



(12) 发明专利

(10) 授权公告号 CN 103379185 B

(45) 授权公告日 2016. 08. 03

(21) 申请号 201210126776. 9

CN 102185774 A, 2011. 09. 14,

(22) 申请日 2012. 04. 26

US 2011246669 A1, 2011. 10. 06,

(73) 专利权人 华为技术有限公司

审查员 李福涛

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

(72) 发明人 康玉东 顾颖杰

(74) 专利代理机构 北京中博世达专利商标代理
有限公司 11274

代理人 申健

(51) Int. Cl.

H04L 29/12(2006. 01)

(56) 对比文件

CN 101729388 A, 2010. 06. 09,

CN 101552803 A, 2009. 10. 07,

CN 101383757 A, 2009. 03. 11,

权利要求书3页 说明书10页 附图3页

(54) 发明名称

一种网络地址转换的方法、设备和系统

(57) 摘要

本发明实施例提供一种网络地址转换的方法、设备和系统，涉及通信技术领域。在第一数据中心将发生迁移的虚拟机 VM 所对应的 NAT 映射表项迁移至第二数据中心后，NAT 控制设备接收网络地址迁移消息，验证该网络地址迁移消息，并根据该网络地址迁移消息将网络地址映射表中的该 NAT 映射表项的归属信息由该第一数据中心更新为该第二数据中心。本发明实施例用于虚拟机 VM 跨数据中心迁移的场景下的网路地址转换，通过 NAT 控制设备对各个数据中心的集中式控制，能够合理规划数据中心中的 NAT 地址资源，并解决由于 VM 的申请与应用不在一个数据中心而造成的释放攻击问题。

在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后，NAT控制设备接收网络地址迁移消息，并验证该网络地址迁移消息

S101

NAT控制设备在对该网络地址迁移消息验证成功后，根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心

S102

1. 一种网络地址转换NAT的方法,应用于虚拟机VM跨数据中心迁移的场景,其特征在于,包括:

在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后,NAT控制设备接收网络地址迁移消息,并验证所述网络地址迁移消息,所述网络地址迁移消息携带有所述NAT映射表项,所述NAT映射表项记录所述VM的私有网络地址与公有网络地址的映射关系;

所述NAT控制设备在对所述网络地址迁移消息验证成功后,根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心,所述网络地址映射表用于记录NAT映射表项以及NAT映射表项的归属信息。

2. 根据权利要求1所述的方法,其特征在于,

所述NAT控制设备接收网络地址迁移消息,具体为:所述NAT控制设备接收所述第一数据中心发送的网络地址迁移消息;则所述验证所述网络地址迁移消息,具体为:向所述第二数据中心验证所述网络地址迁移消息;

或者,

所述NAT控制设备接收网络地址迁移消息,具体为:所述NAT控制设备接收所述第二数据中心发送的网络地址迁移消息;则所述验证所述网络地址迁移消息,具体为:向所述第一数据中心验证所述网络地址迁移消息。

3. 根据权利要求1或2所述的方法,其特征在于,在所述第一数据中心接收到所述VM发送的第一个携带私有网络地址的报文后,所述方法还包括:

所述NAT控制设备接收所述第一数据中心发送的NAT请求消息,所述NAT请求消息携带所述报文的私有网络地址;

根据所述NAT请求消息为所述私有网络地址分配公有网络地址,根据所述私有网络地址和所述公有网络地址建立所述NAT映射表项,将所述NAT映射表项记录在所述网络地址映射表中,且将所述NAT映射表项的归属信息记录为第一数据中心;

向所述第一数据中心发送所述NAT映射表项,以使得所述第一数据中心在保存所述NAT映射表项后,根据所述NAT映射表项将所述VM发送的报文的私有网络地址转换为公有网络地址。

4. 根据权利要求3所述的方法,其特征在于,在所述根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心后,所述方法还包括:

接收所述第二数据中心在所述NAT映射表项相应的第一定时器达到或者超过预设时间时发送的释放请求消息,所述释放请求消息中携带所述NAT映射表项,所述第一定时器在所述第二数据中心未检测到所述NAT映射表项对应的会话连接时启动,并在达到或者超过预设时间时停止;

在确定所述网络地址映射表中记录的所述NAT映射表项的归属信息为所述第二数据中心时,向所述第二数据中心发送释放响应消息,以使得所述第二数据中心删除所述NAT映射表项。

5. 根据权利要求1、2或4所述的方法,其特征在于,所述私有网络地址具体为:私有IP地址或者私有IP地址和私有端口号;

所述公有网络地址具体为：公有IP地址或者公有IP地址和公有端口号。

6. 一种NAT控制设备，应用于虚拟机VM跨数据中心迁移的场景，其特征在于，包括：

迁移消息接收单元，用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后，接收网络地址迁移消息，所述网络地址迁移消息携带有所述NAT映射表项，所述NAT映射表项记录所述VM的私有网络地址与公有网络地址的映射关系；

验证单元，用于验证所述网络地址迁移消息；

更新单元，用于在所述验证单元对所述网络地址迁移消息验证成功后，根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心，所述网络地址映射表用于记录所述NAT映射表项以及所述NAT映射表项的归属信息。

7. 根据权利要求6所述的设备，其特征在于，

所述迁移消息接收单元，具体用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后，接收所述第一数据中心发送的网络地址迁移消息，则所述验证单元，具体用于向所述第二数据中心验证所述网络地址迁移消息；

或者，

所述迁移消息接收单元，具体用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后，接收所述第二数据中心发送的网络地址迁移消息，则所述验证单元，具体用于向所述第一数据中心验证所述网络地址迁移消息。

8. 根据权利要求6或7所述的设备，其特征在于，还包括：

NAT请求接收单元，用于在所述第一数据中心接收到所述VM发送的第一个携带私有网络地址的报文后，接收所述第一数据中心发送的NAT请求消息，所述NAT请求消息携带所述报文的私有网络地址；

分配记录单元，用于根据所述NAT请求消息为所述私有网络地址分配公有网络地址，根据所述私有网络地址和所述公有网络地址建立所述NAT映射表项，并将所述NAT映射表项记录在所述网络地址映射表中，且将所述NAT映射表项的归属信息记录为第一数据中心；

映射表项发送单元，用于向所述第一数据中心发送所述NAT映射表项，以使得所述第一数据中心在保存所述NAT映射表项后，根据所述NAT映射表项将所述VM发送的报文的私有网络地址转换为公有网络地址。

9. 根据权利要求8所述的设备，其特征在于，所述设备还包括：

释放请求接收单元，用于在所述更新单元根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心后，接收所述第二数据中心在针对所述NAT映射表项设置的第一定时器达到或者超过预设时间时发送的释放请求消息，所述释放请求消息中携带所述NAT映射表项，所述第一定时器在所述第二数据中心未检测到所述NAT映射表项对应的会话连接时启动，并在达到或者超过预设时间时停止；

释放响应发送单元，用于在确定所述网络地址映射表中记录的所述NAT映射表项的归属信息为所述第二数据中心时，向所述第二数据中心发送释放响应消息，以使得所述第二数据中心删除所述NAT映射表项。

10. 根据权利要求6、7或9所述的设备，其特征在于，所述私有网络地址具体为：私有IP

地址或者私有IP地址和私有端口号；

所述公有网络地址具体为：公有IP地址或者公有IP地址和公有端口号。

11.一种网络地址转换的系统，应用于虚拟机VM跨数据中心迁移的场景，其特征在于，包括：NAT控制设备、第一数据中心和第二数据中心，

所述第一数据中心，用于将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心；

所述NAT控制设备为权利要求6至10中所述的NAT控制设备；

所述第二数据中心，用于接收所述NAT映射表项。

一种网络地址转换的方法、设备和系统

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及一种网络地址转换的方法、设备和系统。

背景技术

[0002] 网络地址转换(英文:Network Address Translation,简称:NAT)技术属于接入广域网技术,是一种将私有地址/端口转化为公有地址/端口的转换技术,它被广泛应用于各种类型的网络接入方式和各种类型的网络中。

[0003] 现有技术中,随着虚拟技术的引入,虚拟机(英文:Virtual Machine,简称VM)可以在不同的数据中心之间进行迁移,VM申请到的NAT映射表项也会随之迁移,例如,当VM从第一数据中心迁移至第二数据中心时,则VM申请到的NAT映射表项也会随之迁移,但是,由于VM的NAT映射表项的应用依然要通过第一数据中心,而迁移后的VM位于第二数据中心,因此VM在应用该NAT映射表项时需要通过第二数据中心与第一数据中心进行信息交互,这样很容易受到攻击者的释放攻击,例如当VM正在使用某个地址时,攻击者向第一数据中心发送该地址的释放请求消息,就会影响到正在使用该地址的VM。

[0004] 另外,在VM发生迁移时,可能会由于迁移至第二数据中心中的VM较多,超出了该第二数据中心对NAT地址资源的规划,从而影响该VM的正常应用。

发明内容

[0005] 本发明的实施例提供一种网络地址转换的方法、设备和系统,通过NAT控制设备对各个数据中心的集中式控制,合理规划数据中心中的NAT地址资源,并解决由于VM的申请与应用不在一个数据中心而造成的释放攻击问题。

[0006] 为达到上述目的,本发明的实施例采用如下技术方案:

[0007] 一方面,本发明实施例提供一种网络地址转换的方法,应用于虚拟机跨数据中心迁移的场景,包括:

[0008] 在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后,NAT控制设备接收网络地址迁移消息,并验证所述网络地址迁移消息,所述网络地址迁移消息携带有所述NAT映射表项,所述NAT映射表项记录所述VM的私有网络地址与公有网络地址的映射关系;

[0009] 所述NAT控制设备在对所述网络地址迁移消息验证成功后,根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心,所述网络地址映射表用于记录NAT映射表项以及NAT映射表项的归属信息。

[0010] 另一方面,本发明实施例提供一种NAT控制设备,应用于虚拟机跨数据中心迁移的场景,包括:

[0011] 迁移消息接收单元,用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后,接收网络地址迁移消息,所述网络地址迁移消息携带有所述NAT映

射表项，所述NAT映射表项记录所述VM的私有网络地址与公有网络地址的映射关系；

[0012] 验证单元，用于验证所述网络地址迁移消息；

[0013] 更新单元，用于在所述验证单元对所述网络地址迁移消息验证成功后，根据所述网络地址迁移消息将网络地址映射表中的所述NAT映射表项的归属信息由所述第一数据中心更新为所述第二数据中心，所述网络地址映射表用于记录所述NAT映射表项以及所述NAT映射表项的归属信息。

[0014] 另一面，本发明实施例提供一种网络地址转换的系统，应用于虚拟机跨数据中心迁移的场景，包括：NAT控制设备、第一数据中心和第二数据中心，

[0015] 所述第一数据中心，用于将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心；

[0016] 所述NAT控制设备为上述的NAT控制设备；

[0017] 所述第二数据中心，用于接收所述NAT映射表项。

[0018] 本发明实施例提供一种网络地址转换的方法、设备和系统，通过NAT控制设备对各个数据中心的集中式控制，从而对各个数据中心的NAT地址资源进行合理的规划，同时，该NAT控制设备记录该VM对应的NAT映射表项的归属信息，解决了由于VM的申请与应用不在一个数据中心而造成的释放攻击问题。

附图说明

[0019] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0020] 图1为本发明实施例提供的一种网络地址转换的方法示意图；

[0021] 图2为本发明实施例提供的一种网络地址转换方法的流程示意图；

[0022] 图3为本发明实施例提供的一种NAT控制设备的结构示意图；

[0023] 图4为本发明实施例提供的另一种NAT控制设备的结构示意图；

[0024] 图5为本发明实施例提供的另一种NAT控制设备的结构示意图；

[0025] 图6为本发明实施例提供的一种网络地址转换的系统示意图。

具体实施方式

[0026] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0027] 本发明实施例提供一种网络地址转换的方法，如图1所示，该方法应用于VM跨数据中心迁移的场景，该方法的执行主体为NAT控制设备，包括：

[0028] S101、在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后，NAT控制设备接收网络地址迁移消息，并验证该网络地址迁移消息。

[0029] 具体地，VM从第一数据中心迁移至第二数据中心主要有以下三种情况：

[0030] 第一种情况：操作人员通过操作图形用户界面(英文：Graphical User Interface，简称GUI)触发VM从第一数据中心迁移至第二数据中心，VCenter通知网络中心(英文：Net Center，简称：NCenter)：VM已经从第一数据中心迁移至第二数据中心，NCenter触发NAT映射表项的迁移，该VCenter用于管理和监控VM；该NCenter用于管理数据中心(包括第一数据中心和第二数据中心)；

[0031] 第二种情况：当第一数据中心发生异常(例如死机)时，触发VM从第一数据中心迁移至第二数据中心，VCenter通知NCenter：VM已经从第一数据中心迁移至第二数据中心，NCenter触发NAT映射表项的迁移；

[0032] 第三种情况：VCenter通过计算获知第一数据中心的负载较大，触发第一数据中心内的VM从第一数据中心迁移至第二数据中心，VCenter通知NCenter：VM已经从第一数据中心迁移至第二数据中心，NCenter触发NAT映射表项的迁移。

[0033] 其中，第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心，具体可以是，NCenter触发第一数据中心的网关将该发生迁移的VM所对应的NAT映射表项迁移到第二数据中心的网关。

[0034] 其中，该网络地址迁移消息携带有该NAT映射表项，该NAT映射表项记录该VM的私有网络地址与公有网络地址的映射关系，该私有网络地址只能在局域网中使用，无法在广域网中使用，该公有网络地址既可以在广域网中使用，也可以在局域网中使用，因此，VM在从局域网接入广域网时，需要将VM发送的报文的私有网络地址转换为公有网络地址。

[0035] 示例地，NAT控制设备可以接收第一数据中心发送的网络地址迁移消息，并向第二数据中心验证该网络地址迁移消息，具体为，在接收到该网络地址迁移消息后，向第二数据中心发送验证请求消息，第二数据中心在确认该NAT映射表项已经迁入后，向NAT控制设备发送验证响应消息。在NAT控制设备根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由第一数据中心更新为该第二数据中心后，NAT控制设备向第一数据中心发送迁移确认消息，确认该NAT映射表项迁移完成。

[0036] 示例地，NAT控制设备可以接收第二数据中心发送的网络地址迁移消息，并向第一数据中心验证该网络地址迁移消息，具体为，在接收到该网络地址迁移消息后，向第一数据中心发送验证请求消息，第一数据中心在确认NAT映射表项已经迁出后，向NAT控制设备发送验证响应消息。在NAT控制设备根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由第一数据中心更新为该第二数据中心后，该NAT控制设备向第二数据中心发送迁移确认消息，确认该NAT映射表项迁移完成。

[0037] 需要说明的是，该NAT控制设备接收网络地址迁移消息的机制(该NAT控制设备从第一数据中心或者从第二数据中心接收网络地址迁移消息)是提前设置在整个网络地址转换的系统中。

[0038] 具体地，该第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心可以是，第一数据中心将该NAT映射表项发送至第二数据中心，并删除该NAT映射表项，第二数据中心添加该NAT映射表项。

[0039] 进一步地，在VM从局域网接入广域网时，第一数据中心在接收到VM发送的第一个报文的情况下，需要将该报文的私有网络地址转换为相应的公有网络地址，NAT控制设备则为该报文的私有网络地址分配对应的公有网络地址，因此，该方法还包括：

[0040] 在该第一数据中心接收到VM发送的第一个携带私有网络地址的报文后,NAT控制设备接收该第一数据中心发送的NAT请求消息。

[0041] 其中,该NAT请求消息携带该VM发送的第一个报文的私有网络地址。

[0042] NAT控制设备根据该NAT请求消息为该私有网络地址分配公有网络地址,根据该私有网络地址和该公有网络地址建立该NAT映射表项,将该NAT映射表项记录在该网络地址映射表中,且将该NAT映射表项的归属信息记录为第一数据中心。

[0043] 其中,一个NAT映射表项对应一个VM。

[0044] NAT控制设备向该第一数据中心发送该NAT映射表项,以使得该第一数据中心在保存该NAT映射表项后,根据该NAT映射表项将该VM发送的报文(包括该VM发送的第一个报文以及后续发送的报文)的私有网络地址转换为公有网络地址。

[0045] 另外,该第一数据中心可以针对该NAT映射表项设置第二定时器,该第二定时器记录有预设时间,在后续某个时刻该VM不发送和接收报文的情况下,该第二定时器在该第一数据中心未检测到NAT映射表项对应的会话连接时启动,并在达到或者超过预设时间时停止,当第二定时器达到或者超过预设时间时,表示该VM长时间未发送和接收报文,则及时释放该VM对应的NAT映射表项,从而节约了系统资源。进一步地,若在预设时间内,第一数据中心重新收到该NAT映射表对应的会话连接时,则重置该第二定时器。

[0046] S102、NAT控制设备在对该网络地址迁移消息验证成功后,根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心。

[0047] 其中,该网络地址映射表记录有NAT映射表项以及NAT映射表项的归属信息。

[0048] 该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心,即更新后的NAT映射表项归属为第二数据中心。

[0049] 进一步地,在VM由第一数据中心迁移至第二数据中心后,当该第二数据中心没有收到该NAT映射表项对应的会话连接时,该方法还包括:释放NAT映射表项,上述释放NAT映射表项的过程为:

[0050] 接收该第二数据中心在该NAT映射表项相应的第一定时器达到或者超过预设时间时发送的释放请求消息,该释放请求消息中携带该NAT映射表项;

[0051] 在确定该网络地址映射表中记录的该NAT映射表项的归属信息为该第二数据中心时,向该第二数据中心发送释放响应消息,以使得该第二数据中心删除该NAT映射表项。

[0052] 该第一定时器记录有预设时间,在后续某个时刻VM不发送和接收报文的情况下,该第一定时器在该第二数据中心未检测到NAT映射表项对应的会话连接时启动,并在达到或者超过预设时间时停止,当第一定时器达到或者超过预设时间时,表示VM长时间未发送和接收报文,则及时释放该VM对应的NAT映射表项,从而节约了系统资源。

[0053] 另外,若在预设时间内,第二数据中心重新收到该NAT映射表项对应的会话连接时,则重置该第一定时器。

[0054] 需要说明的是,该预设时间是在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心的,另外,在VM从第一数据中心迁移至第二数据中心时,迁移前该预设时间已经记录的时间记为第一预设时间段,将该预设时间减去第一预设时间段后剩下的时间记为第二预设时间段,因此上述该预设时间在第一数

据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心具体为：将该预设时间和该第一预设时间和/或该第二预设时间在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心，例如，若第二定时器记录的预设时间为60秒，在VM迁移前，该预设时间已经记录了20秒，在迁移的过程中，该第二定时器停止记录该预设时间，并将60秒的预设时间和后续还未记录的40秒的预设时间发送至第二数据中心的第一定时器(也可以将60秒的预设时间和已经记录的20秒的预设时间以及后续还未记录的40秒的预设时间发送至第二数据中心的第一定时器)，该第一定时器则从该预设时间的40秒开始记录，当该第二数据中心发送或者接收针对该NAT映射表项的会话连接时，则重置该第一定时器为60秒。

[0055] 在确定该网络地址映射表中记录的该未使用的NAT映射表项的归属信息为该第二数据中心时，NAT控制设备向该第二数据中心发送释放响应消息，以使得该第二数据中心删除该NAT映射表项。

[0056] 本发明上述实施例中，该第一数据中心的动作具体可以由该第一数据中心的网关来执行；该第二数据中心的动作具体可以由该第二数据中心的网关来执行。

[0057] 需要说明的是，上述实施例中的私有网络地址可以是私有IP地址；或者私有IP地址和私有端口号，公有网络地址可以是公有IP地址；或者公有IP地址和公有端口号。

[0058] 采用上述实施例中的方法，通过NAT控制设备对各个数据中心的集中式控制，从而对各个数据中心的NAT地址资源进行合理的规划，同时，该NAT控制设备记录该VM对应的NAT映射表项的归属信息，解决了由于VM的申请与应用不在一个数据中心而造成的释放攻击问题。

[0059] 本发明实施例提供一种网络地址转换的方法，如图2所示，该方法应用于虚拟机VM跨数据中心迁移的场景，包括：

[0060] S201、第一数据中心接收VM发送的第一个携带私有网络地址的报文。

[0061] S202、第一数据中心向NAT控制设备发送NAT请求消息。

[0062] 其中，该NAT请求消息携带该VM发送的第一个报文的私有网络地址。

[0063] S203、NAT控制设备根据该NAT请求消息为该私有网络地址分配公有网络地址，根据该私有网络地址和该公有网络地址建立该NAT映射表项，将该NAT映射表项记录在该网络地址映射表中，且将该NAT映射表项的归属信息记录为第一数据中心。

[0064] 其中，该NAT映射表项记录私有网络地址与公有网络地址的映射关系，一个NAT映射表项对应一个VM，该私有网络地址为专门在局域网中使用的地址，无法在广域网中使用，该公有网络地址既可以在广域网中使用，也可以在局域网中使用。

[0065] S204、NAT控制设备向该第一数据中心发送该NAT映射表项。

[0066] S205、该第一数据中心保存该NAT映射表项，并根据该NAT映射表项将该VM发送的报文的私有网络地址转换为公有网络地址。

[0067] 进一步地，该第一数据中心可以针对NAT映射表项设置第二定时器，该第二定时器记录有预设时间，在后续某个时刻VM不发送和接收报文的情况下，该第二定时器在该第一数据中心未检测到NAT映射表项对应的会话连接时启动，并在达到或者超过预设时间时停止，当第二定时器达到或者超过预设时间时，表示VM长时间未发送和接收报文，则及时释放

该NAT映射表项,从而节约了系统资源。

[0068] 另外,若在预设时间内,第一数据中心重新收到该NAT映射表对应的会话连接时,则重置该第二定时器。

[0069] 需要说明的是,上述的步骤S201至步骤S205描述的是NAT控制设备为第一数据中心接收的VM发送的第一个报文分配NAT映射表项的过程,NAT控制设备后续接收的VM发送的报文,并不需要再次分配NAT映射表项,VM后续发送的报文直接使用该NAT映射表项。

[0070] 当VM从第一数据中心迁移至第二数据中心时,本实施例还包括以下步骤:

[0071] S206、第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心。

[0072] 具体的迁移过程可以参考对S101的描述。

[0073] S207、NAT控制设备接收该第二数据中心发送的网络地址迁移消息。

[0074] 其中,该网络地址迁移消息携带有该NAT映射表项。

[0075] 示例地,NAT控制设备也可以接收该第一数据中心发送的网络地址迁移消息。

[0076] 需要说明的是,该NAT控制设备接收网络地址迁移消息的机制(该NAT控制设备从第一数据中心或者从第二数据中心接收网络地址迁移消息)是提前设置在整个网络地址转换的系统中。

[0077] S208、NAT控制设备向第一数据中心发送验证请求消息。

[0078] 示例地,若NAT控制设备接收该第一数据中心发送的网络地址迁移消息,则该步骤S208为NAT控制设备向第二数据中心发送验证请求消息。

[0079] 该验证请求消息中携带该NAT映射表项。

[0080] S209、第一数据中心在确认该NAT映射表项已经迁出后,向NAT控制设备发送验证响应消息。

[0081] 示例地,若NAT控制设备接收该第一数据中心发送的网络地址迁移消息,则该步骤S209为第二数据中心在确认已经该NAT映射表项已经迁入后,向NAT控制设备发送验证响应消息。

[0082] S210、NAT控制设备根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心。

[0083] 其中,该网络地址映射表记录该NAT映射表项以及该NAT映射表项的归属信息,该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心,即更新后的NAT映射表项归属为第二数据中心,具体可以参考对步骤S102的描述。

[0084] S211、该NAT控制设备向第二数据中心发送迁移确认消息,确认该NAT映射表项迁移完成。

[0085] 示例地,若NAT控制设备接收该第一数据中心发送的网络地址迁移消息,则该步骤S211为该NAT控制设备向第一数据中心发送迁移确认消息,确认该NAT映射表项迁移完成。

[0086] 在VM由第一数据中心迁移至第二数据中心后,当该第二数据中心没有收到该NAT映射表项对应的会话连接时,该第二数据中心需要释放该NAT映射表项,该步骤包括:

[0087] S212、NAT控制设备接收该第二数据中心在该NAT映射表项相应的第一定时器达到或者超过预设时间时发送的释放请求消息。

[0088] 其中,该释放请求消息中携带有该NAT映射表项。

[0089] 该第一定时器记录有预设时间,在后续某个时刻VM不发送和接收报文的情况下,

该第一定时器在该第二数据中心未检测到NAT映射表项对应的会话连接时启动，并在达到或者超过预设时间时停止，当第一定时器达到或者超过预设时间时，表示VM长时间未发送和接收报文，则及时释放该NAT映射表项，从而节约了系统资源。

[0090] 另外，若在预设时间内，第二数据中心重新收到该NAT映射表项对应的会话连接时，则重置该第一定时器。

[0091] 需要说明的是，该预设时间是在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心的，另外，在VM从第一数据中心迁移至第二数据中心时，迁移前该预设时间已经记录的时间记为第一预设时间段，将该预设时间减去第一预设时间段后剩下的时间记为第二预设时间段，因此上述该预设时间在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心具体为：将该预设时间和该第一预设时间和/或该第二预设时间在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心时同时发送至第二数据中心，例如，若第二定时器记录的预设时间为60秒，在VM迁移前，该预设时间已经记录了20秒，在迁移的过程中，该第二定时器停止记录该预设时间，并将60秒的预设时间和后续还未记录的40秒的预设时间发送至第二数据中心的第一定时器(也可以将60秒的预设时间和已经记录的20秒的预设时间以及后续还未记录的40秒的预设时间发送至第二数据中心的第一定时器)，该第一定时器则从该预设时间的40秒开始记录，当该第二数据中心发送或者接收针对该NAT映射表项的会话连接时，则重置该第一定时器为60秒。

[0092] S213、在确定该网络地址映射表中记录的该NAT映射表项的归属信息为该第二数据中心时，NAT控制设备向该第二数据中心发送释放响应消息。

[0093] S214、该第二数据中心在接收到该释放响应消息后，删除该NAT映射表项。

[0094] 需要说明的是，上述实施例中的私有网络地址可以是私有IP地址；或者私有IP地址和私有端口号，公有网络地址可以是公有IP地址；或者公有IP地址和公有端口号。

[0095] 本发明上述实施例中，该第一数据中心的动作具体可以由该第一数据中心的网关来执行；该第二数据中心的动作具体可以由该第二数据中心的网关来执行。

[0096] 采用上述实施例中的方法，通过NAT控制设备对各个数据中心的集中式控制，从而对各个数据中心的NAT地址资源进行合理的规划，同时，该NAT控制设备记录该VM对应的NAT映射表项的归属信息，解决了由于VM的申请与应用不在一个数据中心而造成的释放攻击问题。

[0097] 本发明实施例提供一种NAT控制设备300，用于实现本发明上述各方法，如图3所示，该设备应用于虚拟机VM跨数据中心迁移的场景，包括：

[0098] 迁移消息接收单元301，用于在第一数据中心将发生迁移的虚拟机所对应的NAT映射表项迁移至第二数据中心后，接收网络地址迁移消息。

[0099] 具体地，VM从第一数据中心迁移至第二数据中心主要有以下三种情况：

[0100] 第一种情况：操作人员通过操作图形用户界面(英文：Graphical User Interface，简称GUI)触发VM从第一数据中心迁移至第二数据中心，VCenter通知网络中心(英文：Net Center，简称：NCenter)：VM已经从第一数据中心迁移至第二数据中心，NCenter触发NAT映射表项的迁移，该VCenter用于管理和监控VM；该NCenter用于管理数据中心(包

括第一数据中心和第二数据中心);

[0101] 第二种情况:当第一数据中心发生异常(例如死机)时,触发VM从第一数据中心迁移至第二数据中心,VCenter通知NCenter:VM已经从第一数据中心迁移至第二数据中心,NCenter触发NAT映射表项的迁移;

[0102] 第三种情况:VCenter通过计算获知第一数据中心的负载较大,触发第一数据中心内的VM从第一数据中心迁移至第二数据中心,VCenter通知NCenter:VM已经从第一数据中心迁移至第二数据中心,NCenter触发NAT映射表项的迁移。

[0103] 其中,第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心,具体可以是,Ncenter触发第一数据中心的网关将该发生迁移的VM所对应的NAT映射表项迁移到第二数据中心的网关。

[0104] 其中,该网络地址迁移消息携带有该NAT映射表项,该NAT映射表项记录该VM的私有网络地址与公有网络地址的映射关系,该私有网络地址只能在局域网中使用,无法在广域网中使用,该公有网络地址既可以在广域网中使用,也可以在局域网中使用,因此,VM在从局域网接入广域网时,需要将VM发送的报文的私有网络地址转换为公有网络地址。

[0105] 验证单元302,用于验证该网络地址迁移消息。

[0106] 更新单元303,用于在该验证单元302对该网络地址迁移消息验证成功后,根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心。

[0107] 其中,该网络地址映射表用于记录该NAT映射表项以及该NAT映射表项的归属信息。

[0108] 该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心,即更新后的NAT映射表项归属为第二数据中心。

[0109] 示例地,该迁移消息接收单元301,具体用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后,接收该第一数据中心发送的该网络地址迁移消息,则该验证单元302,具体用于向该第二数据中心验证该网络地址迁移消息。

[0110] 示例地,迁移消息接收单元301,具体用于在第一数据中心将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心后,接收该第二数据中心发送的该网络地址迁移消息,则该验证单元302,具体用于向该第一数据中心验证该网络地址迁移消息。

[0111] 需要说明的是,该NAT控制设备接收网络地址迁移消息的机制(该NAT控制设备从第一数据中心或者从第二数据中心接收网络地址迁移消息)是提前设置在整个网络地址转换的系统中。

[0112] 进一步地,如图4所示,该NAT控制设备300还包括:

[0113] NAT请求接收单元304,用于在该第一数据中心接收到VM发送的第一个携带私有网络地址的报文后,接收该第一数据中心发送的NAT请求消息。

[0114] 其中,该NAT请求消息携带该VM发送的第一个报文的私有网络地址。

[0115] 分配记录单元305,用于根据该NAT请求消息为该私有网络地址分配公有网络地址,根据该私有网络地址和该公有网络地址建立该NAT映射表项,并将该NAT映射表项记录在该网络地址映射表中,且将该NAT映射表项的归属信息记录为第一数据中心。

[0116] 其中,一个NAT映射表项对应一个VM。

[0117] 映射表项发送单元306,用于向该第一数据中心发送该NAT映射表项,以使得该第一数据中心在保存该NAT映射表项后,根据该NAT映射表项将该VM发送的报文(包括该VM发送的第一个报文以及后续发送的报文)的私有网络地址转换为公有网络地址。

[0118] 更进一步地,如图5所示,该NAT控制设备300还包括:

[0119] 释放请求接收单元307,用于在更新单元303根据该网络地址迁移消息将网络地址映射表中的该NAT映射表项的归属信息由该第一数据中心更新为该第二数据中心后,接收所述第二数据中心在所述NAT映射表项相应的第一定时器达到或者超过预设时间时发送的释放请求消息。

[0120] 其中,该释放请求消息中携带该NAT映射表项。

[0121] 该第一定时器记录有预设时间,在后续某个时刻VM不发送和接收报文的情况下,该第一定时器在该第二数据中心未检测到NAT映射表项对应的会话连接时启动,并在达到或者超过预设时间时停止,当第一定时器达到或者超过预设时间时,表示VM长时间未发送和接收报文,则及时释放该VM对应的NAT映射表项,从而节约了系统资源。

[0122] 另外,若在预设时间内,第二数据中心重新收到该NAT映射表项对应的会话连接时,则重置该第一定时器。

[0123] 释放响应发送单元308,用于在确定该网络地址映射表中记录的该NAT映射表项的归属信息为该第二数据中心时,向该第二数据中心发送释放响应消息,以使得该第二数据中心删除该NAT映射表项。

[0124] 本发明上述实施例中,第一数据中心的动作具体可以由第一数据中心的网关来执行;第二数据中心的动作具体可以由第二数据中心的网关来执行。

[0125] 需要说明的是,上述实施例中的私有网络地址可以是私有IP地址;或者私有IP地址和私有端口号,公有网络地址可以是公有IP地址;或者公有IP地址和公有端口号。

[0126] 采用上述实施例中的NAT控制设备,通过该NAT控制设备对各个数据中心的集中式控制,从而对各个数据中心的NAT地址资源进行合理的规划,同时,该NAT控制设备记录该VM对应的NAT映射表项的归属信息,解决了由于VM的申请与应用不在一个数据中心而造成的释放攻击问题。

[0127] 本发明实施例提供一种网络地址转换的系统,如图6所示,该系统应用于虚拟机VM跨数据中心迁移的场景,包括:NAT控制设备300、第一数据中心601和第二数据中心602,

[0128] 该第一数据中心601,用于将发生迁移的VM所对应的NAT映射表项迁移至第二数据中心602。

[0129] 该NAT控制设备为上述各实施例描述的NAT控制设备300。

[0130] 该第二数据中心602,用于接收该NAT映射表项。

[0131] 本发明上述实施例中,第一数据中心的动作具体可以由第一数据中心的网关来执行;第二数据中心的动作具体可以由第二数据中心的网关来执行。

[0132] 需要说明的是,上述NAT控制设备300应用于上述网络地址转换的方法,且该设备中的各个单元也与该方法中的各步骤相对应。

[0133] 采用上述实施例中的网络地址转换系统,通过该NAT控制设备对各个数据中心的集中式控制,从而对各个数据中心的NAT地址资源进行合理的规划,同时,该NAT控制设备记录该VM对应的NAT映射表项的归属信息,解决了由于VM的申请与应用不在一个数据中心而

造成的释放攻击问题。

[0134] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0135] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

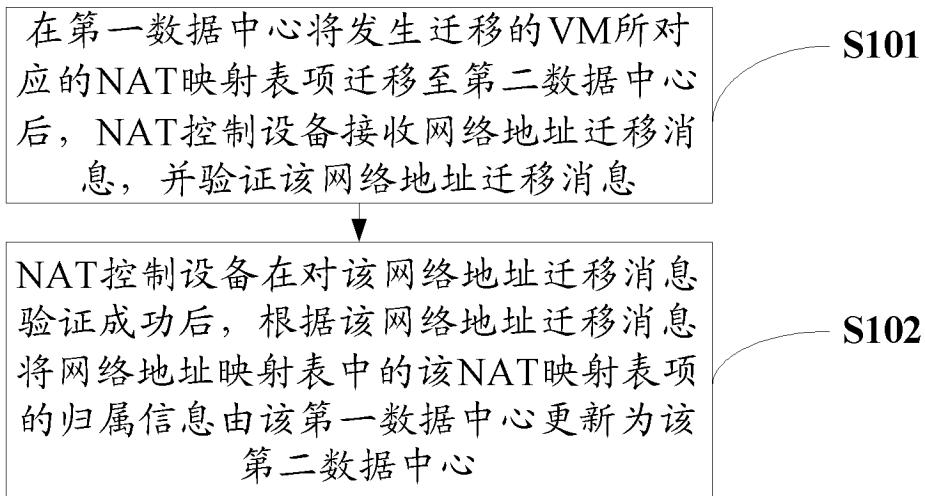


图1

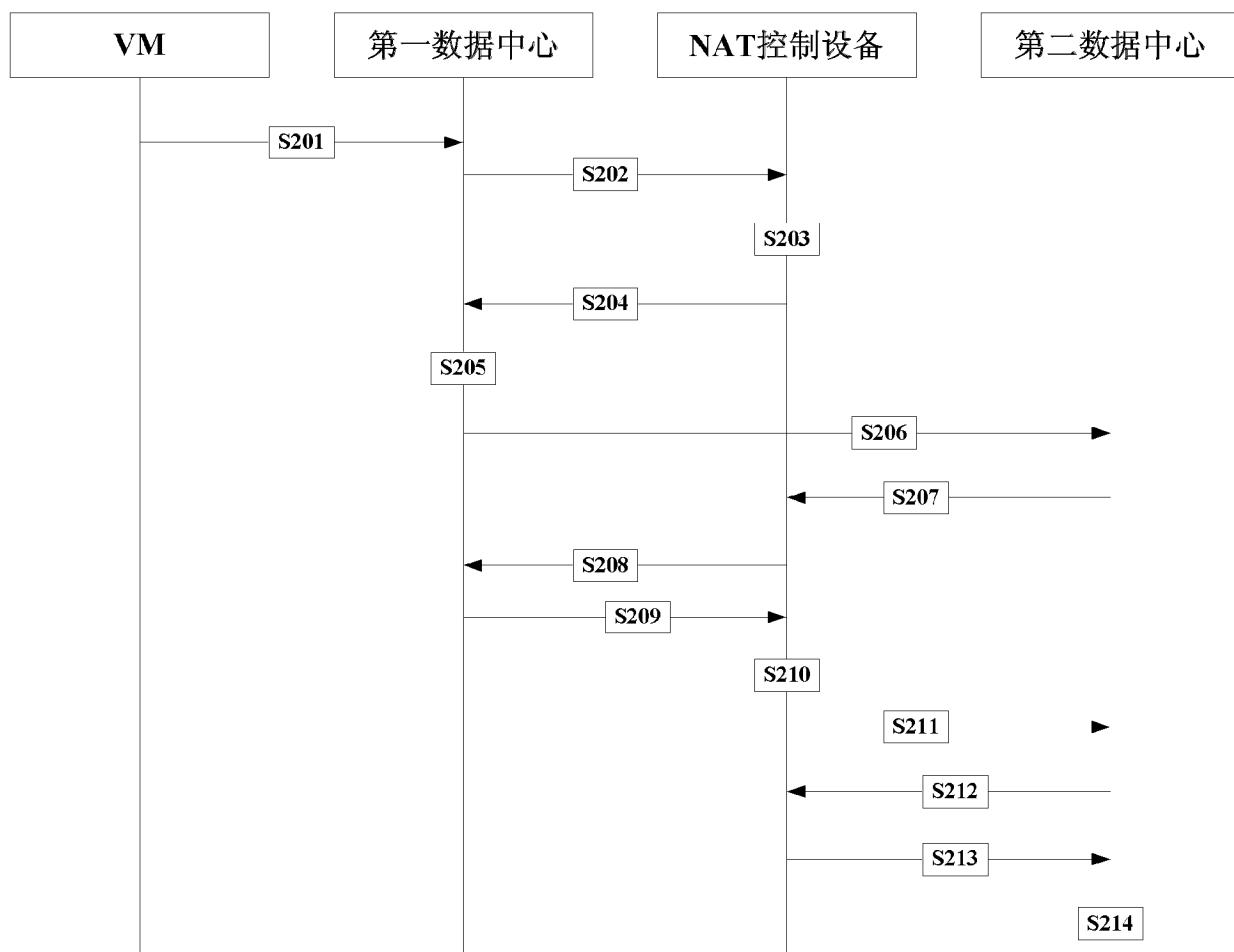


图2

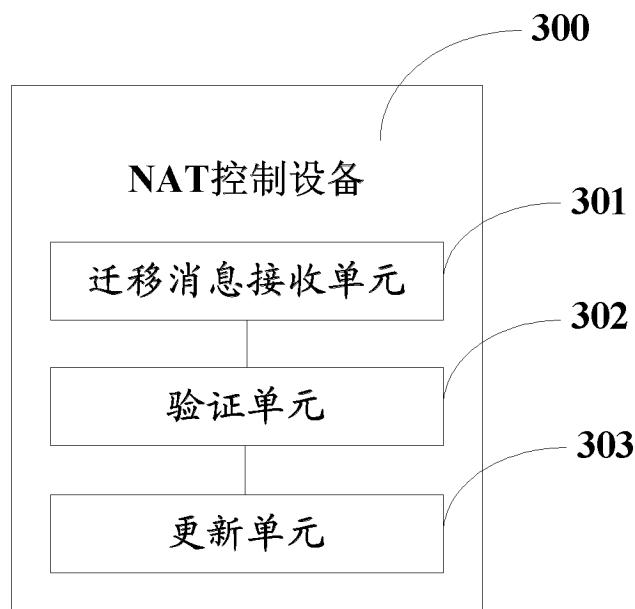


图3

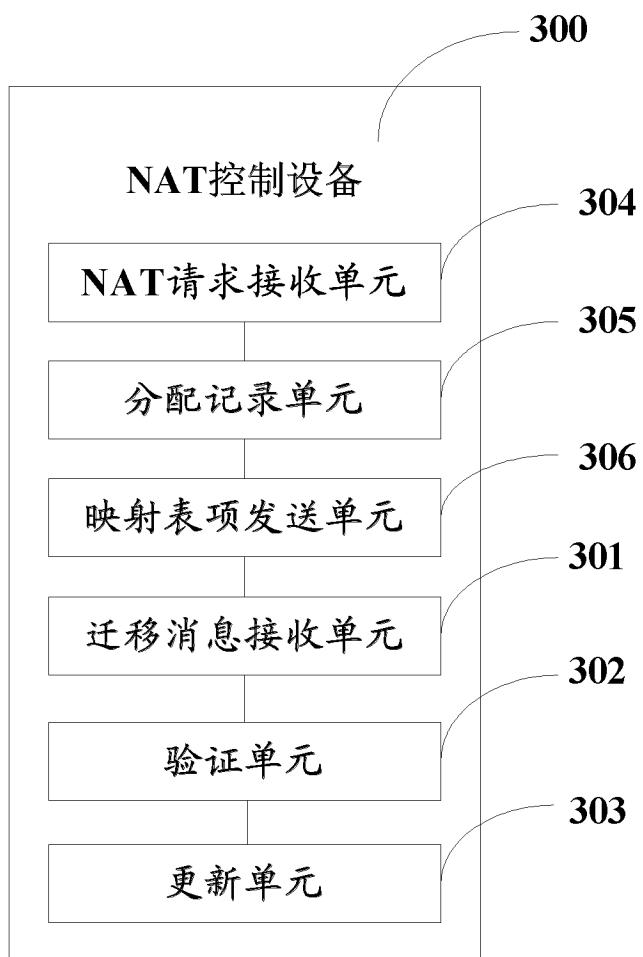


图4

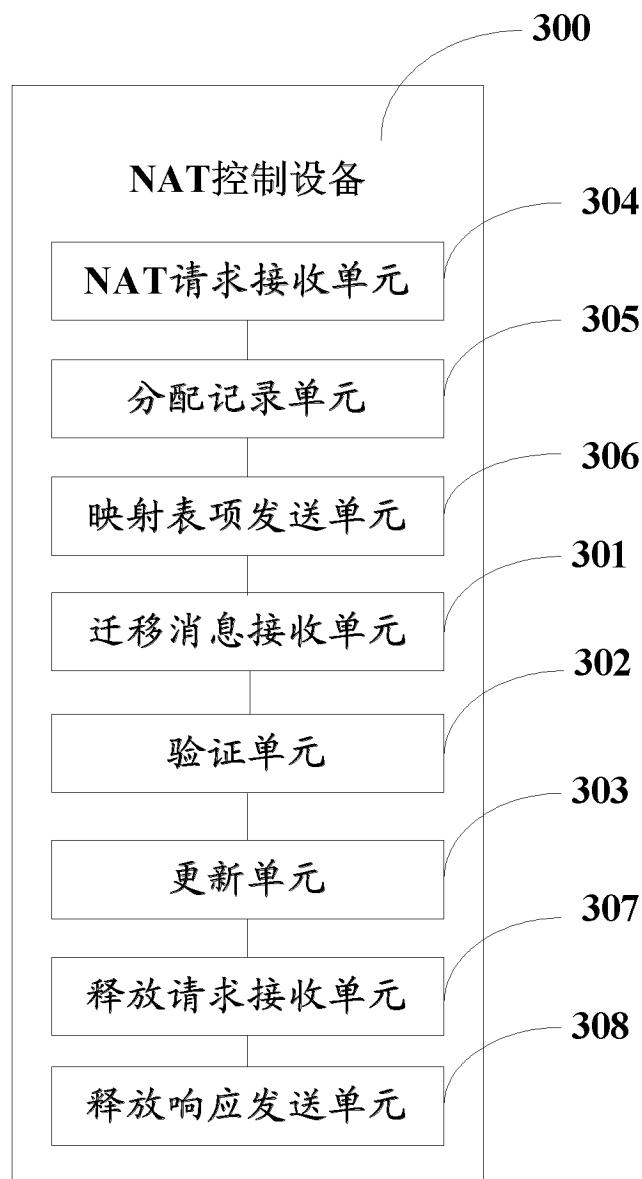


图5

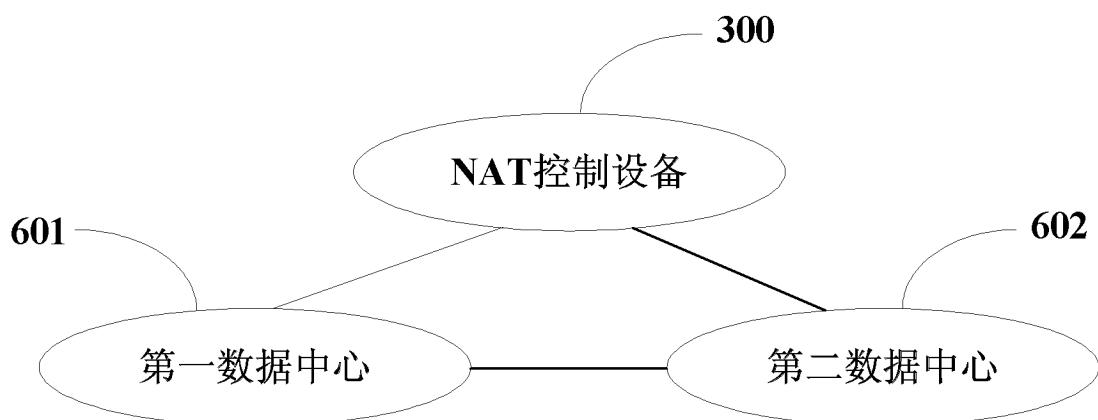


图6