

SIP 中 NAT 穿透技术的研究及实现

韩小燕, 曾桂根, 李 敏

(南京邮电大学 通信与信息工程研究院, 江苏 南京 210003)

摘 要: 随着 IP 数据业务的蓬勃发展, 基于分组的多媒体通信系统标准被广泛运用于视频会议和 IP 电话中, VoIP 是新一代网络时代发展起来的最具代表性和发展前途的应用技术之一, SIP 作为 VoIP 中的一种信令控制协议, 具有很大的增长潜力, 但 SIP 协议在设计时没有考虑到实际网络中会部署很多的 NAT, 为了更好的推广 VoIP 业务的发展, 解决好 SIP 穿越 NAT 的问题将是一个重大的研究课题。文中主要在基于 UDP 穿透技术的基础上为 SIP 中 NAT 穿透提出了一种解决方案。最终在 VC 环境下实现该方案并给出测试结果。

关键词: 会话初始协议; 会话描述协议; 网络地址翻译

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2011)01-0193-04

Research and Implementation of SIP Traversal NAT

HAN Xiao-yan, ZENG Gui-gen, LI Min

(Institute of Signal Processing and Transmission, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: With the rapid development of data service, packet-based multimedia communication system standards are widely used in video conference and IP phone. VoIP developed from new generation network which is one of the most representative and perspective application technologies. SIP as one of signal control protocols of VoIP has great growth potentialities. So in order to extend the development of VoIP service, solving the problem of SIP traversal well will be an important research topic. In this paper, propose a solution for SIP traversal NAT through NATs based on UDP protocol. Finally realize the program in the VC environment and give the test results.

Key words: SIP; SDP; NAT

0 引 言

由于 IP 网络的迅速发展, 使得基于 IP 的语音与视频通信越来越受到大众的青睐, IETF 提出了基于 IP 网络的多媒体通信的应用层控制协议 SIP^[1] (session initiation protocol), 该协议可用于建立、修改和终结多媒体会话与呼叫。但 SIP 协议在设计时没有考虑到实际网络中会部署很多的 NAT, 当前由于 IPV4 地址空间不足, 在部署大量 IPV6 之前大量的终端不得不采用私有网 IP 地址, 而当这些私有网 SIP 用户要接入公网时, 则其业务流将必然途径网络中的 NAT (Network Address Translation) 设备, 现在的 NAT 设备并不支持 SIP 协议的识别和处理。这严重阻碍了 IP 语音与视频通信的普及, 因此研究 SIP 中 NAT 穿透方法, 对推动基于 IP 的语音视频通信的大众化应用具有十分重要

的实际意义。

文中主要在基 UDP 穿透技术的基础上为 SIP 中 NAT 穿透提出了一种解决方案。

1 SIP 协议、NAT 相关技术

1.1 SIP 协议及相关内容

SIP (Session Initiation Protocol, 会话初始协议) 协议是 IETF (Internet Engineering Task Force, 因特网工程任务组) 标准体系中的一部分, 从 SIP 在网络体系中的位置^[2] 可以看出它是一个应用层的控制协议, 专门为基于 IP 的电话应用设计的 VoIP 信令协议, 它的作用是在于建立、修改、释放多媒体会话^[3]。当会话的一端向会话的另一端发出建立多媒体会话的邀请时, 必须在 SIP 的邀请消息中给出描述会话特征的信息。

SIP 协议的主要特点:

① 发起会话, 通过 SDP 协议, SIP 可以在呼叫发起和呼叫进行中对会话参数进行协商, 如会话带宽要求、传输的媒体类型、媒体的编解码格式, 以及对组播和单播的支持等。

收稿日期: 2010-05-01; 修回日期: 2010-08-18

作者简介: 韩小燕 (1984-), 女, 江苏泰州人, 硕士研究生, 研究方向为无线数据与计算; 曾桂根, 副教授, 硕士生导师, 研究方向为信号处理、认知无线电、智能通信终端。

②SIP 可以支持单播会话,也可以支持多播会话。

③SIP 与网络协议独立,即与低层协议无关。

④SIP 支持很多其他协议,如 RSVP, RTP, RTCP, RTSP, SAP 和 SDP 等,但是,SIP 的功能和操作不取决于以上任何协议。

⑤SIP 协议是基于文本的协议,简单灵活,可扩展性好。

⑥SIP 协议是无状态的,服务器可以保持也可以不保持呼叫状态。

⑦SIP 透明支持名字映射和重定向服务,可以实现 ISDN 和 IN 电话用户服务;通过网关,SIP 可以实现 PSTN 电话之间的呼叫。

⑧SIP 支持用户的移动性和移动业务。

SIP 协议有五大基本功能^[4]:

- (1) 用户定位
- (2) 用户能力
- (3) 用户可用性
- (4) 呼叫建立
- (5) 呼叫处理

SIP 是基于文本的协议,SIP 消息分为两大类:客户机到服务器的请求消息(Request)和服务器到客户机的响应消息(Response),请求消息和响应消息这两种消息的格式如下^[5]:

```
generic-message = 起始行(start-line)
                  消息头(message body)
                  空行(CRLF)
                  [消息体(message-body)]
                  其中起始行=请求行/状态行
```

请求行是请求信息的起始行,状态行是响应消息,目前已经定义了 6 种类型的请求消息^[6]: INVITE、ACK、OPTIONS、BYE、CANCEL 和 REGISTER。

消息头分通用头(general-header),请求头(request-header),响应头(response-header)和实体头(entity-header)四种。

消息体是用 SDP 协议描述的,它主要用来描述会话媒体参数,如地址、端口和所使用的编解码器等,会话发起方是用 SDP 描述自己在会话中所要求的参数信息,被叫方将自己所支持的参数与该消息中所描述的参数进行比较以完成协商,然后将协商后的参数也以 SDP 形式进行描述,返回给主叫方。SDP 会话描述由许多文本组成,每个文本行的格式均为: <type>=<value>。

1.2 NAT 的简单介绍

NAT (Network Address Translation)^[7] 即网络地址转换,它是一个 IETF 标准,允许一个机构(包括多个网络节点)以一个地址出现在 Internet 上。NAT 将每

个局域网节点的地址转换成一个 IP 地址,反之亦然。NAT 根据类型不同可分为静态 NAT,动态 NAT 和网络地址端口转换 NAT^[8]。静态地址转换(static NAT)就是将本地地址与全局地址进行一对一映射,并指定在通信过程中进行转换;而动态地址转换(dynamic NAT)则是将本地地址与全局地址进行多对一映射,本地地址到全局地址的翻译不是静态的,而是本地地址与 NAT 地址池中的全局 IP 地址进行动态映射,动态分配一个公用网 IP 地址,当用户连接断开后,再将动态分配的公用网 IP 地址释放而留待其他用户使用。网络地址端口转换(NAT Address Port Translate, NATP)也被称为 PAT (Port Address Translate),它是对动态 NAT 的扩展,NAPT 允许多个本地地址公用一个全局地址,它除了进行 IP 地址的翻译外,同时还对 TCP/UDP 端口号进行翻译。

根据 NAT 工作方式的不同,NAT 类型还可以为全方式 NAT、限制方式 NAT、端口限制式和对称方式 NAT^[9],它们的主要区别在于如何处理外部网络发来的数据包^[10]。

(1) 全方式(Full Cone)NAT 将相同的本地 IP 地址端口发来的请求映射到相同的外部 IP 地址和端口号。任意外部主机通过将报文发送至映射后的外部地址,能够发送报文至内部主机。

(2) 限制方式(Restricted Cone)NAT 将相同的本地 IP 地址和端口发送的请求映射到相同的外部 IP 地址和端口号,与 Full Cone 工作方式不同,只有在内部主机预先将报文发送至外部主机的某个 IP 地址上,外部主机才可以将报文发送至内部主机的特定 IP 地址上。

(3) 端口限制方式(Port Restricted Cone),此工作方式与 Restricted Cone 工作方式相似,但它需要内部主机预先发送报文至外部主机的某个 IP 地址的某个端口上,然后,外部主机才可以将报文发送至内部主机的特定 IP 地址的特定端口上。

(4) 对称方式(Symmetric Cone)NAT 将本地 IP 地址和端口号相同且目的 IP 地址和端口号也相同的所有请求,映射到相同的外部 IP 地址和端口号;本地 IP 地址和端口号相同的请求,但目的 IP 地址不同,则生产不同的地址映射关系;外部主机只有在接收到内部主机发送的报文后,才可以向内部主机发送 UDP 报文。

2 SIP 协议中 NAT 穿越解决方案及实现

2.1 SIP 中 NAT 穿越存在的问题

如图 1 所示的软交换网络中,若终端 A 向终端 B 发起呼叫请求,在终端 A 处会产生原 INVITE 消息包 M,消息包经过路由的 NAPT 后,被转换成新的 INVITE

消息包 N, 转换过程如图 2 所示。

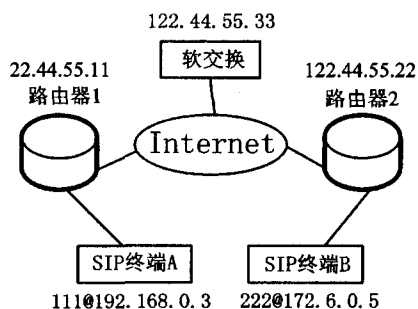


图 1 软交换网络

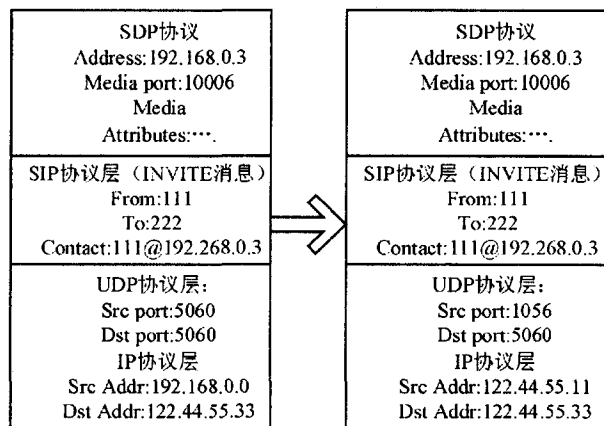


图 2 INVITE 消息包转换

其变换后新 INVITE 信息包 N 中的端口 1056 为 NAT 动态分配的端口号。而终端 B 向软交换注册时, 通过 SIP 协议层的注册消息告诉软交换它的私有地址, 同时, 由于在终端 B 没有主动对外发起连接请求之前, 路由器不会主动为其分配可访问的 IP 地址和端口号, 因此, 终端 A 无法将发起的 INVITE 消息发送给终端 B, 导致呼叫无法连接, 就算 INVITE 消息发送给了终端 B, INVITE 消息中携带的 SDP 信息是用于终端间的媒体协商, 从而选择合适的编解码器, 建立 RTP 媒体流的连接, 但是 INVITE 消息中的 10006 是终端 A 建立 RTP 连接的端口号。当终端收到此 SDP 信息后, 就会试图与 192.168.0.3:10006 建立 RTP 连接, 但由于这是一个内部私有网地址, 因此, 通话也自然无法建立起来。

2.2 SIP 中 NAT 穿越具体问题的具体分析

图 1 中 SIPNAT 穿越问题有两个:

问题一:

一个外网 IP 地址的 SIP 终端想和 NAT 后面的内网 SIP 终端通讯的条件就是要求 NAT 后面的内网 SIP 终端主动向外网 IP 地址的 SIP 终端发起一个 UDP 数据包。

问题二:

SIP 消息中含有未必转换的私有地址而导致通信无法建立。

问题一要靠一个公网 IP 地址的服务器帮助两者来建立连接^[11]。当两个路由后面的内网 SIP 终端分别连接了公网 IP 地址的服务器后, 服务器可以从收到的 UDP 数据包中获取到这两个路由设备的公网 IP 地址和这两个连接建立连接的映射端口。两个内网 SIP 终端可以从服务器上获取到对方的路由设备公网 IP 地址和映射的端口了。首先, 终端 A 登陆服务器 S, 路由器 1 为这次连接建立分配了一个端口 5060, 那么服务器收到终端 A 的地址是 122.44.55.11:1056, 同样, 终端 B 登陆服务器 S, 此次路由器 2 给此次连接分配的端口是 4000, 那么服务器收到终端 B 的地址是 122.44.55.22:4000, 此时终端 A 与终端 B 都可以与服务器 S 通信了, 如果终端 A 此时需要直接发送信息给终端 B, 那么需要在路由器 2 上打一个方向为 122.44.55.11 (即终端 1 的外网地址) 的洞, 则终端 A 发送到 122.44.55.22:4000 的信息, 终端 B 就能收到。这个打洞的命令由服务器 S 来发出。

问题二针对当前非对称方式的 NAT, 内部网络中的 SIP 终端可以通过通用即插即用协议 (Universal Plug and Play, 简称 UPnP) 向路由器查询其映射的外部地址, 该协议是由 Microsoft 公司制定并推广的。通过该协议, 终端可以将自己准备使用的内部地址和端口告诉 NAT 网关, NAT 网关会向其返回映射后的地址和端口。从而可以预先得到公用网出口 IP 和端口, 并由终端直接将公用网信息写入消息包中就可以实现 NAT 设备的穿越。

2.3 综合解决 SIP 中 NAT 穿越问题

将 2.2 节中的两个问题综合起来考虑, 则当终端 A 想呼叫终端 B 时要经过如图 3 所示的过程。

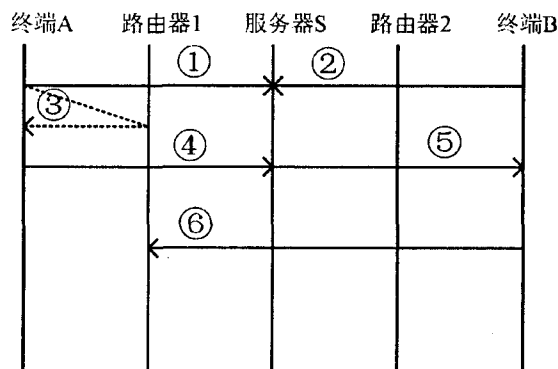


图 3 终端 A 呼叫终端 B

2.3.1 终端 A 要呼叫终端 B 的准备过程

①终端 A 登陆服务器 S;

②终端 B 登陆服务器 S;

③终端 A 向路由器查询其映射的外部地址及端口并返回 (INVITE, RTP 的两个映射端口);

④终端 A 向服务器发送命令给服务器 S, 请求服

务器 S 命令终端 B 向终端 A 方向打洞;

⑤服务器 S 命令终端 B 向终端 A 方向打洞;

⑥终端 B 向终端 A 方向打洞。

如将此服务器 S 的功能做在软交换服务器上,则经历以上过程之后,SIP 终端 A 即可向 SIP 终端发起呼叫,呼叫流程如图 4:

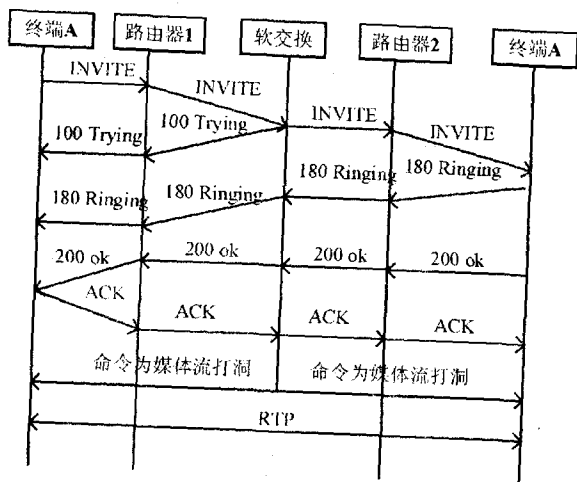


图 4 呼叫过程

2.3.2 终端 A 要呼叫终端 B 的后期过程

若在终端 A 这边利用 UPnp 向路由器 1 查询 192.168.0.3:5060 及 192.168.0.3:5061 映射的外部地址及端口分别为 122.44.55.11:1056 与 122.44.55.11:1058,在终端 B 172.6.0.5:5060 及 172.6.0.5:5061 映射的外部地址及端口分别为 122.44.55.22:1056 与 122.44.55.22:1058;则在图 4 中的 4 个 INVITE 消息变化如图 5 所示。

终端 B 最终收到的 INVITE 消息中携带的 SDP 信息中的 122.44.55.11:1058 是最后要与终端 A 建立的 RTP 连接的在终端这边的外部映射的端口号,终端 B 接受到此消息后,再将自己所支持的参数与该消息中所描述的参数进行比较以完成协商,然后将协商后的参数也以 SDP 形式进行描述,返回给主叫方。在最后建立 RTP 流之前,由服务器来命令两个终端向对方打洞,该命令通过各自登陆的端口来发送,在终端收到这个命令后,则采用进程间的通信来为 RTP 流向对方终端打洞。

2.4 SIP 中 NAT 穿越的实现及测试

硬件环境:三台 PC 机,芯片 P41.8G ; 512M,

两台路由器,

局域网相关设备。

软件环境:在 PC 上安装 Windows 操作系统,并在 VC 环境下根据以上方案编写 SIP 客户端、SIP 服务端(将软交换设备与服务器 S 的功能综合起来)。

网络拓扑及测试结果:

网络拓扑如图 6 所示。

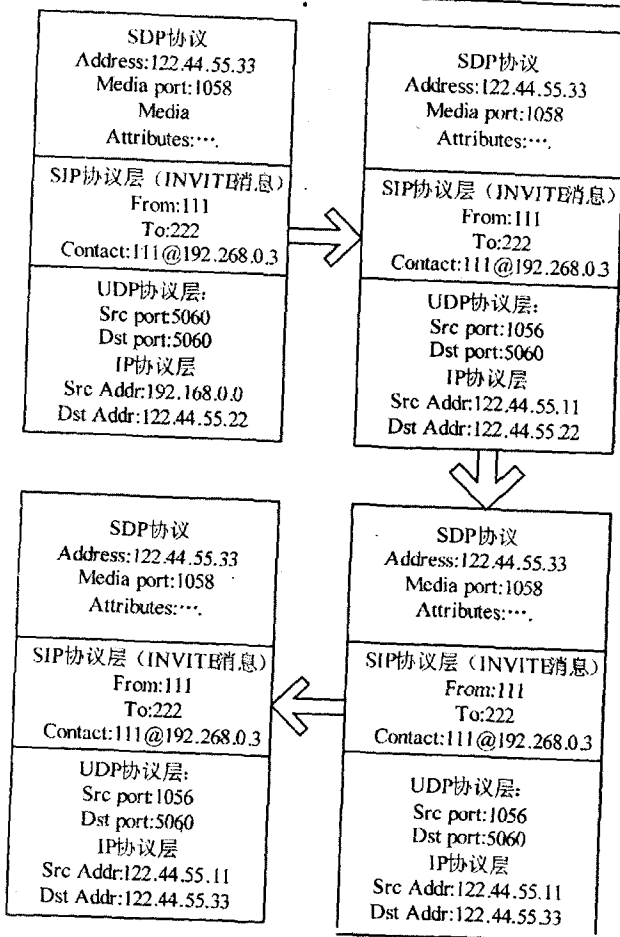


图 5 4 个 INVITE 消息内容的变化

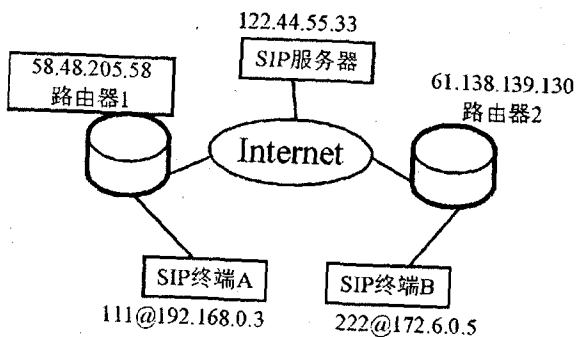


图 6 网络拓扑

我们用终端 A 呼叫终端 B50 次,呼叫成功 48 次,失败 2 次,同样再用终端 B 呼叫终端 A 50 次,呼叫成功 48 次,失败 2 次,时延情况与正常的 SIP 会话相比(无 NAT,非局域网内)使用本方案进行 NAT 穿越时只增加 50~170ms,这对人来说是可以忽略的。

3 结束语

文中针对 SIP 中 NAT 穿越具体问题进行了分析并提出了 SIP 中 NAT 穿越的解决方案,并对该方案进行了测试,该方案最大的优点就是无须对现有 NAT 设备做任何改动,但其局限性也是明显的,及该方案只解

(下转第 201 页)

时输出每个事件及其发生的时间。通过仿真画面和控制台的信息,可以完全掌握整个仿真过程的信息。图5为仿真画面的截图。图6为部分控制台显示的信息。

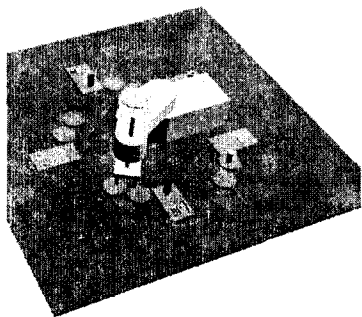


图5 仿真画面截图

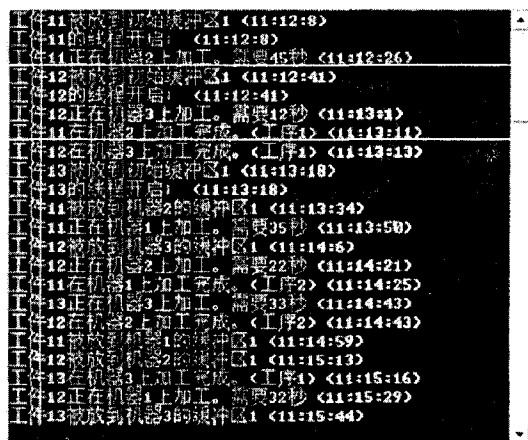


图6 控制台方式下显示的部分信息

文中基于多线程技术对一个简单的单件生产系统的工作过程进行了实时仿真,在此基础上,使用 Creator 对这个单件生产系统建模,并用 Vega Prime 对此模型

进行驱动,最终实现了关于这个单件生产系统的虚拟现实仿真。从仿真结果来看,可以清晰直观地看到单件生产系统的工作过程,证明此方法正确、有效。

参考文献:

- [1] 韦有双,杨湘龙,王飞. 虚拟现实与系统仿真[M]. 北京:国防工业出版社,2004.
- [2] 胡忠东,樊爱华. 虚拟现实工具[J]. 计算机仿真,1997, 14(5): 61-64.
- [3] 张秀山,徐荣花,胡庆丰,等. 虚拟现实技术及编程技巧[M]. 长沙:国防科技大学出版社,1999.
- [4] 袁胜智,谢晓方,曹建,等. 巡逻攻击导弹作战仿真系统研究[J]. 系统仿真学报,2009,21(14):4295-4299.
- [5] 王辰辉,杜宏明. 基于 Vega Prime 的液压挖掘机运动仿真[J]. 机械,2009,36(5):37-39.
- [6] 黄伟,戴余良,王长湖,等. Creator/Vega Prime 在船舶动力装置视景仿真中的应用[J]. 系统仿真技术,2008,4(4):277-281.
- [7] 王海刚,孙俊,郭维勇. 基于 Multigen Creator 和 Vega 的道路交通仿真[J]. 交通与计算机,2007,25(3):149-151.
- [8] 李建国,周俊武,战凯. 基于 MultiGen Creator/Vega 的矿井视景仿真研究[J]. 有色金属(矿山部分),2009,61(1):56-58.
- [9] MultiGen Paradigm, Inc. The MultiGen Desktop Tutor [M]. USA: MultiGen Paradigm,2003.
- [10] MultiGen Paradigm, Inc. Creating Models for Simulations [M]. USA: MultiGen Paradigm,2003.
- [11] MultiGen Paradigm, Inc. Lynx Prime Interface (version2.2) [M]. USA: MultiGen Paradigm,2007.
- [12] MultiGen Paradigm, Inc. Vega Prime 2.2 API Tutorial [M]. USA: MultiGen Paradigm,2007.

(上接第196页)

决了 SIP 穿越非对称 NAT 问题。对于 SIP 穿越对称 NAT 问题则需要更进一步的研究,也是下一步的研究工作。

参考文献:

- [1] Schulzrinne R J, Camarillo H, Johnston G, et al. SI-P: Session Initiation Protocol IETF[S]. RFC3261,2002.
- [2] Rosenberg J, Camarillo G, Schooler E, et al. SIP: Session Initiation Protocol[S]. RFC3261,2002.
- [3] 张荣,武波. SIP 协议的应用研究[J]. 计算机技术与发展,2006,16(6):71-73.
- [4] Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol[S]. RFC3261,2002:55-60.
- [5] 张永强,张捍东,赵金宝. SIP 协议栈研究[J]. 计算机

技术与发展,2007,17(11):49-51.

- [6] 刘洋,侯红. 基于 SIP 协议的 IP 电话技术[J]. 计算机技术与发展,2006,16(4):184-186.
- [7] Egevang K, Francis P. The IP Network Address Translator (NAT)[S]. RFC1631,1994.
- [8] Srisuresh P, Egevang K. Traditional IP Network Address Translator(TraditionalNAT)[S]. RFC 3022,2001.
- [9] Srisuresh P, Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations[S]. RFC 2663, 1999.
- [10] 王南,孙保锁,王月平. P2PSIP 系统中 NAT 穿越方案的研究与设计[J]. 计算机技术与发展,2009,19(10):66-69.
- [11] 钟宝荣,杜红,涂继辉. SIP proxy 系统中穿透 NAT 的实现[J]. 计算机技术与发展,2006,16(11):54-55.