(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 112073244 A
(43)申请公布日 2020.12.11

(21)申请号 202010943021.2

(22)申请日 2020.09.09

(71)申请人 上海诺行信息技术有限公司
地址 201203 上海市浦东新区张衡路666弄2号407-409室

(72)发明人 李佳谋

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/08(2006.01)

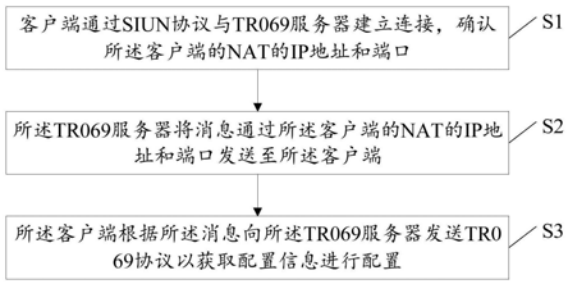
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于TR069协议的消息处理方法及系统

(57)摘要

本发明公开了基于TR069协议的消息处理方法及系统，属于通信技术领域。本发明的客户端通过SIUN协议与TR069服务器建立连接，确认客户端的NAT的IP地址和端口，TR069服务器将消息通过客户端的NAT的IP地址和端口发送至客户端，客户端根据消息向TR069服务器发送TR069协议以获取配置信息进行配置。本发明实现了在不增加系统负担(处理能力及耗电量)的前提下，可通过互联网直接实时操控、管理多个客户端，不受局域网的限制、降低系统，可适用于移动设备，提供了用户的体验效果。



CN 112073244 A

1.一种基于TR069协议的消息处理方法,其特征在于,包括下述步骤:

客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口;

所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端;

所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

2.根据权利要求1所述的基于TR069协议的消息处理方法,其特征在于,所述客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口,包括:

所述客户端通过所述SIUN协议与所述TR069服务器建立连接,获取所述客户端的IP地址和端口;

所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069服务器;

所述TR069服务器根据所述客户端的IP地址和端口,生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

3.根据权利要求1所述的基于TR069协议的消息处理方法,其特征在于,所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端,包括:

所述TR069服务器将消息添置至消息队列;

通过所述SIUN协议对所述消息队列进行检测;

当检测到带有所述客户端的NAT的IP地址和端口的消息时,将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

4.根据权利要求1所述的基于TR069协议的消息处理方法,其特征在于,所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置,包括:

所述客户端对接收到的所述消息进行验证;

若验证通过,则所述客户端向所述TR069服务器发送TR069协议;

所述TR069服务器根据所述TR069协议向所述客户端发送配置信息;

所述客户端根据所述配置信息进行配置。

5.一种基于TR069协议的消息处理系统,其特征在于,包括:

客户端,用于通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口;

所述TR069服务器,用于将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端;

所述客户端还用于根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

6.根据权利要求5所述的基于TR069协议的消息处理系统,其特征在于,所述客户端用于通过所述SIUN协议与所述TR069服务器建立连接,获取所述客户端的IP地址和端口;所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069服务器;所述TR069服务器根据所述客户端的IP地址和端口,生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

7.根据权利要求5所述的基于TR069协议的消息处理系统,其特征在于,所述TR069服务

器用于将消息添置至消息队列,通过所述SIUN协议对所述消息队列进行检测;当检测到带有所述客户端的NAT的IP地址和端口的消息时,将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

8.根据权利要求5所述的基于TR069协议的消息处理系统,其特征在于,所述客户端还用于对接收到的所述消息进行验证;若验证通过,则所述客户端向所述TR069服务器发送TR069协议以获取配置信息进行配置。

基于TR069协议的消息处理方法及系统

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种基于TR069协议的消息处理方法及系统。

背景技术

[0002] TR069是由DSL论坛(www.dslforum.org)所开发的技术规范之一，其全称为“CPE(客户终端设备)广域网管理协议”。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

[0003] TR069的出现正是为了解决这样一个服务难题，在TR069所定义的框架中，主要包括两类逻辑设备：受管理的用户设备和管理服务器(ACS)。在家庭网络环境下，需要从网络侧进行配置和管理的设备，一般都是与运营商业务直接相关的设备，比如家庭网关、机顶盒、IP电话终端等。而所有与用户设备相关的配置、诊断、升级等工作均由统一的管理服务器ACS来完成。

[0004] 现有的网络类型主要包括：完全圆锥型NAT(Full Cone NAT)、地址限制圆锥型NAT(Address Restricted Cone NAT)、端口限制圆锥型NAT(Port Restricted Cone NAT)和对称型NAT(Symmetric NAT)。

[0005] 完全圆锥型NAT，将从一个内部IP地址和端口来的所有请求，都映射到相同的外部IP地址和端口。并且，任何外部主机通过向映射的外部地址发送报文，都可以实现和内部主机进行通信。这是一种比较宽松的策略，只要建立了内部网络的IP地址和端口与公网IP地址和端口的映射关系，所有的Internet上的主机都可以访问该NAT之后的主机。如图1所示，完全圆锥型NAT会将客户机地址{X:y}转换成公共地址{A:b}并绑定，任何外部主机(如：M、P、S)包都可以通过地址{A:b}送到客户主机{X:y}地址上。

[0006] 地址限制圆锥型NAT也是将从相同的内部IP地址和端口来的所有请求映射到相同的公网IP地址和端口。但是与完全圆锥型NAT不同，当且仅当内部主机之前已经向公网主机发送过报文，此时公网主机才能向内网主机发送报文。如图2所示，地址限制圆锥型NAT会将客户机地址{X:y}转换成公共地址{A:b}并绑定，只有来自主机{P}的包才能和主机{X:y}通信。其中主机主机{P}的地址可以是{P:q}、{P:r}。

[0007] 端口限制圆锥型NAT类似于地址限制圆锥型NAT，但是更严格。端口受限圆锥型NAT增加了端口号的限制，当前仅当内网主机之前已经向公网主机发送了报文，公网主机才能和此内网主机通信。如图3所示，端口限制圆锥型NAT会将客户机地址{X:y}转换成公共地址{A:b}并绑定，只有来自主机{P,q}的包才能和主机{X:y}通信。主机{M,n}、{P:r}、{S}的包均不能与主机{X:y}通信。

[0008] 对称型NAT把从同一内网地址和端口到相同目的地址和端口的所有请求，都映射到同一个公网地址和端口。如果同一个内网主机，用相同的内网地址和端口向另外一个目的地址发送报文，则会用不同的映射。这和端口限制型NAT不同，端口限制型NAT是所有请求映射到相同的公网IP地址和端口，而对称型NAT是不同的请求有不同的映射。如图4所示，对

称型NAT会将客户机地址{X:y}转换成公共地址{A:b}并绑定为{X:y}|{A:b}<->{P,q},对称型NAT只接受来自{P,q}的incoming packet(进入包)将其转给{X:y},每次客户机请求一个不同的公网地址和端口,对称型NAT会重新分配一个端口号{C:d},主机{P:r}、{S}的包均不能与主机{X:y}通信。

[0009] 目前采用TR069协议开发,只要设备符合规范,即可连接进入系统,统一配置,下发给设备端。然而,现有的TR069协议只能基于LAN(全称Local Area Network,局域网)工作,如果设备和管理系统不处在一个LAN内,管理系统端无法主动连接到设备,导致不能立即下发配置的操作。

[0010] 根据上述内容可知,若公司要想管理自己的网关设备,就得拥有一个内网环境,部署一个自己的TR069管理系统,目前很多公司也确实是这里来使用的。但是,如果有公司希望能在因特网上方便的管理自己的设备,就会因为TR069协议本身的限制,而难以实现。

[0011] 在因特网环境下,除了实时发送管理配置,还有很多公司会利用轮询机制才实现快速的管理设备,该机制即设备端不停的向TR069管理系统服务器发送http请求,一旦发现TR069系统上有待配置的任务,立即下发到这个设备执行,这样做有两个缺陷:一、设备不可能非常实时发送,一般会间隔10s,30s,一分钟等等发送一次请求到管理系统;二、不间断的发送请求,浪费网络资源,同时耗电。

[0012] 网络设备,例如MIFI(全称Mobile WIFI,移动路由)自身需带电池工作的设备,电量消耗过快,对用户来说,是一个非常难容忍的事情,同时由于基于LTE(全称Long Term Evolution,长期演进技术)网络,每天网络无缘无故的浪费,也使用户有了不愉快的体验。

[0013] 综上所述,现有方案虽然也能实现CPE等设备控制,但是却有诸多限制,主要问题有:

[0014] (1)只有内网部署,才能做到实时管理设备,限定了服务的使用范围,也不利于大数据整合;

[0015] (2)使用http轮询请求服务器,无法做到真正的实时,还费电,对移动设备不适用。;

[0016] (3)如果使用http长连接,服务器会挂载非常多的连接,服务器压力大,需要大批量的硬件设备支持,耗资源。

发明内容

[0017] 针对上述问题,现提供一种旨在实现可通过互联网直接管理多个客户端设备,实时操控的基于TR069协议的消息处理方法及系统。

[0018] 一种基于TR069协议的消息处理方法,包括下述步骤:

[0019] 客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口;

[0020] 所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端;

[0021] 所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0022] 优选的,所述客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的

NAT的IP地址和端口，包括：

[0023] 所述客户端通过所述SIUN协议与所述TR069服务器建立连接，获取所述客户端的IP地址和端口；

[0024] 所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069服务器；

[0025] 所述TR069服务器根据所述客户端的IP地址和端口，生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

[0026] 优选的，所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端，包括：

[0027] 所述TR069服务器将消息添置至消息队列；

[0028] 通过所述SIUN协议对所述消息队列进行检测；

[0029] 当检测到带有所述客户端的NAT的IP地址和端口的消息时，将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

[0030] 优选的，所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置，包括：

[0031] 所述客户端对接收到的所述消息进行验证；

[0032] 若验证通过，则所述客户端向所述TR069服务器发送TR069协议；

[0033] 所述TR069服务器根据所述TR069协议向所述客户端发送配置信息；

[0034] 所述客户端根据所述配置信息进行配置。

[0035] 本发明还提供了一种基于TR069协议的消息处理系统，包括：

[0036] 客户端，用于通过SIUN协议与TR069服务器建立连接，确认所述客户端的NAT的IP地址和端口；

[0037] 所述TR069服务器，用于将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端；

[0038] 所述客户端还用于根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0039] 优选的，所述客户端用于通过所述SIUN协议与所述TR069服务器建立连接，获取所述客户端的IP地址和端口；所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069服务器；所述TR069服务器根据所述客户端的IP地址和端口，生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

[0040] 优选的，所述TR069服务器用于将消息添置至消息队列，通过所述SIUN协议对所述消息队列进行检测；当检测到带有所述客户端的NAT的IP地址和端口的消息时，将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

[0041] 优选的，所述客户端还用于对接收到的所述消息进行验证；若验证通过，则所述客户端向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0042] 上述技术方案的有益效果：

[0043] 本技术方案中，客户端通过SIUN协议与TR069服务器建立连接，确认客户端的NAT的IP地址和端口，TR069服务器将消息通过客户端的NAT的IP地址和端口发送至客户端，客户端根据消息向TR069服务器发送TR069协议以获取配置信息进行配置。本发明实现了在不

增加系统负担(处理能力及耗电量)的前提下,可通过互联网直接实时操控、管理多个客户端,不受局域网的限制、降低系统,可适用于移动设备,提供了用户的体验效果。

附图说明

[0044] 图1为现有的完全圆锥型NAT的原理示意图;

[0045] 图2为现有的地址限制圆锥型NAT的原理示意图;

[0046] 图3为现有的端口限制圆锥型NAT的原理示意图;

[0047] 图4为现有的对称型NAT的原理示意图;

[0048] 图5为本发明所述的基于TR069协议的消息处理方法的一种实施例的方法流程图;

[0049] 图6为本发明所述的基于TR069协议的消息处理系统的一种实施例的原理图。

具体实施方式

[0050] 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作出创造性劳动的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。

[0051] 需要说明的是,在不冲突的情况下,本发明中的实施例及实施例中的特征可以相互组合。

[0052] 下面结合附图和具体实施例对本发明作进一步说明,但不作为本发明的限定。

[0053] 如图5所示,本发明提供了一种基于TR069协议的消息处理方法,包括下述步骤:

[0054] S1.客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口;

[0055] S2.所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端;

[0056] S3.所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0057] 需要说明的是,TR069是基于http1.1协议实现的。在TR069服务器上融合了SIUN服务,由于http协议是无状态的,并且无法实现在网络锥形中的穿透,使用了UDP协议(全称User Datagram Protocol,中文名是用户数据报协议),专门负责网络穿透机制。

[0058] 在本实施例中,客户端通过SIUN协议与TR069服务器建立连接,确认客户端的NAT的IP地址和端口,TR069服务器将消息通过客户端的NAT的IP地址和端口发送至客户端,客户端根据消息向TR069服务器发送TR069协议以获取配置信息进行配置。本发明实现了在不增加系统负担(处理能力及耗电量)的前提下,可通过互联网直接实时操控、管理多个客户端,不受局域网的限制、降低系统,可适用于移动设备,提供了用户的体验效果。

[0059] 在优选的实施例中,步骤S1所述客户端通过SIUN协议与TR069服务器建立连接,确认所述客户端的NAT的IP地址和端口,包括:

[0060] 所述客户端通过所述SIUN协议与所述TR069服务器建立连接,获取所述客户端的IP地址和端口;

[0061] 所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069

服务器；

[0062] 所述TR069服务器根据所述客户端的IP地址和端口，生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

[0063] 在优选的实施例中，步骤S2所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端，包括：

[0064] 所述TR069服务器将消息添置至消息队列；

[0065] 通过所述SIUN协议对所述消息队列进行检测；

[0066] 当检测到带有所述客户端的NAT的IP地址和端口的消息时，将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

[0067] 在优选的实施例中，步骤S3所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置，包括：

[0068] 所述客户端对接收到的所述消息进行验证；

[0069] 若验证通过，则所述客户端向所述TR069服务器发送TR069协议；

[0070] 所述TR069服务器根据所述TR069协议向所述客户端发送配置信息；

[0071] 所述客户端根据所述配置信息进行配置。

[0072] 如图6所示，本发明还提供了一种基于TR069协议的消息处理系统，包括：

[0073] 客户端，用于通过SIUN协议与TR069服务器建立连接，确认所述客户端的NAT的IP地址和端口；

[0074] 进一步地，所述客户端用于通过所述SIUN协议与所述TR069服务器建立连接，获取所述客户端的IP地址和端口；所述客户端通过所述TR069协议将所述客户端的IP地址和端口发送至所述TR069服务器；所述TR069服务器根据所述客户端的IP地址和端口，生成所述客户端的IP地址和端口与所述客户端的NAT的IP地址和端口之间的映射关系。

[0075] 所述TR069服务器，用于将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端；

[0076] 进一步地，所述TR069服务器用于将消息添置至消息队列，通过所述SIUN协议对所述消息队列进行检测；当检测到带有所述客户端的NAT的IP地址和端口的消息时，将所述消息根据所述客户端的NAT的IP地址和端口的映射关系发送至所述客户端。

[0077] 所述客户端还用于根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0078] 进一步地，所述客户端用于对接收到的所述消息进行验证；若验证通过，则所述客户端向所述TR069服务器发送TR069协议以获取配置信息进行配置。

[0079] 在本实施例中，客户端在连接TR069服务器之前，首先使用SIUN协议与TR069服务器连接，SIUN协议本身需要和TR069服务器之间来回请求好几次，以确认设备端的最外层NAT的IP地址和端口，有了这个IP和端口，TR069服务器在有配置下发时，首先使用UDP发送消息到这里，这个最外层NAT的IP和端口和CPE设备的IP，端口会有一个映射关系，当消息传达到最外层NAT的IP和端口，经过NAT匹配，路由到确定的设备，这样设备就收到了服务端下发的请求。具体过程如下：

[0080] 客户端连接TR069服务器的STUN服务，获取客户端的IP和端口；

[0081] 客户端利用TR069协议，将获取到的IP和端口发送给TR069服务器；

[0082] 操作人员利用TR069管理界面服务,配置参数;

[0083] 配置的参数通过TR069平台发送到队列;

[0084] TR069 STUN从监听的队列中获取到带有IP和端口的消息,利用UDP消息发送到客户端;

[0085] 客户端接收到消息后进行验证;

[0086] 通过验证后,客户端立即发送TR069协议,去获取管理员的配置。

[0087] 本发明基于TR069标准协议,具备穿透功能的服务器来管理客户端,获取基本数据,同时也可以将这部分数据提供给第三方,进行数据挖掘,处理。

[0088] 本发明采用SIUN(全称Simple Traversal of UDP over NATs,NAT的UDP简单穿越,中文名网络协议)穿透,将SIUN穿透技术和TR069协议完美结合,使用户设备和管理服务器不管是在同一个内网,还是因特网上面,都可以实时管控,满足设备管理者的需求,同时也解决了设备使用者的顾虑。

[0089] 以上所述仅为本发明较佳的实施例,并非因此限制本发明的实施方式及保护范围,对于本领域技术人员而言,应当能够意识到凡运用本发明说明书及图示内容所作出的等同替换和显而易见的变化所得到的方案,均应当包含在本发明的保护范围内。

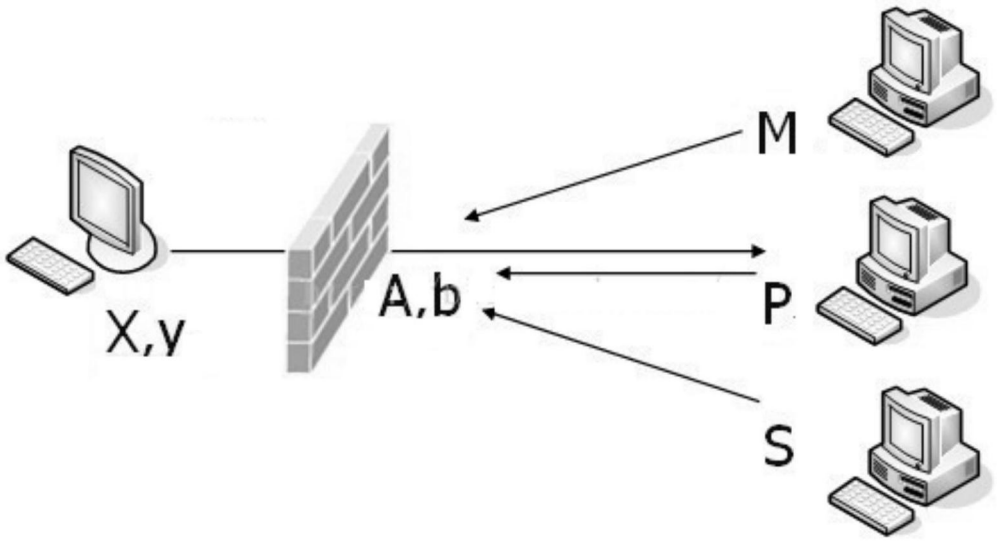


图1

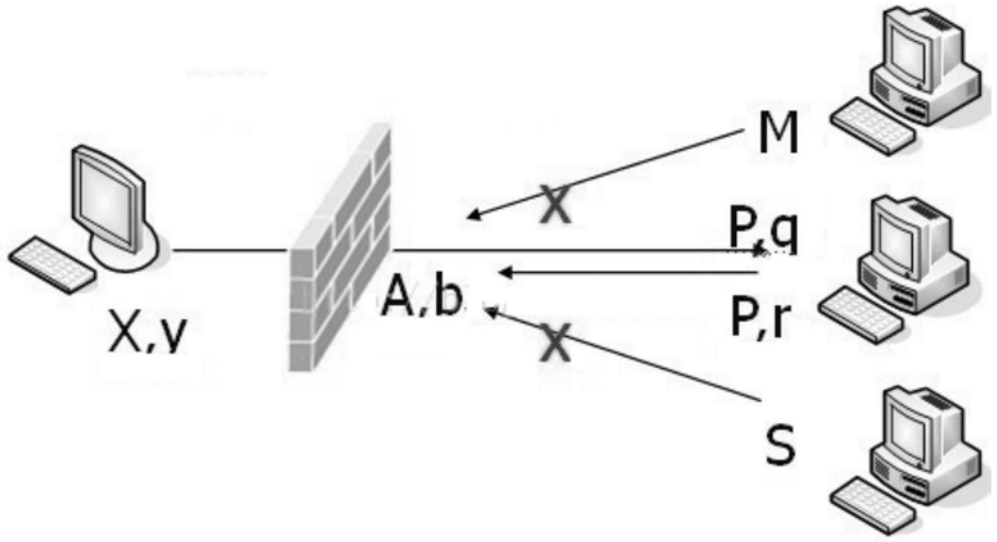


图2

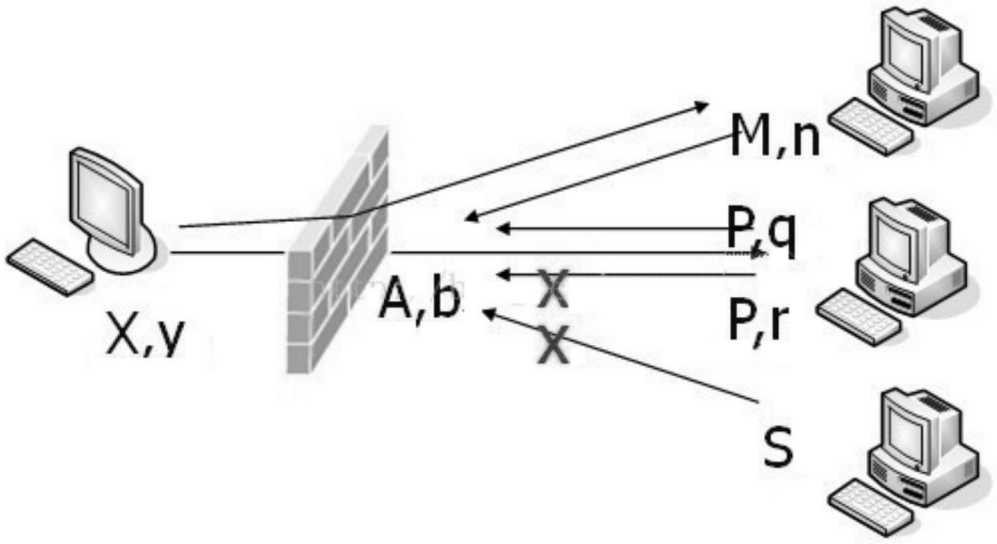


图3

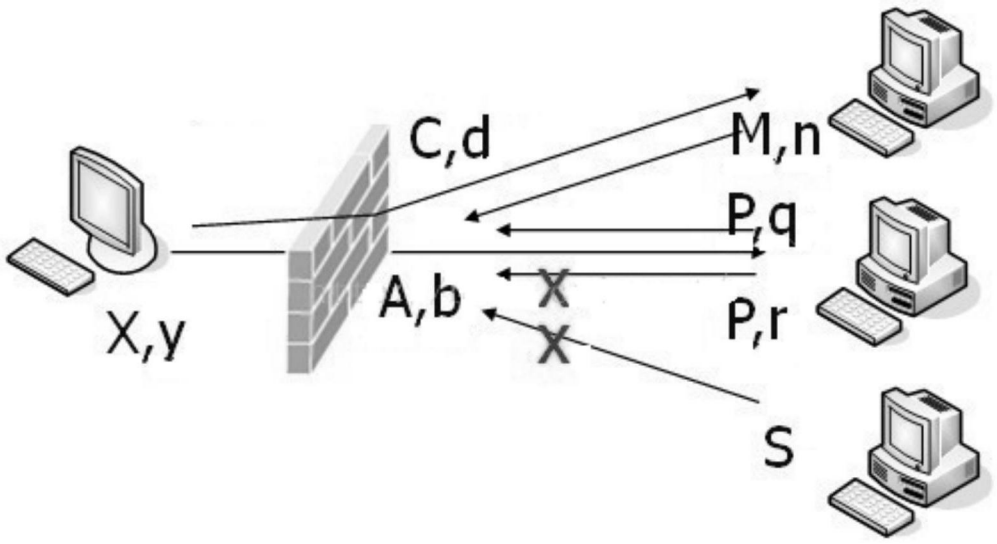


图4

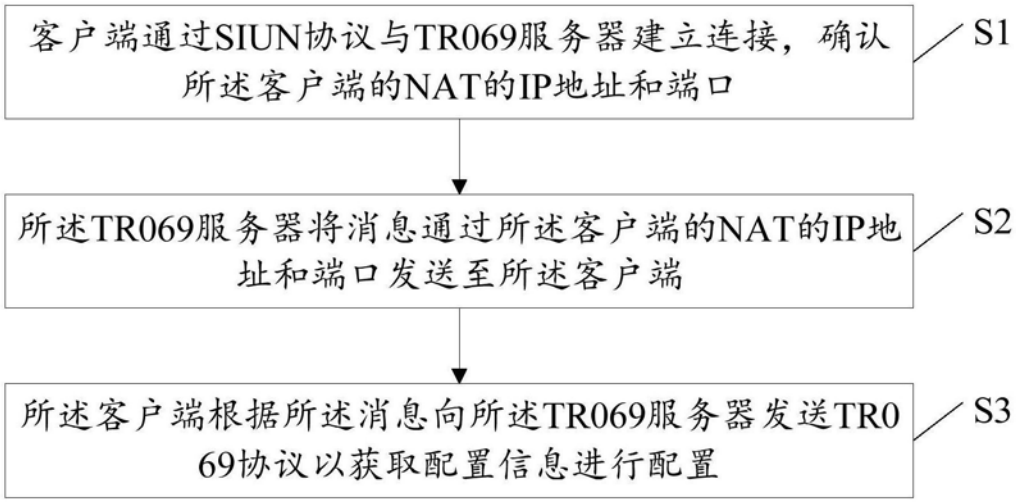

客户端通过SIUN协议与TR069服务器建立连接，确认所述客户端的NAT的IP地址和端口
S1
所述TR069服务器将消息通过所述客户端的NAT的IP地址和端口发送至所述客户端
S2
所述客户端根据所述消息向所述TR069服务器发送TR069协议以获取配置信息进行配置
S3

图5

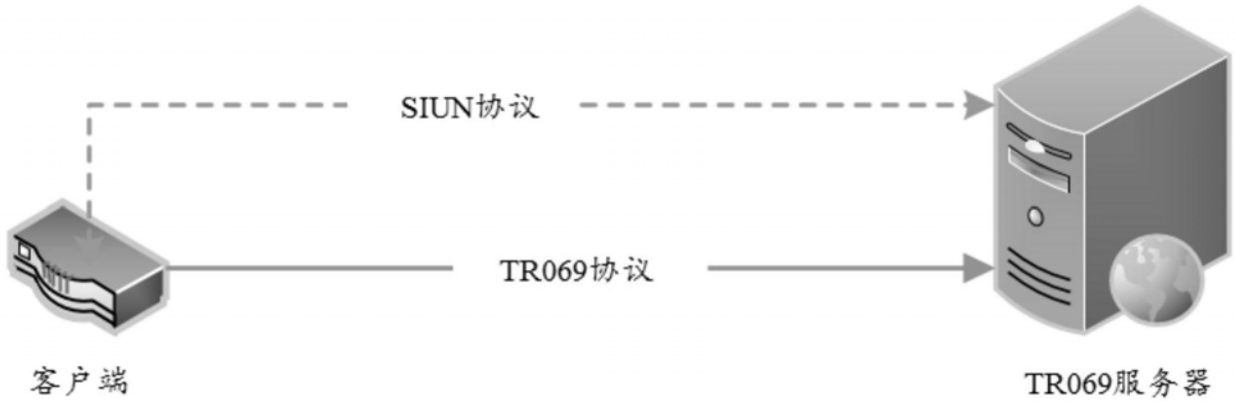

SIUN协议
TR069协议
客户端
TR069服务器

图6