(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104660728 A
(43)申请公布日 2015.05.27

(21)申请号 201510080442.6

(22)申请日 2015.02.13

(71)申请人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 徐晓灼 王志新

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中

(51)Int.Cl.
H04L 29/12(2006.01)

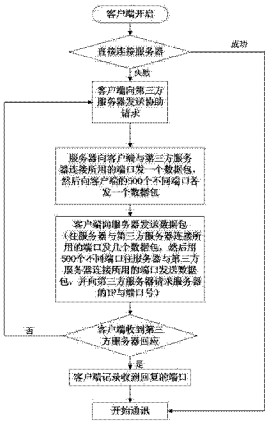
权利要求书1页 说明书3页 附图2页

(54)发明名称

基于智能家居控制系统的NAT穿透方法

(57)摘要

本发明提供了一种基于智能家居控制系统的NAT穿透方法，包括以下步骤：步骤一，客户端直接连接服务器；步骤二，客户端请求第三方服务器的协助；步骤三，服务器往客户端与第三方服务器连接所用的端口发一个数据包；步骤四，第三方服务器通知客户端；步骤五，服务器收到客户端的数据包后，如果客户端收到第三方服务器回应，第三方服务器将服务器的IP和端口号回复给客户端，客户端则可以记录下收到回复的端口，使用该端口与服务器通讯；如果客户端未收到第三方服务器回应，则认为信息丢失，客户端重新向第三方服务器发送协助请求，从步骤二开始重复进行。本发明穿透成功率高，穿透过程简单。



CN 104660728 A

1. 一种基于智能家居控制系统的 NAT 穿透方法，其特征在于，包括以下步骤：

步骤一，客户端直接连接服务器；若服务器的 IP 位于公网 IP 中，则直接连接成功，否则客户端连接失败，则需要继续进行步骤二，借助第三方服务器的协助；

步骤二，客户端请求第三方服务器的协助；

步骤三，服务器往客户端与第三方服务器连接所用的端口发一个数据包，然后往客户端的五百个不同端口发各发一个数据包；

步骤四，第三方服务器通知客户端，服务器已向客户端的五百个端口发完数据包，客户端确认收到信息后，向服务器与第三方服务器连接所用的端口发多个数据包；若服务器和客户端都在锥形 NAT 或者服务器在不限制端口的锥形 NAT 后，此时连接成功，然后用五百个不同端口往服务器与第三方服务器连接所用的端口发数据包，并向第三方服务器请求服务器的 IP 与端口号；

步骤五，服务器收到客户端的数据包后，如果客户端收到第三方服务器回应，第三方服务器将服务器的 IP 和端口号回复给客户端，客户端则记录下收到回复的端口，使用该端口与服务器通讯；如果客户端未收到第三方服务器回应，则认为信息丢失，客户端重新向第三方服务器发送协助请求，从步骤二开始重复进行。

2. 根据权利要求 1 所述的基于智能家居控制系统的 NAT 穿透方法，其特征在于，所述第三方服务器指的是一个有公网 IP 的用于协助双方进行 NAT 穿透的服务器，客户端须保证必要时连接第三方服务器的可靠性。

3. 根据权利要求 1 所述的基于智能家居控制系统的 NAT 穿透方法，其特征在于，所述客户端是手机客户端。

4. 根据权利要求 1 所述的基于智能家居控制系统的 NAT 穿透方法，其特征在于，所述第三方服务器在正常工作的条件下处于开启状态，时刻准备接收客户端与服务器信息；当第三方服务器接收到一条信息后，首先判断这条信息是否是客户端发送的协助请求，若是，则回复客户端已收到协助请求，并将客户端的 IP 地址和端口号发送给服务器；若判断此条信息不是协助请求，则需进一步判断此条信息是否为服务器发送数据包完成后的信息，若是，则回复服务器已收到该消息，并通知相应的客户端，服务器已向它的五百个端口发完数据包，客户端可以继续进行下一步操作；若不是，则最后判定该信息是否是客户端请求返回服务器 IP 和端口号的信息，若是，则向客户端发送服务器的 IP 和端口号，若不是，则判定此信息为无用信息，弃置并重新开始接收消息。

基于智能家居控制系统的 NAT 穿透方法

技术领域

[0001] 本发明涉及电气工程领域，具体地，涉及一种基于智能家居控制系统的 NAT 穿透方法。

背景技术

[0002] 网络地址转换技术(Network Address Translation，NAT)的基本功能是用一个或几个 IP 地址来实现一个内网中的所有主机和公网中主机的通信，使一个机构内的所有用户通过有限的数个（或一个）合法 IP 地址访问 Internet，不仅可以有效节省 Internet 中有效 IP 的数量，也可以提高网络通信的安全性。

[0003] 智能家居控制系统包括服务器、客户端、第三方服务器与硬件模块等。其中，客户端 APP 必须与用户的服务器进行网络通信才能对控制相关设备的运行。在服务器端有公网 IP 或者服务器端与客户端在同一局域网中时，可以顺利地利用网络进行通讯。但是如果服务器端没有公网 IP 并且与客户端不在同一个局域网中，那么服务器端是不能被客户端直接连接的。要在这种情况下实现通讯，就要实现有效的 NAT 穿透。然而，随着 IPv4 地址的枯竭，很多地方的网络运营商选择把大量用户介入到自己的内网中，再通过运营商级 NAT 让这些用户共享一个或多个公网 IP 进行上网，因此为了保证家中的智能家居控制系统能在大部分情况下正常工作，就必须解决 NAT 穿透问题。常规 NAT 穿透常常有穿透成功率低、穿透过程复杂的问题。

发明内容

[0004] 针对现有技术中的缺陷，本发明的目的是提供一种基于智能家居控制系统的 NAT 穿透方法，其穿透成功率高，穿透过程简单。

[0005] 根据本发明的一个方面，提供一种基于智能家居控制系统的 NAT 穿透方法，其特征在于，包括以下步骤：

[0006] 步骤一，客户端直接连接服务器；若服务器的 IP 位于公网 IP 中，则直接连接成功，否则客户端连接失败，则需要继续进行步骤二，借助第三方服务器的协助；

[0007] 步骤二，客户端请求第三方服务器的协助；

[0008] 步骤三，服务器往客户端与第三方服务器连接所用的端口发一个数据包，然后往客户端的五百个不同端口发各发一个数据包；

[0009] 步骤四，第三方服务器通知客户端，服务器已向客户端的五百个端口发完数据包，客户端确认收到信息后，向服务器与第三方服务器连接所用的端口发多个数据包；若服务器和客户端都在锥形 NAT 或者服务器在不限制端口的锥形 NAT 后，此时连接成功，然后用五百个不同端口往服务器与第三方服务器连接所用的端口发数据包，并向第三方服务器请求服务器的 IP 与端口号；

[0010] 步骤五，服务器收到客户端的数据包后，如果客户端收到第三方服务器回应，第三方服务器将服务器的 IP 和端口号回复给客户端，客户端则记录下收到回复的端口，使用该

端口与服务器通讯；如果客户端未收到第三方服务器回应，则认为信息丢失，客户端重新向第三方服务器发送协助请求，从步骤二开始重复进行。

[0011] 优选地，所述第三方服务器指的是一个有公网 IP 的用于协助双方进行 NAT 穿透的服务器，客户端须保证必要时连接第三方服务器的可靠性。

[0012] 优选地，所述第三方服务器在正常工作的条件下处于开启状态，时刻准备接收客户端与服务器信息；当第三方服务器接收到一条信息后，首先判断这条信息是否是客户端发送的协助请求，若是，则回复客户端已收到协助请求，并将客户端的 IP 地址和端口号发送给服务器；若判断此条信息不是协助请求，则需进一步判断此条信息是否为服务器发送数据包完成后的信息，若是，则回复服务器已收到该消息，并通知相应的客户端，服务器已向它的五百个端口发完数据包，客户端可以继续进行下一步操作；若不是，则最后判定该信息是否是客户端请求返回服务器 IP 和端口号的信息，若是，则向客户端发送服务器的 IP 和端口号，若不是，则判定此信息为无用信息，弃置并重新开始接收消息。

[0013] 与现有技术相比，本发明具有如下的有益效果：

[0014] 一，穿透成功率高。经计算，对于服务器端在端口限制锥形 NAT，客户端在对称型 NAT 后的情况能达到 97.8％的理论穿透成功率。对于更为容易穿透的情况，服务器和客户端均处在锥形 NAT 后，或服务器端处在不限制端口的锥形 NAT 后，穿透成功率可以达到 100％。

[0015] 二，穿透时间短，效率高。客户端与服务器端工作正常、网络条件良好的的情况下，NAT 穿透在几十至几百毫秒内即可完成。

[0016] 三，在最常见的客户端和服务器端均处在同一公网 IP 的情况下，不需要借助第三方服务器的协助，穿透过程快速、直接、简单且有效，数据传输稳定且基本无延时。

附图说明

[0017] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0018] 图 1 为本发明基于智能家居控制系统的 NAT 穿透方法的流程图。

[0019] 图 2 为是第三方服务器的运行流程图。

具体实施方式

[0020] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进。这些都属于本发明的保护范围。

[0021] 如图 1 所示，本发明基于智能家居控制系统的 NAT 穿透方法包括以下步骤：

[0022] 步骤一，客户端（比如手机客户端）开启后，直接连接服务器，判断是否需要进行 NAT 穿透。具体来说，若服务器的 IP 位于公网 IP 中，则可以直接连接成功，通过公网进行网络通讯，并不需要 NAT 穿透，否则客户端连接失败，则需要继续进行步骤二，借助第三方服务器的协助。

[0023] 步骤二，客户端请求第三方服务器的协助。这里的“第三方服务器”指的是一个有

公网 IP 的用于协助双方进行 NAT 穿透的服务器，客户端须保证必要时连接第三方服务器的可靠性。这里，客户端向第三方服务器发送消息，第三方服务器接收消息后，对客户端进行回应，告知客户端协助信息已收到，并将客户端的 IP 地址和端口号发送给服务器，以便服务器发送数据包。

[0024] 步骤三，服务器往客户端与第三方服务器连接所用的端口发一个数据包，然后往客户端的五百个不同端口发各发一个数据包。这样做的目的是为了在服务器的 NAT 上打洞，它并不需要被客户端收到，所以对每个端口各发一个数据包即可。发送结束后通知第三方服务器发送过程已完成。

[0025] 步骤四，第三方服务器通知客户端，服务器已向客户端的五百个端口发完数据包，客户端确认收到信息后，向服务器与第三方服务器连接所用的端口发多个数据包；若服务器和客户端都在锥形 NAT 或者服务器在不限制端口的锥形 NAT 后，此时连接成功，然后客户端用五百个不同端口向服务器与第三方服务器连接所用的端口发数据包，并向第三方服务器请求服务器的 IP 与端口号。这是穿透成功最重要的一步，之所以要发几个数据包而不是一个是因为要尽量减少丢包带来的影响。

[0026] 步骤五，服务器收到客户端的数据包后，如果客户端收到第三方服务器回应，第三方服务器将服务器的 IP 和端口号回复给客户端，客户端则可以记录下收到回复的端口，使用该端口与服务器通讯；如果客户端在一定时间内未收到第三方服务器回应，则可以认为信息丢失，客户端重新向第三方服务器发送协助请求，从步骤二开始重复进行。

[0027] 第三方服务器运行流程图如图 2 所示。第三方服务器在整个系统的运行过程中非常重要，但其逻辑较为简单，只要根据收到的请求进行相应的动作即可，它不需要考虑 NAT 穿透的进度，而 NAT 穿透步骤的正确性则主要由客户端保证。在正常工作的条件下，第三方服务器处于开启状态，时刻准备接收客户端与服务器信息；当第三方服务器接收到一条信息后，首先判断这条信息是否是客户端发送的协助请求（当客户端在步骤一中直接连接服务器失败后，向第三方服务器发送协助请求），若是，则回复客户端已收到协助请求，并将客户端的 IP 地址和端口号发送给服务器；若判断此条信息不是协助请求，则需进一步判断此条信息是否为服务器发送数据包完成后的信息（步骤三中服务器向客户端的五百个不同端口发各发一个数据包），若是，则回复服务器已收到该消息，并通知相应的客户端，服务器已向它的五百个端口发完数据包，客户端可以继续进行下一步操作；若不是，则最后判定该信息是否是客户端请求返回服务器 IP 和端口号的信息（步骤四中客户端向第三方服务器请求服务器的 IP 与端口号），若是，则向客户端发送服务器的 IP 和端口号（步骤五中第三方服务器将服务器的 IP 和端口号回复给客户端），若不是，则判定此信息为无用信息，弃置并重新开始接收消息。

[0028] 以上对本发明的具体实施例进行了描述。需要理解的是，本发明并不局限于上述特定实施方式，本领域技术人员可以在权利要求的范围内做出各种变形或修改，这并不影响本发明的实质内容。

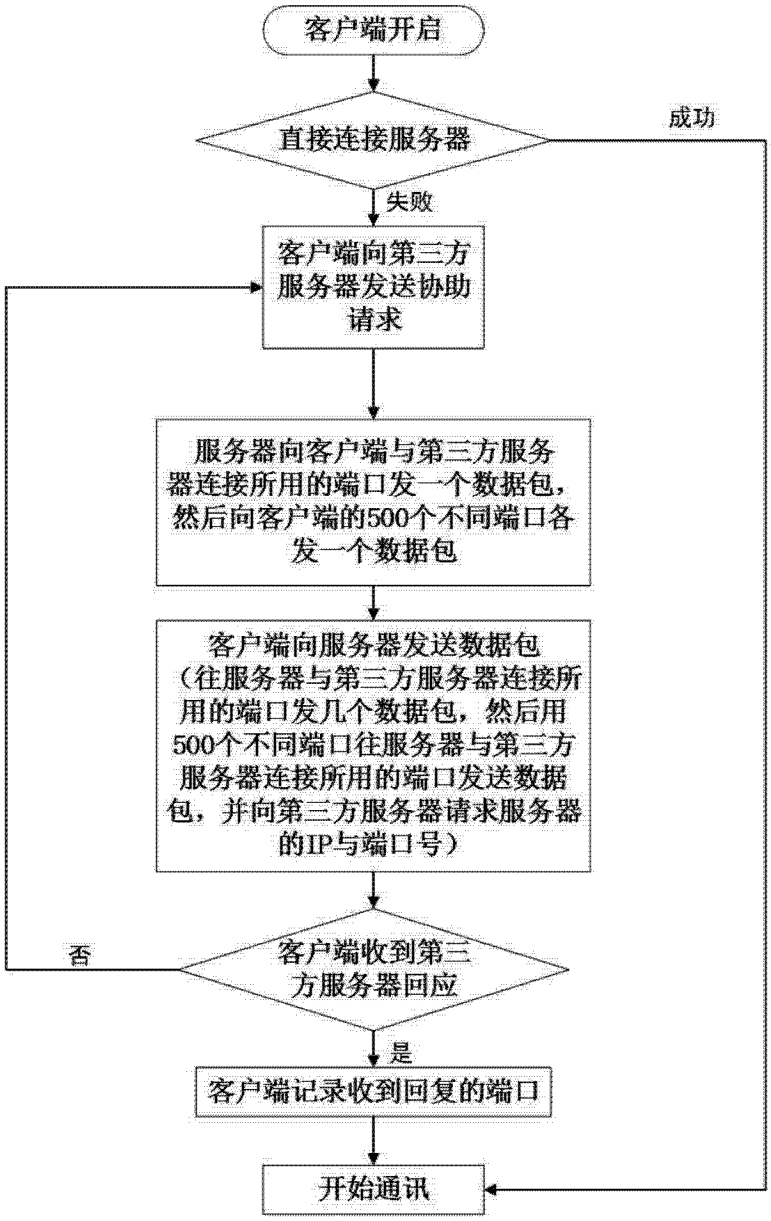

客户端开启
直接连接服务器
成功
失败
客户端向第三方服务器发送协助请求
服务器向客户端与第三方服务器连接所用的端口发一个数据包，然后向客户端的500个不同端口各发一个数据包
客户端向服务器发送数据包（往服务器与第三方服务器连接所用的端口发几个数据包，然后用500个不同端口往服务器与第三方服务器连接所用的端口发送数据包，并向第三方服务器请求服务器的IP与端口号）
客户端收到第三方服务器回应
否
是
客户端记录收到回复的端口
开始通讯

图 1

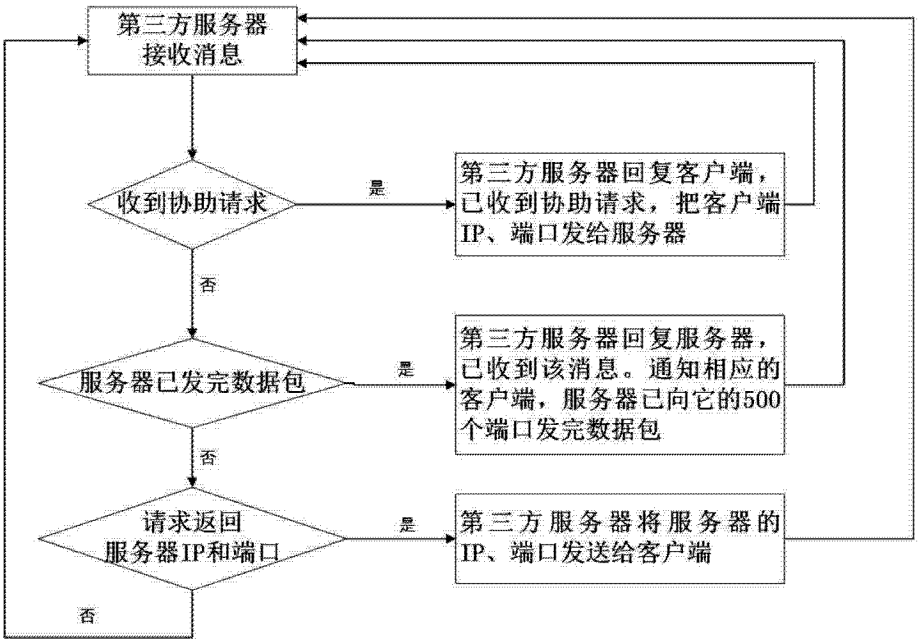

第三方服务器
接收消息
收到协助请求
是
第三方服务器回复客户端，已收到协助请求，把客户端IP、端口发给服务器
否
服务器已发完数据包
是
第三方服务器回复服务器，已收到该消息。通知相应的客户端，服务器已向它的500个端口发完数据包
否
请求返回
服务器IP和端口
是
第三方服务器将服务器的IP、端口发送给客户端
否

图 2