的包头携带有源地址 10.10.10.11, 目的地址 10.10.10.101。

报文 4 的包头携带有源地址 10.10.10.10, 目的地址 10.10.10.101。

303、VPC-GW 将报文 3 和报文 4 根据路由表记载的路由信息向 NTP 服务器发送。

基于前述限定, 流量从虚拟私有网络中的用户侧流向私有网络侧相关方法的实现过程, 参照图 13 所示报文转发流程, 该流程包括:

401、NTP 服务器将应答报文 3 的报文 5 和应答报文 4 的报文 6 返回给 VPC-GW。

报文 5 的包头携带有源地址 10.10.10.101, 目的地址 10.10.10.11。

报文 6 的包头携带有源地址 10.10.10.101, 目的地址 10.10.10.10。

402、VPC-GW 接收到报文 5 和报文 6 后, VPC-GW 分别将接收到的报文 5 和报文 6 进行 VLAN 格式到 VXLAN 格式的转换, 得到报文 7 和报文 8。

报文 7 的包头携带有外部源地址 10.10.10.100, 外部目的地址 10.10.10.11, 虚拟网络标识 1111111, 内部源地址 100.64.10.10, 内部目的地址 192.168.1.100。

报文 8 的包头携带有外部源地址 10.10.10.100, 外部目的地址 10.10.10.10, 虚拟网络标识 222222, 内部源地址 100.64.10.10, 内部目的

地址 192.168.1.100。

403、VPC-GW 分别将报文 7 发送至用户 A，以及，将报文 8 发送至用户 B。

以上示例中对于各网络设备网络地址的设定、各网络支持的报文格式的选择，格式转换的前后结果均不作限定，只是示意性的说明，其它可适用的技术均可结合于此。

结合前述描述可以推断出，本方案实施例并不局限于虚拟私有网络、私有网络及公共网络的组网架构中，还可以适用于其它多种类型构成的网络架构中。因此，本方案实施例提供了一种数据传输的总设计方案，应用于某两个网络间的报文转发设备上。

适用于服务请求流程的方法如图 14 所示，包括：

501、接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围。

502、对所述第一目的地址进行地址转换，得到第二目的地址。

503、根据所述第二目的地址以及所述第一报文，生成第二报文。

504、将所述第二报文向与第二类网络发送。

适用于服务请求应答流程的方法如图 15 所示，包括：

601、接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址。

602、对所述第一源地址进行地址转换，得到第二源地址；所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户

所在虚拟私有网络已配置的地址范围。

603、根据所述第二源地址以及所述第一报文，生成第二报文。

604、将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

另外，本方案实施例还提供以一个 VPC 发送端、一个 SLB、一台云端服务器为交互设备所实现的本方案提供的方法流程，其如图 16 所示。其中，VPC 发送端中包含有：VPC 虚拟机、VTEP。可以理解的是，该三方交互流程适用于任意个 VPC 发送端、任意个 SLB 和任意个云端服务器之间的交互。

VPC 是用户在公有云上租用的私有云空间，通过虚拟化技术在云端形成用户私有的服务器空间，其承载有用户的应用服务，叫做应用服务器或 VPC 虚拟。

VPC 虚拟机借助网络隔离技术，保障用户数据在各自所租用的应用服务器中的安全性。用户可将业务关联的应用服务部署在各自的应用服务器的虚拟机之上，由云端各个 VPC 虚拟机进行业务流程处理。例如，银行系统可以不必再自备数据库与业务处理服务器，而将转账业务部署在云端的 VPC 虚拟机中，由承载了转账业务的 VPC 虚拟机与云端服务器共同实现转账业务。各个 VPC 虚拟机与物理实体机一样，也具备各自的 IP 地址。在本实施例中，VPC 虚拟机的 IP 为 192.168.1.100。

VTEP 是 VLAN 隧道终端，其是由硬件或软件予以实现的支持 VxLan 的设备，可以作为一个中间层来对 VxLan 报文进行封装和解封装。对于 VPC 发送端来说，VTEP 根据虚拟网络标识 VNI、IP 来封装 VxLan 头，完

成对应用服务器发出的原始请求包的封装。同理，当 VPC 发送端接收由云端服务器返回的数据包时，该数据包也需要经由 VTEP 进行解封装，得到 VxLan 报文，进行获取到 VNI 和内层报文的目的 IP 地址，确定出目的 VPC 虚拟机，以将内层报文发送到该目的 VPC 虚拟机。在本实施例中 VTEP 的 IP 地址为：10.10.10.11，相应的虚拟网络标识为 1111111。

SLB 为服务器负载调度器，其可以通过对请求进行转发来完成多台服务器的负载均衡以及跨网络访问。SLB 既可以是硬件实体，也可以是硬件实体上的虚拟装置，SLB 既可以与云端服务器网络进行通信，也可以与 VTEP 进行通信。通常，SLB 选定后，为 SLB 预先配置好 VPC 用户对应的 SLB 的私有网络内部 IP，该 SLB 的私有网络内部 IP 用于使 SLB 与 VPC 网络内的应用服务器进行交互，以使两者的交互如同在同一私有网络中进行通讯。该 SLB 还需要存储有云端服务器的实际网络地址与配置给 VPC 用户的服务器地址之间的对应关系，以使得 SLB 能够正常转发将 VPC 用户与云端服务器之间的数据通信。该 SLB 的 IP 地址为 10.10.10.100。

云端服务器为为用户提供各项云服务的设备。可处理由 SLB 转发过来的各项用户请求。其实际 IP 地址为 10.10.10.101，而配置给 VPC 用户的 IP 地址为 100.64.10.10。

基于前述设定，该方法流程包括：

s1、VPC 虚拟机发送原始请求包，以向所述云端服务器请求服务。

其中，原始请求包中的源 IP 是 VPC 发送端中 VPC 虚拟机的 IP 地址（192.168.1.100），目的 IP 是与预先配置给 VPC 用户的云端服务器的私有网络内部 IP 地址（100.64.10.10）。

s2、VTEP 基于 VxLan 协议对原始请求包进行封装，构造得到 Vxlan 包。

Vxlan 数据包的包头携带外部源地址（VTEP 的私有网络内部 IP 地址 10.10.10.11），外部目的地址（SLB 的私有网络内部 IP 地址 10.10.10.100），虚拟网络标识 1111111，内部源地址（VPC 虚拟机的在 VPC 网络内的 IP 地址 192.168.1.100），内部目的地址（配置给用户的云端服务器 IP 地址 100.64.10.10）。

s3、VTEP 将请求数据包向 SLB 发送。

s4、SLB 接收到该请求数据包后，对其进行解析。将该请求数据包由 VxLAN 格式转换为 VLAN 格式。

在此步骤中，SLB 从中解析出原始请求包，并将原始请求包中的源 IP 修改为 SLB 自身的 IP 地址（10.10.10.100）、将目的 IP 地址修改为云端服务器的 IP（10.10.10.101），原始请求包中的数据包内容保持不变，形成转发请求包，并将该转发请求包发送给云端服务器。

s5、SLB 向云端服务器发送转发请求包。

s6、云端服务器获取到 SLB 转发的请求包后，对其中数据包内的数据进行相应处理，并生成原始响应包。

s7、根据 SLB 自身的私有网络内部 IP 地址将该原始响应包发送到 SLB。

s8、SLB 接收到云端服务器发送的原始响应包后，对其进行解析。将该响应数据包由 VLAN 格式转换为 VxLAN 格式。

在该步骤中，SLB 对其中的地址内容进行修改，将原始响应包中源 IP 修改为云端服务器的 IP（100.64.10.10）、目的 IP 修改为 VPC 虚拟机的 IP

地址（192.168.1.100），原始响应包中的数据包保持不变，形成转发响应包。再将该转发响应包连同虚拟网络标识 VNI（1111111）等信息一起封装得到 VxLan 包该 Vxlan 数据包的包头携带外部源地址（SLB 的私有网络内部 IP 地址 10.10.10.100），外部目的地址（VTEP 的私有网络内部 IP 地址 10.10.10.11），虚拟网络标识 1111111，内部源地址（配置给用户的云端服务器 IP 地址 100.64.10.10），内部目的地址（VPC 虚拟机的在 VPC 网络内的 IP 地址 192.168.1.100）。

s9、SLB 将转发响应数据包发送给 VTEP。

s10、VTEP 接收到封装后的转发响应数据包后，对其进行解封装，并根据解封装后得到的 VNI 和目的 IP，确定 VPC 虚拟机。

s11、VTEP 将解封装得到的响应数据包发送给 VPC 虚拟机，实现整个应用服务器与云端服务器的交互过程。

另外，在为 VPC 用户提供加密服务的过程中，本方案实施例还提供以一个 VPC 发送端、一个 SLB、一台云端加密机为交互设备所实现的本方案提供的方法流程，其如图 17 所示。其中，VPC 发送端中包含有：VPC 虚拟机、VTEP。可以理解的是，该三方交互流程适用于任意个 VPC 发送端、任意个 SLB 和任意个云端加密机之间的交互。

在该实施例中，VPC 虚拟机的 IP 为 192.168.1.100。TEP 的 IP 地址为：10.10.10.11，相应的虚拟网络标识为 1111111。

SLB 的 IP 地址为 10.10.10.100。

云端加密机实际 IP 地址为 10.10.10.101，配置给 VPC 用户的 IP 地址为 100.64.10.10。

基于此处的设定，相应的方法流程如下，包括：

t1、VPC 虚拟机发送原始待加密请求包，以向所述云端加密机请求加密服务。

其中，原始待加密请求包中的源 IP 是 VPC 发送端中 VPC 虚拟机的 IP 地址（192.168.1.100），目的 IP 是与预先配置给 VPC 用户的云端加密机的私有网络内部 IP 地址（100.64.10.10）。

t2、VTEP 基于 VxLan 协议对原始待加密请求包进行封装，构造得到 Vxlan 包。

Vxlan 数据包的包头携带外部源地址（VTEP 的私有网络内部 IP 地址 10.10.10.11），外部目的地址（SLB 的私有网络内部 IP 地址 10.10.10.100），虚拟网络标识 1111111，内部源地址（VPC 虚拟机的在 VPC 网络内的 IP 地址 192.168.1.100），内部目的地址（配置给用户的云端加密机 IP 地址 100.64.10.10）。

t3、VTEP 将待加密请求数据包向 SLB 发送。

t4、SLB 接收到该待加密请求数据包后，对其进行解析。将该待加密请求数据包由 VxLAN 格式转换为 VLAN 格式。

在此步骤中，SLB 从中解析出原始待加密请求包，并将原始待加密请求包中的源 IP 修改为 SLB 自身的 IP 地址（10.10.10.100）、将目的 IP 地址修改为云端加密机的 IP（10.10.10.101），原始待加密请求包中的数据包内容保持不变，形成待加密请求转发包，并将该待加密请求转发包发送给云端加密机。

t5、SLB 向云端加密机发送待加密请求转发包。

t6、云端加密机获取到 SLB 转发的待加密请求转发包后，对其中数据包内的数据进行相应加密处理，并生成原始加密包。

t7、根据 SLB 自身的私有网络内部 IP 地址将该原始加密包发送到 SLB。

t8、SLB 接收到云端加密机发送的原始加密包后，对其进行解析。将该原始加密包由 VLAN 格式转换为 VxLAN 格式。

在该步骤中，SLB 对其中的地址内容进行修改，将原始加密包中源 IP 修改为云端加密机的 IP（100.64.10.10）、目的 IP 修改为 VPC 虚拟机的 IP 地址（192.168.1.100），原始加密包中的数据包保持不变，形成转发加密包。再将该转发加密包连同虚拟网络标识 VNI（1111111）等信息一起封装得到 VxLan 包该 Vxlan 数据包的包头携带外部源地址（SLB 的私有网络内部 IP 地址 10.10.10.100），外部目的地址（VTEP 的私有网络内部 IP 地址 10.10.10.11），虚拟网络标识 1111111，内部源地址（配置给用户的云端加密机 IP 地址 100.64.10.10），内部目的地址（VPC 虚拟机的在 VPC 网络内的 IP 地址 192.168.1.100）。

t9、SLB 将加密数据转发包发送给 VTEP。

t10、VTEP 接收到封装后的加密数据转发包后，对其进行解封装，并根据解封装后得到的 VNI 和目的 IP，确定 VPC 虚拟机。

t11、VTEP 将解封装得到的加密数据包发送给 VPC 虚拟机，实现整个应用服务器与云端加密机的交互过程。

前述 t1 至 t11 仅是针对加密过程的一种示例，对于其它服务的实现流程也可参照此处描述的步骤。

本方案实施例还提供了一种网络设备，用以实现前述各方法流程，其

组成如图 18 所示，包括：

接收单元 71，用于接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围。

转换单元 72，用于对所述第一目的地址进行地址转换，得到第二目的地址。

生成单元 73，用于根据所述第二目的地址以及所述第一报文，生成第二报文。

发送单元 74，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

可选的是，所述转换单元 72 具体用于对所述第一报文进行解析，得到内部目的地址和虚拟网络标识；根据所述内部目的地址，确定所述第一目的地址，以及，根据所述虚拟网络标识确定所述虚拟私有网络用户所在虚拟私有网络的网络标识信息；在预配置的地址映射表中查找与所述第一目的地址以及所述网络标识信息共同对应的目的地址；当查找到与所述第一目的地址以及所述网络标识信息共同对应的目的地址时，则将查找到的目的地址确定为所述第二目的地址。

可选的是，所述生成单元 73，具体用于当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式；按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

可选的是，所述生成单元 73，具体用于将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一

报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；所述第二包头信息至少包括源地址和目的地址；将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

可选的是，所述发送单元 74，具体用于根据所述第二目的地址以及路由表，确定下一跳设备，所述下一跳设备位于所述虚拟私有网络用户所在虚拟私有网络外部；将所述第二报文向所述下一跳设备发送。

可选的是，所述指定地址不属于指定网络已配置的地址范围。

可选的是，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

可选的是，所述虚拟私有网络为 VPC 网络。

可选的是，所述第一格式为 VXLAN 格式，所述第二格式为 VLAN 格式。

本方案实施例中还提供了一种网络设备，其组成如图 19 所示，包括：

接收单元 81，用于接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；

转换单元 82，用于对所述第一目的地址进行地址转换，得到第二目的地址；

生成单元 83，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元 84, 用于将所述第二报文向与第二类网络发送。

本方案实施例还提供了一种网络设备, 其组成如图 20 所示, 包括:

接收单元 91, 用于接收网络设备发送的第一报文, 所述第一报文携带有第一源地址。

转换单元 92, 用于对所述第一源地址进行地址转换, 得到第二源地址; 所述第二源地址为指定地址, 所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围。

生成单元 93, 用于根据所述第二源地址以及所述第一报文, 生成第二报文。

发送单元 94, 用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

可选的是, 所述转换单元 92, 还具体用于对所述第一报文进行解析, 得到所述第一源地址; 在预配置的地址映射表中查找与所述第一源地址对应的源地址; 当查找到与所述第一源地址对应的源地址时, 则将查找到的源地址确定为所述第二源地址。

可选的是, 所述生成单元 93 具体用于当所述第一报文符合第一格式时, 将所述第一格式转化为所述第二格式; 按照所述第二格式, 将所述第一报文携带的报文信息和所述第二源地址进行封装, 得到所述第二报文。

可选的是, 所述生成单元 93 还具体用于将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息; 其中, 所述第一包头信息至少包括源地址和目的地址; 所述第二报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址; 将所

述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

可选的是，所述指定地址不属于指定网络已配置的地址范围。

可选的是，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

可选的是，所述虚拟私有网络为 VPC 网络。

可选的是，所述第一格式为 VLAN 格式，所述第二格式为 VXLAN 格式。

本方案实施例还提供了一种网络设备，如图 21 所示，包括：

接收单元 1001，用于接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址。

转换单元 1002，用于对所述第一目的地址进行地址转换，得到第二源地址；所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围。

生成单元 1003，用于根据所述第二目的地址以及所述第一报文，生成第二报文。

发送单元 1004，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

本方案实施例所提供的数据传输的网络设备，使得虚拟私有网络内的用户只需能够提供业务服务的私有网络，就能够获取各项由相应服务器提供的服务，使得虚拟私有网络内部的用户不需要通过访问除私有网络外的其它网络来获取服务，从而为用户节省了流量。

另外，针对网络设备的实现，本方案实施例还提供了一种可能的实现方式，如图 22 所示，为网络设备 110 的简化框图。该网络设备 110 可以包括与一个或多个数据存储工具连接的处理器 1101，该数据存储工具可以包括存储介质 1102 和内存单元 1103。网络设备 110 还可以包括输入接口 1104 和输出接口 1105，用于与另一装置或系统进行通信。被处理器 1101 的 CPU 执行的程序代码可存储在内存单元 1102 或存储介质 1103 中。

网络设备 110 中的处理器 1101 调用上述程序代码，以执行下属各步骤：

所述处理器 1101，用于通过所述输入接口 1104 接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围；对所述第一目的地址进行地址转换，得到第二目的地址；根据所述第二目的地址以及所述第一报文，生成第二报文；通过所述输出接口 1105 将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

可选的是，所述处理器 1101，还用于对所述第一报文进行解析，得到内部目的地址和虚拟网络标识；根据所述内部目的地址，确定所述第一目的地址，以及，根据所述虚拟网络标识确定所述虚拟私有网络用户所在虚拟私有网络的网络标识信息；在预配置的地址映射表中查找与所述第一目的地址以及所述网络标识信息共同对应的目的地址；当查找到与所述第一目的地址以及所述网络标识信息共同对应的目的地址时，则将查找到的目的地址确定为所述第二目的地址。

可选的是，所述处理器 1101，还用于当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式；按照所述第二格式，将所述第一报

文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

可选的是，所述处理器 1101，还用于将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；所述第二包头信息至少包括源地址和目的地址；将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

可选的是，所述处理器 1101，还用于根据所述第二目的地址以及路由表，确定下一跳设备，所述下一跳设备位于所述虚拟私有网络用户所在虚拟私有网络外部；以及通过所述输出接口 1105 将所述第二报文向所述下一跳设备发送。

可选的是，所述指定地址不属于指定网络已配置的地址范围。

可选的是，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

可选的是所述虚拟私有网络为 VPC 网络。

可选的是所述第一格式为 VXLAN 格式，所述第二格式为 VLAN 格式。

另外，在其它可能的实现方式中，所述处理器 1101，还用于通过所述输入接口 1104 接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；对所述第一目的地址进行地址转换，得到第二目的地址；根据所述第二目的地址以及所述第一报文，生成第二报文；通过所述输出接口 1105 将所述

第二报文向与第二类网络发送。

基于如图 22 所示组成,所述处理器 1101 还用于通过输入接口 1104 接收网络设备发送的第一报文,所述第一报文携带有第一源地址;对所述第一源地址进行地址转换,得到第二源地址;所述第二源地址为指定地址,所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围;根据所述第二源地址以及所述第一报文,生成第二报文;通过输出接口 1105 将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

可选的是,所述处理器 1101,还用于对所述第一报文进行解析,得到所述第一源地址;在预配置的地址映射表中查找与所述第一源地址对应的源地址;当查找到与所述第一源地址对应的源地址时,则将查找到的源地址确定为所述第二源地址。

可选的是,所述处理器 1101,还用于当所述第一报文符合第一格式时,将所述第一格式转化为所述第二格式;按照所述第二格式,将所述第一报文携带的报文信息和所述第二源地址进行封装,得到所述第二报文。

可选的是,所述处理器 1101,还用于将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息;其中,所述第一包头信息至少包括源地址和目的地址;所述第二报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址;将所述第二包头信息和所述报文信息进行封装,得到所述第二报文;所述第二包头信息中携带的源地址为所述网络设备的地址,携带的目的地址为所述第二目的地址。

可选的是，所述指定地址不属于指定网络已配置的地址范围。

可选的是，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

可选的是，所述虚拟私有网络为 VPC 网络。

可选的是，所述第一格式为 VLAN 格式，所述第二格式为 VXLAN 格式。

另外，在其它可能的实现方式中，所述处理器 1101，还用于通过所述输入接口 1104 接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址；对所述第一目的地址进行地址转换，得到第二源地址；所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；根据所述第二目的地址以及所述第一报文，生成第二报文；通过所述输出接口 1105 将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

本方案实施例所提供的数据传输的网络设备，使得虚拟私有网络内的用户只需能够提供业务服务的私有网络，就能够获取各项由相应服务器提供的服务，使得虚拟私有网络内部的用户不需要通过访问除私有网络外的其它网络来获取服务，从而为用户节省了流量。

上述实施例中，存储介质可以是只读存储器（Read-Only Memory，ROM），或是可读写的，例如硬盘、闪存。内存单元可为随机存取存储器（Random Access Memory，RAM）。内存单元可与处理器物理集成或集成在存储器中或构建为单独的单元。

处理器为上述设备（该设备为上述服务器或者上述客户端）的控制中心，并提供处理装置，用于执行指令，进行中断操作，提供计时功能以及

多种其他功能。可选地，处理器包括一个或多个中央处理单元（CPU），例如图 12 中示出的 CPU 0 和 CPU 1。上述设备中包括一个或者多个的处理器。处理器可为单核（单 CPU）处理器或多核（多 CPU）处理器。除非另有声明，描述为用于执行任务的例如处理器或存储器的部件可实现为通用部件，其暂时用于在给定时间执行任务，或实现为专门制造用于执行该任务的特定部件。此处所用的术语“处理器”指一个或多个装置，电路和/或处理核，用于处理数据，例如计算机程序指令。

被处理器的 CPU 执行的程序代码可存储在内存单元或存储介质中。可选地，存储在存储介质中的程序代码可以被复制入内存单元以便处理器的 CPU 执行。处理器可执行至少一个内核（例如 LINUX™、UNIX™、WINDOWSTM、ANDROID™、IOSTM），众所周知，该内核用于通过控制其他程序或过程的执行、控制与外围装置的通信以及控制计算机设备资源的使用来控制上述设备的操作。

以上所述仅为本方案的较佳实施例，并不用以限制本方案，凡在本方案的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本方案的保护范围之内。

权利要求书

1、一种数据传输的方法，其特征在于，应用于网络设备，包括：

接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

对所述第一目的地址进行地址转换，得到第二目的地址；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

2、根据权利要求1所述的方法，其特征在于，所述对所述第一目的地址进行地址转换，得到第二目的地址包括：

对所述第一报文进行解析，得到内部目的地址和虚拟网络标识；

根据所述内部目的地址，确定所述第一目的地址，以及，根据所述虚拟网络标识确定所述虚拟私有网络用户所在虚拟私有网络的网络标识信息；

在预配置的地址映射表中查找与所述第一目的地址以及所述网络标识信息共同对应的目的地址；

当查找到与所述第一目的地址以及所述网络标识信息共同对应的目的地址时，则将查找到的目的地址确定为所述第二目的地址。

3、根据权利要求2所述的方法，其特征在于，所述根据所述第二目的地址以及所述第一报文，生成第二报文包括：

当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格

式；

按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文。

4、根据权利要求3所述的方法，其特征在于，所述当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式包括：

将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；所述第二包头信息至少包括源地址和目的地址；

则所述按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文包括：

将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

5、根据权利要求4所述的方法，其特征在于，所述将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送包括：

根据所述第二目的地址以及路由表，确定下一跳设备，所述下一跳设备位于所述虚拟私有网络用户所在虚拟私有网络外部；

将所述第二报文向所述下一跳设备发送。

6、根据权利要求5所述的方法，其特征在于，所述指定地址不属于指定网络已配置的地址范围。

7、根据权利要求6所述的方法，其特征在于，所述指定地址属于

100.64.0.0 至 100.64.0.10 的地址范围中。

8、根据权利要求 7 所述的方法，其特征在于，所述虚拟私有网络为 VPC 网络。

9、根据权利要求 8 所述的方法，其特征在于，所述第一格式为 VXLAN 格式，所述第二格式为 VLAN 格式。

10、根据权利要求 9 所述的方法，其特征在于，所述第一目的地址和所述第二目的地址对应于同一服务器。

11、根据权利要求 10 所述的方法，其特征在于，所述服务器为网络时间协议 NTP 服务器或加密服务器。

12、一种数据传输的方法，其特征在于，包括：

接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；

对所述第一目的地址进行地址转换，得到第二目的地址；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向第二类网络发送。

13、一种数据传输的方法，其特征在于，包括：

接收网络设备发送的第一报文，所述第一报文携带有第一源地址；

对所述第一源地址进行地址转换，得到第二源地址；所述第二源地址为指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

根据所述第二源地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

14、根据权利要求 13 所述的方法，其特征在于，所述对所述第一源地址进行地址转换，得到第二源地址包括：

对所述第一报文进行解析，得到所述第一源地址；

在预配置的地址映射表中查找与所述第一源地址对应的源地址；

当查找到与所述第一源地址对应的源地址时，则将查找到的源地址确定为所述第二源地址。

15、根据权利要求 13 所述的方法，其特征在于，所述根据所述第二源地址以及所述第一报文，生成第二报文包括：

当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式；

按照所述第二格式，将所述第一报文携带的报文信息和所述第二源地址进行封装，得到所述第二报文。

16、根据权利要求 15 所述的方法，其特征在于，所述当所述第一报文符合第一格式时，将所述第一格式转化为所述第二格式包括：

将所述第一报文中符合第一格式的第一报头信息替换为符合第二格式的第二包头信息；其中，所述第一包头信息至少包括源地址和目的地址；所述第二报头信息至少包括内部源地址、内部目的地址、虚拟网络标识、外部源地址和外部目的地址；

则所述按照所述第二格式，将所述第一报文携带的报文信息和所述第二目的地址进行封装，得到所述第二报文包括：

将所述第二包头信息和所述报文信息进行封装，得到所述第二报文；
所述第二包头信息中携带的源地址为所述网络设备的地址，携带的目的地址为所述第二目的地址。

17、根据权利要求 15 所述的方法，其特征在于，所述指定地址不属于指定网络已配置的地址范围。

18、根据权利要求 17 所述的方法，其特征在于，所述指定地址属于 100.64.0.0 至 100.64.0.10 的地址范围中。

19、根据权利要求 18 所述的方法，其特征在于，所述虚拟私有网络为 VPC 网络。

20、根据权利要求 19 所述的方法，其特征在于，所述第一格式为 VLAN 格式，所述第二格式为 VXLAN 格式。

21、根据权利要求 20 所述的方法，其特征在于，所述第一源地址和所述第二源地址对应于同一服务器。

22、根据权利要求 21 所述的方法，其特征在于，所述服务器为 NTP 服务器或加密服务器。

23、一种数据传输的方法，其特征在于，包括：

接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址；

对所述第一目的地址进行地址转换，得到第二源地址；所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户在虚拟私有网络已配置的地址范围；

根据所述第二目的地址以及所述第一报文，生成第二报文；

将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

24、一种网络设备，其特征在于，包括：

接收单元，用于接收虚拟私有网络用户发送的第一报文，所述第一报文携带的第一目的地址为指定地址，所述指定地址不属于所述虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

转换单元，用于对所述第一目的地址进行地址转换，得到第二目的地址；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络外部发送。

25、一种网络设备，其特征在于，包括：

接收单元，用于接收第一类网络内用户发送的第一报文，所述第一报文携带的第一目的地址为第二类网络内的指定地址，所述指定地址不属于所述第一类网络已配置的地址范围，同时也不属于第三类网络已配置的地址范围；

转换单元，用于对所述第一目的地址进行地址转换，得到第二目的地址；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与第二类网络发送。

26、一种网络设备，其特征在于，包括：

接收单元，用于接收网络设备发送的第一报文，所述第一报文携带有第一源地址；

转换单元，用于对所述第一源地址进行地址转换，得到第二源地址；
所述第二源地址为指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

生成单元，用于根据所述第二源地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

27、一种网络设备，其特征在于，包括：

接收单元，用于接收第二类网络内设备发送的第一报文，所述第一报文携带有第一源地址；

转换单元，用于对所述第一目的地址进行地址转换，得到第二源地址；
所述第二源地址为第二类网络内的指定地址，所述指定地址不属于虚拟私有网络用户所在虚拟私有网络已配置的地址范围；

生成单元，用于根据所述第二目的地址以及所述第一报文，生成第二报文；

发送单元，用于将所述第二报文向与所述虚拟私有网络用户所在虚拟私有网络内部发送。

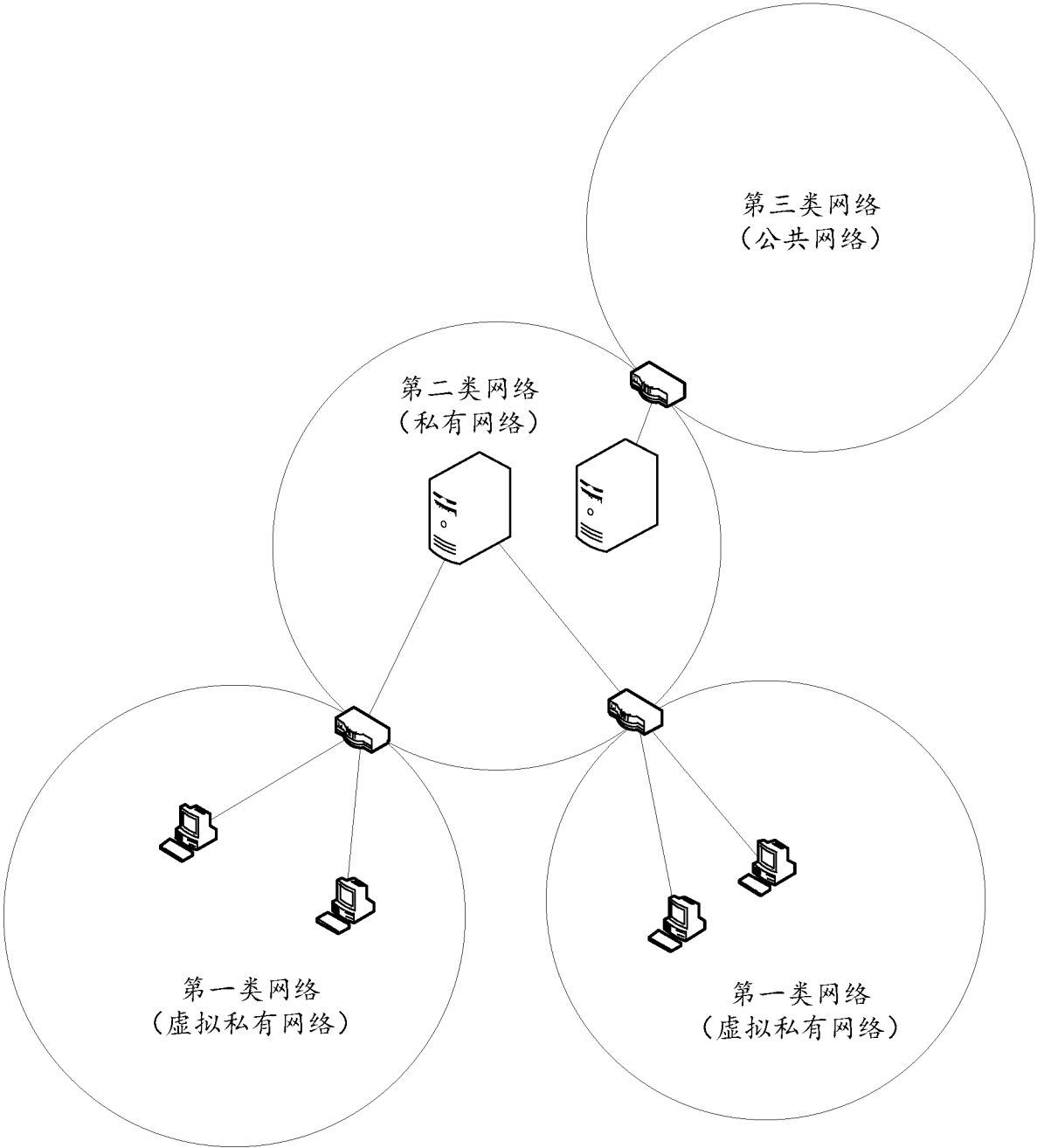


图 1

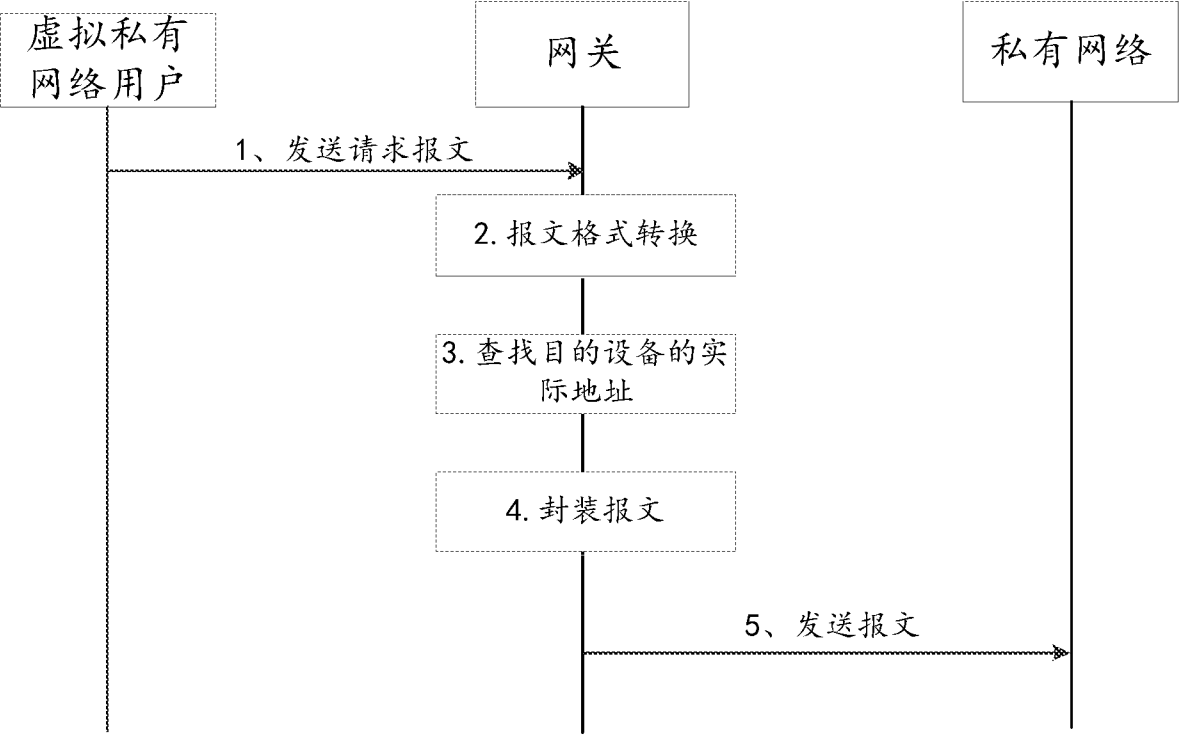


图 2

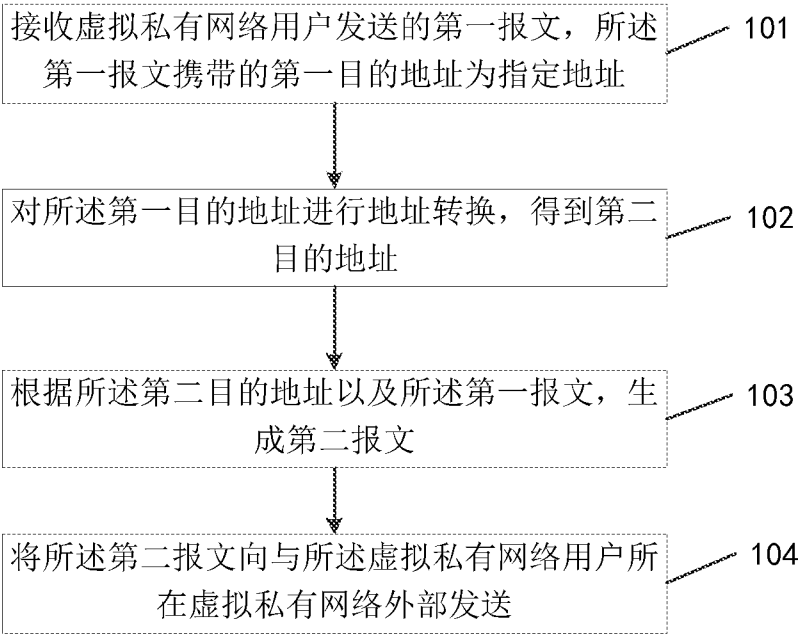


图 3

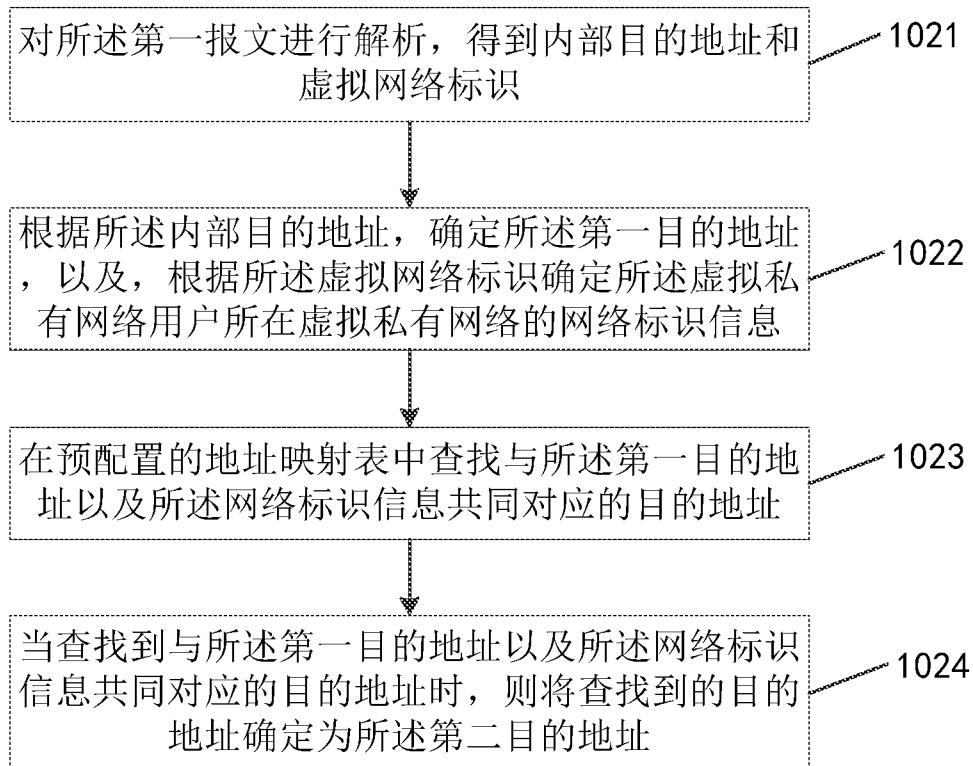


图 4

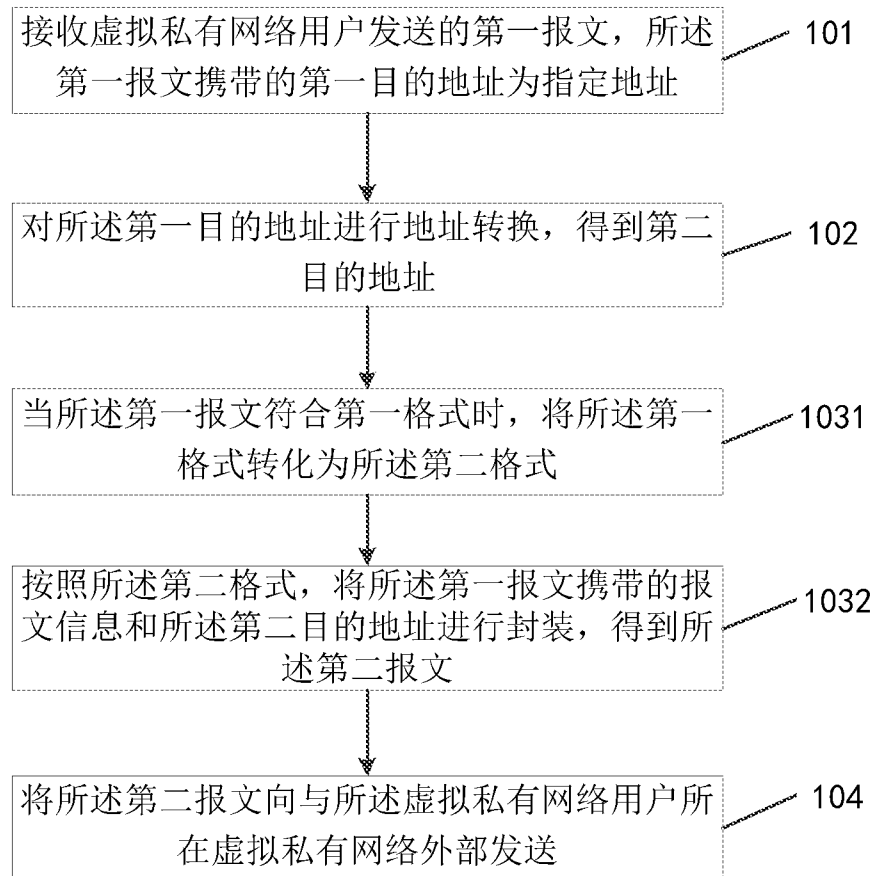


图 5

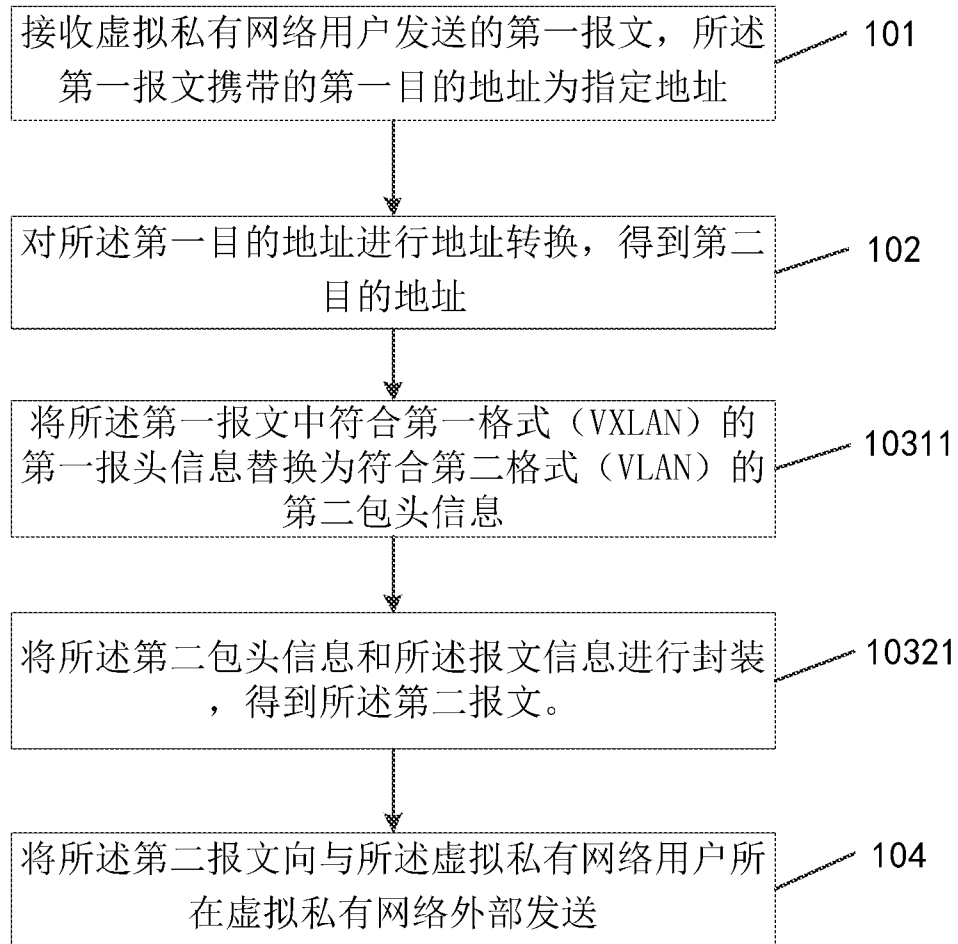


图 6

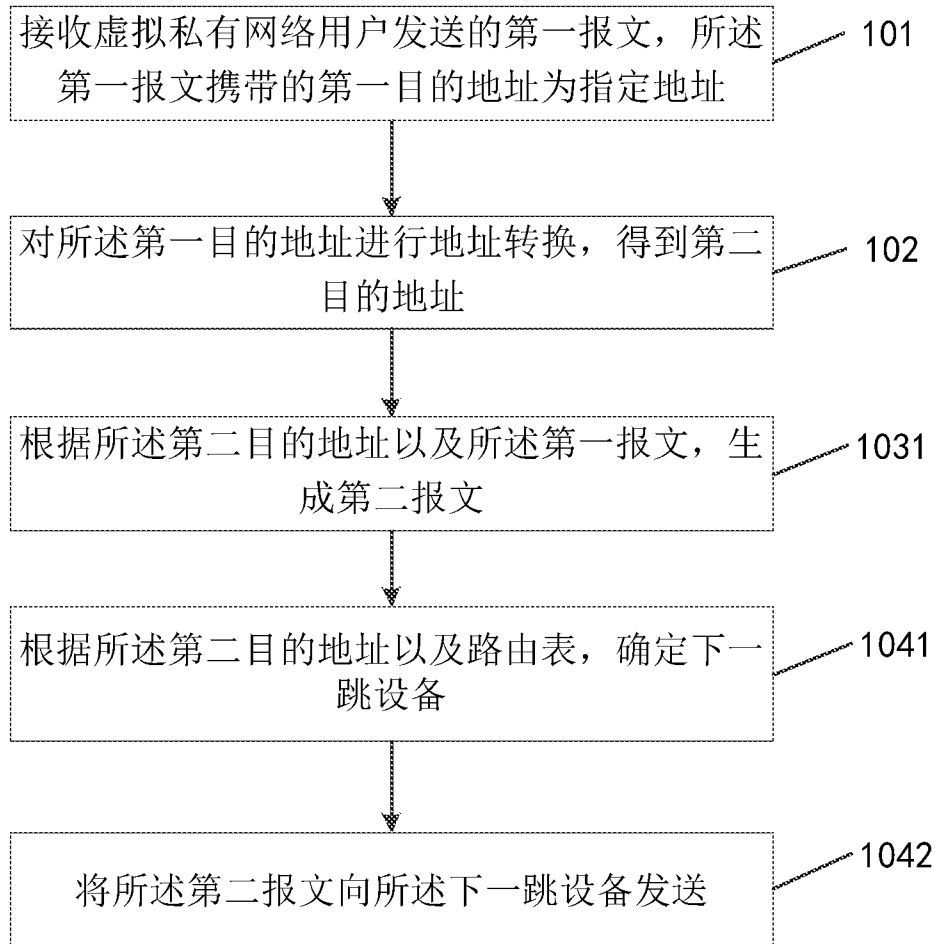


图 7

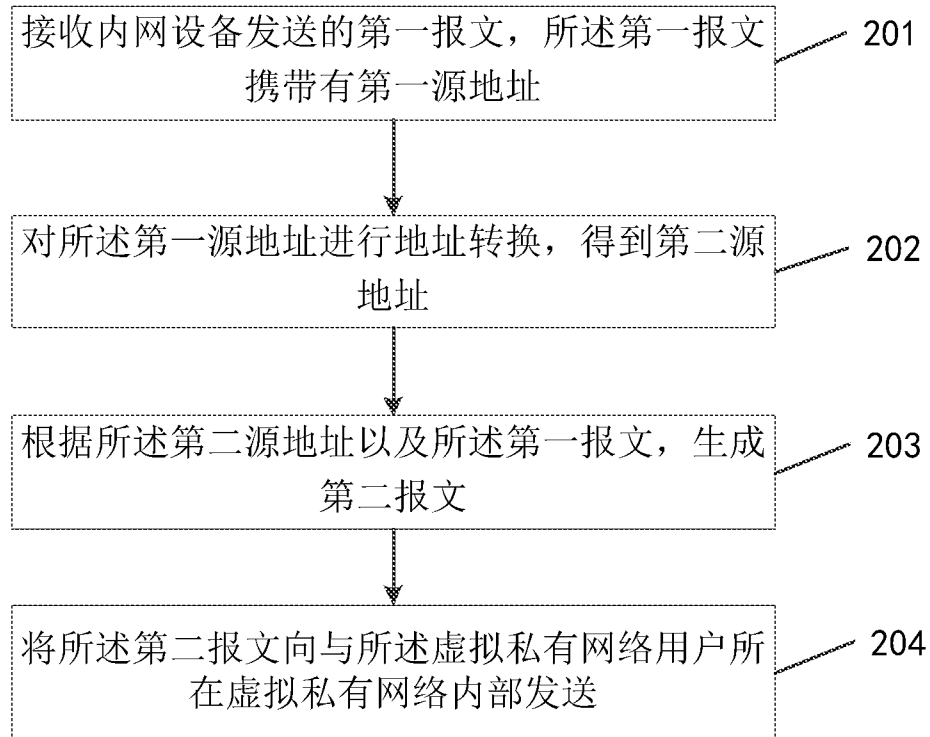


图 8

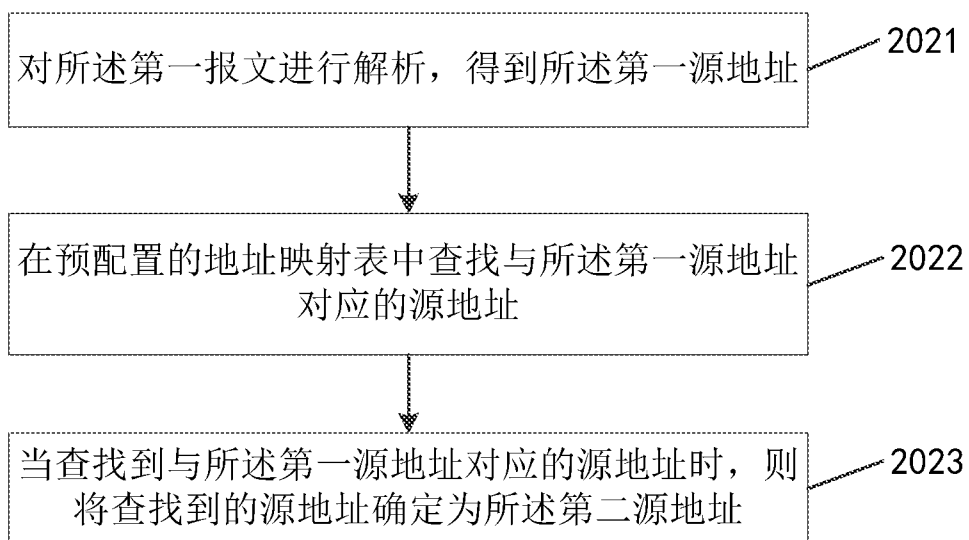


图 9

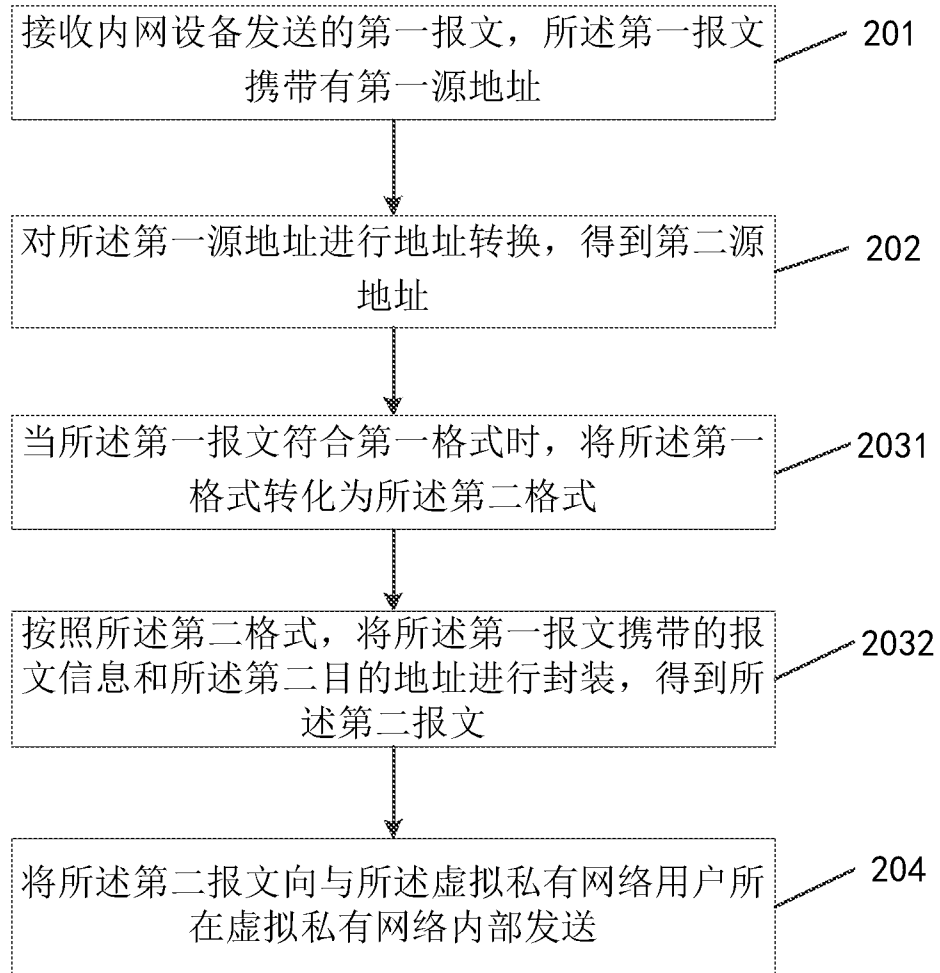


图 10

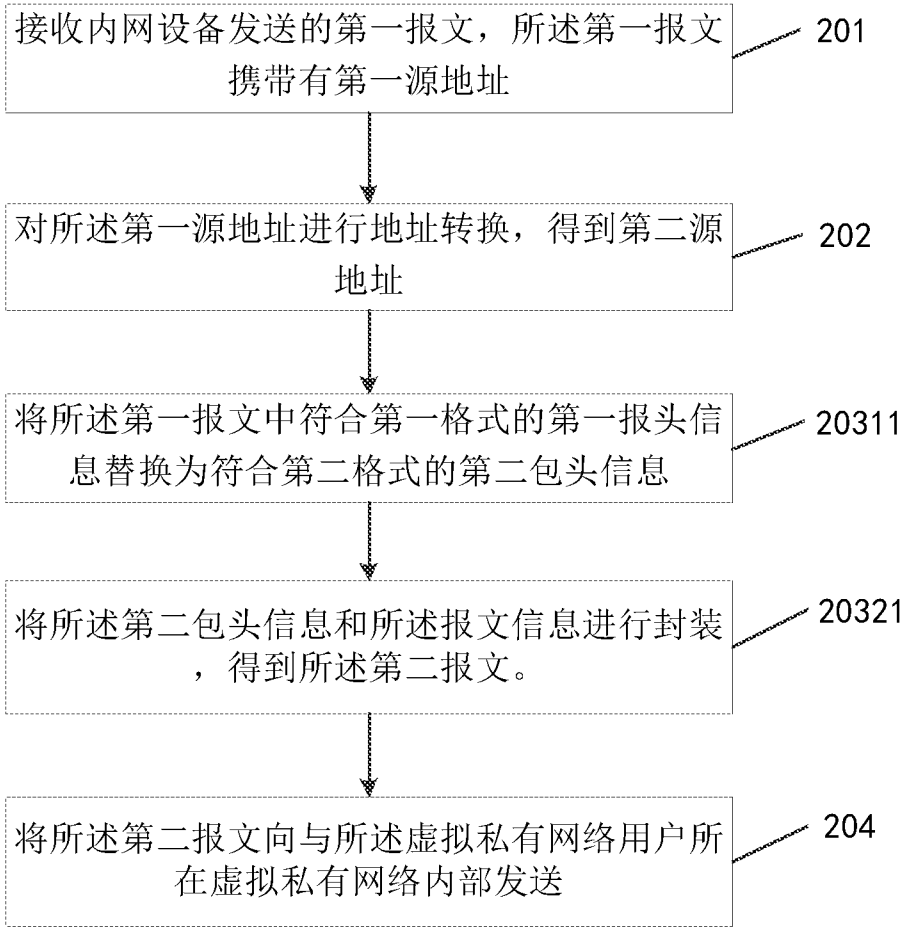


图 11

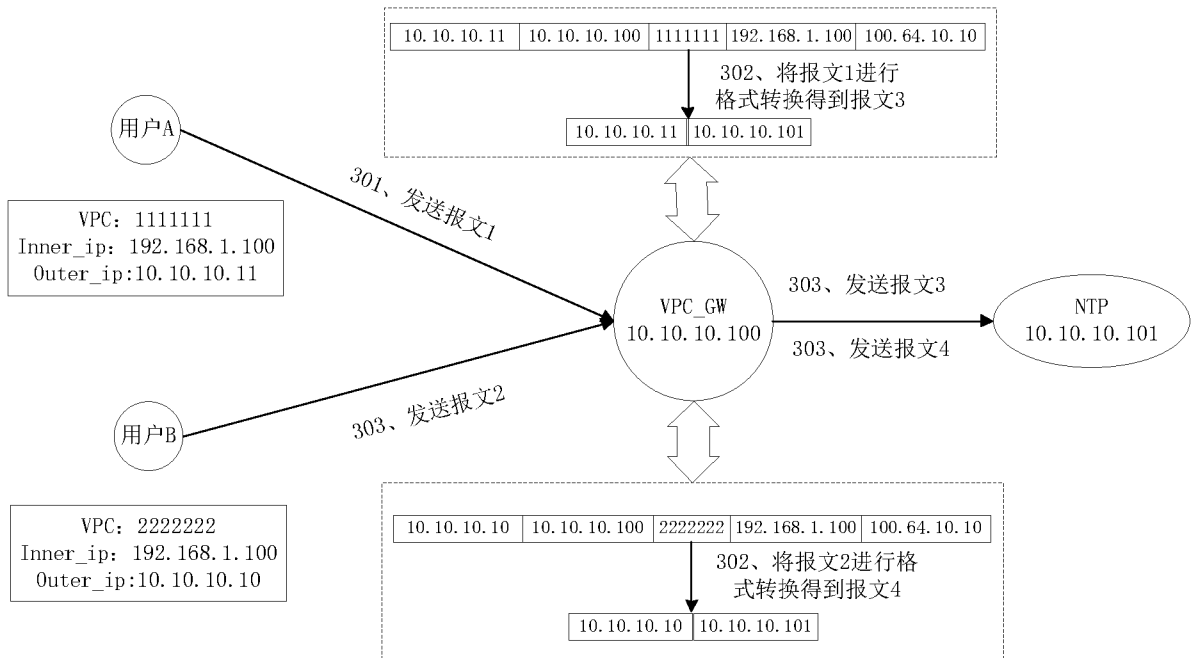


图 12

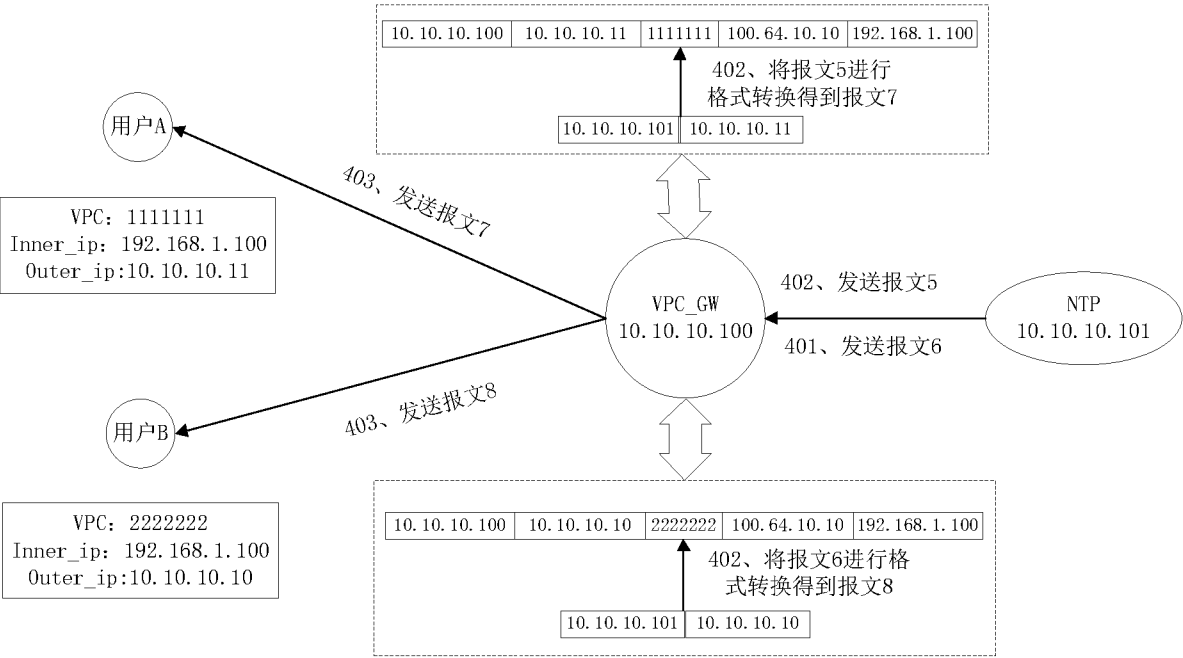


图 13

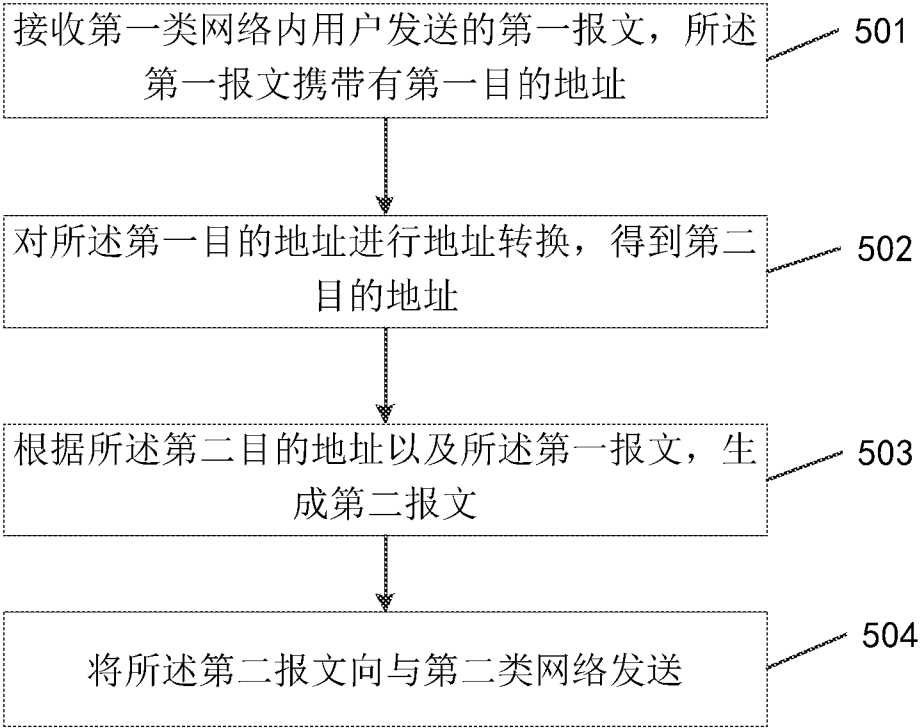


图 14

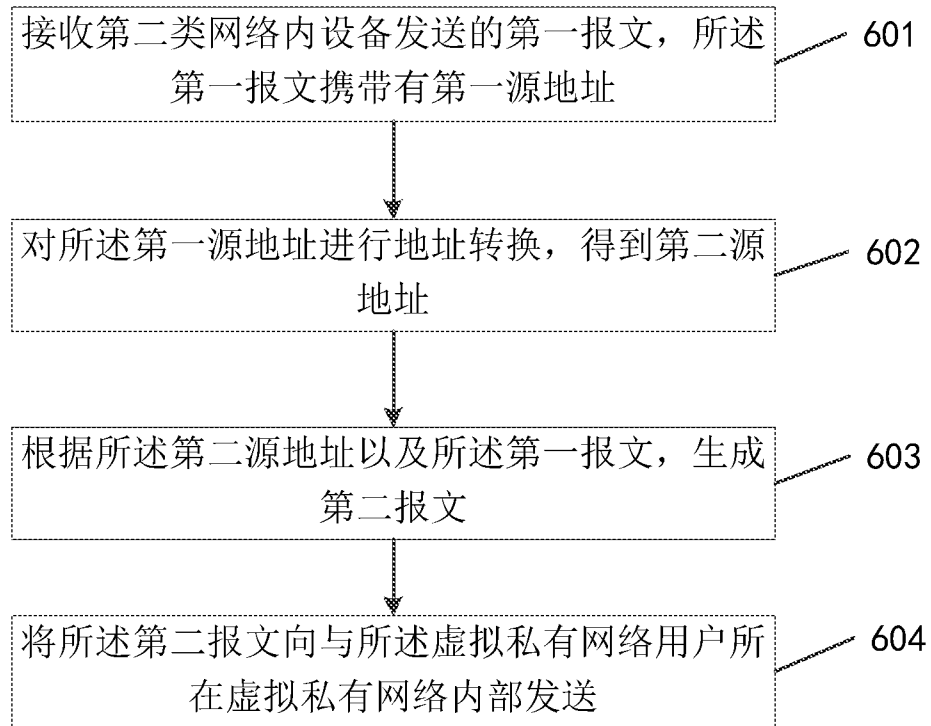


图 15

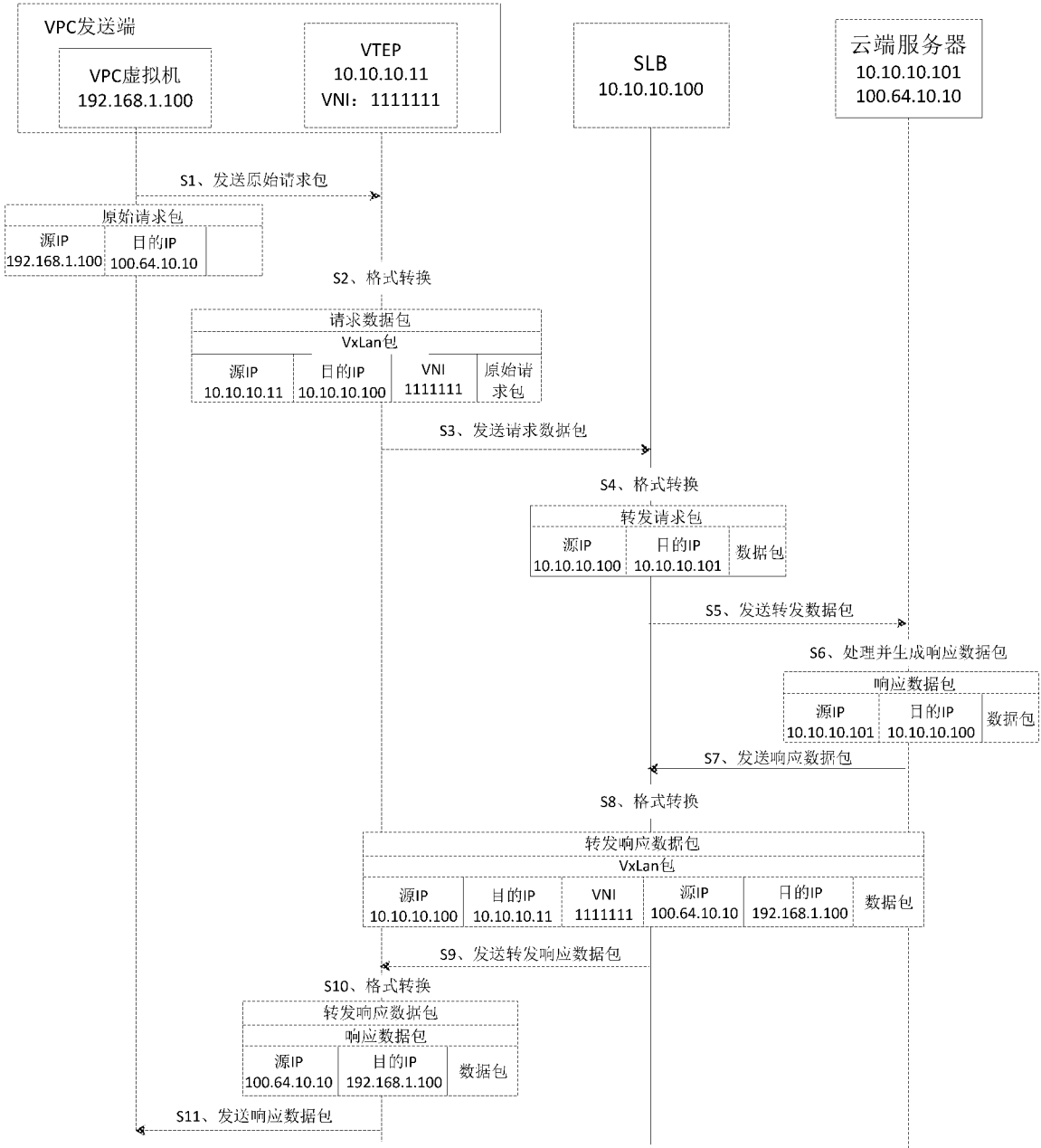


图 16

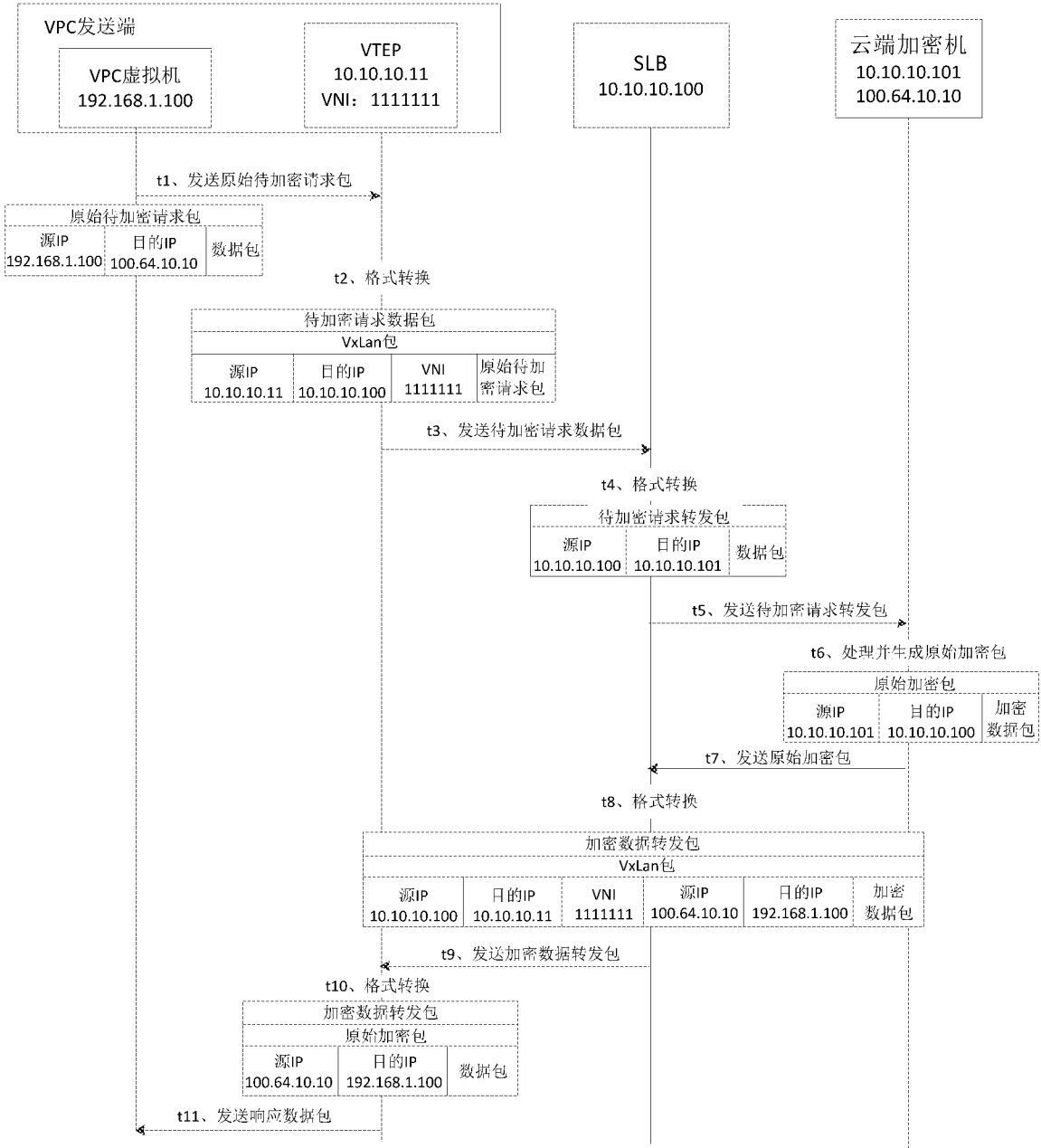


图 17

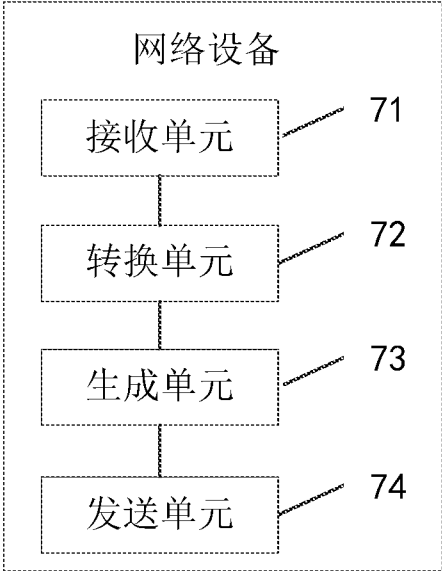


图 18

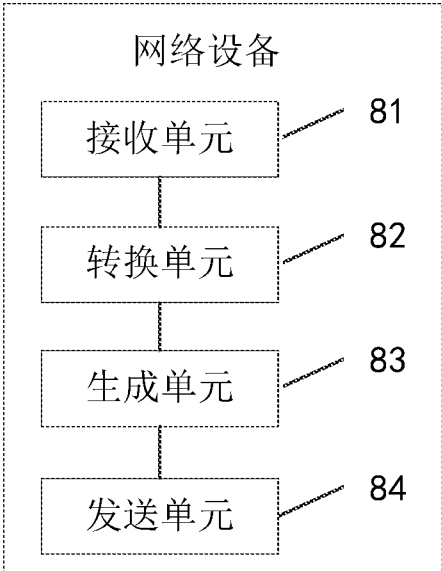


图 19

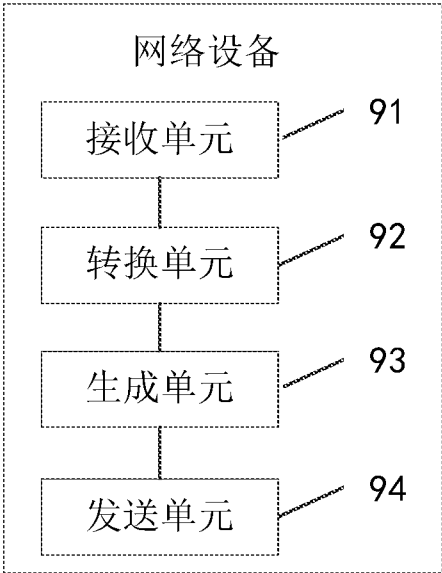


图 20

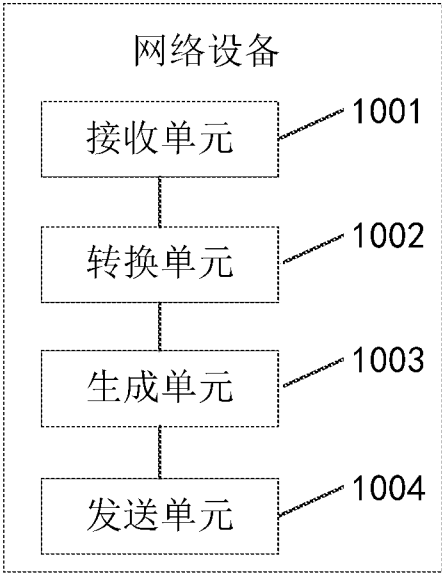


图 21

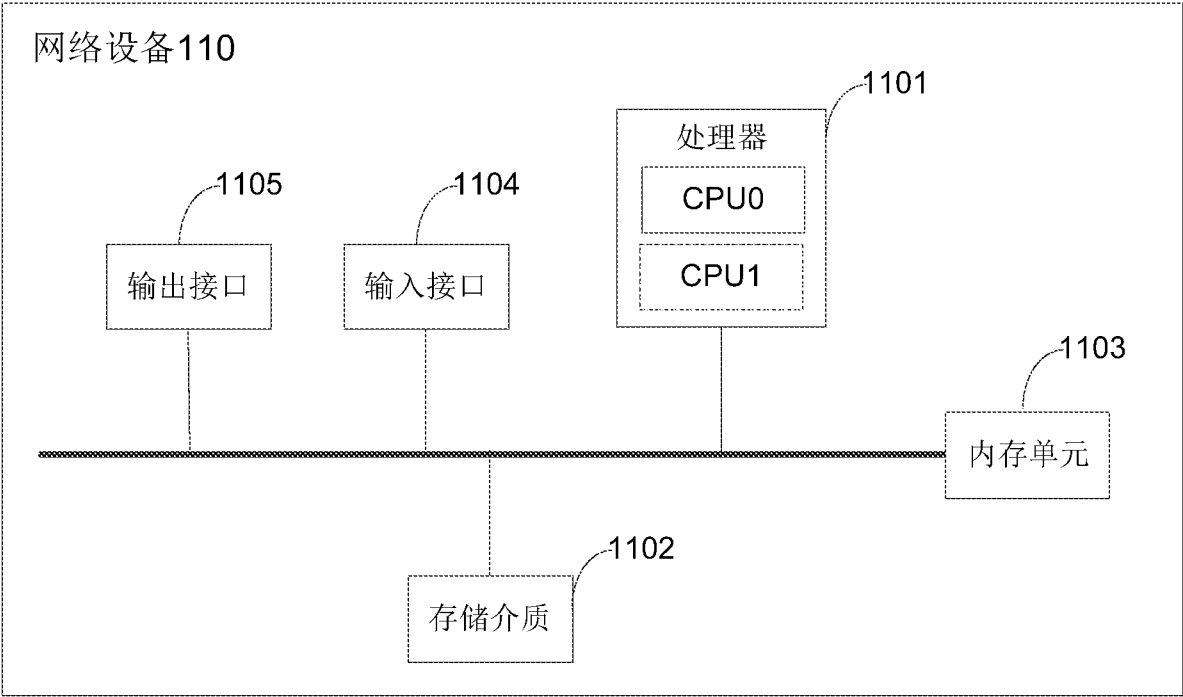


图 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/102386

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 12/46 (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)

CNABS; VEN; CNKI: 地址, 转换, 翻译, 目的, 目标, 虚拟私有网络, 虚拟专用网, 云, 私有, 内部, 外部, 指定, 真实, 实际,
address, translat+, destination, virtual private network, cloud, private, internal, exterior, assign+, real

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105491082 A (HUAWEI TECHNOLOGIES CO., LTD. et al.) 13 April 2016 (13.04.2016), description, paragraphs [0057]-[0065] and [0099]-[0107], and claims 6-8	1-27
A	CN 104639363 A (INSTITUTE FOR INFORMATION INDUSTRY) 20 May 2015 (20.05.2015), entire document	1-27
A	CN 105122231 A (ACCELERATION SYSTEMS LLC.) 02 December 2015 (02.12.2015), entire document	1-27
A	US 2006182103 A1 (PHANTOM TECHNOLOGIES LLC.) 17 August 2006 (17.08.2006), entire document	1-27

☐ 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 01 December 2017	Date of mailing of the international search report 11 December 2017
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 PENG, Yuan Telephone No. (86-10) 62411268

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/102386

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105491082 A	13 April 2016	US 2017185546 A1	29 June 2017
		WO 2016041453 A1	24 March 2016
		EP 3188446 A4	30 August 2017
		EP 3188446 A1	05 July 2017
CN 104639363 A	20 May 2015	US 9705847 B2	11 July 2017
		JP 2015095894 A	18 May 2015
		TW 201519621 A	16 May 2015
		US 2015131674 A1	14 May 2015
		TW I538461 B	11 June 2016
		JP 5855630 B2	09 February 2016
		US 9258226 B2	09 February 2016
		CA 2897105 A1	10 July 2014
CN 105122231 A	02 December 2015	WO 2014107482 A1	10 July 2014
		HK 1215814 A1	15 September 2016
		KR 20150114491 A	12 October 2015
		IL 239730 A	31 August 2015
		MX 346342 B	14 March 2017
		RU 2015132089 A	09 February 2017
		MX 2015008609 A	08 January 2016
		IL 239730 D0	31 August 2015
		EP 2941716 A4	21 December 2016
		AU 2014204085 A1	06 August 2015
		PH 12015501503 A1	28 September 2015
		JP 2016507968 A	10 March 2016
		EP 2941716 A1	11 November 2015
		US 2014219280 A1	07 August 2014
US 2006182103 A1	17 August 2006	None	

国际检索报告

国际申请号

PCT/CN2017/102386

A. 主题的分类

H04L 29/06(2006.01)i; H04L 12/46(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))

CNABS;VEN;CNKI:地址, 转换, 翻译, 目的, 目标, 虚拟私有网络, 虚拟专用网, 云, 私有, 内部, 外部, 指定, 真实, 实际, address, translat+, destination, virtual private network, cloud, private, internal, exterior, assign+, real

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
X	CN 105491082 A (华为技术有限公司等) 2016年 4月 13日 (2016 - 04 - 13) 说明书第0057-0065、0099-0107段, 权利要求6-8	1-27
A	CN 104639363 A (财团法人资讯工业策进会) 2015年 5月 20日 (2015 - 05 - 20) 全文	1-27
A	CN 105122231 A (加速系统有限责任公司) 2015年 12月 2日 (2015 - 12 - 02) 全文	1-27
A	US 2006182103 A1 (PHANTOM TECHNOLOGIES LLC) 2006年 8月 17日 (2006 - 08 - 17) 全文	1-27

☐ 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

2017年 12月 1日

国际检索报告邮寄日期

2017年 12月 11日

ISA/CN的名称和邮寄地址

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

传真号 (86-10)62019451

受权官员

彭媛

电话号码 (86-10)62411268

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/102386

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	105491082	A	2016年 4月 13日	US	2017185546	A1	2017年 6月 29日
				WO	2016041453	A1	2016年 3月 24日
				EP	3188446	A4	2017年 8月 30日
				EP	3188446	A1	2017年 7月 5日
CN	104639363	A	2015年 5月 20日	US	9705847	B2	2017年 7月 11日
				JP	2015095894	A	2015年 5月 18日
				TW	201519621	A	2015年 5月 16日
				US	2015131674	A1	2015年 5月 14日
				TW	I538461	B	2016年 6月 11日
				JP	5855630	B2	2016年 2月 9日
CN	105122231	A	2015年 12月 2日	US	9258226	B2	2016年 2月 9日
				CA	2897105	A1	2014年 7月 10日
				WO	2014107482	A1	2014年 7月 10日
				HK	1215814	A1	2016年 9月 15日
				KR	20150114491	A	2015年 10月 12日
				IL	239730	A	2015年 8月 31日
				MX	346342	B	2017年 3月 14日
				RU	2015132089	A	2017年 2月 9日
				MX	2015008609	A	2016年 1月 8日
				IL	239730	D0	2015年 8月 31日
				EP	2941716	A4	2016年 12月 21日
				AU	2014204085	A1	2015年 8月 6日
				PH	12015501503	A1	2015年 9月 28日
				JP	2016507968	A	2016年 3月 10日
				EP	2941716	A1	2015年 11月 11日
				US	2014219280	A1	2014年 8月 7日
US	2006182103	A1	2006年 8月 17日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)