[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610011805.1

[45] 授权公告日 2009 年 5 月 6 日

[11] 授权公告号 CN 100486176C

[22] 申请日 2006.4.27

[21] 申请号 200610011805.1

[73] 专利权人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦 A 座 6 层

[72] 发明人 耿国庆 张 远 张功应

[56] 参考文献

WO2005104484A1 2005.11.3

KR20060028975A 2006.4.4

JP2004147132A 2004.5.20

CN1561061A 2005.1.5

CN1744521A 2006.3.8

审查员 彭 媛

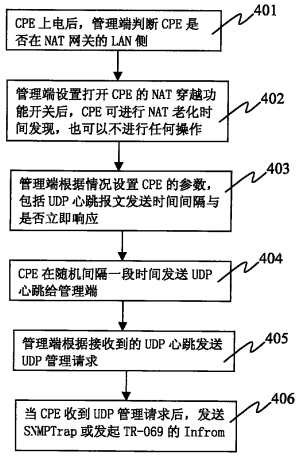
权利要求书 2 页 说明书 12 页 附图 3 页

[54] 发明名称

一种穿越网络地址翻译网关对用户侧设备进行管理的方法

[57] 摘要

本发明公开了一种穿越网络地址翻译网关对用户侧设备进行管理的方法，包括：用户侧设备上电后，由管理端确定用户侧设备是否在局域网侧；管理端设置并打开处于局域网侧的所述用户侧设备的网络地址翻译网关穿越功能开关，由用户侧设备自行选择进行网络地址翻译的老化时间发现操作或不进行任何操作；管理端设置用户侧设备的参数；用户侧设备根据时间间隔向管理端发送心跳报文；管理端向用户侧设备发送用户数据报协议管理请求；用户侧设备根据管理请求，利用多种协议的报文与管理端进行联系，由管理端完成对用户侧设备的主动管理。 本发明保证了管理端管理的实时性，适用于管理使用 SNMP 协议或 TR－069 协议相关技术的用户侧设备。



1、一种穿越网络地址翻译网关对用户侧设备进行管理的方法，其特征在于，包括如下步骤：

步骤一，用户侧设备上电后，由管理端确定用户侧设备是否在网络地址翻译网关的局域网侧；

步骤二，管理端设置处于局域网侧的所述用户侧设备的网络地址翻译网关穿越功能开关参数，所述用户侧设备自行选择进行网络地址翻译的老化时间发现操作或不进行任何操作；

步骤三，管理端确定所述用户侧设备的用户数据报协议的心跳报文发送时间间隔以及管理端是否立即响应所述心跳报文，以及设置所述用户侧设备的参数，其中，所述心跳报文包括设备标识参数；

步骤四，所述用户侧设备根据所述时间间隔向管理端发送所述心跳报文；

步骤五，管理端向所述用户侧设备发送用户数据报协议管理请求；

步骤六，所述用户侧设备根据所述管理请求，利用多种协议的报文与所述管理端进行联系，由所述管理端完成对用户侧设备的主动管理。

2、根据权利要求 1 所述的方法，其特征在于，所述老化时间发现操作包括如下步骤：

步骤 a，用户侧设备通过端口发送老化时间报文给管理端，记录所述老化时间报文的发送时刻，并打开端口监听管理端发回的响应；

步骤 b，管理端收到所述老化时间报文后，每隔一预定时间返回一基于用户数据报协议的探测报文；

步骤 c，如果用户侧设备在一设定的时间段内未收到所述探测报文，则认为网络地址翻译的地址映射关系已经老化，用户侧设备将最后一次收到所述探测报文的时刻与所述发送时刻之间的差值作为老化时间；

步骤 d，如果发现所述老化时间或者在长时间内无法发现所述老化时间，用户侧设备发送老化发现结束报文给管理端，管理端存储所述老化时间并根据所述结束报文或者根据管理端的自身情况停止发送所述探测报文。

3、根据权利要求 2 所述的方法，其特征在于，所述步骤 d 中，所述自

身情况为：管理端未接收到所述结束报文，并且在持续发送所述探测报文 30 分钟后自动结束所述探测报文的发送。

4、根据权利要求 2 所述的方法，其特征在于，所述步骤 b 中的所述预定时间为 10 秒，所述步骤 c 中的所述设定的时间段为五分钟。

5、根据权利要求 1 所述的方法，其特征在于，所述步骤一中，所述管理端通过比较所述用户侧设备上电上报的地址与实际收到的报文地址，来确定用户侧设备是否在网络地址翻译网关的局域网侧。

6、根据权利要求 2 所述的方法，其特征在于，在所述步骤三中，如果发现了老化时间，则所述心跳报文发送时间间隔设定为小于或等于所述老化时间，否则所述时间间隔为默认的时间段。

7、根据权利要求 6 所述的方法，其特征在于，在所述步骤三中，如果设定了立即响应所述心跳报文，则管理端收到所述心跳报文后立即给与响应，并且如果所述用户侧设备未等到所述响应会进行心跳报文的重发；如果没有设定立即响应，则只有在管理端需要管理用户侧设备时才会发送响应。

8、根据权利要求 6 所述的方法，其特征在于，在所述步骤四中，所述用户侧设备在所述时间间隔的范围内取随机数，并根据所述随机数发送所述心跳报文。

9、根据权利要求 1 所述的方法，其特征在于，在所述步骤五中，管理端在收到所述心跳报文后发送所述管理请求，或者在需要管理的时候随时发送所述管理请求。

10、根据权利要求 1 所述的方法，其特征在于，所述步骤六中，所述多种协议的报文为 SNMP Trap 或 TR-069 Inform，并且在管理过程中停止发送所述心跳报文。

一种穿越网络地址翻译网关对用户侧设备进行管理的方法

技术领域

本发明涉及网络地址翻译协议的穿越技术，特别是涉及穿越网络地址翻译协议对局域网侧的用户侧设备进行主动管理的方法。

背景技术

本发明涉及的英文简称如下：

ACS：Auto-Configuration Server。自动配置服务器；

CPE：Customer Premise Equipment。用户前端设备；

UDP：User Datagram Protocol。用户数据报协议；

TCP：Transmission Control Protocol。传输控制协议；

LAN：Local Area Network。局域网；

WAN：Wide Area Network。广域网；

ICMP：Internet Control Message Protocol。因特网控制信息协议；

NAT：Network Address Translation。网络地址翻译；

TR-069:Technical Report - 069 CPE WAN Management Protocol.用户前端设备广域网管理协议；

SNMP：Simple Network Management Protocol 简单网络管理协议；

CPE 是放在用户家中或者企业内部的终端设备，如 ADSL MODEM、机顶盒、IAD（综合接入设备），是由电信公司提供，通过网线或者电话线连接到电信网络中的设备。随着近年来电信网络和 IP 技术的不升级和发展，视频技术、流媒体技术应用不断推陈出新，用户侧的终端设备种类越来越丰富，功能越来越强大、智能化程度也越来越高。起初因特网刚刚起步的时候，个人用户或者单位若想接入网络，都必需连接 MODEM(调制解调器),通过 MODEM，家庭用户可以享受因特网丰富的信息和资源。随着近年来科技的不断进步，使用各种新技术的终端也陆续进入千家万户：使用无线宽带接入技术的 AP（接入点）设备；使用 VoIP 技术的 IAD 设备、IP PHONE 设备；使用宽带 IP 和流媒

体技术的机顶盒设备；无线蓝牙设备接入设备等；越来越被大众接受使用。随着用户侧电信终端数目不断增多，在给用户带来方便和给运营商带来巨大收益的同时，也同时带来了管理上的问题。对于用户来说，期望功能越来越强，却要求这些电子设备越来越智能化、简单化，不需要或者很少的配置和维护，最好设备可以自管理和零维护；对于电信运营商而言，希望增强对 CPE 设备的管理能力和力度，提高业务服务质量和用户故障反应能力，同时可对恶意的用户行为进行监控和追查。

随着网络规模的不断扩大，接入设备数目的日益增多，电信运营商的可用 IP 地址资源正在不断的耗尽，电信运营商分配给家庭用户和单位用户的可用 IP 地址也越来越少。目前，运营商为一般家庭用户只能提供一个合法地址,对于这么多的网络终端设备只有通过 NAT 方式进行用户侧的地址转换，实现多个用户侧设备公用一个外网地址。NAT（Network Address Translation）即网络地址翻译，是网络工程任务组制定的一个标准和规范(RFC 1631)。NAT 就是在局域网内部网络中使用内部地址，而当 NAT 的 LAN（局域网）侧设备要与外部网络进行通讯时，就在网关（可以理解为网络的统一出口）处，将 LAN 侧地址替换成 WAN（广域网，如 Internet）侧地址，从而可在 WAN 侧上正常访问。NAT 可以使多台计算机、终端设备共享一条连接，这一功能很好地解决了用户 IP 地址紧缺的问题。这时，NAT 屏蔽了内部网络，所有内网设备对于外网来说是不可见的，而内网计算机用户通常不会意识到 NAT 的存在。

NAT 目前有三种类型：静态 NAT(Static NAT)、动态地址 NAT(Pooled NAT)、网络地址端口转换 NAPT（Port－Level NAT)。

其中静态 NAT 设置起来最为简单和最容易实现的一种，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。而动态地址 NAT 则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，三种 NAT 方案各有利弊。

动态地址 NAT 只是转换 IP 地址，它为每一个内部的 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号，对于频繁的远程联接也可以采用动态 NAT。当远程用户联接上之后，动态地址 NAT 就会分配给他一个 IP 地址，

用户断开时，这个 IP 地址就会被释放而留待以后使用。

网络地址端口转换 NAPT（Network Address Port Translation）是目前家庭或者企业常用的转换方式。它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的端口号。

由于 NAT 可以屏蔽内网拓朴信息，起到了防火墙的作用，外网的设备不能随意的对 NAT 内网进行访问。管理数据也无法穿越，使得电信运营商对用户侧的电信设备无法进行直接的管理，必需等待 CPE 设备主动发起连接之后获取映射的地址，并且在 NAT 上产生了地址映射关系，才能进行相应的管理。这种情况使得管理端对 CPE 管理实时性不高，无法对用户提供实时周到的服务，对 CPE 出现的故障和告警也无法实时的响应和解决。并且随着用户群的不断扩大，NAT 穿越的问题将会越来越普遍和棘手。

目前有一种通过 NAT 进行双向访问的方法，该方法基于长连接(即双方先建立通讯连接，连接建立后不断开，然后再进行报文发送和接收)的应用而实现。因为位于 NAT 内部的终端可以自由访问位于 NAT 外部的终端，所以首先由位于 NAT 内部的终端向位于 NAT 外部的终端发起呼叫，请求建立连接。在上述的连接建立后，会话双方中的一方终端以一定的周期向另一方终端发送数据包以保持双方的长连接，该周期为一个小于本地 NAT 失效周期为时间间隔。

该方法存在以下不足：

1)该访问方法基于 TCP 长连接，连接双方需要定期的发送报文维护 TCP 连接。对于数量巨大的用户终端来说，服务器需要占用大量的资源和链接带宽，处理性能差，很难取得实际的管理效果。

2)该方法没有给出获取 NAT 失效周期（即 NAT 地址映射老化时间）的方法。对于不同的 NAT，老化时间不同，不能统一处理，增加了管理的难度。

3)该处理方法不能与 CPE 设备标准的管理协议（TR-069、SNMP）很好的结合。

所以该方法并不适合穿越 NAT 管理数目巨大的 CPE 设备。

在 DSL（数字用户线路）论坛中，提出了穿越 NAT 实施 TR-069 远程管理的技术报告 TR-111，应用 TR-069 进行家庭网管设备远程管理。TR-111 利用

现有的STUN（Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators。）机制，结合TR-069管理特点，CPE通过发现NAT的老化时间，并通过不间断发送UDP绑定报文维护NAT的映射关系。ACS可通过基于UDP的链接请求报文通知CPE进行Inform，进入主动管理流程。

该方法存在以下不足：

1)实现相对复杂，CPE和管理端为实现该功能都需要做大量的工作。

2)NAT老化时间发现需要占用临时的2个NAT地址转换条目，而NAT上的条目是有限的，对于比较大的内网环境（如大型酒店）来说，NAT的地址映射条目本身已经很紧张，这种机制无法实施。

3)专为TR-069管理协议设计，不适合通过SNMP协议进行管理的设备。

目前也有一些其它穿越NAT的方法，但是需要在网络环境中增加代理服务器或者中继服务器，或者需要修改NAT配置或预留端口。这些方法对现有网络和配置改动较大，不适合运行商的管理思路和方式。

发明内容

本发明所要解决的技术问题是提供一种穿越网络地址翻译网关对用户侧设备进行管理的方法，解决现有NAT穿越技术实现复杂，不适合较大的内网环境及不能通用于各种协议进行管理的技术问题。

为达到上述目的，本发明提供了一种穿越网络地址翻译网关对用户侧设备进行管理的方法，其特点在于，包括如下步骤：

步骤一，用户侧设备上电后，由管理端确定用户侧设备是否在网络地址翻译网关的局域网侧；

步骤二，管理端设置并打开处于局域网侧的所述用户侧设备的网络地址翻译网关穿越功能开关参数，所述用户侧设备自行选择进行网络地址翻译的老化时间发现操作或不进行任何操作；

步骤三，管理端确定所述用户侧设备的用户数据报协议的心跳报文发送时间间隔以及管理端是否立即响应所述心跳报文，以及设置所述用户侧设备的参数，其中，所述心跳报文包括设备标识参数；

步骤四，所述用户侧设备根据所述时间间隔向管理端发送所述心跳报

文；

步骤五，管理端向所述用户侧设备发送用户数据报协议管理请求；

步骤六，所述用户侧设备根据所述管理请求，利用多种协议的报文与所述管理端进行联系，由所述管理端完成对用户侧设备的主动管理。

上述的方法，其特点在于，所述老化时间发现操作包括如下步骤：

步骤 a，用户侧设备通过端口发送老化时间报文给管理端，记录所述老化时间报文的发送时刻，并打开端口监听管理端发回的响应；

步骤 b，管理端收到所述老化时间报文后，每隔一预定时间返回一基于用户数据报协议的探测报文；

步骤 c，如果用户侧设备在一设定的时间段内未收到所述探测报文，则认为网络地址翻译的地址映射关系已经老化，用户侧设备将最后一次收到所述探测报文的时刻与所述发送时刻之间的差值作为老化时间；

步骤 d，如果发现所述老化时间或者在长时间内无法发现所述老化时间，用户侧设备发送老化发现结束报文给管理端，管理端存储所述老化时间并根据所述结束报文或者根据管理端的自身情况停止发送所述探测报文。

上述的方法，其特点在于，所述步骤 d 中，所述自身情况为：管理端未接收到所述结束报文，并且在持续发送所述探测报文 30 分钟后自动结束所述探测报文的发送。

上述的方法，其特点在于，所述步骤 b 中的所述预定时间为 10 秒，所述步骤 c 中的所述设定的时间段为五分钟。

上述的方法，其特点在于，所述步骤一中，所述管理端通过比较所述用户侧设备上电上报的地址与实际收到的报文地址，来确定用户侧设备是否在网络地址翻译网关的局域网侧。

上述的方法，其特点在于，在所述步骤三中，如果发现了老化时间，则所述心跳报文发送时间间隔设定为小于或等于所述老化时间，否则所述时间间隔为默认的时间段。

上述的方法，其特点在于，在所述步骤三中，如果设定了立即响应所述心跳报文，则管理端收到所述心跳报文后立即给与响应，并且如果所述用户侧设备未等到所述响应会进行心跳报文的重发；如果没有设定立即响应，则只有在管理端需要管理用户侧设备时才会发送响应。

上述的方法，其特点在于，在所述步骤四中，所述用户侧设备在所述时间间隔的范围内取随机数，并根据所述随机数发送所述心跳报文。

上述的方法，其特点在于，在所述步骤五中，管理端在收到所述心跳报文后发送所述管理请求，或者在需要管理的时候随时发送所述管理请求。

上述的方法，其特点在于，所述步骤六中，所述多种协议的报文为 SNMP Trap 或 TR-069 Inform，并且在管理过程中停止发送所述心跳报文。

本发明的技术效果在于：

本发明方法利用了现有 CPE 设备支持的管理协议的技术特点，采用 TR-069 协议的 Inform 方法和 SNMP 管理协议方法，使得管理端可以实时或准实时的对 CPE 设备进行主动的管理，如故障检测、性能监控、状态查询。通过这种方法，保证了管理端管理实时性，缩短了管理周期。同时该方法可以透明的穿越现有各种类型的 NAT 网关，而不需要对现有 NAT 配置进行任何的改造，保证了用户侧的已有设备与设备配置的安全性和完整性。该发明方法适用 SNMP 协议或 TR-069 协议相关技术，可使用统一的流程和消息管理目前几乎所有的 CPE 设备，而不需要指定 CPE 的协议类型。

附图说明

图 1 为本发明实施例所述的 NAT 老化时间发现流程示意图；

图 2 为本发明实施例所述的 CPE 发送 UDP 心跳报文，管理端进行响应和管理的流程示意图；

图 3 为本发明实施例所述的管理端主动发送 UDP 管理请求报文，进入 TR-069 或 SNMP 管理流程；

图 4 为本发明方法的步骤流程图。

具体实施方式

下面结合附图对本发明处理方法进行说明。

本发明主要是克服管理端穿越 NAT 管理 CPE 的种种困难，提供一种穿越

NAT 管理 CPE 设备的实现方法，采用精简的 NAT 老化时间发现机制，发现 NAT 地址映射的老化周期；CPE 可按照 NAT 老化周期或者管理端设置的时间间隔发送 UDP 心跳报文；管理端可以根据 UDP 报文进行回应，通知 CPE 是否需要发送 TR-069 的 Inform 消息或者发送 SNMP Trap 消息；管理端也可以不必等待 CPE 的 UDP 心跳报文而直接下发 UDP 管理请求报文，当 CPE 收到后进行同样的处理。

图 4 为本发明方法的步骤流程图，本发明的实现方法包括以下步骤：

步骤 401，CPE 上电后，管理端判断 CPE 是否在 NAT 网关的 LAN 侧；

步骤 402，管理端设置打开 CPE 的 NAT 穿越功能开关后，CPE 可进行 NAT 老化时间发现，也可以不进行任何操作。

步骤 403，管理端根据情况设置 CPE 的参数，包括 UDP 心跳报文发送时间间隔与是否立即响应；

步骤 404，CPE 在随机间隔一段时间发送 UDP 心跳给管理端；

步骤 405，管理端根据接收到的 UDP 心跳发送 UDP 管理请求；

步骤 406，当 CPE 收到 UDP 管理请求后，发送 SNMP Trap 或发起 TR-069 的 Infrom。

所述步骤 401 中，管理端通过 CPE 上电上报的地址与实际收到报文的地址进行比较，判断 CPE 是否在 NAT 的 LAN 侧。

所述步骤 402 中，若发现 CPE 在 NAT 的 LAN 侧，则打开其 NAT 穿越开关。

所述步骤 402 中，CPE 可在 NAT 穿越功能开关打开后，启动 NAT 老化时间发现功能，并记录发现的 NAT 老化时间。CPE 也可不进行任何操作。

所述步骤 402 中，CPE 若启动 NAT 老化时间发现，通过端口 P1 发送 UDP 的 NAT 老化时间报文给管理端。打开 P1 端口监听管理端发回的响应。同时打开计时器，记录当前时间为 T1。此时，CPE 发送报文的地址为（A1,P1）经过 NAT 转换为（A1’,P1’）。

所述步骤 402 中，管理端收到 CPE 的 NAT 老化时间发现报文后，每隔一段时间向（A1’,P1’）发送基于 UDP 的探测报文。

所述步骤 402 中，CPE 当很久（如 5 分钟）未收到管理端的探测报文，即认为 NAT 地址映射关系已经老化，就将最后一次收到报文的时间 T2 与 T1 的差值（T2-T1）作为 NAT 的老化时间。

所述步骤 402 中，CPE 发现 NAT 老化后，或者无法发现老化时间，将发送基于 UDP 的 NAT 老化发现结束报文给管理端，管理端收到报文后停止发送探测报文。

所述步骤 402 中，由于 UDP 协议的不可靠性，管理端可能无法收到 NAT 老化时间发现结束报文，但是会在持续发送响应 30 分钟后自动结束发送探测报文。

所述步骤 402 中，CPE 结束 NAT 老化发现流程后，设置相关参数供管理端读取。参数包括：NAT 老化时间发现标志、（若已经发现了 NAT 的老化时间）NAT 老化时间。

所述步骤 403 中，管理端查询 CPE 是否发现了 NAT 老化时间。根据 NAT 的老化时间发现结果，设置 CPE 的 UDP 心跳发送时间间隔：如果发现了老化时间，最大时间间隔为 NAT 老化时间；若 CPE 没有发现 NAT 时间，则时间间隔为默认的时间段。

所述步骤 403 中，管理端设置是否立即响应参数。如果该参数为真，则管理端只要收到 CPE 的 UDP 心跳报文后，就会给与响应，响应中指示是否需要 CPE 立即发送 SNMP Trap 或进行 Inform。否则，只有管理端在需要管理 CPE 时才会发送响应报文。

所述步骤 404 中，CPE 在设置好的时间间隔范围内取随机数，使用地址（A1，P1）发送 UDP 心跳报文。

所述步骤 404 中，若管理端在步骤 403 中设置了立即响应参数为真，则会在收到 CPE 的 UDP 心跳后发送响应。否则不进行任何操作。

所述步骤 404 中，管理端在步骤 403 中设置了立即相应参数为真，则 CPE 在发送完 UDP 心跳后，会等待管理端的响应，若超时，则重发 3 次。在 3 次重发中，任何一次收到了管理端的响应，则不再重发。

所述步骤 405 中，管理端可在收到 UDP 心跳后发送 UDP 管理请求报文，也可以在需要管理的时候随时发送 UDP 管理管理请求报文。

所述步骤 406 中，CPE 在收到管理端的请求报文后，将发起 TR-069 的 Inform 或者是 SNMP Trap。当进入管理流程后，关闭 UDP 心跳发送。当流程结束后，立即发送 UDP 心跳。

所述步骤 406 中，CPE 在收到管理端的请求报文后，可发送 SNMP Trap，

当管理端收到 SNMP Trap 后，发送 SNMP 管理报文（如 SNMP GET/SET）。报文目的地址/目的端口是收到 SNMP Trap 的源地址/源端口，这样报文就会经过 NAT 转发给 CPE 设备。

当 CPE 与管理端进行通讯后，NAT 上会创建相应 LAN 侧地址与 WAN 侧地址的映射关系条目，当映射关系失效后，管理端发送给 CPE 的报文将会被 NAT 阻挡，不会转发相应的 CPE。由于 NAT 老化时间的存在，给管理端主动管理 CPE 设备带来了困难，但是利用这种原理可发现 NAT 老化时间，为穿越 NAT 提供帮助。

如图 1 所示，本发明的 NAT 老化时间发现流程采用以下的步骤和技术环节：

其中 A1、A1’、A3 为 IP 地址，P1、P1’、P3 为端口。

步骤 101：CPE 打开 UDP 端口 P1 进行监听。

步骤 102：CPE 从（A1，P1）发送 UDP 的 NAT 老化时间发现报文给管理端（A3，P3），记录当前时间为 T1，并开始计时。

步骤 103：管理端收到 CPE 的报文后，定时发送 UDP 的 NAT 老化时间探测报文给收到报文的源地址。

步骤 104：CPE 在收到上一个探测报文后 5 分钟之内再也没有收到报文，则认为 NAT 地址映射条目已经老化，计算 NAT 的老化时间。

步骤 105：CPE 从（A1，P1）发送 UDP 的 NAT 老化时间发现结束报文给管理端。

所述的步骤 102 中，CPE 发送报文的地址在经过 NAT 映射为(A1’,P1’)，也就是管理端收到报文的地址。

所述的步骤 102 中，若 CPE 发送报文后很久没有收到管理端的响应，则通过 PING 等方式检查管理端链路是否连通。如果链路不通，则退出流程。否则，重发 3 次 NAT 发现报文，若仍然没有收到报文，则退出流程。

所述的步骤 103 中，管理端收到报文后，发送 NAT 老化时间探测报文。并且每隔 10 秒发送一次。

所述的步骤 104 中，如果 CPE 在 5 分钟之内都没有收到管理端发来的响应报文，则将上次收到响应的时间 T2 与 T1 的差值（T2-T1）作为 NAT 老化时间。

所述的步骤104中，当CPE发现了NAT老化时间后，记录NAT老化时间发现标志和具体的时间，管理端可以查询相应的参数。

所述的步骤105中，管理端收到CPE的结束报文则停止发送响应报文。如果UDP报文丢失，管理端没有收到该报文，管理端在持续发送30分钟自动停止发送。

如图2所示，CPE发送UDP心跳以及管理端响应的流程采用以下的步骤和技术环节：

步骤201：CPE从（A1,P1）发送UDP心跳报文给管理端（A3，P3）。

步骤202：管理端收到报文后，发送UDP管理请求报文。

步骤203：CPE收到管理端响应后，根据相应报文的类型，发起TR-069的Inform或者发送SNMP Trap。然后进入相应的管理操作流程。

步骤204：管理流程结束后，CPE立即发送UDP心跳报文，然后UDP心跳发送进程休眠。休眠结束后，准备下一次发送UDP心跳报文。

所述的步骤201中，由于经过了NAT地址转换，CPE发送的UDP心跳报文需要包括设备ID（DeviceId）参数，否则管理端无法将该消息与相应的CPE设备关联。

所述的步骤201中，如果管理端已经设置CPE需要等待管理端响应，则每次CPE发送心跳之后，管理端都会给予响应。CPE在每次发送完UDP心跳报文都后，都需要等待响应。如果超时没有收到响应，则重发3次。若3次都没有收到响应，则退出流程。

所述的步骤201中,如果管理端已经设置CPE不需要等待管理端响应，则每次CPE发送心跳之后，管理端只会在需要管理CPE时发送UDP管理请求报文。此时CPE不会等待响应，也不重试。

所述的步骤202中，如果管理端设置CPE需要等待响应，则会对每次收到的报文进行响应，在响应报文中指示是否需要立即对CPE进行管理。

所述的步骤202中，如果管理端设置CPE不需要等待响应，则在需要对CPE进行管理时发送UDP管理请求报文。

所述的步骤203中，当CPE进入管理端的管理流程后，不再发送UDP心跳报文。

所述步骤203中，若CPE发送SNMP Trap，管理端发送SNMP管理报文。

报文的目的地址/目的端口与收到 SNMP Trap 的源地址/源端口一致。

所述的步骤 204 中，由于管理端管理的 CPE 数目可能较多，为避免大量 CPE 同时发送 UDP 心跳带来的大量并发情况，CPE 选择在一个时间段内随机休眠相应的时间。

对于管理端已经可以管理的 CPE 设备，管理端在需要立即进行管理时，可以发 UDP 请求报文，指示 CPE 进行 Inform 或者发送 SNMP TRAP。当然，可能由于 NAT 地址映射关系的老化，报文可能会被 NAT 阻挡。管理端可重试 3 次，若都没有收到 CPE 的响应，则认为 NAT 地址映射已经老化。可等待接收到 UDP 心跳时，通过响应发送 UDP 管理请求报文。

如图 3 所示，管理端发送 UDP 管理请求报文以及 CPE 响应的流程采用以下的步骤和技术环节：

步骤 301：管理端从（A3，P3）向（A1’，P1’）发送 UDP 管理请求报文。

步骤 302：当 CPE 从（A1，P1）收到报文后，发起 TR-069 的 Inform 或 SNMP TRAP，进入管理流程。

所述的步骤 301 中，(A1’，P1’)是 CPE 发送 UDP 心跳的地址（A1，P1）经过 NAT 转化后管理端收到报文的地址。

所述的步骤 301 中，当管理端发送 UDP 管理请求报文结束后，可能存在以下两种情况：

1)若超时未收到任何响应，则重发 3 次该报文。并且 3 次都没有收到响应

2)若收到来自 NAT 网关 WAN 侧地址的 ICMP 端口不可达报文

若出现上述两种情况，说明 NAT 地址条目已经老化，则管理端需要等待 CPE 发送 UDP 心跳，通过 UDP 的心跳响应报文发送管理请求。

所述的步骤 302 中，若 NAT 上的地址映射条目仍然存在，NAT 将会从（A1’，P1’）收到的报文转发给（A1，P1）。

本发明实施例的主要原理是：当 NAT 地址映射关系老化失效后，外部地址发来的请求报文将被 NAT 阻挡，此时内网地址的设备将无法收到相应的消息；CPE 上电后与管理端通信，管理端判断其是否在 NAT 的 LAN 侧，并打开 NAT 穿越开关；CPE 在打开 NAT 发现开关后可进行 NAT 的老化时间操作或不

进行任何操作；CPE 通过向管理端发送 NAT 老化时间发现报文，管理端收到报文后不断发送探测报文，直到 CPE 无法收到探测报文，向管理端发送 NAT 老化时间结束报文为止，以此时间段计算出 NAT 老化时间；管理端根据情况设置 CPE 的 UDP 心跳发送时间间隔；CPE 在管理端设置的发送时间间隔内发送 UDP 心跳，基于 NAT 一出一进、一出多进的原则，管理端收到 UDP 心跳后，回应给 CPE 的报文不会被 NAT 阻挡，CPE 收到报文之后可按照要求发起 TR-069 Inform 或者 SNMP Trap；当管理端需要立即管理 CPE 时，发送 UDP 管理请求报文给 CPE，若此时 NAT 地址映射关系未失效，CPE 收到请求后可立刻响应，若已经失效，管理端将无法收到 CPE 的响应或收到来自 NAT 网关的 ICMP（Internet 控制信息协议） 端口不可达报文，此时管理端需要在收到 CPE 的 UDP 心跳之后重新发送 UDP 管理请求。

本发明实施例方法在管理端穿越 NAT 管理 CPE 设备的过程中，管理端设置 CPE 参数、NAT 地址映射老化时间发现、发送 UDP 心跳、UDP 管理请求等操均采用强加密方式进行加密，并且对收到报文的源地址进行验证，保证通信的安全。

以上所述仅为本发明的较佳实施例，并非用来限定本发明的实施范围；凡是依本发明所作的等效变化与修改，都被本发明的专利范围所涵盖。

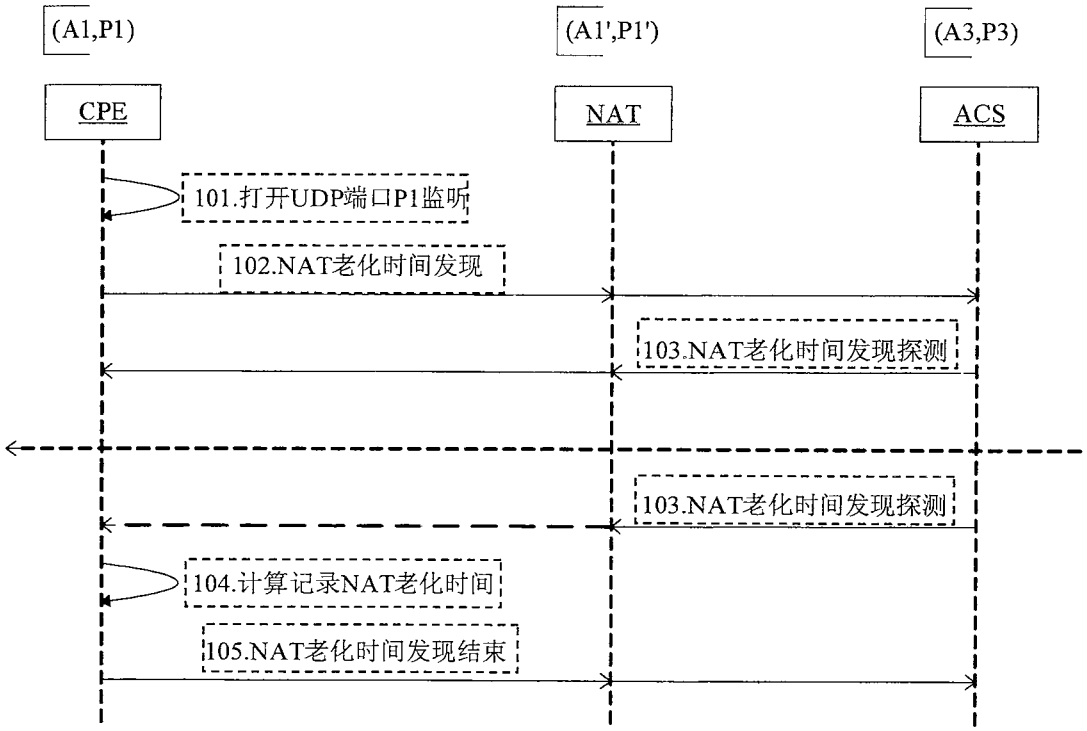

(A1,P1)
(A1',P1')
(A3,P3)
CPE
NAT
ACS
101.打开UDP端口P1监听
102.NAT老化时间发现
103.NAT老化时间发现探测
103.NAT老化时间发现探测
104.计算记录NAT老化时间
105.NAT老化时间发现结束

图 1


(A1,P1)
(A1',P1')
CPE
NAT
ACS
201.发送UDP心跳报文(DeviceId)
202.UDP管理请求
203.发起TR-069的Inform或者是SNMP TRAP
管理流程
结束管理流程
204.发送UDP心跳报文(DeviceId)

图 2

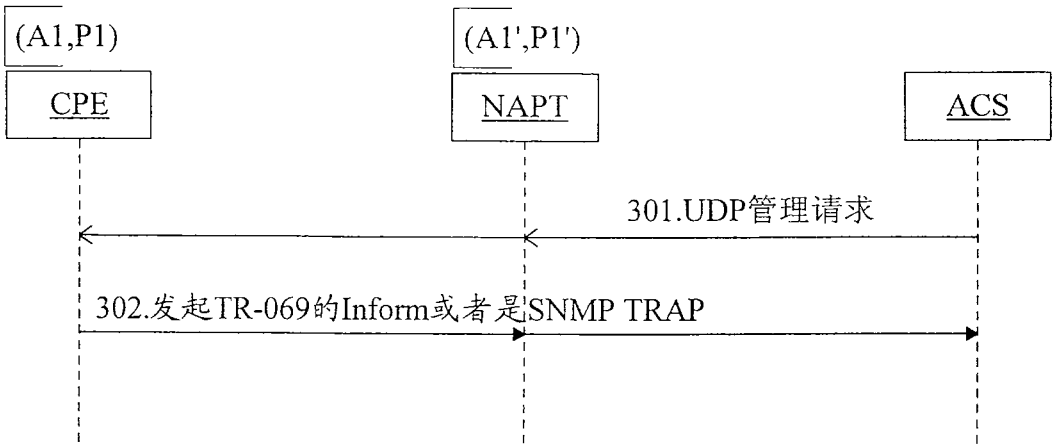

(A1,P1)
(A1',P1')
CPE
NAPT
ACS
301.UDP管理请求
302.发起TR-069的Inform或者是SNMP TRAP

图 3

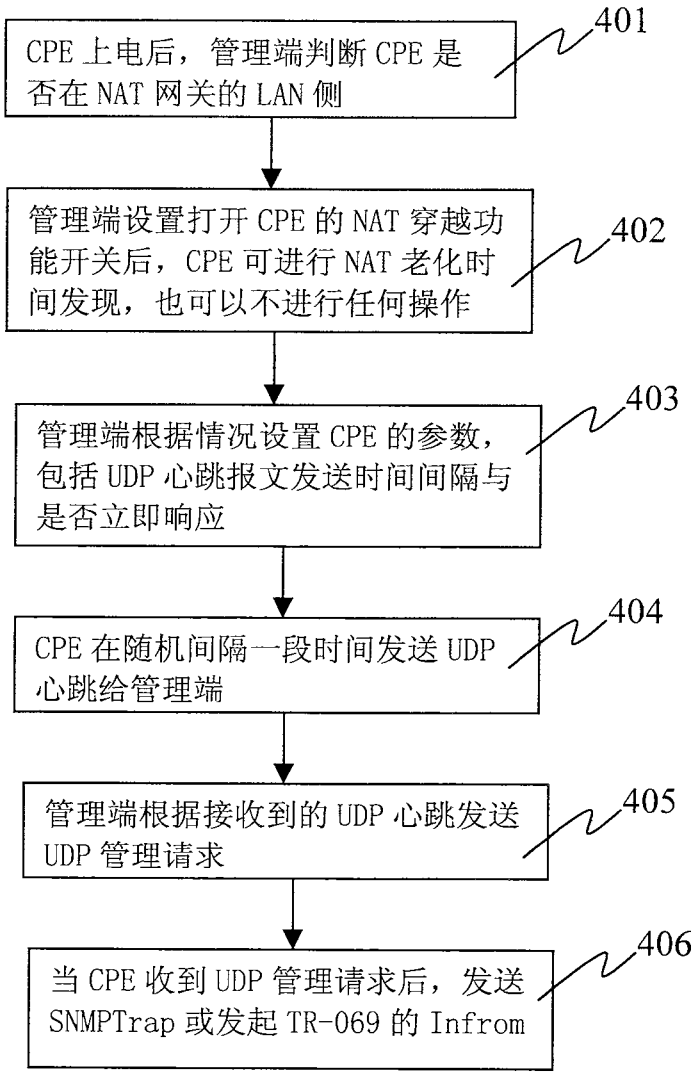

CPE 上电后，管理端判断 CPE 是否在 NAT 网关的 LAN 侧
401
管理端设置打开 CPE 的 NAT 穿越功能开关后，CPE 可进行 NAT 老化时间发现，也可以不进行任何操作
402
管理端根据情况设置 CPE 的参数，包括 UDP 心跳报文发送时间间隔与是否立即响应
403
CPE 在随机间隔一段时间发送 UDP 心跳给管理端
404
管理端根据接收到的 UDP 心跳发送 UDP 管理请求
405
当 CPE 收到 UDP 管理请求后，发送 SNMPTrap 或发起 TR-069 的 Infrom
406

图 4