无线 VOIP 网络中 SIP 穿越 NAT 的设计与实现①

Design and Implementation of SIP Through NAT in Wireless VOIP Network

龙寿阳　陈名松　陈　锋　(桂林电子科技大学 信息与通信学院 广西 桂林 541004)

摘　要： SIP 是 IETF 提出的 IP 电话信令协议，作为 NGN 重要协议之一，广泛应用于数据、语音、视频等多媒体通信业务中。但网络中大量 NAT 的 存在加上 SIP 本身不支持信令和媒体流的穿越，限制了其在广域网上的应用和发展。对目前主要的 NAT 穿越方案进行了详细的阐述和比较之后，设计并实现了一种基于 STUN 协议的 NAT 穿越方案。该方案目前已成功应用于基于 PDA 的无线 VOIP 网络中，并可推广到其它基于 SIP 协议的终端上，为 VOIP 业务的推广应用扫清了障碍。

关键词： 下一代网络 会话发起协议 网络地址穿越 简单 UDP 穿越 NAT 个人数字助理

1　引言

随着近年网络和通信技术的不断发展， SIP[1]在 VOIP 和视频会议业务中得到了越来越广泛的应用，而且随着宽带网络的普及，将拥有更加广阔的市场前景。但是也带来一个值得关注的问题：为了解决网络安全问题和 IPV4 地址资源匮乏问题，大量企业和网络采用了 NAT。而基于 SIP 的 VOIP 技术却无法顺利通过它们。本文将在对各种解决方案的基本原理和性能进行分析和比较之后，结合实际情况，采用了基于 STUN[2] 的 NAT 穿越方案，实现对 SIP 信令的穿越，而媒体流的穿越则通过对所有可用媒体地址进行连接检查来实现，在一个实际项目中成功实现了 NAT 的穿越。

2　相关背景知识

2.1 SIP 简介

SIP(Session Initiation Protocol，会话发起协议)是由 IETF(Interne 工程任务组)提出的 IP 电话信令协议。它的主要目的是为了解决 IP 网中的信令控制，以及同软交换 Soft Switch 的通信，从而构成下一代的增值业务平台，对电信，银行，金融等行业提供更好的增值业务。它用于发起会话，它能控制多个参与者参加的多媒体会话的建立和终结，并能动态调整和修改会话属性，如会话带宽要求、传输的媒体类型(语音、视频和数据等)、媒体的编解码格式、对组播和单播的支持等[3]。

2.2 NAT 概述

NAT(Network Address Translate，网络地址转换)是私网 IP 地址和公网 IP 地址相互转换的一种技术，这样就使得私网用户可以访问公网资源。NAT 的实现主要有四种：full cone，restricted cone，port restricted cone和 symmetric cone其中前面三种内部 IP 都会映射到同一公网 IP 上面，不同的只是 NAT 是不是需要激活或者有没有端口的限制；第四种会根据目地地址的不同而映射到不同的公网 IP 地址。

2.3 SIP 无法穿越 NAT 的原因分析[4]

SIP 建立会话有 2 个过程，分别是 SIP 信令的连接和 RTP 媒体流的建立，因此，SIP 穿越 NAT 的问题实质上是 SIP 信令以及媒体流穿越 NAT 网关的问题。

首先 SIP 信令无法穿越 NAT 是因为当 SIP 终端在向 SIP 服务器发起注册时，其注册的 IP 地址为私网地址，会导致其他 SIP 终端无法通过这个私网地址呼叫到相应的 SIP 终端。另外一个原因是 NAT 给 SIP 终端分配的地址映射有一定的时间限制，一旦超过这个时间而该终端没有再发起建立映射的要求，那么这个映射就会消失或供其他终端使用。

再次造成媒体流不通的主要原因是当公网中的 IP

① 基金项目:2008 广西研究生创新项目(2008105950810M418);广西科学研究与技术开发计划(桂攻科 0630004-5N)
收稿时间:2009-02-10

© 中国科学院软件研究所 http://www.c-s-a.org.cn

包经过 NAT 需要访问私网资源时，NAT 将此包的目的地址改为某一私网 IP 地址。在 SIP 通信中，媒体的相关信息存放在 SDP 的包体中。在 SDP 包中由字段 c 和 m 描述本次媒体所使用的 IP 地址和端口号。在 NAT 后的 SIP 用户代理在发送这个 INVITE 消息时，SDP 的 c 和 m 字段就带有了私网地址，从而导致媒体流无法建立。

2.3 SIP 穿越 NAT 的常用的几种解决方案[5]

(1) ALG(Application Level Gateway)

在 NAT 上加入能够对于具体应用协议(如 SIP)感知的模块，通过对于具体应用协议的感知，进行针对不同协议的具体 NAT 穿越处理。对于每一种应用协议都需要一个 ALG 实例来支持。SIP 需要一个，H.248 需要一个，如此等等。因此每增加一种新的协议，或者现有协议修改了，都需要一个新的 ALG 来支持。因此这种机制在实际应用中复杂度高，可扩展性差，受到很大限制。

(2) MIDCOM(Middle box Communication)[5]

这是一大类方法，因其中非常典型的一种采用了 IETF 的 MIDCOM 协议而得名。该类方法的共同特点是需要一个辅助设备(当然可以做在 NAT 上)来支持。该设备对于具体的应用协议是感知的，了解其具体的穿越需求。该设备通过一种通信协议来请求或控制 NAT，创建特定的地址/端口绑定关系或者打开特定端口允许该应用协议的数据流通过。但是并非所有的 NAT 都能够支持某种类似 MIDCOM 的请求或控制协议，因此这类技术在实际中的应用也受到一定的局限。

(3) STUN(Simple Traversal of UDP Through Network Address Translators)[6]

STUN 即 UDP 对 NAT 的简单穿越方式，是穿越非对称 NAT 的非常有效的方法。原理是利用非对称 NAT 映射和目标地址无关的特性，通过从公众网上 STUN 服务器获得内网主机在 NAT 的映射端口，再把映射的地址放在如 RTP 和 RTCP 报文的负载中。从而使外部主机直接使用 NAT 映射后的 IP 和端口进行通信。这样媒体流报文负载中的地址信息在经过 NAT 时就无需被修改了，只需按普通 NAT 流程转换报文头部分的 IP 地址即可，而负载中的 IP 地址信息和报文头中的地址信息是一致的。STUN 方式只支持 UDP 承载的协议，它不要求对 NAT 设备升级，但需要提供 STUN Server，同时终端需要支持 STUN Client 功能。

(4) TURN(Traversal Using Relay NAT)[7]

TURN 即通过转发方式穿越 NAT。与 STUN 方式类似，TURN 方式也是在公众网上有一个服务器，不过该服务器的作用是转发所有通过 NAT 的报文，TURN 服务器为每一个向 TURN 申请的内网主机分配端口，内网的主机也同样需要向服务器询问地址和端口，但是不同与 STUN 的是，TURN 服务器返回的不是内网在 NAT 的映射地址和端口，而是 TURN 服务器为了转发报文而开放的端口和 TURN 服务器地址。TURN 方式不仅可以穿越非对称 NAT，还可以穿越对称 NAT。NAT 设备不需要解析报文，不会增加 NAT 设备的负担，但所有报文需经 TURN 转发，TURN 就成为瓶颈。需要提供 TURN Server，同时终端需要支持 TURN Client 功能。

经过对几种常用的穿越方案的优缺点等方面的分析，加上目前在家庭和中小企业网内的大部分都是非对称的 NAT，本文采用的是 STUN 的穿越方式，技术比较成熟普遍，顺利的穿越我们项目实践中提供的 NAT。

3 穿越方案的设计

在我们整个穿越方案的设计中，选择了好几套不同的方案。在 UA1 用户端，我们分别用 PDA、PC 机和 USB phone 三种不同的终端参与了测试，在外网的服务器虽然我们采用的是精简的 Mini server 服务器，通过有效配置，它有效的发挥了 SIP 和 STUN 服务器应该具有的作用。而在另外一端的局域网内，NAT 用的还是美国网件公司的 WGR614，为了以示区别，配置它的 IP 地址为 202.120.0.1，在网内，我们同样用 PC 机装有了 Windows 下嵌入了 STUN 客户端的 SIP 终端。

3.1 方案拓扑模型

同一般的 SIP 终端穿越 NAT 不同的是，这种设计的 UA1 是采用了基于 Windows Mobile 5.0 的 PDA 终端。Windows Mobile 操作系统是微软公司针对移动设备而开发的精简操作系统，主要用在智能手机、掌上设备(PDA)等移动终端上，Windows Mobile 将熟悉的 Windows 桌面扩展到了个人设备中，具有和 Windows 兼容的 API 方式，由 Wince 发展而来，属 Wince 具体定制产品。它的使用给无线 VOIP 的应用提供了一个更方便更灵活的发展方向。

© 中国科学院软件研究所 http://www.c-s-a.org.cn

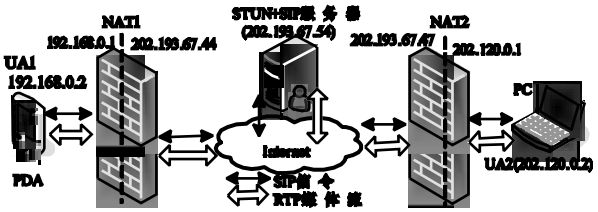

图 1　SIP 穿越 NAT 的系统拓扑模型

上图就是 UA1(PDA)穿越 NAT 系统拓扑模型图，为了方便又不失一般性，UA2 选择的是位于另外一私网上的一个客户端 PC，它的 IP 为 202.120.0.2，而 UA1 的 IP 为 NAT 后面的内网 IP，地址是 192.168.0.2，它们对外都是不可见的，图中将 STUN 和 SIP 服务器都设置在同一台主机上，其 IP 地址是 202.193.67.54，图中的黑白双向箭头标明出了媒体流和 SIP 信令的处理情况，还有其中的端口变化情况。

3.2 基于 STUN 的 SIP 终端软件模型

PDA 客户端是在原有的 SIP UA 中嵌入了 STUN 客户端，对每一个使用 STUN 协议的 SIP 终端来说，每一个 SIP 终端也是支持 STUN 协议的客户端，这样就要求 SIP 终端增加对 STUN 协议的支持。所以 SIP+STUN 客户端(PDA)的软件模型如图 2 所示：

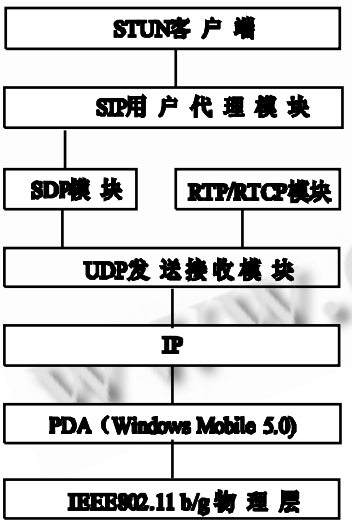

图 2　基于 STUN 的 SIP 终端软件模型

从上图中我们可以看出，整个的无线 VOIP 客户端软电话是建立在 PDA 硬件和 Windows Mobile 5.0 操作系统平台之上，而无线信号发射、传输和接收是遵照 IEEE 802.11 b/g 协议标准来实现的，当客户端 UA1 要与 NAT 以外的客户端用户通信时，通过 STUN 客户端就可以得出 NAT 的映射地址和端口值，每次注册或者呼叫之前，SIP UA 都需要修改 SIP 消息中的所有局域网地址为映射后地址，然后再发送出去。当 SIP 信令消息在通过 NAT 时，就不要修改 IP 包负载中的的 SIP 信令消息，只需要通常 NAT 流程修改 IP 包头的地址信息就可以了。这样负载中地址信息和 IP 包头中的地址信息是一致的，SIP 消息就能够穿越 NAT。当被呼叫用户根据 SIP 消息中的地址返回响应时，NAT 接收到响应后，会根据映射关系将响应送达局域网内的呼叫发起用户。这样 SIP 消息就能穿越 NAT。

RTP/RTCP 控制的媒体流信息是通过 SDP 来描述的，放在 SIP 消息中。当修改 SIP 消息时，也需要修改 SDP 部分的媒体流端口为映射端口，由于 STUN 事先已经在 NAT 上建立起媒体流的 NAT 映射表，所以媒体流就可以通过 NAT 上已经建立好的映射通道进行传输，媒体流就能够穿越 NAT 了。

3.3 STUN 客户端的设计

STUN 客户端的功能主要有四个。第一个就是查询，该查询流程可以通过三种测试请求来判断出口 NAT 的信息，而出口 NAT 的信息又包括多种情况，可以由下面这个图来说明具体查询 NAT 类型的工作流程：

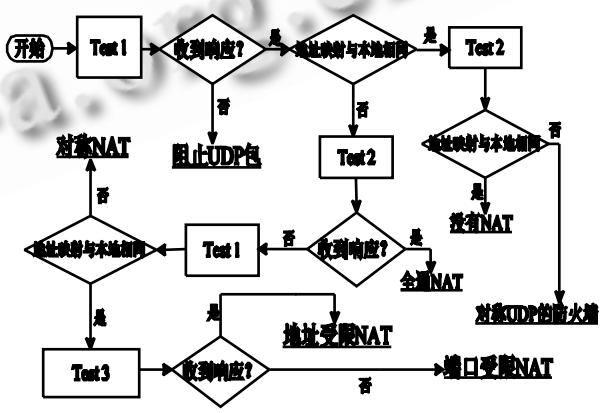

图 3　NAT 检测工作流程图

上图中该流程的工作环境是 STUN 客户端运行在局域网，STUN 服务器运行在公网上。所用到的三种测试请求分别是：Test1 为 STUN 客户端发送一个没有设置任何标志和响应地址属性(RESPONSE-

© 中国科学院软件研究所 http://www.c-s-a.org.cn

ADDRESS)的 STUN 请求到 STUN 服务器；Test2 为 STUN 客户端发送一个带有 changeIP 和 changeport 标志的请求；Test3 为 STUN 客户端发送一个只带有 change port 标志的请求。

STUN 客户端第二个主要功能就是向 NAT 外的 STUN 服务器发送绑定请求，通过请求来得到 NAT 分配的映射地址和端口号。目的端口固定为 STUN 协议众所周知的端口 3478。这里的请求有两种类型：使用 UDP 发送的绑定请求和通过 TCP 使用 TLS 发送的共享秘密请求，绑定请求用于确定 NAT 分配的映射地址和端口号。STUN 客户端的第三个功能是测试出口对称 NAT 的端口分配规则，来预测 NAT 的端口映射号；第四个是将得到的 NAT 类型、映射地址、端口号和预测端口都填入和 SIP UA 共享的接口文件中，按照事先协商好的顺序和格式保存，以供 SIP UA 读取进而好修改 SIP 消息。

4 NAT穿越方案实现

第三部分设计了基于 STUN 协议的 SIP 穿越 NAT 方案，STUN 客户端模块作为设计方案的基础，在整个 SIP 软终端处于非常重要的位置，此节在重要描述 SIP-NAT 穿越流程和实现过程的基础上，对整个方案中的 STUN 客户端实现进行了描述。

4.1 SIP 终端的工作流程

SIP 终端的设计是本方案中最重要的一个步骤，方案的思想主要体现在客户端的设计方面，如何使得原有的 SIP 终端支持 STUN 客户端是该设计的关键。根据前面的设计及软件模型模块的分工，SIP 终端的 NAT 穿越工作流程如下图 4 所示，在 SIP 用户代理初始化之后，启动 STUN 客户端，而客户端通过与其 STUN 服务器通信，检测是否存在 NAT，并得到 NAT 的类型、NAT 映射到公网地址以前绑定的生存周期等。如果存在 NAT 而且是位于非对称类型 NAT 之后，则接着执行通道保持，注册，呼叫连接的步骤，但是在这些过程当中，需要对 SIP 消息做一些修改，把 SIP 消息中携带的用于建立呼叫连接和媒体通信的地址信息改为 NAT 绑定的公网地址和端口，因为私网地址在公网上是不可路由的。在呼叫链接建立后就可以建立连接并进行 RTP 媒体流的通信。如果不存在 NAT 就不需要执行 NAT 穿越的流程，用户可以直接进行连接并进行 RTP 媒体流的通信。由于 STUN 自身不支持对称 NAT 的穿越，所以如果是位于对称 NAT 之后，穿越流程结束。

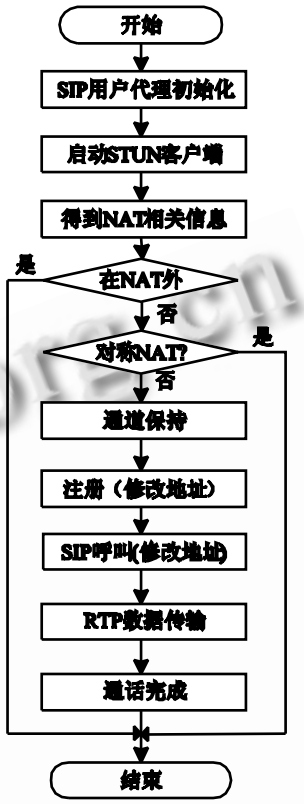

图 4 SIP 终端的 NAT 穿越流程

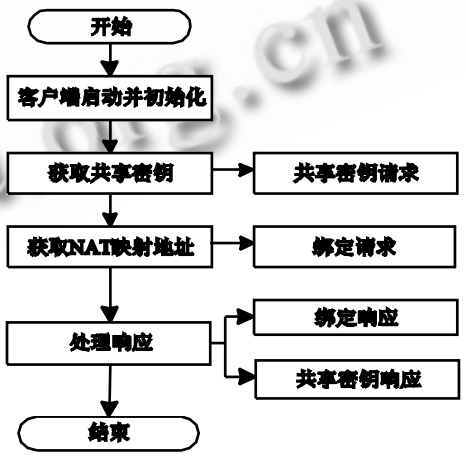

图 5 STUN 客户端软件执行过程

在 SIP 终端的整个穿越过程中，STUN 客户端部分的实现是很关键的一部分。在图 5 中给出了 STUN 客户端的软件执行过程，在客户端启动并初始化之后，首先运行 STUN 服务器发现子模块，得到 STUN 服务器的地址之后，客户端向服务器发送共享密钥请求获

© 中国科学院软件研究所 http://www.c-s-a.org.cn

取来临时用户名和密码，这个过程是通过基于 TCP 的 TLS 连接和 STUN 服务器实现协商的。

4.2 SIP 穿越 NAT 的实现过程

在图 1 的系统拓扑模型中，SIP 终端可以位于图中不同位置，为了不失一般性，假设两个不同 NAT 后面的不同终端进行实践测试。下面详细描述他们的 NAT 穿越实现过程。

(1) STUN 查询

SIP终端UA1(PDA)上电之后，启动STUN客户端，通过与 STUN 服务器通信，检测到它和 STUN 服务器之间存在 NAT 以及 NAT 的类型，如果是非对称 NAT，就分别从 192.168.0.2:5060 和 192.168.0.2:7078 发送 Binding Request 至 STUN 服务器，假设 NAT 分配的端口分别为 9990 和 9995，这样在 NAT 中就建立了两个地址映射 (192.168.0.2:5060，202.193.67.44:9990) 和 (192.168.0.2:707 ，202.193.67.44:9995)，一个用于 SIP 信令传输，另一个用于媒体流的传输。

(2) 通道保持

STUN 客户端通过与 STUN 服务器交互检测到 NAT 绑定的生存期，假设为 T。如果在时间 T 内没有数据通过 NAT 绑定的端口，绑定就会失效，这样先前建立好的 RTP 和 SIP 通道都无效了，为此我们采取如下策略：

STUN 客户端通过与 STUN 服务器交互检测到 NAT 绑定的生存期，假设为 T。如果在时间 T 内没有数据通过 NAT 绑定的端口，绑定就会失效，这样先前建立好的 RTP 和 SIP 通道都无效了，为此我们采取如下策略：

(a) SIP 通道保持：每隔时间 t(略小于 T)从 192.168.0.2:5060 向服务器的 5060 端口发送数据包。定期往服务器的 5060 端口发包就保证了在 T 时间内有数据通过 NAT 绑定的用于 SIP 通信的端口，使绑定一直有效。同时先由 NAT 内部向服务器的 5060 端口发包，使得从服务器的 5060 端口路由过来的 INVITE 请求可以被 NAT 路由到内网，从而实现外网用户主动和内网用户建立连接。

(b) RTP 通道保持：每隔时间 t(略小于 T)从 192.168.0.2:7078 向 STUN 服务器的默认监听端口 3478 发送 Binding Request 刷新 RTP 绑定。

(3) 注册

如果查询到 NAT 是非对称的，SIP 终端就可以用查询到的用于传输 SIP 信令的映射地址和端口向服务器注册，注册过程和正常的 SIP 注册一样，但是要对 Register 请求消息做如下修改：

(a) 把 via 域中 SIP URI 参数中的私有地址改为 NAT 绑定的地址 202.193.67.44:9990

(b) 把contact域中SIP URI参数中的私有地址改为 NAT 绑定的地址 202.193.67.44:9990

(4) SIP 呼叫建立

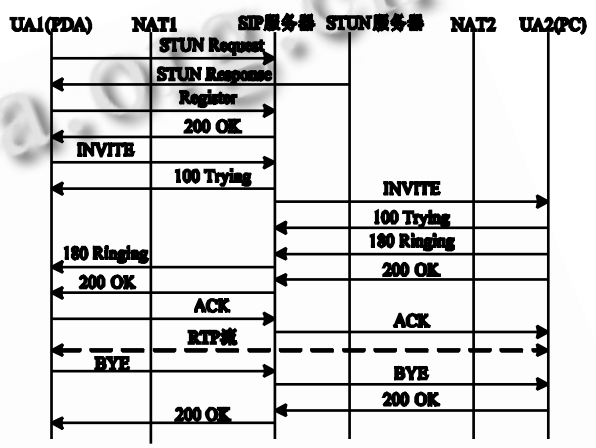

图 6　NAT 情况下 SIP 呼叫流程图

图 6 是 UA1(PDA)为主叫时 SIP 呼叫的流程。和正常的 SIP 呼叫基本上是一样的，只是需要对 SIP 消息做一些修改，其他操作按 SIP 标准规则处理,UA2(PC)的动作和 UA1 类似。当 UA1 为主叫，在发送请求消息时对 SIP 消息作如下修改:

(a) 修改 via 域，把 SIP URI 参数中的私有地址改为 NAT 映射的地址 202.193.67.44:9990

(b) 如果存在 contact 头域，则把 SIP URI 参数中的私有地址改为 202.193.67.44:9990

(c) from 域中 SIP URI 参数中的私有地址用 202.193.67.44:9990 替换；

(d) SDP 消息体中 c 行中的主机地址用 NAT 映射的公网 IP 地址 202.193.67.44 替换，m 行中的端口也用 NAT 绑定的 RTP 端口 9995 替换。

4.3 RTP 流穿越 NAT 的实现

在运行我们设计的 SIP 终端之后，SIP 消息中的用于建立 SIP 呼叫连接和媒体连接的地址信息都被替换为 NAT 映射的公网地址信息，这样 SIP 呼叫连接就可以成功建立。在 SIP 消息穿越 NAT 之后，双方就可以

© 中国科学院软件研究所 http://www.c-s-a.org.cn

开始媒体流的通信了。下面描述 RTP 媒体流穿越 NAT 的过程。

SIP 使用 SDP 进行媒体协商。建立 SIP 呼叫连接的过程中，发送 INVITE 请求和返回 200OK 响应的时候，SDP 消息体 c 字段中的内网 IP 地址和 m 字段的端口号已被改写为 NAT 映射的用于 RTP 媒体流传输的公网地址和端口，这些地址是可以在公网上路由的。这样在 SIP 呼叫连接建立之后，双方就会根据协商好的地址和端口发送和接收媒体流，进行端到端得直接通信，所以 RTP 流可以顺利穿越 NAT 设备。

5 结语

文章的创新点在于把一般用于台式 PC 或者专用 VOIP 电话中的 SIP 软终端通过嵌入了 STUN 客户端，应用在现今较为流行的无线掌上设备 PDA 上，这为把 SIP 软终端应用到未来的 3G 智能手机等无线移动设备上提供了更多的参考。另外，NAT 穿越还有很多值得研究的领域，对于如何用成熟的技术来解决目前网络存在的所有种类的 NAT，如何在不需要架设服务器的情况下，即基于 P2P 技术的分布式 NAT 穿越方式，都是我们需要进一步深入研究的方向。不过之所以存在 NAT穿越的问题是由于IPV4地址资源的缺乏，因此加快研究和普及 IPV6 技术才是长期的解决方案。

参考文献

1 Rosenberg J, Schulzrinne H, Camarillo G. SIP:Session Initiation Protocol. IETF RFC 3261, 2002－06.

2 Rosenberg J, Weinberger J, Huitema C, et al. STUN-simple Traversal of User Datagram Protocal(UDP) Through Network Address Translators(NATs). IETF RFC 3489, 2003－03.

3 张智江,张云勇,刘韵洁.SIP 协议及其应用.北京:电子工业出版社, 2005:1－2,6－7.

4 高扬,糜正琨. SIP 协议的 NAT 穿越研究.重庆邮电学院学报(自然科学版), 2006,18(4):503－507.

5 张波,胡瑞敏,边学工.一种实现 SIP 穿越 NAT 的新方案.计算机工程, 2005,31(2):119－121.

6 刘春燕,陈名松,冼莉莉.基于端口探测的 SIP 穿越 NAT 的设计和实现.计算机工程,2008,(9):114－116.

7 许先斌,万庆.一种解决 SIP NAT 的方案的设计与实现.计算机应用, 2004,(4):119－121.

© 中国科学院软件研究所 http://www.c-s-a.org.cn