北京邮电大学

硕士学位论文

# NAT环境下VoIP的解决方案与性能研究——SIP，RTP协议在VoIP中的应用

姓名：刘涛

申请学位级别：硕士

专业：软件工程

指导教师：王安生;罗宗贶

20040601

## 独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：刘洋　　日期：2024.6.24

## 关于论文使用授权的说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密在__年解密后适用本授权书。非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：刘洋　　日期：2024.6.24

导师签名：[illegible]　　日期：2024.6.24

# 摘 要

随着 IP 网的高速发展，VoIP 也得到了越来越多的服务提供商和 IP 网用户的关注。利用 VoIP 的技术，用户可以通过计算机网络，如因特网，来打电话。VoIP 将用户话机上的语音和多媒体信号转换称数字信号，然后通过因特网传送，而另一端的用户话机再将数字信号转换回来。这样，用户可以呼叫如何一个符合号码规则的用户了。用户也可以用带有麦克的电脑来通话。

NAT/Firewalls 处在虚拟的商用网络的边缘。通常住宅 DSL 用户也绑带了基于软件的 Firewall 和 NAT。这样 NAT/Firewalls 对商业和住宅用户都有影响。这个问题可以从两部分来看：一方面，虽然 Firewall 能动态的打开和关闭多个端口，有些端口正是 VoIP 信令，如 SIP，所要用到的，但 Firewall 的存在能使一些主动到来的会话消息无效。另一方面，NAT 可以阻止双向的语音和多媒体通信，因为，客户端（如 SIP 电话）要把私网的地址与端口添加到消息包中，而这些私网地址在公网上是不可路由的。

同时,SP 正期望着 VoIP 解决一些商业问题。对于网络接入商，VoIP 可以帮助留住商业客户。对于 ISP，在数据网和因特网上提供语音和多媒体业务能增加收入和利润。对于长途运营者，VoIP 可以降低费用,提供更多的服务。

但是一些技术问题却阻碍了运营商从 VoIP 中得到好处。在这些问题中，NAT 和 Firewall 是个关键问题。

本文先阐述这个阻碍 VoIP 在用户和商业中普及的关键问题。在第一章，将讨论 VoIP 的发展和关键技术。第二章介绍了 SIP，SDP，RTP 协议和 Vocal 系统。第三章讨论了 NAT 技术及其对 VoIP 的影响。在第四章中，介绍了几种穿越 NAT 的方法，然后介绍了我们在项目中提出的解决方案。关于方案的实施与测试分别在第五和第六章中介绍。最后，文章还讨论了一些在我们解决 NAT 问题时遇到的新问题，这些问题将在以后得到进一步的研究。

[关键字]

VoIP、SIP 会话初始化协议、H.323、RTP 实时传输协议、NAT、RSVP 资源预留协议

# Abstract

With the rapid development of IP networks, more and more Service Providers and IP network users give their attention in VoIP (Voice over IP). VoIP allows users to make telephone calls by using a computer network, or a data network as Internet. VoIP converts voice and multimedia signals to digital signals that can travel over the internet, and then converts them back at the other end, so users can speak to anyone with a regular phone number. VoIP may also allow users to make a call directly by using a microphone with a computer.

NAT/Firewalls are located at the virtual border of all business networks. Often a software-based Firewall and NAT are bundled in residential DSL packages as well, so the problem of NAT/Firewalls affects both business users and residential users. This problem consists of two components. Though today's Firewalls are able to dynamically open and close multiple ports as required by VoIP signalling protocols such as SIP, they remain ineffective at securely supporting unsolicited incoming sessions. NAT can prevent two-way voice and multimedia communication because the private IP addresses and ports inserted by client devices (SIP phones, video conferencing stations etc.) in the packet payload are not routable in public networks.

On the other hand, Service Providers are looking forwards VoIP to solve some of their business challenges. For local access companies, this is about retaining business customers. For ISPs it's about increasing revenue and profit by offering voice and multimedia services on top of existing data and Internet services. For long-distance carriers, they want to reduce costs and offer enhanced services by VoIP.

Unfortunately, a number of technical problems have prevented Service Providers and carriers alike from realizing these benefits. In these problems, NAT devices and Firewalls is a key issue.

This paper discusses the key issue that inhibits VOIP to be popular with the users and businesses. In chapter 1, development of VOIP and the main feature and key technology of VOIP are presented. In chapter 2, SIP, RTP, SDP and Vocal are introduced. In chapter 3, we know that the technology of Network Address Translator (NAT) which has grown up for the solution of IP address shortage and network security has become the problem of the deployment of VoIP. This Paper analyzes some existing mechanisms for the traversal of IP voice through NAT, and our project gives a solution to the key issue in chapter 4. In chapter 5 and 6, our team implements and tests this project. At last, the paper discusses some questions .When getting over the issue, we meet these questions which will be researched later.

**[Key Words]**

VoIP, SIP, H.323, RTP, NAT, SDP,RSVP

# 第一章 绪论

## 1.1 研究背景

VoIP 全称：Voice Over Internet Protocol，Internet 电话技术是目前 Internet 应用领域的一个热门话题。它实现了语音在 Internet 上的实时传送。其基本原理是：通过语音的压缩算法对语音数据编码进行压缩处理，然后把这些语音数据按 TCP / IP 标准进行打包，经过 IP 网络把数据包送至接收地，再把这些语音数据包串起来，经过解压处理后，恢复成原来的语音信号，从而达到由互联网传送语音的目的[21]。IP 电话的核心与关键设备是 IP 网关，它把各地区电话区号映射为相应的地区网关 IP 地址。这些信息存放在一个数据库中，数据接续处理软件将完成呼叫处理、数字语音打包、路由管理等功能。在用户拨打长途电话时，网关根据电话区号数据库资料，确定相应网关的 IP 地址，并将此 IP 地址加入 IP 数据包中，同时选择最佳路由，以减少传输时延，IP 数据包经 Internet 到达目的地的网关。在一些 Internet 尚未延伸到或暂时未设立网关的地区，可设置路由，由最近的网关通过长途电话网转接，实现通信业务。

### 1 1.1 VoIP 主要优点：[12]

1、消除长途话费。企业成功使用 VOIP 语音网关之后，能够完全消除公司各分部之间高昂的跨国，跨区长途话费。新一代 VOIP 的外线打出功能还将覆盖面由公司内部各点之间扩大到城市与城市，国家与国家之间。

2、清晰、稳定、低延时的话音质量。

3、先进的拨号规划。先进的拨号规划和地址对应功能，令其轻而易举的连接到 PBX 交换机上，灵活且多样化的拨号通达各个目的地。

4、节省带宽资源。电路交换电话消耗的带宽为 64kbit/s，而 IP 电话只需 8-10kbit/s，从而节省了带宽，降低了成本。

5、便于集成智能。VOIP 电话网集成了计算机网的智能模块，可以灵活地控制信令和连接，有利于各种增值业务的开发。

6、开放的体系结构。IP 电话的协议体系是开放式的，有利于各个厂商产品的标准化和之间的互相连通。

7、多媒体业务的集成。IP 电话网络同时支持语音、数据、图象的传输，为将来全面提供多

媒体业务打下了基础。

### 1.1.2 VoIP 主流信令协议 [1] [2]

目前在 VoIP 领域有两个完全独立的信令协议(在这里我们不讨论 MGCP[19])：国际电联电信标准部（International Telecommunications Union - Telcommunication Standardization Sector，ITU-T）的 H.323 协议簇和因特网工程任务组（Internet Engineering Task Force，IETF）的 SIP（Session Initiation Protocol）协议[3] [4]。两种协议相比较而言有以下几点异同：[7]

a. 开发速度：SIP 当然的优于 H.323，协议简单，不过如果 H.323 原语部分可以比较好的解析的话，事实上两者开发速度相差不大。

b. 多播：在这个方面 IETF 具有优势，有非常强大的应用经验的，SIP 已经设计在很多多播的骨干网络上，h.323v1，v2 要使用多单播同时进行的方式才能完成，不过 H.323v3 版本多播的支持就已经非常不错了。

c. 地址的运用上 SIP 使用 Url 上的机制非常灵活，这样可以让 SIP 以一种非常灵活的方式重定向到非 SIP 服务器上去，被另外一个 SIP 呼叫的 SIP 终端也能重定向到某个网页或者是电子邮件地址。对于 H.323 而言，命名的机制就非常混乱了，从 ASN.1 的文件我们可以看到有 h323-ID，url-ID，transport-ID，email-ID，partynumber 等等。

d. 对于 SIP 而言，所有的消息都采用文本编码，所以 SIP 消息非常简单，这样在开发的时候简单的网络检测就可以调试，反观 H.323 协议采用了 PER 或者 BER 的二进制编码方式，信令不是非常直观。

e. 系统资源的消耗上，SIP 比较大，每次服务器发出通告的时候，都需要建立一个监听套接字，这样的结果势必造成大量的闲置套接字，假设在建立一个完整的 Proxy/Register/RTP Gateway/三者和而为一的园区出口网关的时候，资源上势必会非常的紧张，这个是不能不予以考虑的问题。相反 H.323 在打开逻辑通道的情况下（OpenLogicalChannel 消息）只建立一个套接字。但随着计算机硬件的高速发展，资源消耗不在是首要的问题.

f. SIP 没有会议控制能力，所以仅仅只能做到点对点的媒体通讯，而 H.323 一开始就考虑了会议功能，其中还包含了 H.332 会议控制协议。但利用 SIP 灵活性建立会议控制已不是难题。[23]

总之，H.323 符合通信领域传统的设计思想，进行集中、层次控制，采用 H.323 协议便于与传统的电话网相连。SIP 模式的优点是与 Internet 紧密结合，在风格上遵循因特网一贯坚持的简练、开放、兼容和可扩展等原则，适于开发新的、与互联网结合的语音应用；其缺点是在组网、管理、运营、计费方面的考虑还有待成熟，在与传统 PSTN 网的互联互通方面还有待完善。但我们应该看到 SIP 简单灵活、分布式控制等优点。随着软交换等技术的发展，SIP 必将取代 H.323，成为 IP 领域内运用最广泛的信令控制协

议。

## 1.2 VoIP 关键技术及所面临的问题

### 1.2.1 VoIP 关键技术[10] [16]

传统的 IP 网络主要是用来传输数据业务，采用的是尽力而为的、无连接的技术，因此没有服务质量保证，存在分组丢失、失序到达和时延抖动等情况。数据业务对此要求不高，但话音属于实时业务，对时序、时延等有严格的要求。因此必须采取特殊措施来保障一定的业务质量。VOIP 的关键技术包括信令技术、编码技术、实时传输技术、服务质量（QoS）保证技术、以及网络传输技术等。

1. 信令技术[31]

信令技术保证电话呼叫的顺利实现和话音质量，目前被广泛接受的 VOIP 控制信令体系包括 ITU-T 的 H.323 系列和 IETF 的会话初始化协议。这里只讨论技术.

SIP 是一种比较简单的会话初始化协议。它提供会话或呼叫的建立与控制功能。SIP 可以应用于多媒体会议、远程教学及 Internet 电话等领域。SIP 既支持单点发送（Unicast）也支持多点发送，会话参加者和媒体种类可以随时加入一个已存在的会议。SIP 可以用来呼叫人或机器设备，如呼叫一个媒体存储设备记录一个会议，或呼叫一个点播电视服务器向会议播放视频信号。SIP 是一种应用层协议，可以用 UDP 或 TCP 作为其传输协议。而且 SIP 是一种基于文本的协议，用 SIP 规则资源定位语言描述，这样易于实现和调试，更重要的是灵活性和扩展性好。由于 SIP 仅作于初始化呼叫，而不是传输媒体数据，因而造成的附加传输代价也不大。SIP 的 URL 甚至可以嵌入到 web 页或其它超文本链路中，用户只需用鼠标一点即可发出一个呼叫。另外建立呼叫快，支持传送电话号码的特点。

2. 编码技术

话音压缩编码技术是 IP 电话技术的一个重要组成部分。目前，主要的编码技术有 ITU—T 定义的 G.729，G．723 等。其中 G.729 可将经过采样的 64kbit/s 话音以几乎不失真的质量压缩至 8kbit/s。由于在分组交换网络中，业务质量不能得到很好保证，因而需要话音的编码具有一定的灵活性，即编码速率、编码尺度的可变可适应性。G.729 原来是 8kbit/s 的话音编码标准，现在的工作范围扩展至 6.4-11.8kbit/s，话音质量也在此范围内有一定的变化，但即使是 6.4kbit/s，话音质量也还不错，因而很适合在 VOIP 系统中使用。G．723.1 采用 5.3/6.3kbit/s 双速率话音编码，其话音质量好，但是处理时延较大，它是目前已标准化的最低速率的话音编码算法。此外，静音检测技术和回声消除技术也是 VOIP 中十分关键的技术。静音检测技术可有效剔除静默信号，从而使话音信号的占用带宽进一步降低到 3.5kbit/s 左右；回声消除技术主要利用数字滤波器技术来消除对通话质量影响很大回声干扰，保证通话质量。这点在时延相对较大的 IP 分组网络中尤为重要。

3. 实时传输技术 实时传输技术主要是采用实时传输协议 RTP。

RTP 是提供端到端的包括音频在内的实时数据传送的协议。RTP 包括数据和控制两部分，后者叫 RTCP。RTP 提供了时间标签和控制不同数据流同步特性的机制，可以让接收端重组发送端的数据包。

4. QoS 保障技术

VOIP 中主要采用资源预留协议（RSVP）以及进行服务质量监控的实时传输控制协议 RTCP 来避免网络拥塞，保障通话质量。

5. 网络传输技术

VOIP 中网络传输技术主要是 TCP 和 UDP，此外还包括网关互联技术、路由选择技术、网络管理技术以及安全认证和计费技术等。由于实时传输协议 RTP 提供具有实时特征的、端到端的数据传输业务，因此 VOIP 中可用 RTP 来传送话音数据。在 RTP 报头中包含装载数据的标识符、序列号、时间戳以及传送监视等，通常 RTP 协议数据单元是用 UDP 分组来承载，而且为了尽量减少时延，话音净荷通常都很短。IP、UDP 和 RTP 报头都按最小长度计算。VOIP 话音分组开销很大，采用 RTP 协议的 VOIP 格式，在这种方式中将多路话音插入话音数据段中，这样提高了传输效率。

## 1.2.2 VoIP 发展所面临的问题[36]

当前的 IP 协议（IPv4），是在 1981 年由 RFC791 标准化的。尽管它现在已非常成熟，取得了巨大的成功，但是随着用户数量的增加，网络带宽的成倍增长，新的应用需求的出现，已经暴露出其当初设计不足的地方，逐渐显出过时的征兆。IPv4 面临的最大的问题是地址资源耗尽问题，这个问题是 IPv4 本身存在的缺陷，只有对其进行较大的修改才能解决。

从 20 世纪 90 年代初以来，国际上已经开始讨论下一代的 IP 协议体系了。经过多年的讨论，各种方案的比较权衡，下一代的 IP 协议体系目前已经基本制定完成，并分配了版本号 6，称为 IPv6[9]。但是由于 IPv6 要考虑到与现有网络的兼容性问题，以及具体实施过程中的一些不可知因素，IPv6 取代 IPv4 还需要时日。

为了缓解 IP 地址短缺的压力以及基于安全考虑，人们提出了网络地址翻译（Network Address Translator，NAT[11]）技术，该方案能有效缓解 IP 地址不够分配的问题，具体办法就是在内部网络中使用内部地址，通过 NAT 把内部地址翻译成合法的 IP 地址在 Internet 上使用。这样做可以在一定程度上缓解 IP 地址不够用的问题，由于其简单易实现，现在已经得到广泛的应用。

然而，存在 NAT 设备后的 IP 语音和视频设备仅有内部 IP 地址，这些地址在公众网上是不可路由的，这样就严重地制约了 IP 电话和视频会议的应用。解决这个问题也就成为 VoIP 发展中至关重要的事情。

## 1.3 研究目的

长期以来，NAT 对 VOIP 的影响是制约其发展应用的一个重要因素。面对这个问题，许多厂商采用了不同的方式来解决。但大多数要么以修改 NAT 牺牲安全来实现；要么以更改 SIP 协议，牺牲系统的通用性为代价来实现(往往是一些大的公司，垂直的研发力量让他们有条件发展自己的协议)；即使有的厂商没有牺牲以上两点，但却只能对特定的 NAT 有效，而面对稍微严格一些的 NAT，就无能为力了.

我们研究的目的是设计出基于 SIP 协议的，在不对 NAT 设备的配置进行任何修改、不对具有 NAT 功能的设备进行任何升级，不修改用户的终端设备的前提下，使得语音透明通过 NAT 的解决方案。开发出了在 VOIP 中更为实用的软件，完成 NAT 环境下 IP 终端之间互相通信的测试，并改善了一些性能。本论文着重于基于 SIP 的 VoIP Server 的研究，实现和性能上的改进。

## 1.4 作者的工作和实现情况

经过近一年的研究和开发，作者最终在 Linux 平台上完成了预定的研究目标。同时也看到了不少的有待解决的新问题。

在研究过程中做的主要工作是:

第一: SIP 协议虽然比 H323 有诸多的优点，但 H323 相对应用的比较成熟，支持的厂商比较多。而新兴的 SIP 有些地方还待完善，还没有多少厂商进行大规模的商用。所以可借鉴的资料和经验并不多。所以作者花在调研的时间比较多。

第二: 作者经过大量的调研，在深刻理解了相关 RFC 的基础上，总结了多种穿越 NAT 的方案。通过分析比较，提出了自己的方案，并加以论证和实施。

第三: 设计了信令穿越 NAT 的具体方案，用代码实现了信令穿越 NAT。

第四:定义了 MPMS，并设计，实现了该服务器，从而完成了媒体流穿越 NAT 的工作。

第五:通过一些算法和工程处理方式改善了系统的性能。

第六:在实践中发现了一些问题，解决了部分问题，也为今后的研究提出了一些新问题。

目前该系统已在中信网络运行，不光做过国内通话的测试，也做过国际语音业务的测试，效果良好。

## 1.5 论文的主要内容与结构

文章共分为七章.

第一章为绪论。 主要介绍了研究背景。主要介绍了 VOIP 及其优点，比较了两个协议 SIP，H323 的优缺点.还指出了 VOIP 发展的关键技术与面临问题。最后介绍了作者的研究目

的和作者的工作情况。

第二章对有关的协议概述，并简介了 vocal 系统。 在协议概述中主要介绍了 SIP，SDP，RTP，RTCP 等协议，尤其重点介绍了 SIP 和 RTP 协议。 还简单介绍了我们用的 SIP 协议栈，VOVIDA 的 vocal 系统。

第三章分析了 NAT 和 NAT 对 VOIP 应用的影响.首先介绍了 NAT 与 Firewall 的产生背景与工作原理。 然后对 NAT 和 Firewall 的综合应用进行了分类。 另外，还分析了 NAT 对信令和媒体流影响的原因，为后来的分析和解决方案的提出做准备。

第四章提出了 8 种解决方案，分析比较这些解决方案的优缺点。 这 8 种解决方案有的是厂商已经用过的，有的是作者在制定方案过程中想出来的过渡方案，并不理想。 最终，制定了一个能够满足目标的方案。

第五章介绍了所选方案的系统结构;以及系统中各部分的实现。 先是拿出了所选方案的系统结构，然后按照程序设计的思路，将系统分成多个模块，对各个模块进行设计和实现。其中主要列出了 MS，MPMS 和 RS 模块。

第六章测试。可以说测试在作者的这个项目中占了很长时间。 首先是测试内容的分析，测试方法的选择，测试环境的搭建，然后是测试工具的选择，都影响着项目的进度。 作者通过局域网内模拟公网的穿越 NAT 的测试，找到一些问题，修改后，将系统真正放在公网上测试， 测试了国内和国际的语音业务，都取的良好的效果。 但在处理多路通话并发时遇到了瓶颈问题，经过对方案的改进，改善了通话的质量。 另外在测试中还发现了一些其他问题，有的已经解决，有的还有待今后解决。

第七章是对作者先前工作的总结，也对这个课题的将来做了新的展望。

# 第二章 协议概述与 VOCAL 简介

要解决语音穿越 NAT 问题，主要问题实现信令和媒体流的通信。下面重点介绍本论文所涉及的信令控制协议 SIP，会话描述协议 SDP，以及媒体的实时传输协议 RTP。

## 2.1 SIP 协议概述[14]

SIP 协议是一个用于建立，更改和终止多媒体会话的应用层控制协议[3]。它是 IETF 多媒体数据和控制体系结构的一部分。该协议大量借鉴了成熟的超文本传输协议（Hyper Text Transfer Protocol，HTTP）协议，并且具有易扩展，易实现等特点。

正如 SIP 名字所隐含的——用于发起会话。它可以用来创建、修改以及终结多个参与者参加的多媒体会话进程。参与会话的成员可以通过组播方式、单播连网或者两者结合的形式进行通信。

SIP 中有客户机和服务器之分。客户机是指为了向服务器发送请求而与服务器建立连接的应用程序。用户助理（User Agent）和代理（Proxy）中含有客户机。服务器是用于向客户机发出的请求提供服务并回送应答的应用程序。共有四类基本服务器：

a) 用户助理服务器（User Agent Server，UAS）：当接到 SIP 请求时它联系用户，并代表用户返回响应。

b) 代理服务器（Proxy Server）：代表其它客户机发起请求，既充当服务器又充当客户机的媒介程序。在转发请求之前，它可以改写原请求消息中的内容。

c) 重定向服务器（Redirect Server）：它接收 SIP 请求，并把请求中的原地址映射成零个或多个新地址，返回给客户机。

d) 注册服务器（Register Server）：它接收客户机的注册请求，完成用户地址的注册。

用户终端程序往往需要包括用户助理客户机和用户助理服务器。代理服务器、重定向服务器和注册服务器可以作为公众性的网络服务器。在 SIP 中还经常提到定位服务器的概念，但是定位服务器不属于 SIP 服务。

SIP 在设计上充分考虑了对其它协议的扩展适应性。它支持许多种地址描述和寻址，包括用户名@主机地址、被叫号码@PSTN 网关地址、普通电话的描述等。这样，SIP 主叫按照被叫地址就可以识别出被叫在传统电话网上的位置，然后通过一个与传统电话网相连的网关发起并建立呼叫。SIP 最强大之处就是用户定位功能。SIP 本身含有向注册服务器注册的

功能，也可以利用其它定位服务器 DNS（Domain Name System）、LDAP（Lightweight Directory Access Protocol）等提供的定位服务来增强其定位功能。

SIP 共规定了六种信令：INVITE、ACK、CANCEL、OPTIONS、BYE、REGISTER。其中 INVITE 和 ACK 用于建立呼叫，完成三次握手，或者用于建立以后改变会话属性；BYE 用以结束会话；OPTIONS 用于查询服务器能力；CANCEL 用于取消已经发出但未最终结束的请求；REGISTER 用于客户向注册服务器注册用户位置等消息。

SIP 协议支持三种呼叫方式：由用户助理客户机（User Agent Client，UAC）向用户助理服务器（UAS）直接呼叫，由 UAC 在重定向服务器的辅助下进行重定向呼叫和由代理服务器代表 UAC 向被叫发起呼叫。

SIP 协议可以与其它协议相互合作，例如：RSVP 用于预约网络资源，RTP 用于传输实时数据并提供服务质量（QoS）反馈，RTSP（Real-Time Stream Protocol）[15]用于控制实时媒体流的传输，SAP（Session Announcement Protocol）用于通过组播发布多媒体会话，SDP 用于描述多媒体会话。但是 SIP 协议的功能和实施并不依赖这些协议。

### 2.1.1 SIP URL （SIP 统一资源定位器）

SIP 寻址的对象是主机所带的用户，由 SIP URL（Uniform Resource Locator，统一资源定位器）标识。SIP URL 的表示方法为用户@主机（user@host）。用户部分是用户名或电话号码。主机部分是域名或用数字表示的网络地址。

用户的 SIP 地址可以由带外（out-of-band）获得，可以通过现有媒体代理（例如：目录服务器，DNS 服务器）得到，可以包含在某些邮件的消息头中，或者可能记录在以前的邀请过程里。

一个 SIP 地址可以指定个人、一个团体中第一个有空的人或者是整个团体。地址的格式，例如：sip:liutao@bupt.edu.cn，通常并不足以表达主叫的意图。

如果用户选择了能够从他的姓名和组织联系推测的地址，那么传统的用不公开电话号码的方法来保证隐私的方法就会受到威胁。但是与传统电话不同的是，SIP 协议提供身份验证和访问控制机制，并且还可以利用底层安全机制，因此客户程序可以拒绝未授权或不受欢迎的呼叫尝试。

### 2.1.2 SIP Location Server

SIP Location Server 用来定位。当客户需要发送请求时，它要么发送到在本地配置好的 SIP 代理服务器上（就像 HTTP 协议）不管 Request-URI（Uniform Resource Identifiers，统一

资源标识符）是什么，要么发送到 Request-URI 所对应的 IP 地址和端口。

对于第二种情况，客户必须确定目的服务器的协议、IP 地址和端口。客户应该按照以下步骤来得到这些信息。除非另外规定，客户每一步都应该用 Request -URI 中列出的端口号与服务器联系。如果 Request-URI 中未列出端口号，就使用默认端口 5060。如果 Request-URI 中指定了传输协议（TCP 或 UDP）就用该协议，否则用 UDP（如果支持 UDP）。如果尝试失败，或客户不支持 UDP，再尝试 TCP。

客户应该能够解释明确的网络通知（如因特网控制报文协议 ICMP 消息），例如：服务器不可达，而不是仅依靠超时机制（time-out）。如果客户发现在某个地址上服务器不可达，就应该采取与收到 400 类错误响应相同的措施。

客户通过查询 DNS 来得到一个或多个 SIP 服务器地址。其过程如下：

1.如果 Request-RUI 的主机部分是一个 IP 地址，客户就用它与服务器联系。否则进行下一步。

2.客户查询 DNS 服务器得到 Request-URI 主机部分所对应的 IP 地址。如果 DNS 没有返回地址记录，客户就终止，因为无法定位服务器。

对于如何选择 SIP 服务器的主机名并没有强制规定，但鼓励用户使用 sip. domain name（例如：sip.bupt.edu.cn）的形式命名他们的 SIP 服务器。用户可能只知道被叫的电子邮件地址而不是一个完整的 SIP-URL。这时，用给电子邮件地址的域名部分加“sip.”前缀拼成一个 SIP URL 来与服务器通信的实现可能性会增加。将来，这种实现方法可能没有必要，因为更好的 DNS 技术将被广泛应用。

客户可以将成功的 DNS 查询结果缓存起来。一个成功的查询在其返回结果中包含服务器的地址记录，可用其中的任何一个地址与服务器联系。当用户想给同一个主机发送消息时，它必须像刚收到名字服务器的回答一样开始查询。客户的操作必须遵循 RFC1035 中有关 DNS 过期后缓存失效的规程。

### 2.1.3 SIP 事务

一旦主机部分被 SIP 服务器解析，客户就可以向服务器发出请求并且从服务器接收响应。一个请求（包括重发的）与由它引发的所有响应构成一个 SIP 事务。针对同一个请求的所有响应都包含相同的 Call-ID、CSeq、To 和 From 头域（可能再加一个 To 域所带的标签（tag））。这样就能使响应和请求相匹配。跟在 INVITE 请求之后的 ACK 请求并不属于该事务，因为它可能经过不同的主机集合。

如果使用 TCP 协议，那么一个 SIP 事务的所有请求和响应都通过一个 TCP 连接来传送。

同一个客户向同一个服务器发送的多个 SIP 请求可以使用相同的 TCP 连接，也可以为每个请求建立新的连接。

如果客户用单播 UDP 发送请求，那么响应就被发送到 Via 头域中包含的下一个地址。如果用组播（multicast）UDP 发送请求，那么响应就被发送到相同的组播地址和端口。对 UDP，可以用重传机制来获得可靠性。

SIP 的消息格式和操作是独立于传输协议的。

### 2.1.4 SIP 邀请

一个成功的 SIP 邀请包括两个请求，INVITE 后面跟一个 ACK。INVITE 请求邀请被叫加入某个会议或建立一个两点的会话。当被叫发出同意加入呼叫的响应以后，主叫要向它发送一个 ACK 请求来确认已经收到了这个响应。如果主叫不想参与这个呼叫，它应发送一个 BYE 请求而不是 ACK。

一个 SIP 请求典型地包含一个会话描述（例如用 SDP 协议），为被叫提供充分的信息以便加入会话。对多点会话来说，会话描述列举了允许向整个会话发布的媒体类型和格式。对单点会话来说，会话描述列举了主叫所期望的媒体类型、格式以及可用于接收媒体数据的地址。不管是哪种情况，如果被叫接受呼叫，它就会在响应中返回类似的描述来列出它希望使用的媒体。对于多点会话，只有当被叫不能接受主叫所描述的媒体或是它希望通过单播来接收数据时才应该返回会话描述。

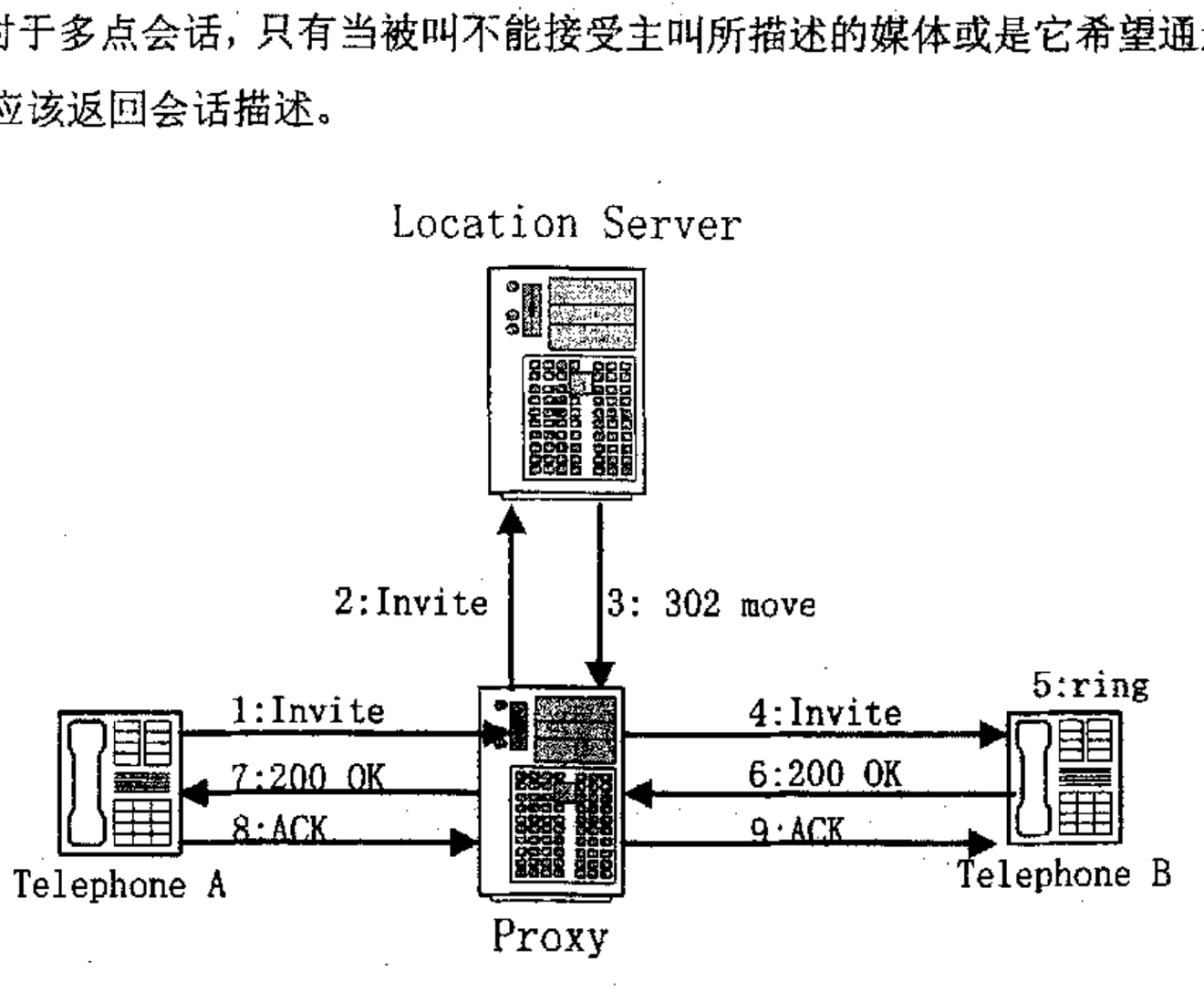


图 2—1：SIP 基本呼叫信令流程

上图显示了协议中 INVITE 方法是如何与代理服务器交互的。 下面那张图显示了 INVITE 方法是如何与重定向服务器交互的。上图中，代理服务器收到 INVITE 请求 （第 1

步），向定位服务器查询全部或部分地址（第 2 步），得到更确切的地址（第 3 步）。然后代理服务器向定位服务返回的地址发送一个 SIP INVITE 请求（第 4 步），用户助理服务器提醒被叫（第 5 步）并返回一个成功指示给代理服务器（第 6 步）。代理服务器向主叫返回成功消息（第 7 步）。主叫再向被叫发送一个 ACK 请求（第 8 步）表示确认该消息。注意：ACK 请求也可以不经过代理服务器直接发送给被叫。所有的请求和响应拥有相同的 Call-ID。

### 2.1.5 用户注册

客户可以发送 REGISTER 请求使代理服务器或重定位服务器知道它的地址，也可以用这个消息向服务器建立它的呼叫特性。

用户使用 REGISTER 消息将 To 头域中列出的地址注册到服务器上。用户助理客户可以在该地址侦听，获得其它用户的位置，但它们不响应该消息。因为请求是按到达顺序被处理的，用户应该在收到一个注册请求的响应以后再发送另外一个请求。

REGISTER 消息的头域包含如下内容：

To：包含需要新建或更新注册的 address-of-record。

From：包含登记负责者的 address-of-record。

Request-URI：包含注册的目标，即注册成员的地址。

Call-ID：所有由同一个客户发出的注册请求应含有相同的 Call－ID。

CSeq：具有相同 Call－ID 的请求的 CSeq 应该是递增的。

Contact：所有将来向 To 域中的地址发出的请求都应重定向到这个头域中包含的地址。如果请求中不包含 Contact 头域，则原注册保持不变。

服务器可以选择任意时间段作为注册的生命期。到期的未更新的注册会被自动清除。对注册请求的响应中包含 Expire 头域指出该次注册的生命期，默认值是一小时。客户也可以在注册请求的 Expire 头域中提出对生命期的要求。服务器实际采用的生命期不能超过客户请求的值。

客户可以发出一个期望生命期为零，Contact 头域是“*”的注册请求来实现注销。

REGISTER 请求消息应该经过认证，因为它可以用来重定向以后的请求。

## 2.2 SDP（Session Description Protocol）协议概述[6]

### 2.2.1 功能概述

会话启动协议是在 RFC 2327 中定义的。RFC 摘要中写到："SDP 是为了会话通告、会话邀请和其他形式的多媒体会话启动而描述多媒体会话过程。"[7]所谓多媒体会议就是多媒体发送者、接收者和从发送者到接收者的数据流的集合。视频电话会议呼叫就是多媒体会话的一个典型例子。Internet 一般采用松弛方式实现多媒体会议，其主要机制就是通过会话公告（session announcement）将会议的地点、时间、媒体和建立等信息告知每一个可能的参会者。用户收到此公告，获知会议的多播组地址和数据流的 UDP 端口号后，就可以自由的加入此会议。SDP 传送这类会话信息的协议。SDP 语法简单易懂，已经被接受作为基于文本的 IP 信令协议中呼叫参数协商的编码方法。它定义了会话描述的统一格式，但是不定义多播地址的分配方案和 SDP 消息的放松，也不支持媒体编码方案的协商，这些功能均由下层传送协议完成。

SDP 描述的信息封装在传送协议中发送，典型的会话传送协议包括：会话公告协议（SAP）、SIP、RTSP、HTTP 和使用 MIME（Multipurpose Internet Mail Extensions）的 E-mail。

采用 SIP 传送时，其数据包格式为"头部+文本净荷"，头部属于 SIP 呼叫控制信息，文本净荷就是 SDP 会话描述部分描述的媒体信息。

SDP 传递的是多媒体会话的媒体流信息，这些媒体流是多点到多点信息流，且只在规定的时间区段内存在，这些时间区段可能是不连续的，但可以重复发生。SDP 描述有两个目的，一是告知某会话的存在，二是给出参与该会话所必需的信息[27]。

1. SDP 描述包括：

会话名和目的；会话激活的时间区段；构成会话的媒体；接收这些媒体所需的信息（地址、端口、格式等）；会话所用的带宽信息（任选）；会话负责人的联系信息（任选）。

2. 媒体信息的具体内容包括：

媒体类型（视频、音频等）；传送协议（RTP/UDP/IP、H.320 等）；媒体格式（H.261 视频、MPEG 视频等）；媒体地址和端口。

3. 时间信息的具体内容包括：

会话的开始和结束时间，可用多组时间段；对于每个时间段，可以指定重复时间。

除此以外，SDP 还可以创建专用会话，即该会话描述需作加密处理。此时，会话传送

协议必须能传送解密密钥及加密方法等信息。

### 2.2.2 SDP 格式

SDP 会话描述完全是文本形式，采用 UTF-8 编码的 ISO10646 字符集。之所以采用文本形式而不采用诸如 ASN.1 的二进制编码方式，是为了提高描述的可携带性，使其可以用各种传送协议传送，并可用各种文本工具软件生成和处理会话描述。为了减少描述所用的开销，便于差错检测，SDP 采用了紧凑型编码，并且严格规定了各字段的顺序和格式。

SDP 会话描述由许多文本行组成，每个文本行的格式均为：<type>=<value>

其中，<type>恒为单个字符，需区分大小写。<value>为结构化文本串，其格式取决于<type>，也需区分大小写。一般由多个字段组成，各字段由一个空格符分隔，也可以是一个自由格式的文本串。“=”符号两侧不允许有空格。

会话描述包括两个部分：会话级描述和媒体级描述。会话级描述部分给出适用于整个会话和所有媒体流的描述信息，它以“v=”文本行开始。媒体级描述部分给出只适用于该媒体流的信息，它以“m=”文本行开始。一个会话描述可以包含零个或多个媒体级描述。如果在媒体级描述中没有重新定义，会话级描述给定的值就是所有媒体的缺省值。

SDP 定义的类型（type）字母很少。如果 SDP 语法分析器不能识别描述中的某一类型字母，则应将整个描述丢弃。属性机制（“a=”行）供 SDP 扩展其应用或媒体范围，可以根据应用、媒体或会话的需要增加属性值。如果接收方不理解某属性值，则予以丢弃。

## 2.3 RTP 实时传输协议[5]

实时传输协议 RTP 是最典型、最广泛的服务于流媒体的传输层协议，VoIP 系统普遍采用 RTP 协议。

RTP 是用于 Internet 上针对多媒体数据流的一种传输协议[17]。RTP 被定义为在一对一或一对多的传输情况下工作，其目的是提供时间信息和实现流同步。RTP 通常使用 UDP 来传送数据，但 RTP 也可以在 TCP 或 ATM（Asynchronous Transfer Mode）等其他协议之上工作。当 RTP 工作于一对多的传输情况下时，依靠底层网络实现组播，利用 RTP over UDP 模式实现组播的传输就是其典型应用。RTP 传输协议有如下一些特点：

### 1. 协议灵活性

RTP 协议不具备传输层协议的完整功能，其本身也不提供任何机制来保证实时地传输数据，不支持资源预留，也不保证服务质量。RTP 报文甚至不包括长度和报文边界的描述，而

是依靠下层协议提供长度标识和长度限制。另外，RTP 协议将部分传输层协议功能（比如流量控制）上移到应用层完成，简化了传输层处理，提高了该层效率。

### 2. 数据流和控制流分离

RTP 协议的数据报文和控制报文使用相邻的不同端口，这样大大提高了协议的灵活性和处理的简单性。

### 3. 协议的可扩展性和适用性

RTP 协议通常为一个具体的应用来提供服务，通过一个具体的应用进程实现，而不作为 OSI（Open System Interconnection）体系结构中单独的一层来实现，RTP 只提供协议框架，开发者可以根据应用的具体要求对协议进行充分的扩展。

虽然 RTP 协议是为多媒体数据流传输而设计的，但是其用途不仅限于此，RTP 协议还可以用于连续数据的存储，交互式分布仿真和一些控制、测量的应用中。

## 2.4 RTCP 传输控制协议

RTP 协议本身包括两部分：RTP 数据传输协议和 RTCP 传输控制协议。为了可靠、高效地传送实时数据，RTP 和 RTCP 必须配合使用，通常 RTCP 包的数量占所有传输量的 5%。

RTP 实时传输协议主要用于负载多媒体数据，并通过包头时间参数的配置使其具有实时的特征。RTCP 传输控制协议主要用于周期的传送 RTCP 包，监视 RTP 传输的服务质量。在 RTCP 包中，含有已发送的数据包的数量、丢失的数据包的数量等统计资料。因此，服务器可以利用这些信息动态地改变传输速率，甚至改变有效载荷类型，实现流量控制和拥塞控制服务。下文将对 RTP 传输协议和 RTCP 传输控制协议分别进行描述。

RTP 本身并不能为按顺序传送数据包提供可靠的传送机制，也不提供流量控制或拥塞控制，它依靠传输控制协议 RTCP 提供这些服务。

RTP 的控制协议 RTCP 通过在会话用户之间周期性地递交控制报文来完成监听服务质量和交换会话用户信息等功能。根据用户间的数据传输反馈信息，可以制定流量控制的策略，而会话用户信息的交互，可以制定会话控制的策略。

RTCP 协议将控制包周期发送给所有连接者，应用与数据报文相同的分布机制。底层协议提供数据与控制包的复用，如使用单独的 UDP 端口号。

RTCP 执行下列四大功能

（1）提供数据发布的质量反馈，这是 RTCP 最主要的功能。作为 RTP 传输协议的一部分，与其他传输协议的流和阻塞控制有关。反馈对自适应编码控制直接起作用。反馈功能由

RTCP 发送者和接收者报告执行。

（2）发送带有称作规范名字（CNAME）的 RTP 源持久传输层标识。如发现冲突，或程序重新启动，既然 SSRC 标识可改变，接收者需要 CNAME 跟踪参加者。接收者也需要 CNAME 与相关 RTP 连接中给定的几个数据流联系。

（3）用于控制 RTCP 包数量的数量用语。前两种功能要求所有参加者发送 RTCP 包，因此，为了 RTP 扩展到大规模数量，速率必须受到控制。

（4）传送最小连接控制信息。如参加者辨识。最可能用在“松散控制”连接，那里参加者自由进入或离开，没有成员控制或参数协调，RTCP 充当通往所有参加者的方便通道，但不必支持应用的所有控制通讯要求。

RTCP 报文格式与 RTP 报文类似，包括固定的报文头部分和可变长结构元素，结构元素的意义由 RTCP 报文的类型决定，因为通常 RTCP 包非常小，一般把多个 RTCP 包合并为一个 RTCP 包，然后利用一个底层协议所定义的报文格式进行发送。

RTCP 报文头部参数首先要区别携带不同控制信息的 RTCP 报文的类型，RTCP 报文的类型主要有以下几种：（1）SR：发送报告，当前活动发送者发送、接收统计。（2）RR：接收报告，非活动发送者接收统计。（3）SDES：源描述项，包括 CNAME。（4）BYB：表示结束。（5）APP：应用特定函数。

其中最主要的 RTCP 报文是 SR 和 RR。通常 SR 报文占总 RTCP 包数量的 25%，RR 报文占 75%。类似于 RTP 数据包，每个 RTCP 报文以固定的包头部分开始，紧接着的是可变长结构元素，但是以 32 位长度为结束边界。在 RTCP 报文中，不需要插入任何分隔符就可以将多个 RTCP 报文连接起来形成一个 RTCP 组合报文。由于需要底层协议提供整体长度来决定组合报文的结尾，所以在组合报文中没有单个 RTCP 报文的显式计数。

RTCP 控制报文的发送周期是变化的，与报文长度 L、用户数 N 和控制报文带宽 B 相关：周期 P=L×N / B。原因是 RTP 设计成允许应用自动扩展的模式，连接数可从几个到上千个。在一般的音频会议中，因为同一时刻一般只有两个人说话，所以数据流和控制流都是内在限制的，控制流不会对传输造成影响。而在组播发送模式下，给定连接数据率独立于用户数，仍是常数，但控制流量不是内在限制的。如果每个参加者以固定速率发送接收报告，控制流量将随参加者数量线性增长，因此，速率必须按比例下降。

## 2.4 VOCAL 简介[29]

我们所做的研究是在在 Linux 系统下，基于 vovida 开放源代码 VOCAL[27]（版本 1.5.0）。该开放源代码是 Cisco 公司 VoIP 工作组在 UNIX 下做的一个 SIP 协议的实现，该实现包括

了 SIP 协议中所定义的客户端和服务器的基本功能.但在实际应用中还有一些功能和性能上的问题需要解决. Vocal 支持 Session Initiation Protocol (SIP， RFC 3261)， MediaGateway Control Protocol (MGCP ) 和 H.323 设备.也支持通过相关网关连接的模拟电话。

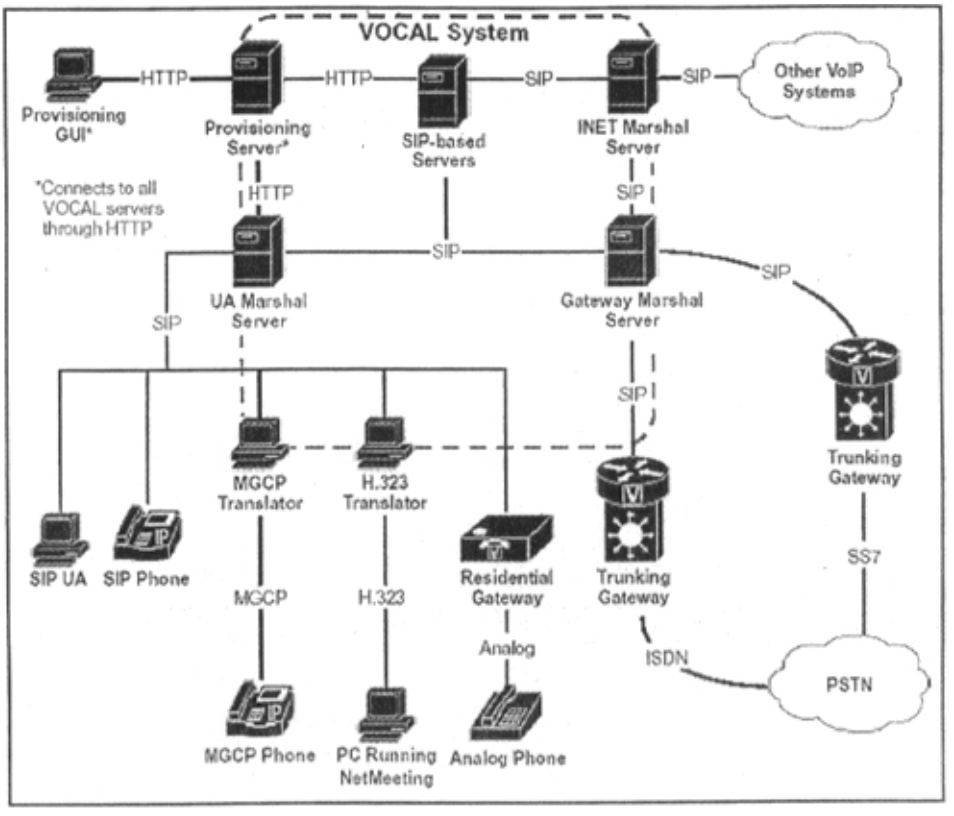


图 2—2：Vocal 结构图

图中就是一个 vocal 系统的系统组成.在这里我们主要注意它关于基于 SIP 的通话功能的模块，从图中来看，就是 UA Marshal Server，以后简称 MS，Provisioning Server，简称 PS 还有 SIP-based Servers 中的 Redirect Server，简称 RS，和通称为终端的 SIP UA，SIP Phone. 在后面的的五章中会详细介绍它们的功能和工作原理。

# 第三章 NAT/Firewall 及其对 VOIP 的影响

## 3.1 NAT/Firewall 概述

### 3.1.1 NAT 与 Firewall[11]

1. NAT [18] [20]

网络地址转换（NAT）是一个 Internet 标准，置于两网间的边界，其功能是将公网可见的 IP 地址与私网所用的地址相映射，这样，每一受保护的私网可重用特定范围的 IP 地址(例如 192.168.x.x)，而这些地址是不用于公网的。从公网来的含公网地址信息的数据包先到达 NAT，NAT 使用预设好的规则(其组元包含源地址、源端口、目的地址、目的端口、协议)来修改数据包，然后再转发给私网接受点。对于流出私网的数据包也须经过这样的转换处理。NAT 服务有两个主要目的：

许多公司使用 NAT 用作一个网络安全设备，因为它隐藏了内部 IP 地址，如果黑客不知道特定计算机的 IP 地址，想要攻击那台计算机是更困难的。

NAT 让一个公司可以使用更多的内部 IP 地址，因为这些地址仅仅在内部使用，不可能与被别的公司和组织的 IP 地址产生冲突。

2. 防火墙 [33] [34]

为了网络的安全性，公司一般都安装防火墙，它是一个放于私有网的设备，用来保护网络资源免受外部的恶意破坏。

防火墙检查从外部进来的每个数据包的 IP 地址和目的端口号，它经常如此设置：如果防火墙内的一台计算机 A 向防火墙外的一台计算机 B 主动发出请求要数据，防火墙会让外部计算机 B 的数据包通过，而且当且仅当数据包的目的地址和端口号与防火墙内发起请求的计算机 A 的地址和端口号相同；如果计算机 B 发来的数据包仅仅目的地址是防火墙内发起请求的计算机 A 的地址，而端口号不是计算机 A 发出请求的那个端口号，防火墙也将会丢弃那个外来的数据包。

防火墙总是被配置过滤掉所有不请自到的网络通信，有一个例外是在防火墙内提供 Web Server 供外部访问。在这种情况下，公司会配置防火墙允许目的地址是 Web Server 的 IP 地址且目的端口号为 80 的数据包通过，这就使得公司外部可以主动向公司的 Web Server 发起

请求得到一些公司放在 Server 上的数据。

### 3.1.2 NAT/Firewall 分类

在实际应用过程中，许多用户，尤其是企业常常将 NAT 与 Firewall 结合起来使用，这样的情况更复杂，本文在不说明的情况下，所说的 NAT 泛指 NAT 与 Firewall 的结合使用。在结合使用的情况下，可以分成 4 类。

1. Full cone(完全模式):

私网地址和端口与它对外表现的地址和端口是对应的，公网主机 IP3，Port3 可向 IP 2，Port 2 发包，再由 NAT 根据地址映射池向 IP 1，Port 1 发包。


图 3－1：NAT/Firewall 分类（1）

2. Restricted Cone(限制模式):

私网地址和端口与它对外表现的地址和端口是对应的，但与 full cone 不同的是，只有当私网先向 IP 3 发包后， NAT 才不会阻拦来自 IP 3 的包。

3. Port Restricted Cone(端口限制模式):

与 Restricted 相似， 私网地址和端口与它对外表现的地址和端口是对应的，但只有当私网先向 IP 3 的 Port 3 发包后， NAT 才不会阻拦来自 IP 3 的 Port 3 的包。

4. Symmetric(对称模式):

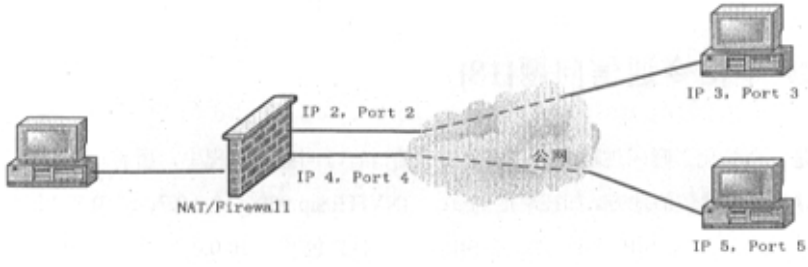


图 3－2：NAT/Firewall 分类（2）

来自 IP 1，Port 1，到 IP 3，Port3 的包对外表现的地址与同样来自于 IP 1，Port 1 但目

标是到 IP 5，Port 5 的包对外表现的地址是不同的。

## 3.2 在基于 SIP 协议的 VOIP 应用中，NAT 带来的问题

基于 IP 的语音和视频通讯协议，如 SIP，要求终端之间使用 IP 地址和数据端口来建立数据通信通道。因此存在一个两难境地：为了建立数据连接终端必须随时侦听外来的呼叫，而防火墙却通常被配置来阻止任何不请自到的数据包通过。

即使网络管理者打开防火墙上的一个端口来接收呼叫建立数据包，例如 5060 端口，但 IP 语音和视频通讯协议还要求打开许多别的端口接收呼叫控制信息来建立语音和视频通道，这些端口号事先并不知道，是动态分配的，这也就是说网络管理者为了允许语音和视频通讯将不得不打开防火墙上所有的端口，防火墙也就失去了存在的意义。由于网络安全的原因，很少企业会让他们的网络防火墙如此开放。

在 IP 语音和视频通讯中 NAT 问题也是常见的问题。一个 NAT 设备允许一个公司为局域网上设备分配私有的 IP 地址。不幸的是控制 Internet 上信息流向的路由设备仅仅能把数据送到具有可路由 IP 地址（公众 IP 地址）的设备。

NAT 后的终端可以向位于相同局域网上的任何别的终端发起呼叫，因为在局域网内的这些 IP 地址是可路由的，然而他们的 IP 地址是私有的，对局域网外来说是不可路由的，因此 NAT 后的终端不能接收局域网外终端的呼叫。

即使 NAT 内的终端可以向 NAT 外的终端发起呼叫，这仍然存在问题。当进行呼叫时，发起呼叫的终端 A 的 IP 地址会包含在数据包负载中，根据 SIP 协议被呼叫的终端 B 收到呼叫建立(call setup)数据包后，会从该数据包负载中获取终端 A 的 IP 地址，并开始发送音频和视频数据到这个 IP 地址的终端 A。如果这个 IP 地址是私有的，Internet 路由器将丢弃从外部终端发送往内部终端的音频和视频数据包，因为这些数据包正被送往一个不可路由的 IP 地址。这个呼叫将显示已经连接上，但 NAT 后的终端 A 将永远不会收到外部终端 B 的音频和视频。

### 3.2.1 VOIP 中信令通信问题[18]

图 3—3 是一个简化了呼叫过程图。在这个简单的语音呼叫业务过程中，所有打着红叉的地方都是 NAT 阻碍通信的地方。如在对应的 3： INVITE sip:999@10.0.0.7：5060 SIP/2.0（SDP of 10.0.0.2:5004），SIP Proxy 会把这 SIP 的 INVITE 包发到 10.0.0.7 地址的 5060 端口上，但实际按照最严格的 NAT（上面讨论的 Symmetric 模式的 NAT），这个包是无法到达话机 B 的，通话当然也无法建立，因为话机 B 在 NAT 后，网络无法正确的直接路由的。其他的几个有红叉的地方也有类似的问题。

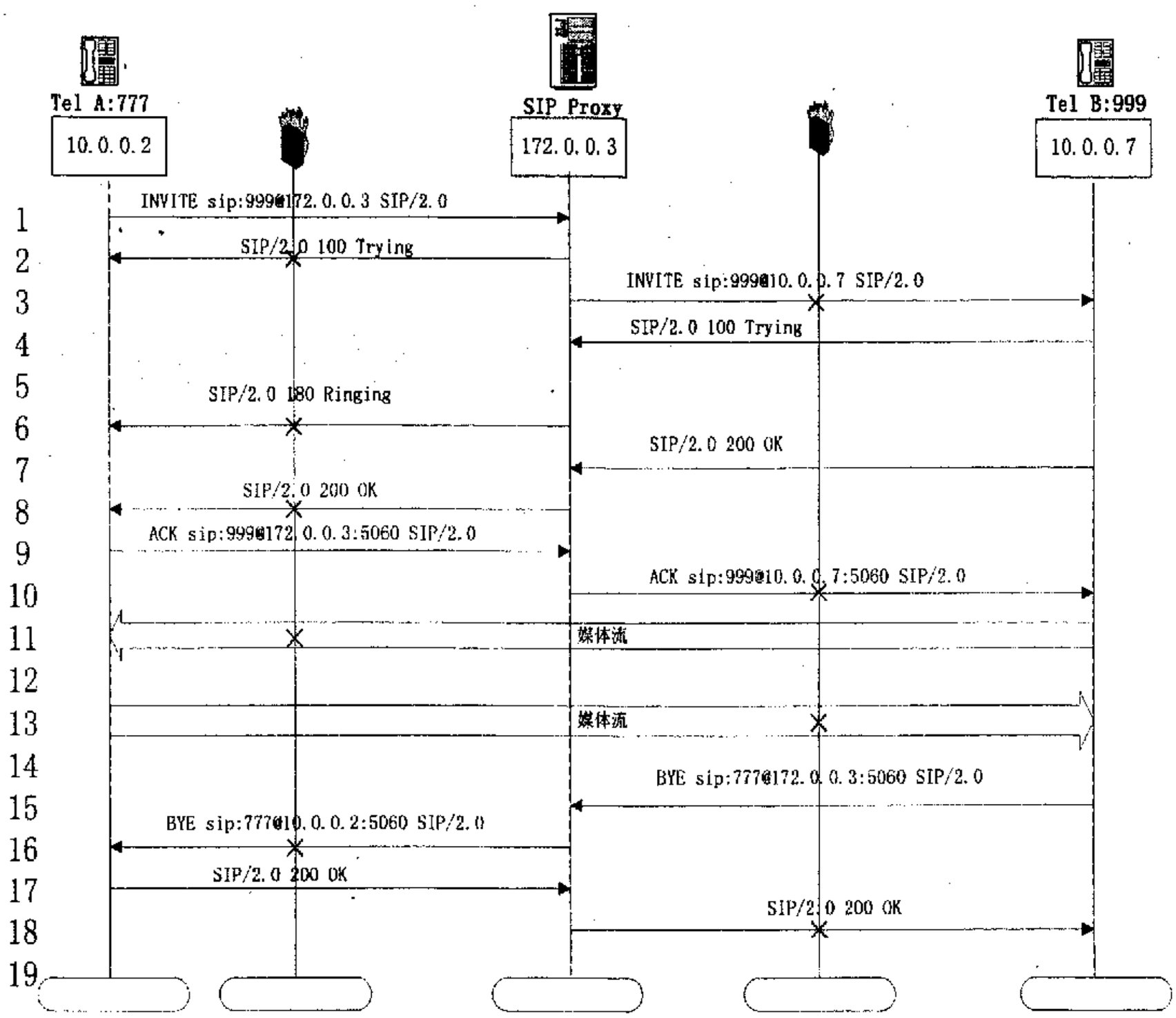


图 3—3：NAT 对信令和媒体流地影响

## 3.2.2 VOIP 中媒体流通信问题[18]

同样，多媒体协议一般使用 RTP 来传输媒体流。RTP 使用 UDP 协议，而且没有固定的端口。当 A 呼叫 B 时，INVITE 包里的 SDP 就描述了话机 A 为通话所准备的地址与端口 如 10.0.0.2:5004 ，这样在通话正常建立起来后，话机 B 的媒体流 RTP 包的目的地址，就应该是 10.0.0.2:5004 ，但有 NAT 的影响，这个包是无法到达 A 的。同样的道理，B 在给 A 发回 SIP 包 200 OK （SDP of 10.0.0..7:5005）时也告诉 A 了准备的地址与端口，A 在通话建立后，向 10.0.0..7:5005 发的包一样遭到 NAT 的影响，无法到达目的地址。

# 第四章 解决方案的制定与分析比较

## 4. 1 各种方案及其优缺点[24] [32]

其实解决防火墙和 NAT 问题的一个最简单的办法就是避免使用它们，对大多数机构来说，这种方法太冒险，网络安全没有保证，而且要得到足够多的可路由的 IP 地址或许是困难的，昂贵的。因此大多数希望利用 IP 进行多媒体通讯的机构将不可避免的面对防火墙或 NAT 的挑战。事实上，大多数机构都同时使用了防火墙和 NAT，因此单单解决其中一个问题还不够。现有的一些解决办法如下：

### 4.1.1. 使用 PSTN 网关

如果不太关心在局域网外是否基于 IP 通信，那么可以使用网关把局域网上的 IP 语音和视频转换为公共电路交换网上的 PSTN 语音和视频。使用这样一个网关就不用关心网络防火墙的穿透问题了，因为没有数据包要通过防火墙。这也解决了 NAT 问题，所有到局域网内终端的呼叫都是可路由的，因为通过网关进入局域网的呼叫都是可路由的。今天大多数 IP 电话都是通过一个网关和非 IP 电话来进行通讯的。网关方法是一个局部解决方案，要求所有参与呼叫者在最后一道 NAT 和防火墙后要有一个相应的网关。

### 4.1.2. DMZ Proxy

通过把 MS 放在所谓的 DMZ 区域来解决防火墙和 NAT 穿越问题。DMZ 是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。网络结构如下图所示。

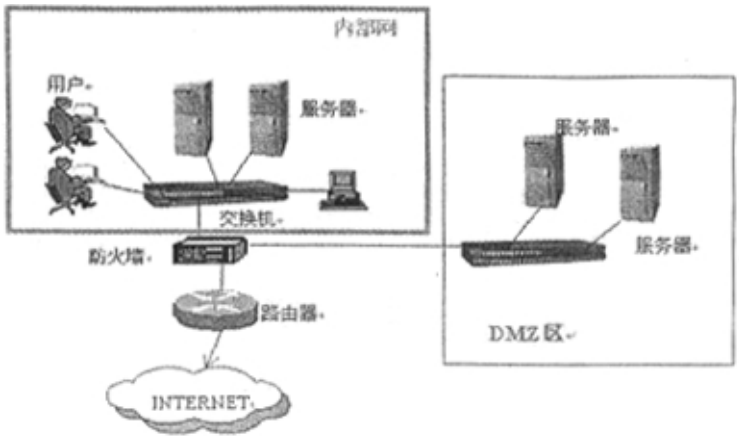


图 4－1：DMZ 网络结构

放在 DMZ 区域的 Proxy 被装上两块网卡，这样一块网卡提供访问私有网络的入口，另一块网卡提供访问公网 Internet 的入口。这个解决方案的一个最大缺点是即使是进行点对点的呼叫也得需要使用 Proxy，另外如果在呼叫路径上有多个 NAT 设备，那么在每个 NAT 设备的位置都需要放置一个 Proxy。

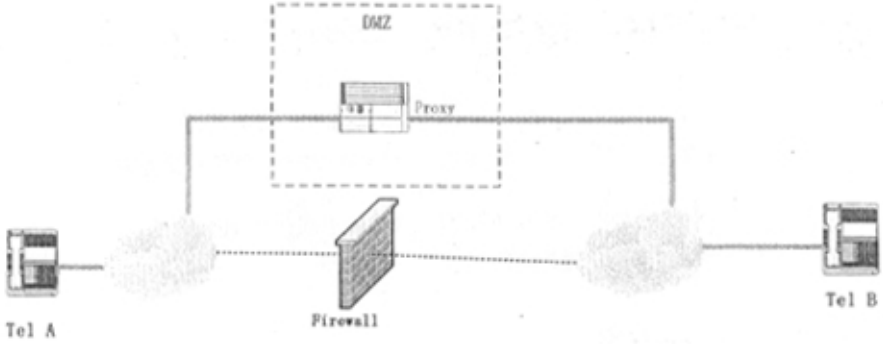


图 4－2：利用 DMZ 穿越 NAT

## 4.1.3. 应用层网关[26]

应用层网关（Application layer gateways）是被设计能识别指定 IP 协议（如 H.323 和 SIP 协议）的防火墙，也被叫做 ALG Firewall。它不是简单地察看包头信息来决定数据包是否可以通过，而是更深层的分析数据包负载内的数据，也就是应用层的数据。H.323 和 SIP 协议都在负载中放了重要的控制信息，例如语音和视频终端使用哪一个数据端口来接收别的终端的语音和视频数据。通过分析哪一个端口需要打开，防火墙动态地打开那些被应用的端口，

而所有别的端口依然安全地保持关闭状态。

如果一个 NAT 被应用来屏蔽内部 IP 地址，这时 ALG 就需要一个代理，一些防火墙生产厂商把代理结合到 ALG 上越过 NAT。

主要的防火墙厂商如 Cisco， Checkpoint， Gauntlet 都对他们的防火墙产品提供 H.323 ALG 升级功能，但市场上大多数防火墙还不支持 ALG。这种解决方案还有一些缺点：由于要分析数据包负载，这样就加重了防火墙的处理任务，影响网络的运行，成为潜在的网络瓶颈；并且如果这儿有多层防火墙和 NAT，则在呼叫路径上的每个防火墙都必须被升级来支持 ALG 功能；对大多数公司的网络来说防火墙是关键部件，在一些公司增加一个 ALG 或许是困难的。

### 4.1.4. 虚拟专用网(VPN)

VPN 技术是当前在 IP 网络上提供安全通讯的方法之一，在同一个 VPN 网内可以解决防火墙穿越问题；不久的未来，确保网络安全和 QoS 的 VPRN 技术将是 IP 网上进行多媒体通讯的最有潜力的解决方案。

在 VPN 技术中，在 UDP 和 TCP 层下的 IPSec 层被用来提供安全的 IP 通讯，但由于基于 VPN 技术的 IPSec 层使用它自己的连接标识符而不是 UDP 或 TCP 端口，而且 IPSec 上面的层要被加密，这套自己的机制对 NAT 尤其是 NAPT 是不可通过的。为了解决 NAT 穿越问题，最好选择由一个生产商提供的整合防火墙，NAPT 和 VPN 功能的解决方案。

另外，虽然 VPN 方案是很安全的，但它仅仅允许位于同一个 VPN 内的设备进行通讯，而无法与位于公众网的终端用户进行通讯。

### 4.1.5. 隧道穿透方案

一般企业网都不想升级或者改动他们的防火墙和 NAT 设备的配置，也不想让内外的交互通讯绕过这些设备，采用允许 IP 语音和视频穿越防火墙和 NAT 的隧道穿透方案也许是最合适的，目前提供此类解决方案的有美国的 Ridgeway 公司。

隧道穿透解决方案由两个组件构成，Server 软件和 Client 软件。Client 放在防火墙内的私有网，它同时具有 UA 功能和代理功能，私有网内的终端注册到 Client 上，它和防火墙外的 Server 创建一个信令和控制通道，可以把所有的注册和呼叫控制信令转发到 Server，也把音视频数据转发到 Server，在转发时它把内部终端发送的和外部发往终端的数据包的地址和端口号替换为自己的。Server 放在防火墙外的公众空间，可以位于服务提供商网络或者位于

企业网的 DMZ 区域，Server 扮演代理的角色，从 Client 收到的所有注册和呼叫信令都被 Server 转发到 SIP Proxy。

Server 和 Client 之间的通讯主要通过两个固定的端口来传输数据，这两个端口是 2776 和 2777 端口，被 IANA 机构分配给 Ridgeway 的系统。

当私网内 Client 启动时：

1．它与 Server 上的 2776 端口建立一个固定连接用来传送控制和状态信息；

2．它监听私网内 SIP 终端注册和请求信息；

当一个终端启动时：

1．终端通过 Client/Server 之间的连接发送注册信息到中心呼叫控制中心；

2．Server 分配给每一个注册的终端一个唯一的端口号（与 Server 的 IP 地址对应）。

当一个终端呼叫防火墙外的另一个终端时，所有的数据包都通过 Client 路由到 Server，返回的数据也从 Server 通过 Client 路由回到终端。当呼叫被建立后，Client 确保所有必需的经过防火墙的音视频通道保持开放，这样音视频数据可以通过这些防火墙上开放的通道进行传输。

使用这种方法 IP 地址信息被很好的屏蔽，因为所有的数据包通过 Server 来路由转发，每个终端好像看来在直接地和 Server 进行通信，而不是和别的终端，这保证了终端的 IP 地址在网络外不可得到。而且这种方法在大多数情况下不用对防火墙配置进行任何修改。对于那些防火墙设置限制打开向外的端口的情况，管理员可以创建简单的原则来允许从 Client 到 Server 上两个固定的端口 2776 和 2777 的向外的连接。

这个方法不仅仅局限于企业应用，服务提供商可以把 Server 放在 ISP 网络的中枢向小企业和用户提供防火墙和 NAT 穿越服务。不管是企业用户还是服务提供商应用，呼叫终端变得如此简单，仅需下载一个 Client 软件装在 PC 上，而且不用关心在呼叫建立的路径上存在多少个防火墙或 NAT 设备。

这个方法最大的缺点是所有经过防火墙的通讯都必须经由 Server 来进行中转，这会引起潜在的瓶颈，这个经由 Client 和 Server 的过程会增加少于 5ms 的延迟。但是这又是必须的，因为 Server 是防火墙唯一信任的设备。

### 4.1.6 STUN

STUN (Simple Traversal of User Datagram Protocol Through Network Address Translators ).RFC3489.要终端先向 Stun 服务器发消息，Stun 服务器检测出终端所在的 Nat 的对外 IP 和 Port，并告知终端，终端收到后向外发请求时，就用 Stun 告诉它的对外地址来构造 SIP 和 SDP 消息。目前来说：Stun 不能使 TCP 连接穿越 NAT;不能使 UDP 包穿越对称模式的 NAT;当通话双方再同一 NAT 后，使用 Stun 不能正常工作;Stun 是一个放在公网上的服务器。

### 4.1.7 B2BUA Server[25]

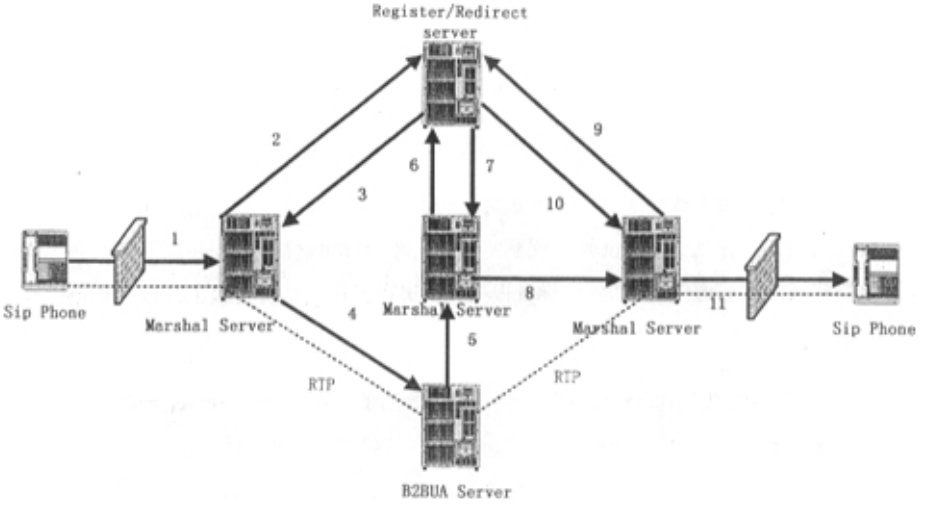


图 4－3：用 B2BUA Server 穿越 NAT 网络原理

draft-ietf-sip-rfc2543bis-04.txt[13]中 Back-to-Back User Agent（B2BUA）。背靠背用户助理：也称作 B2BUA。话机先向 Register Server 发注册包，返回来的 200 OK 会告诉话机在防火墙后，话机用 TCP 连接与 B2BUA 建立通道，以后话机的通话都通过 B2BUA 代理。当 B2BUA 收到来自终端的 INVIET 请求时，就作为一个逻辑实体用户助理服务器 UAS 对这个请求进行处理。为了响应这个请求，B2BUA 又作为用户助理客户端 UAC 向外发起请求。与代理服务器不同的是，B2BUA 保持有完整的呼叫状态，并且必须参与到一次呼叫的所有过程中。

### 4.1.8 WXH－BUPT 方案

作者的研究和试验工作都是在 vocal 的 SIP 协议栈上开展的。根据 vocal 的特点和 SIP 协议的特点，修改 vocal 各服务器之间交互的信令，从终端来看出去的和进来的信令都是标

准的 SIP 协议和 RTP，RTCP 协议增加相应的媒体流代理服务器。所做的修改都在服务器组里完成，与终端所处企业的 NAT 无关，也与终端无关。对于终端或者用户来说，他们无需知道他们是否在 NAT 后，只要遵循协议标准，就能正常通信。方案具体内容在第五章介绍。

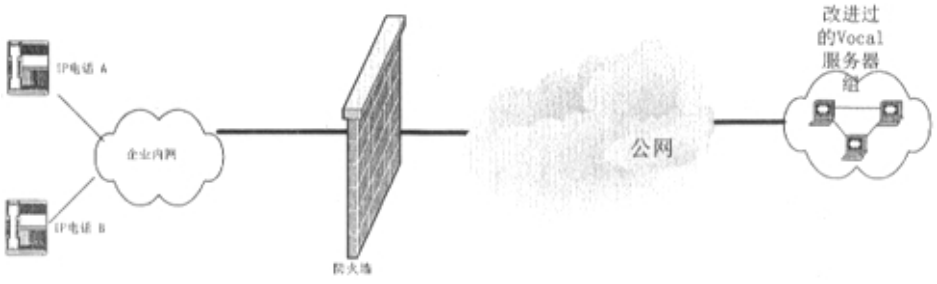


图 4－4：WXH－BUPT 方案

## 4. 2 解决方案的选择

以上所述的解决方案各有利弊，综合比较如下：

| | 适合企业还是 ISP | 是否需要对 NAT 进行升级 | 能穿越的 NAT 类型 | 是否需要附加设备 | 是否需要更改协议 |
|---|---|---|---|---|---|
| 使用 PSTN 网关 | 企业 | 否 | 1，2，3，4 | 是 | 否 |
| DMZ Proxy | ISP | 否 | 1，2，3，4 | 是 | 否 |
| 应用层网关 | 企业、ISP | 是 | 1，2，3，4 | 否 | 否 |
| 虚拟专用网 VPN | 企业 | 是 | 1，2，3，4 | 否 | 否 |
| 隧道 | 企业、ISP | 否 | 1，2，3，4 | 是 | 否 |
| STUN | 企业 | 否 | 1，2，3， | 是 | 是 |
| B2B Server | 企业、ISP | 否 | | 是 | 是 |
| WXH-BUPT 解 | 企业、ISP | 否 | 1，2，3，4 | 是 | 否 |

| | | | | | |
|---|---|---|---|---|---|
| 决方案 | | | | | |

表 4－1：各方案的比较

上表中 NAT 的分类是按（3.1.2）中的对 NAT 的分类规定的。具体如下：

1 －－ Full cone(完全模式)

2 －－ Restricted Cone(限制模式)

3 －－ Port Restricted Cone(端口限制模式)

4 －－ Symmetric(对称模式)

经过比较可以得到结论，WXH-BUPT 的方案的适用范围广，并且无需对 NAT 设备进行升级改造，也无需在内部网络中增加设备，更重要的是能透明穿透多层 NAT，相比较而言是最佳的解决方案。

# 第五章 所选方案的具体实现

## 5.1 系统结构

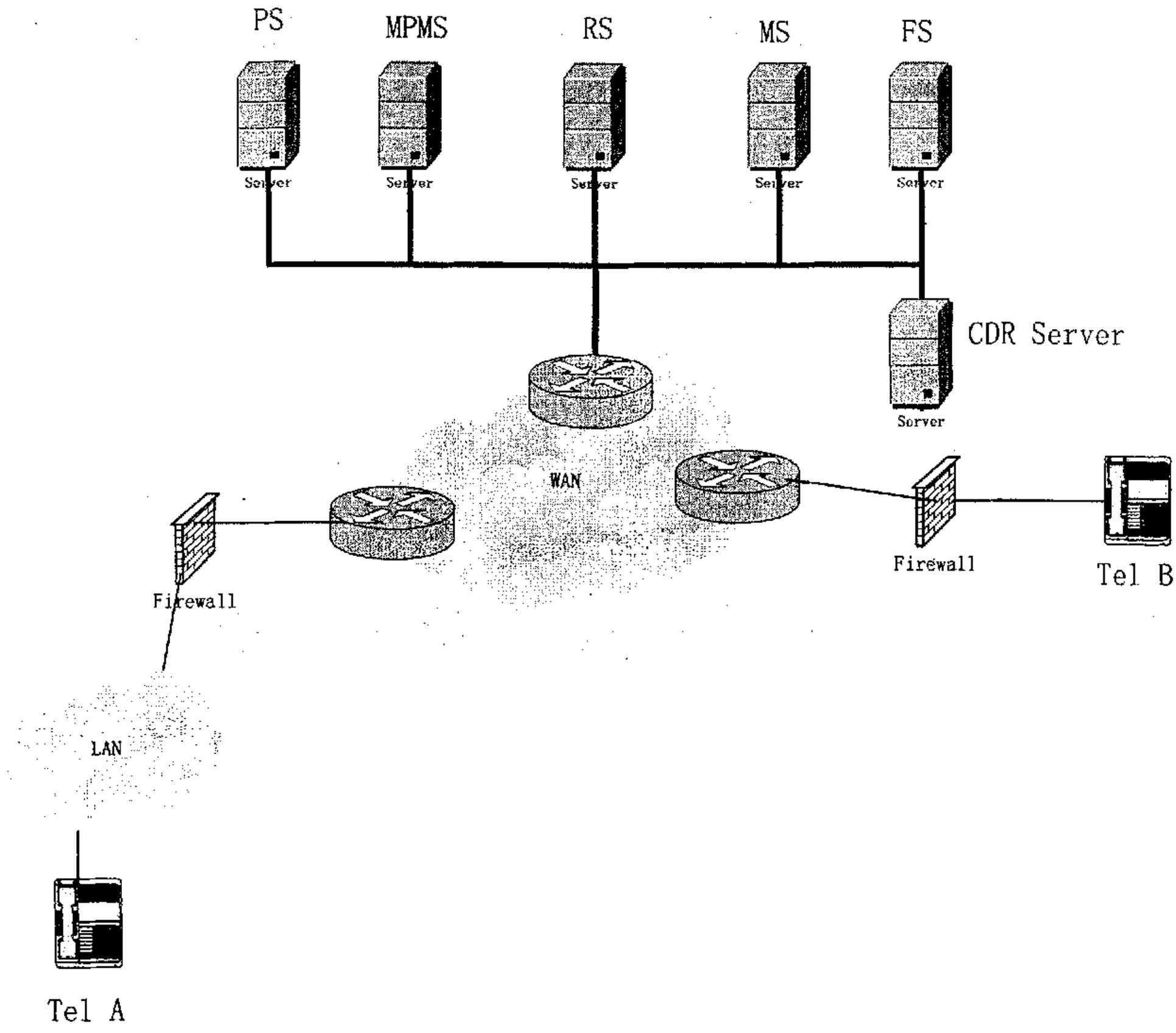


图 5－1：系统结构图

图中包含多个服务器和终端设备，其用途分别介绍如下。

**1. Tel A ， Tel B（User Agent－－SIP IP 电话终端）：**

可以是标准的，也可以是系统提供的。UA 可以是单独的硬件，也可以是运行在 PC 机上的软件。

**2. FS （Feature Server）：**

FS 服务器是 SIP 代理服务器的一种实现，用 CPL 脚本语言书写， Feature Server

提供一些可扩展性业务，如 Call Forward ， Call Screening， Call Blocking， Call Transfer， Call Return， Call Waiting 等业务。

### 3. CDR Server: [28]

CDR 服务器通过 TCP 连接与 Marshal server 通信，当呼叫开始时，Marshal server 通知 CDR 服务器，CDR 服务器记录主、被叫的电话号码、呼叫日期、呼叫时间、呼叫经过的 Marshal server 的 IP，并将数据传入数据库。当呼叫结束时，Marshal server 通知 CDR 服务器，CDR 服务器记录呼叫结束日期，呼叫结束时间并传入数据库。

### 4. MS （Marshal Server）

功能：作为 UA 的代理服务器提供注册，通话和认证服务；负责收集关于响铃时间，会话开始和结束时间的信息，通过 CDR API 向 CDR 汇报。是系统与外围设备连接的唯一接口，完成 Proxy、用户认证、计费功能。它对进入系统的消息进行检查与转换，并记录日志。它支持以下三种认证方式：无认证、基于 IP 的认证和基于 HTTP Digest 的认证。在信令穿越防火墙时，需判断所来 SIP 消息是否来自于 NAT 后，并对在上端个服务器中传送的消息修改以协助穿越 NAT。

接口：

MrshlOpRegister：处理 SIP 线程接收的 REGISTER 消息；

MrshlOpInvite：处理 SIP 线程接收的 INVITE 消息；

MrshlOpAck：处理 SIP 线程接收的 ACK 消息；

MrshlOpBye：处理 SIP 线程接收的 BYE 消息；

MrshlOpCancel：处理 SIP 线程接收的 CANCLE 消息；

MrshlOpStatus：处理 SIP 线程接收的状态消息；(包括 1××，2××，3××，4××，5××)

### 5. RS （Redirect Server）

功能：

1). 定制 RS 需要知道的关于用户的数据，包括用户的用户名，公、私网地址，相关的特征服务，以及相关信息的 timestamp，每次用户注册修改相关的 timestamp。

2）提供路由信息(DialPlanContainer)：

是一个有序列表，表项为正规表达式和目标矢量，为电话号码提供路由信息。如果被叫方的电话号码和一个正规表达式匹配，则相应的目标向量将呼叫路由到正确的服务器和终端上。要注意列表条目的顺序，首先匹配的条目将作为路

由信息。

3）RSMirror：

支持系统冗余。如果RS接收到的注册信息来自于其它的RS，则该RS不做任何工作，否则对接收到的注册信息做镜象复制到其它的RS。

4）RSServerContainer：

用于追踪活跃的服务器，当服务器出现故障时选择替代的服务器。RSServerContainer映射IP地址到一个结构，该结构提供服务器类型和该类型服务器所归属的组。组容器映射组名到该组内活跃服务器的列表，组内服务器能完成相同的功能。

5）HeartbeatTxThread(HBTx)：

定期发出一个heartbeat（是一个多点传送的UDP包），告诉其它的服务器它现在仍是活跃状态。发消息的时间间隔在PS中设置。

6）HeartbeatRxThread(HBRx)：

接收所有的heatbeat包，并在RS服务器容器内根据IP地址索引是否有该服务器。如果有记录，则RS查询该服务器的组名，RS能够在组容器内找到相应服务器的记录，加以标识表明收到该服务器的heartbeat。

7）Housekeeping：

定期运行，时间间隔同 heartbeats。它查看服务器容器内的各个服务器，如果该服务器发出了heartbeat，如果是则将未收到heartbeat的计数器加1，如果达到界值则housekeeping认为该服务器出错，则用该服务器所在组内其它的活跃服务器代替。

8）判断通话双方是否有任何一方在放火墙后，若有则重定向信令到MP。并且判断是否有重定向到MP的循环，并避免该循环。

接口：

OpAck：响应Sip线程接收的SIP ACK消息；

OpInvite：响应SIP线程接收的SIP INVITE消息；

OpOptions：响应SIP线程接收的SIP OPTIONS消息；

OpRegister：响应SIP线程接收到的SIP REGISTER消息；

OpStatus：响应SIP线程接收到的Status的状态消息；

## 6. PS （Provision Server）

功能：

1) 传输/协议模块：

负责与系统外部的交互。负责socket管理和传输层协议；

2) 命令模块：

负责解释发送给PS的命令行；

3) 数据存储模块：

a) 存储用户的基本信息、用户定制的特征服务等和各个服务器的配置信息；

b) 某些用户与某信息相关，则建立一个匹配图，该信息对应一用户组。该用户组内用户以IP地址和端口形式存储，则该信息改变时，则将相关修改快速的传递到对应的用户组内用户；

4) 参数配置模块：

读取运行服务器所需要的参数和相关信息；

5) 冗余 PS 之间的同步；

a) 冗余 PS 之间是 master 和 slave 的形式，每个 PS 上随机产生一个计时器，首先超时的 PS 成为 master，令一 PS 则成为 slave;

b) 监听冗余 PS 的心跳，结果不发送给其它的服务器；

c) 同步 PS。

6) 核心处理模块：

PS 的总控程序。系统启动时，从参数配置模块读取相关信息。

a) 分配线程处理各服务器上等待的需要处理的数据；（？）

b) 数据管理。

### 7. MPMS （media proxy marshal server）

功能：

1．作为穿越防火墙媒体流的代理服务器提供呼叫建立和通话服务。

2．在信令由 RS 转来时为通信双方在表目内增加一条记录，记录包括以下表项：(该记录在 MP 的代码中为一个呼叫资源 call source)

| Call_ID | IP_FWA | Port_FWA | Port_MPA | Port_MPB | IP_FWB | Prot_FWB |
|---|---|---|---|---|---|---|
| Call_ID(AB) | 0 | 0 | PMPA | PMPB | 0 | 0 |

其中此时填写为通信双方媒体流开的两个端口及 Call_ID，其余表项暂时为 NULL。

3．当 callee 返回 200OK 时根据记录内的表项 打开端口开端口，其中为 RTP 开偶数端口，RTCP 该偶数端口+1；

4．接收 caller 和 callee 发来的第一个 RTP 包，在表内相应的记录内记录通信双方经防火墙转变后的地址 IP:port；

5．修改呼叫建立时经过 MP 的 invite，和 200 OK 里的 SDP 内容；

6．在 Bye，或 Cancel 时删除地址映射表。

7．接收来自 MS 的关于通话没正常终止的信息，来删除地址映射表。（应该以 MS 为依据）。

接口：

``````MrshlOpRegister：处理 SIP 线程接收的 REGISTER 消息；

MrshlOpInvite：处理 SIP 线程接收的 INVITE 消息；

MrshlOpAck：处理 SIP 线程接收的 ACK 消息；

MrshlOpBye：处理 SIP 线程接收的 BYE 消息；

MrshlOpCancel：处理 SIP 线程接收的 CANCLE 消息；

MrshlOpStatus：处理 SIP 线程接收的状态消息：(包括 1××，2××，3××，4××，5××)

MPOpRtp：处理 MPMS 接收到的媒体流。

## 5. 2 系统各部分的实现

### 5.2.1 整体设计
``````

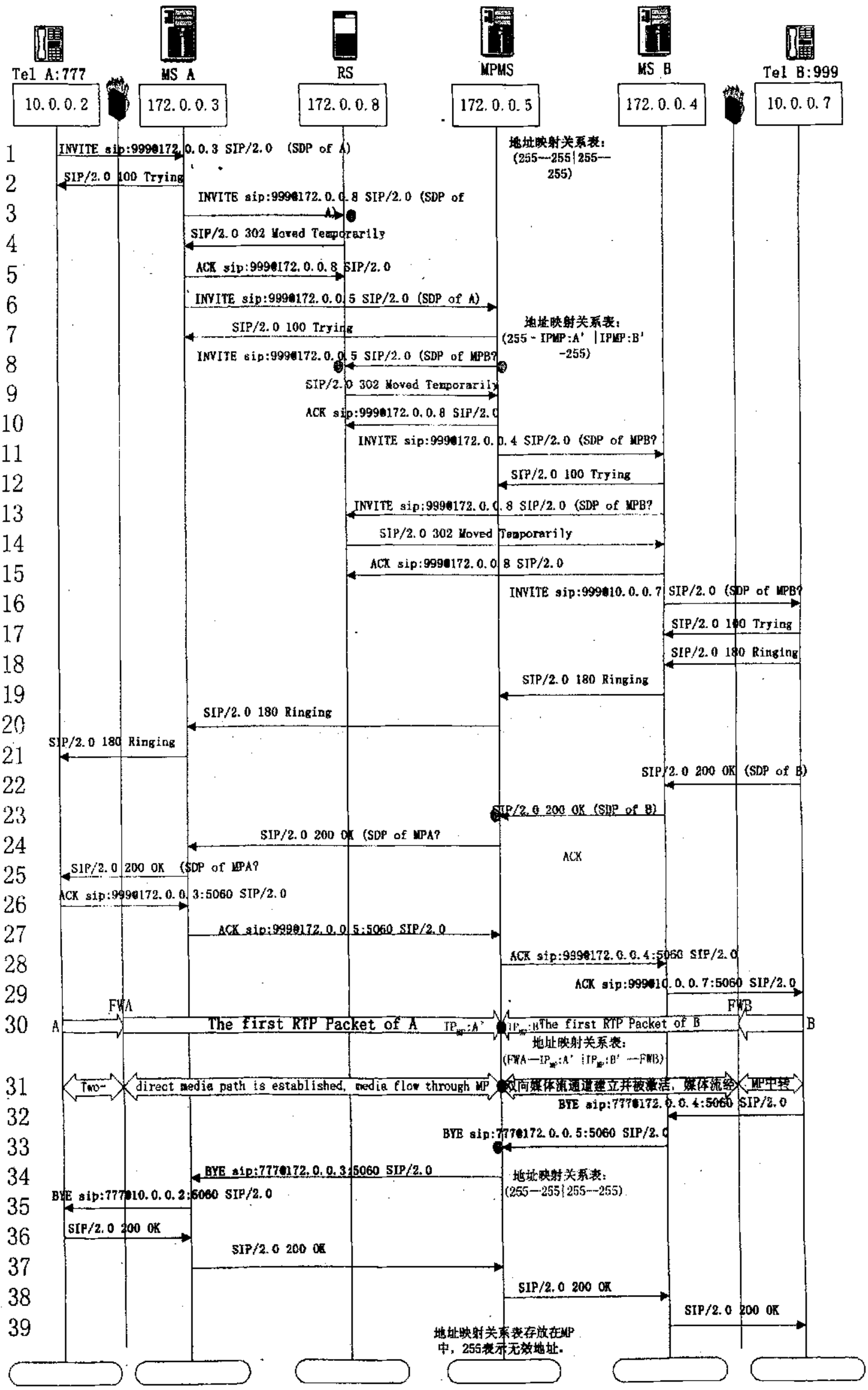


图 5—2：信令与媒体流流程图

功能上设计思路为：从终端的角度看，终端只需要发送和接受标准的 SIP 协议包，而真正的穿越 NAT 的工作都在上端完成，也就是说，任何遵循 SIP 协议标准的终端都可以实现信令与媒体流透明穿透 NAT。这就需要在上端对 SIP 信令中的一些关于地址的头域的内容根据他探测到的实际地址信息做一些修改。

系统的主要设备在各种业务中的关系。把各种设备看成模块，各业务与这些模块的关系是：

| | UA | PS | RS | MPMS | MS | PBX |
|---|---|---|---|---|---|---|
| 通话（公网，无防火墙） | m | o 1 | m | - | m | o 4 |
| 通话（公网，有防火墙） | m | o 2 | m | m | m | o 5 |
| 通话（私网） | m | - | - | - | - | m |
| 注册（向 RS） | m | o 6 | m | - | m | - |
| 注册（向 PBX） | m | - | - | - | - | m |
| Cancel（公网） | m | - | - | o 3 | m | - |
| Cancel（私网） | m | - | - | - | - | - |
| 呼叫转移 | m | o | o | o | o | o |

表 5—1：系统设备与业务关系

m：表示用例要用该模块。

- ：表示用例不用该模块。

o ：表示根据具体情况来决定。

o 1 ，o 2 ，o 6 表示在认证的时候可能要用到 PS。

o 3　表示如果呼叫建立是通过 MPMS 了，那 Cancel 时也要经过 MPMS。

o 4 ，o 5 表示如果私网有 PBX，则优先找 PBX，让 PBX 来重定向。

呼叫转移的几个 o 表示业务流程与原通话，待建立的新通话的双方所处情况来决定。

PBX 是为增强系统性能而添加的设备，如负责同一私网呼叫的交换，与 PSTN 互通。

## 5.2.2　主要模块直接合作图

### 5.2.2.1 与 MS 相关的主要操作

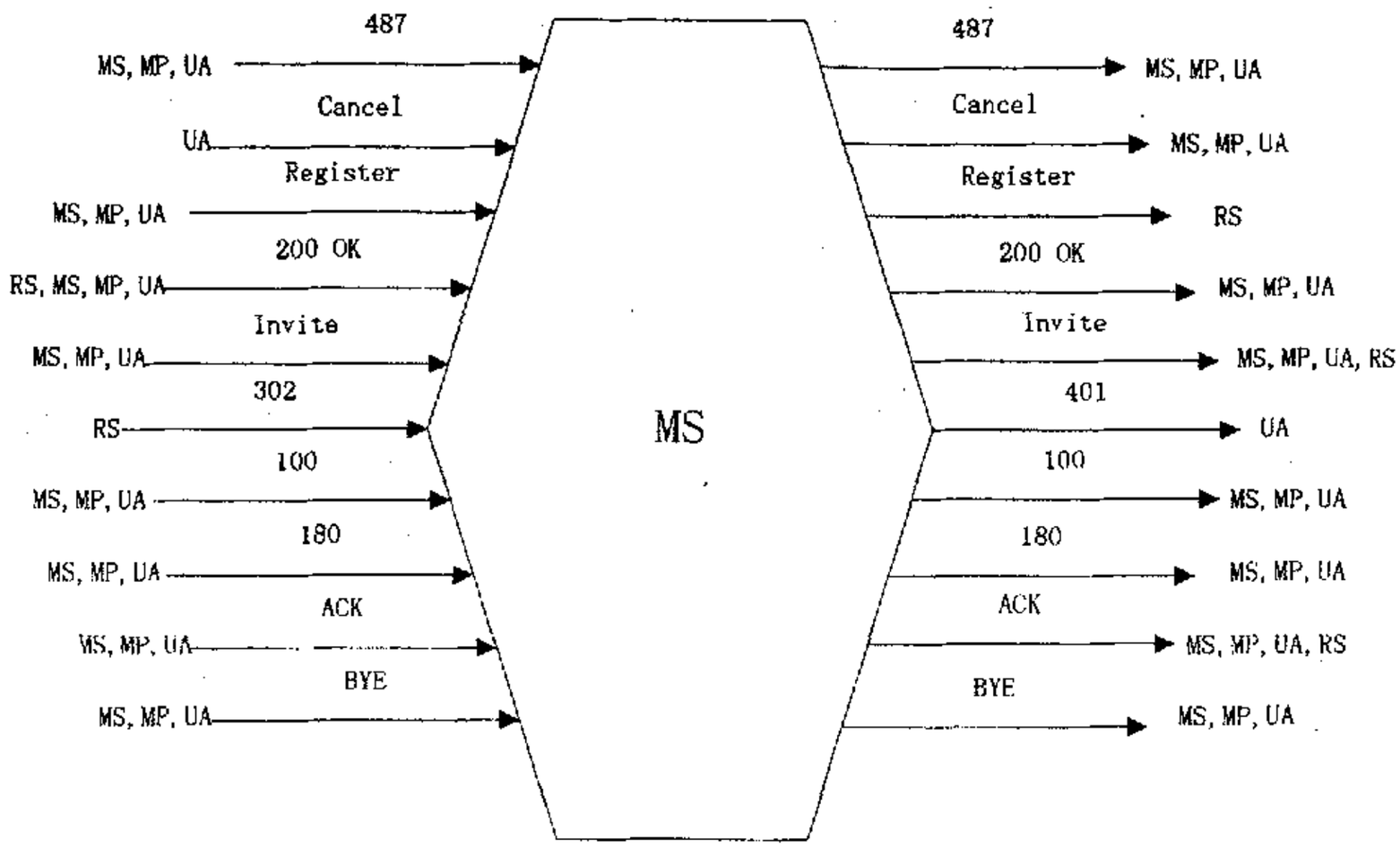


图 5—3：MS 模块合作图

MrshlOpRegister：处理 REGISTER 消息；

MrshlOpInvite：处理 INVITE 消息；

MrshlOpAck：处理 ACK 消息；

MrshlOpBye：处理 BYE 消息；

MrshlOpCancel：处理 CANCLE 消息；

MrshlOpStatus：处理状态消息；(包括 1××，2××，3××，4××，5××，6××)。

#### 5.2.2.2 与 RS 相关的主要操作

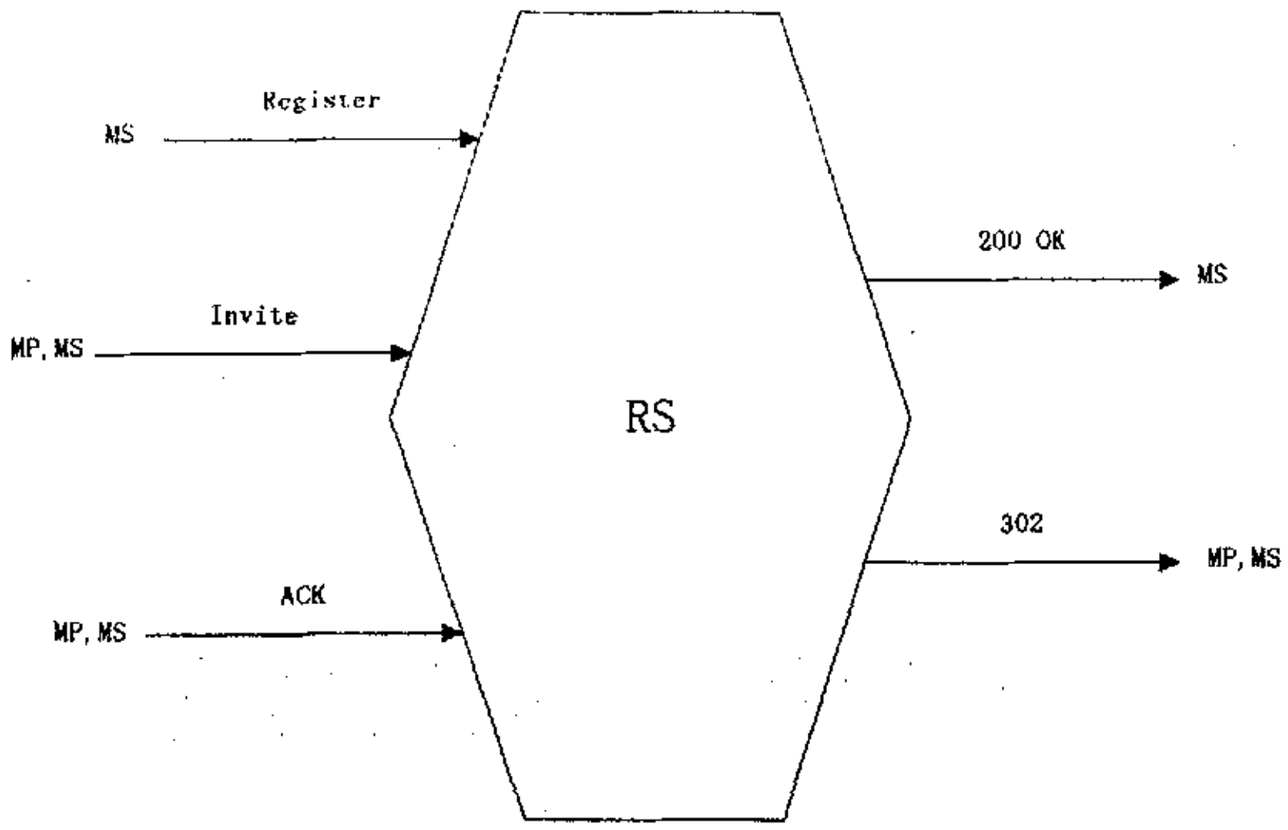


图 5—4：RS 模块合作图

OpAck：处理 ACK 消息；

OpInvite：处理 INVITE 消息；

OpOptions：处理 OPTIONS 消息；

OpRegister：处理 REGISTER 消息；
OpStatus：处理 Status 的消息；

#### 5.2.2.3 与 MPMS 相关的操作

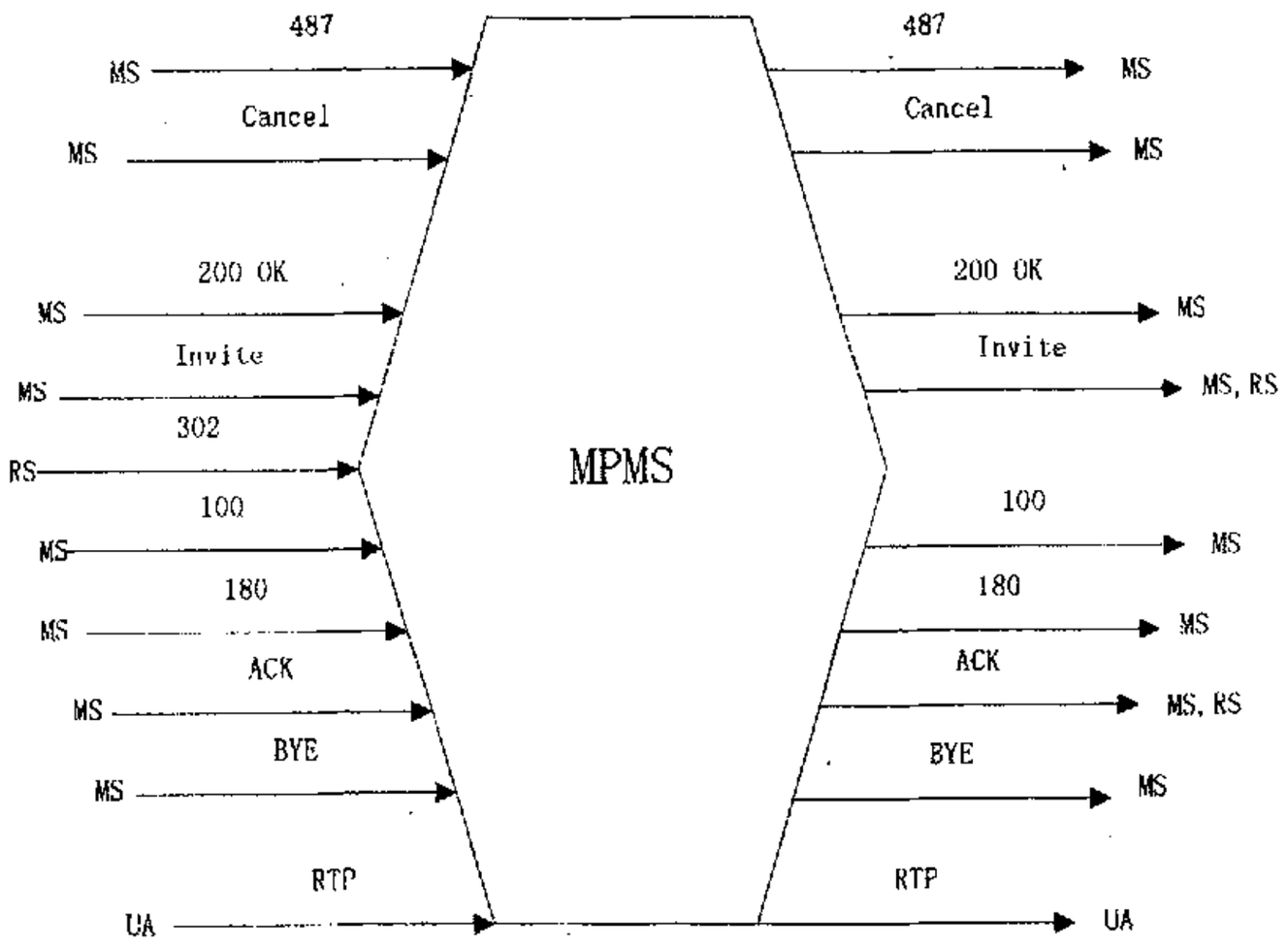


图 5—5：MPMS 模块合作图

MrshlOpRegister：处理 REGISTER 消息；
MrshlOpInvite：处理 INVITE 消息；
MrshlOpAck：处理 ACK 消息；
MrshlOpBye：处理 BYE 消息；
MrshlOpCancel：处理 CANCLE 消息；
MrshlOpStatus：处理状态消息；(包括 1××，2××，3××，4××，5××)
MPOpRtp：处理 MPMS 接收到的媒体流 RTP。

### 5.2.3 主要模块设计

#### 5.2.3.1 MS 模块

**1.MS 对 Register 的处理子模块**

MrshlOpRegister：处理 SIP 线程接收的 REGISTER 消息。
处理流程：

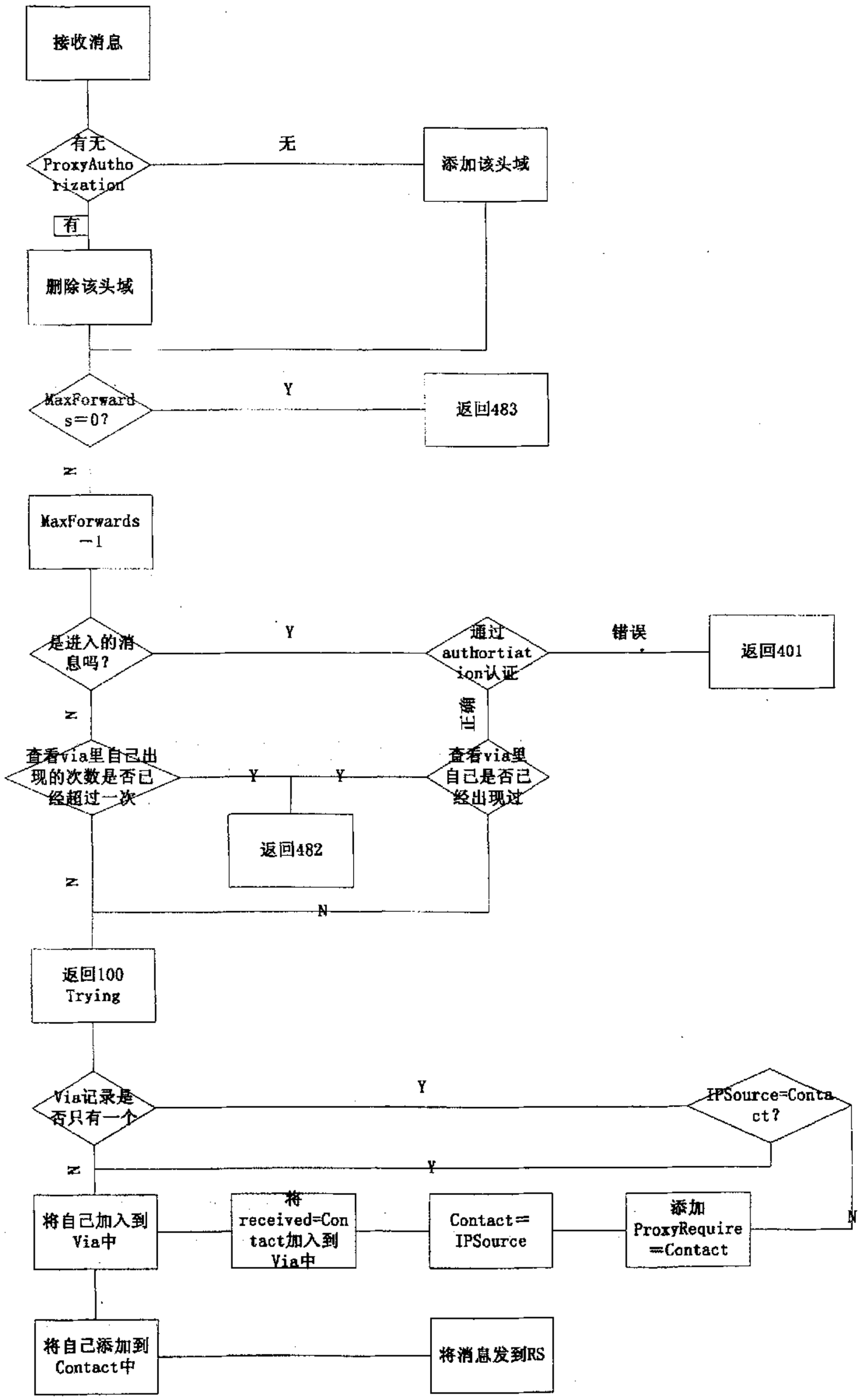


图 5—6：MrshlOpRegister 流程图

## 2.MS 对 Invite 的处理子模块

MrshlOpInvite：处理 SIP 线程接收的 Invite 消息。
处理流程：

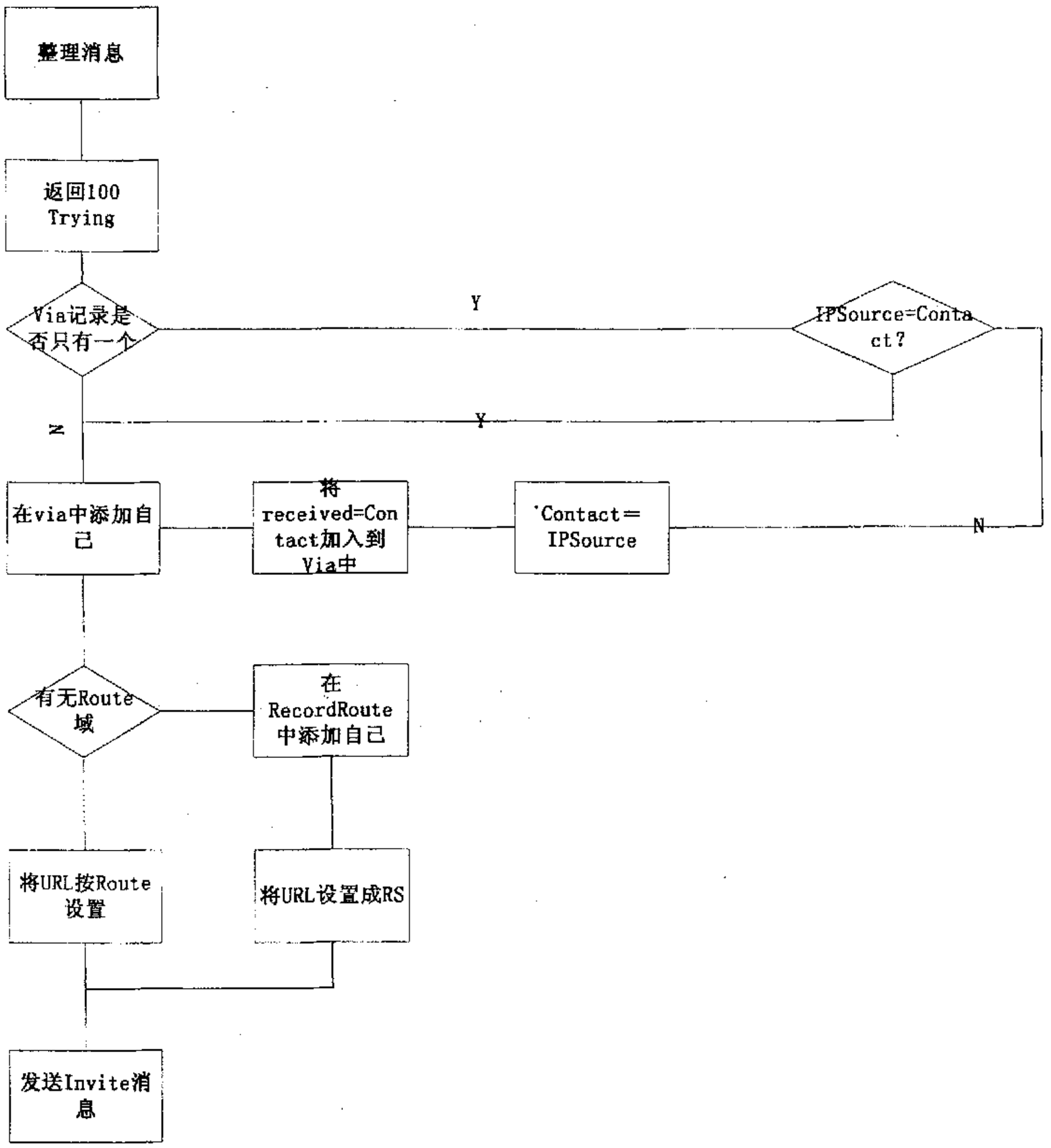


图 5－7：MrshlOpInvite 流程图

## 3.MS 对 ACK 的处理子模块

MrshlOpACK：处理 SIP 线程接收的 ACK 消息。
处理流程：

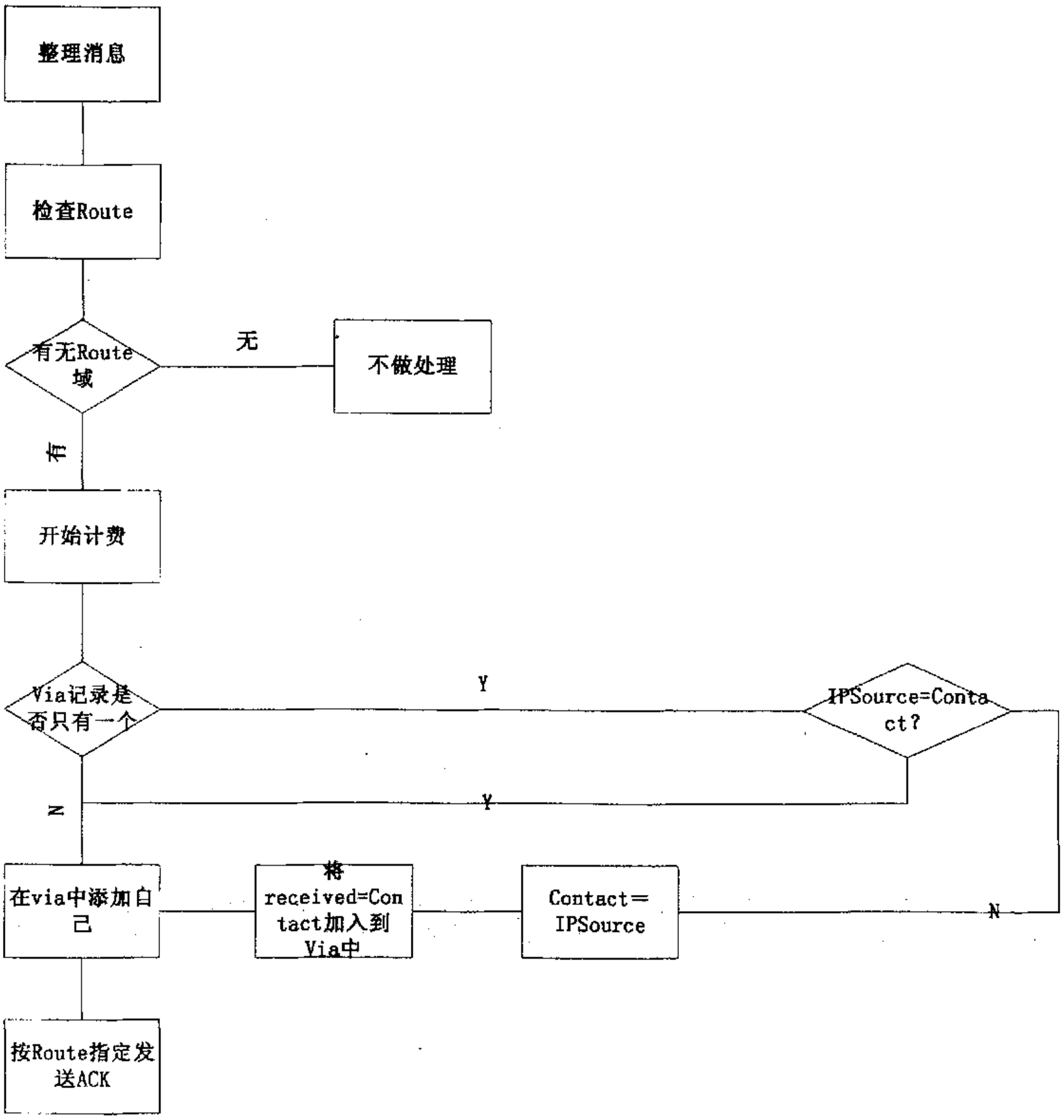


图 5－8：MrshlOpACK 流程图

## 4.MS 对 Bye 的处理子模块

MrshlOpBye：处理 SIP 线程接收的 Bye 消息。
处理流程：

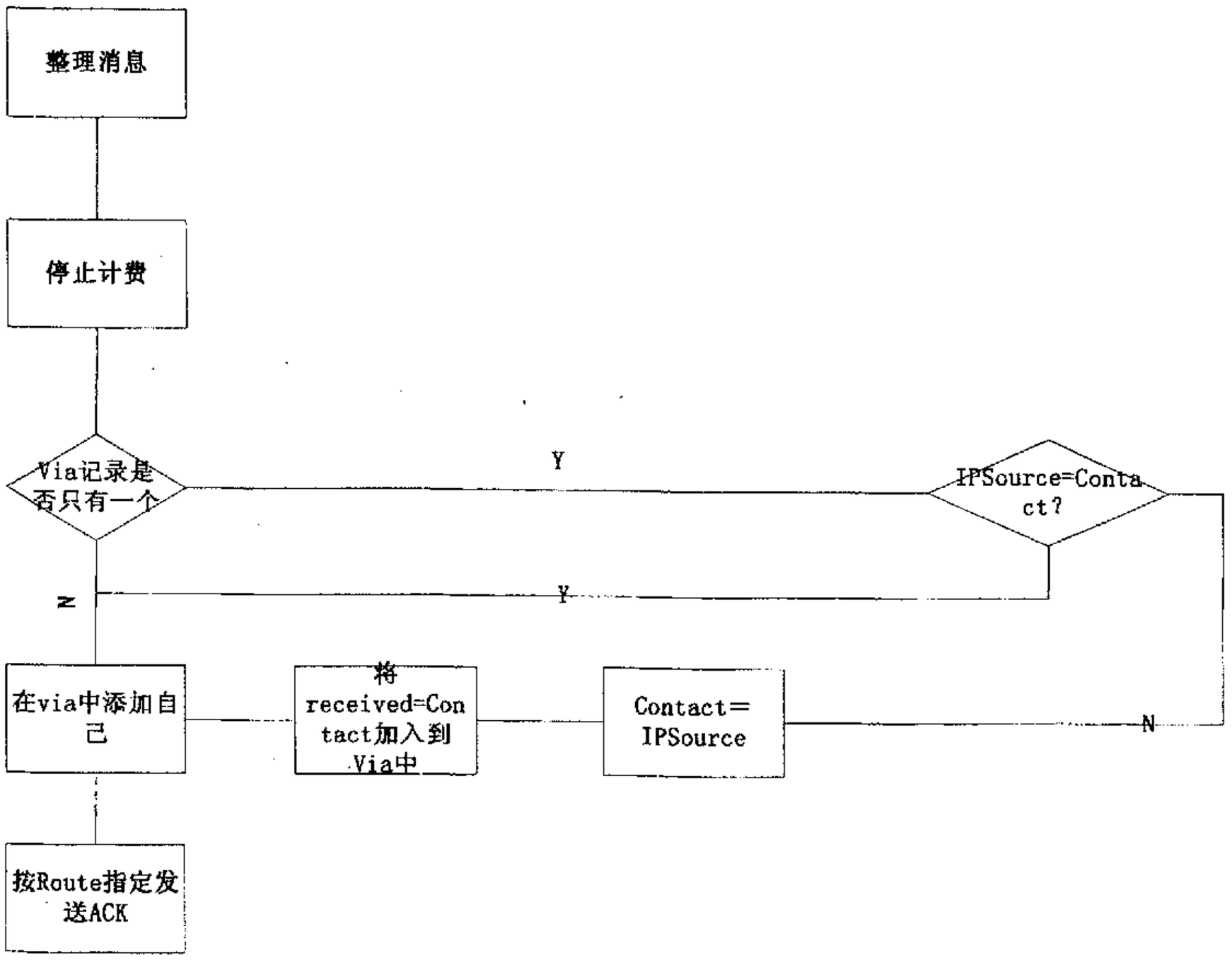


图 5—9：MrshlOpBye 流程图

## 5.MS 对 Cancel 的处理子模块

MrshlOpCancel：处理 SIP 线程接收的 Cancel 消息。

处理流程：

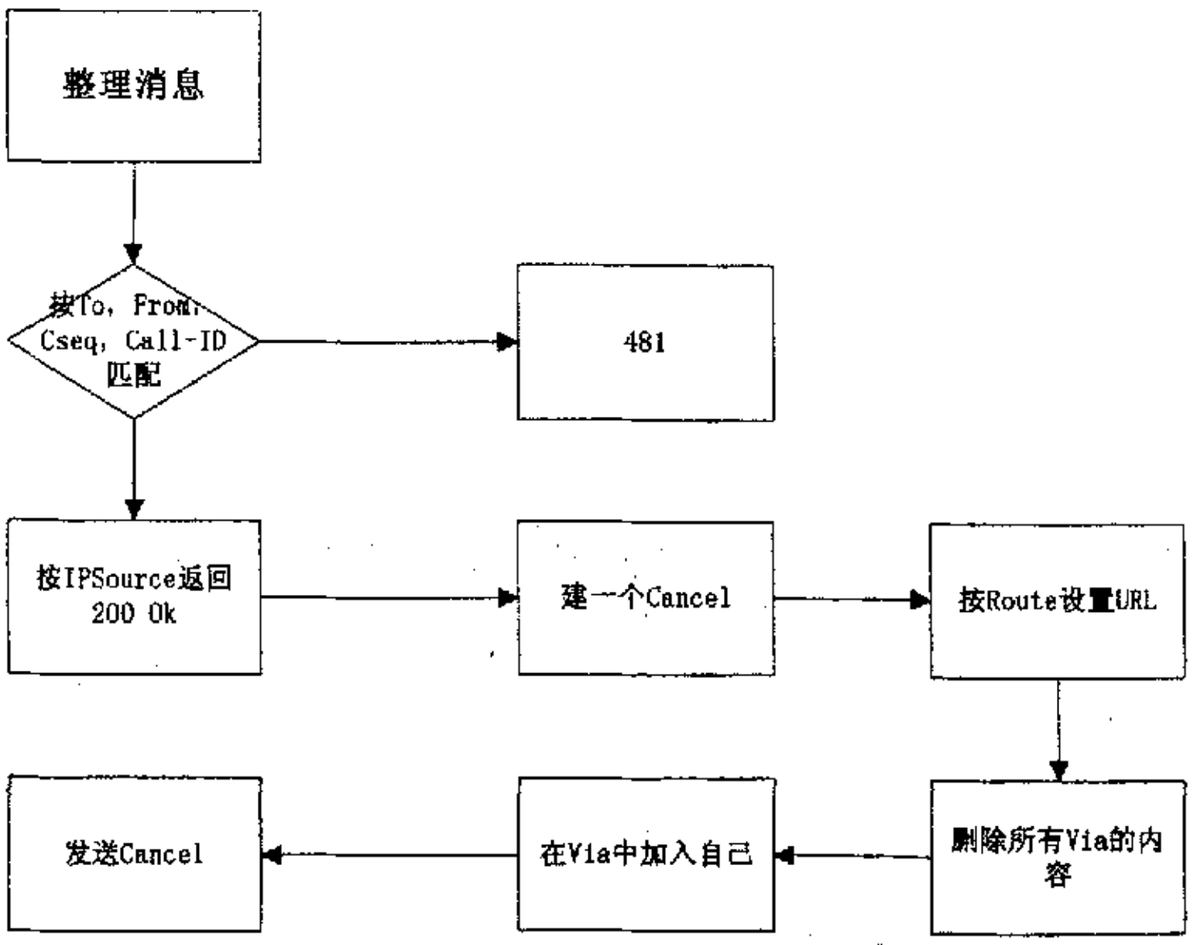


图 5—10：MrshlOpCancel 流程图

## 6.MS 对 180 Ringing ， 183Session Progress 的处理子模块

MrshlOpStatus：处理 SIP 线程接收的 180 Ringing ， 183Session Progress 消息。
处理流程：

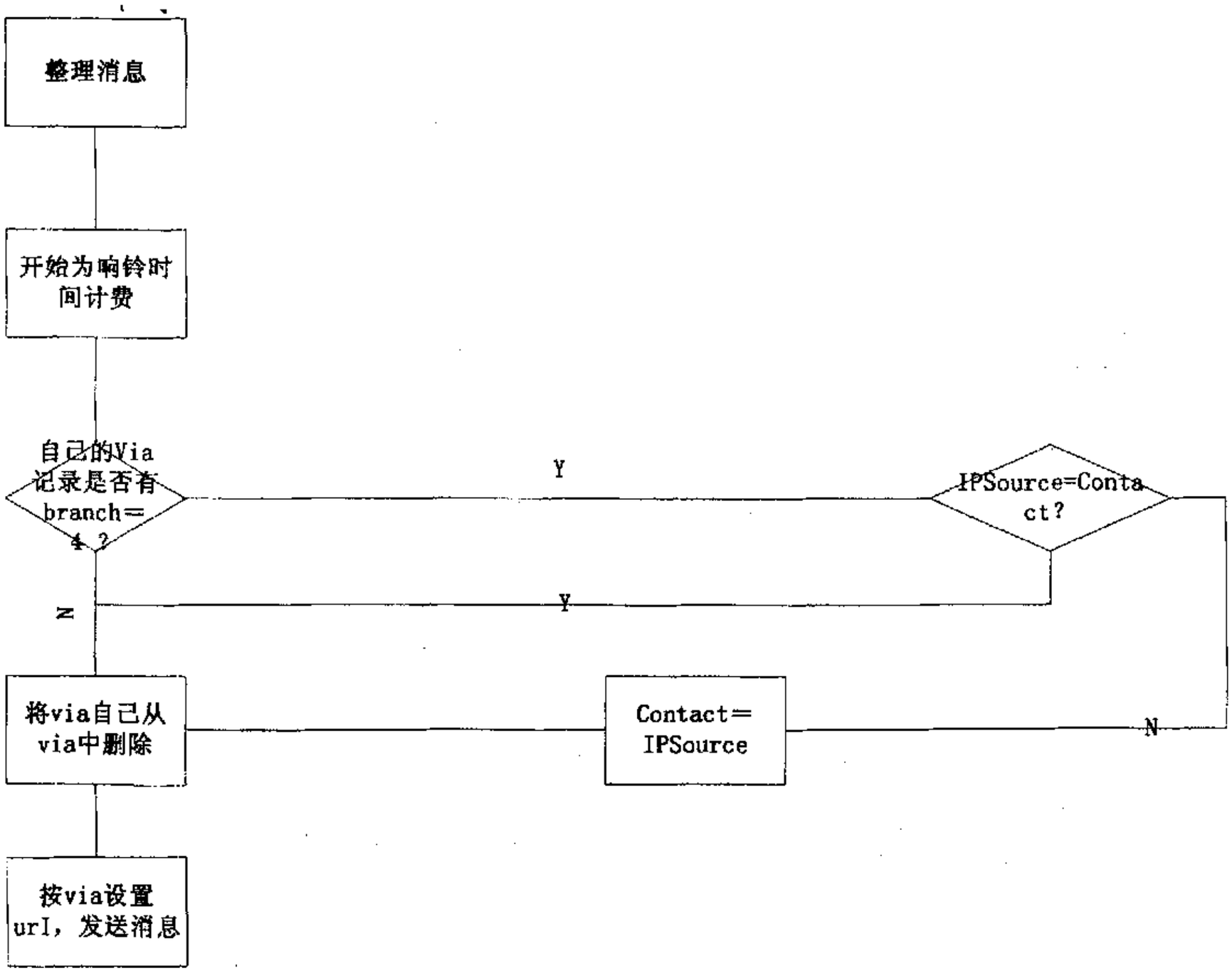


图 5－11：MrshlOpStatus，180 ring 流程图

## 7.MS 对 200 OK 的处理子模块

MrshlOpStatus：处理 SIP 线程接收的 200 OK 消息。
处理流程：

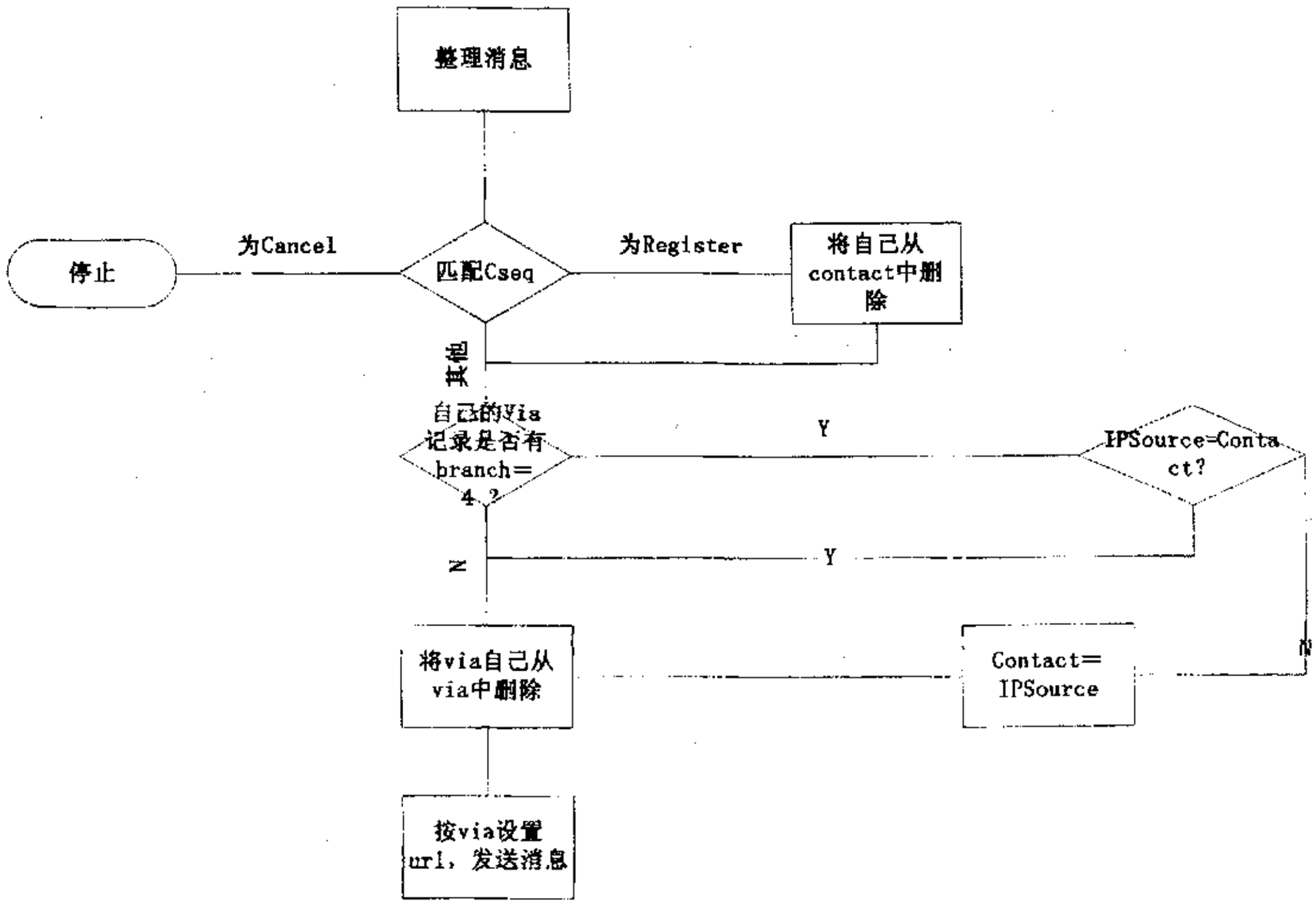


图 5－12：MrshlOpStatus，200 OK 流程图

## 8.MS 对 302 Moved Temporarily 的处理子模块

MrshlOpStatus：处理 SIP 线程接收的 302 Moved Temporarily 消息。

处理流程：

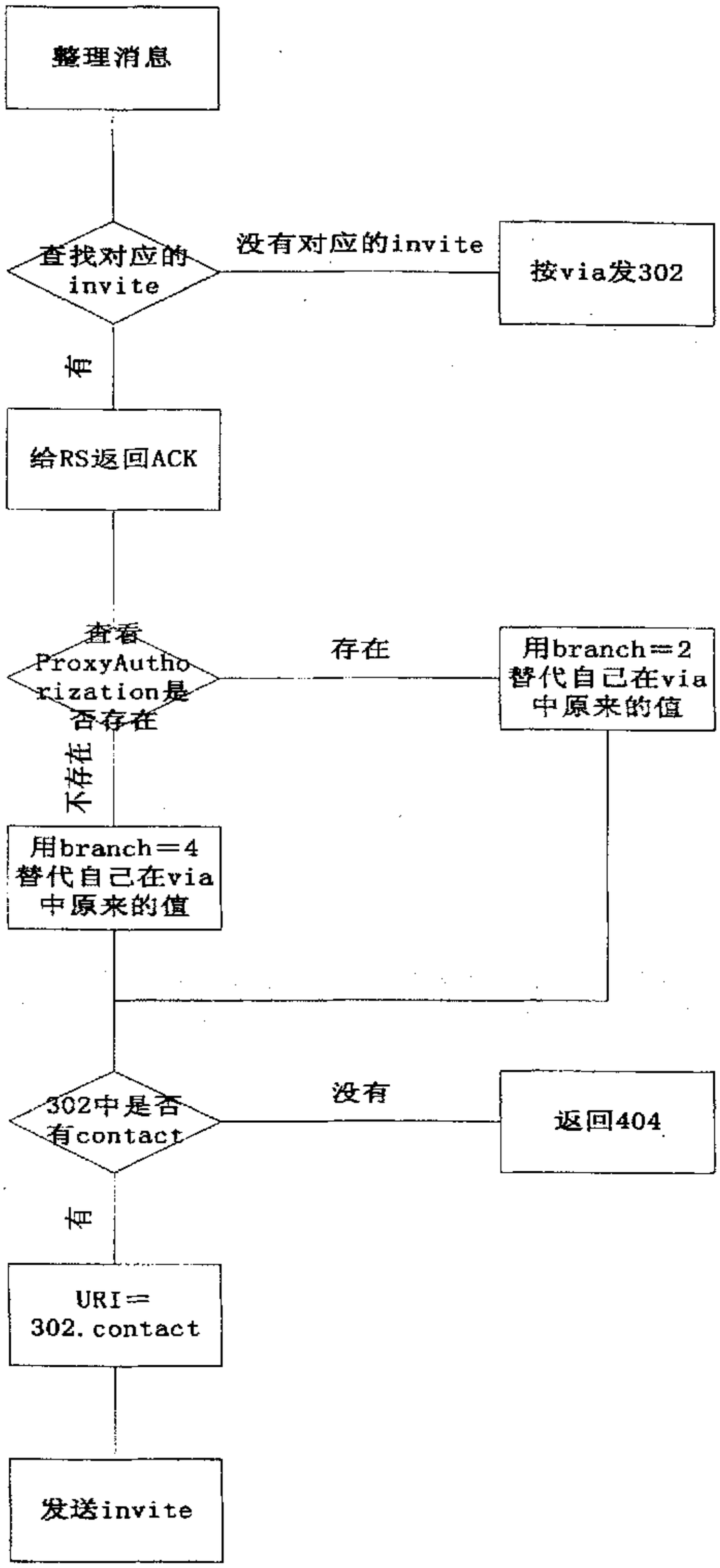


图 5－13：MrshlOpStatus，302 Moved 流程图

### 5.2.3.2 MPMS 模块。

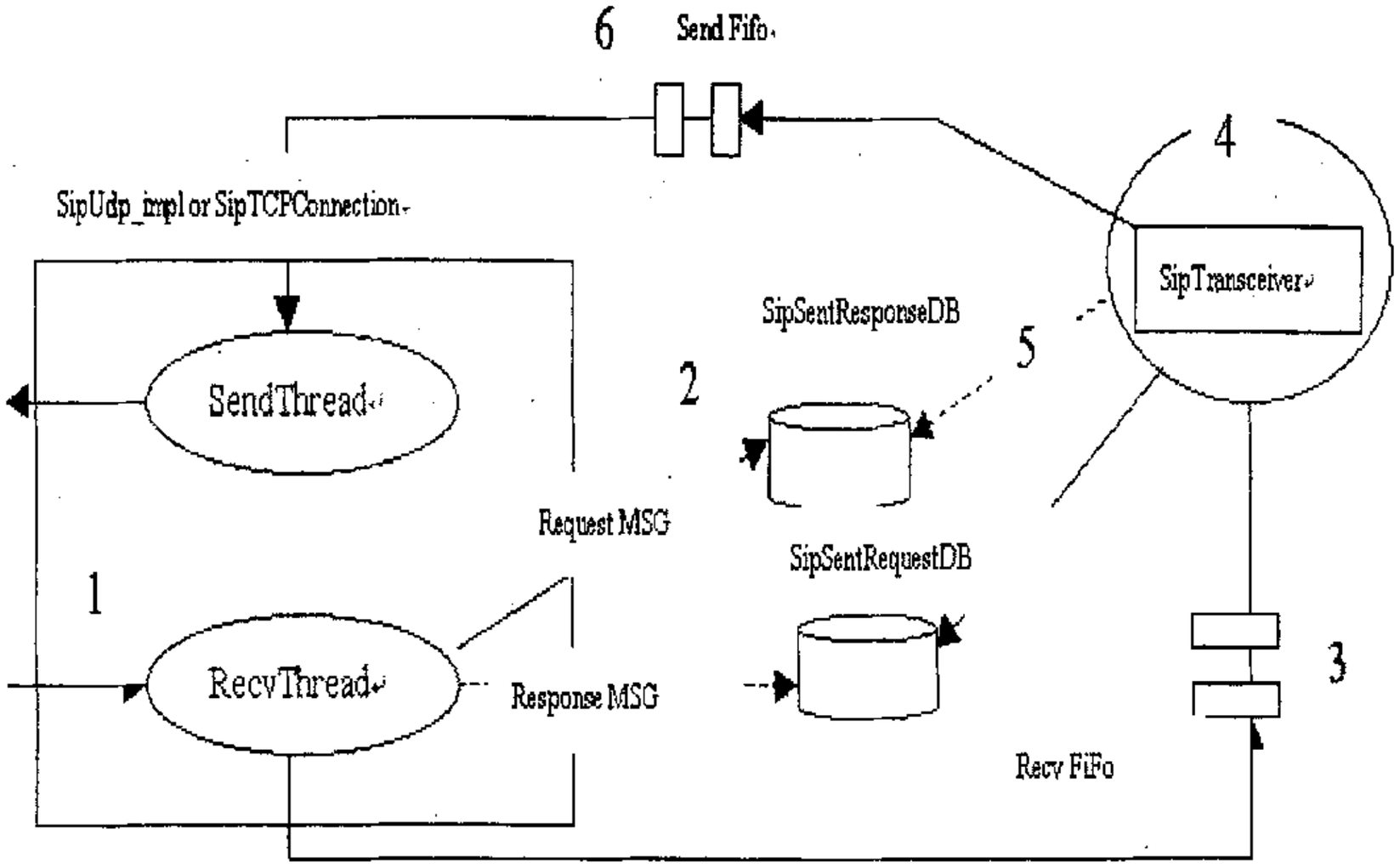


图 5－14：MPMS 对信令的处理

MPMS 收到用 SIP 线程接收到信令后先将消息放到 SipSentRequestDB 中，主要是先判断是否是 SipSentRequestDB 中已有的消息（以 Call ID 为依据），主要是防止重复处理同一条消息，当判断是新消息后就将消息放到 RecvFiFo 中，然后由 Work 线程来处理消息。处理完的消息先放到 SipSentResponseDB 中，然后在送往 Send Fifo 中，由 SIP 线程发送出去。

## 1.MPMS 对 Invite 的处理子模块

MPOpInvite：处理 SIP 线程接收的 Invite 消息。
处理流程：

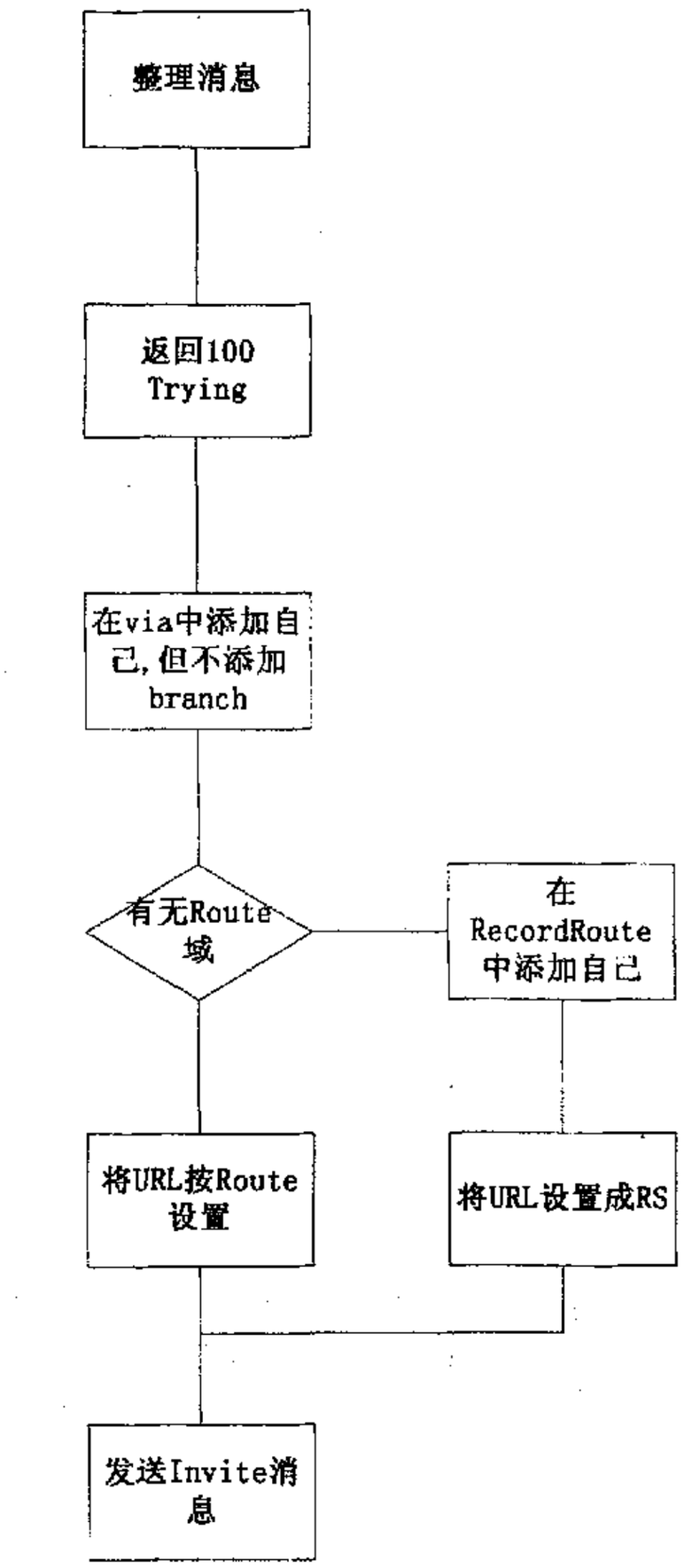


图 5－15：MPOpInvite 流程图

## 2.MPMS 对 ACK 的处理子模块

MPOpACK：处理 SIP 线程接收的 ACK 消息。
处理流程：

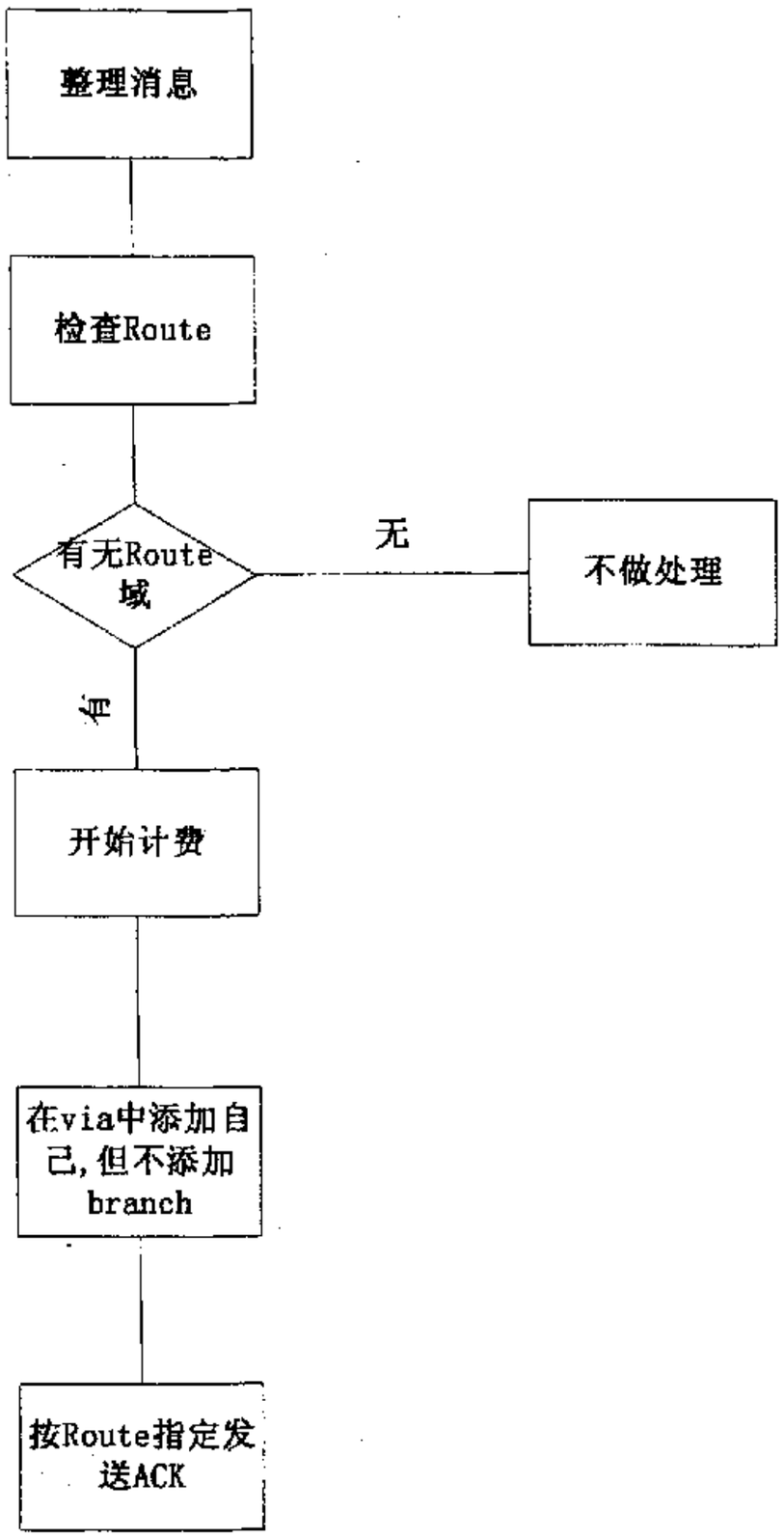


图 5－16：MPOpACK 流程图

## 3.MPMS 对 Bye 的处理子模块

MrshlOpBye：处理 SIP 线程接收的 Bye 消息。

处理流程：

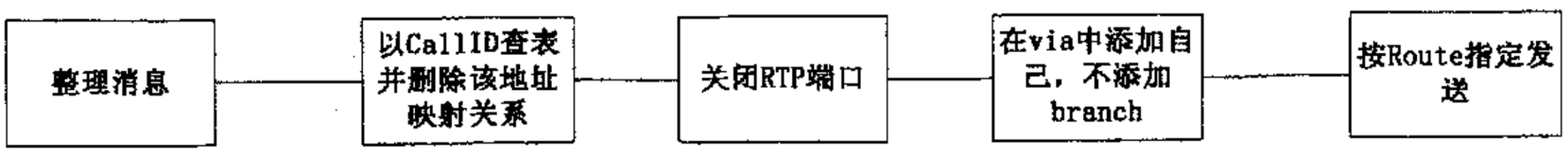


图 5－17：MrshlOpBye 流程图

## 4.MPMS 对 Cancel 的处理子模块

MrshlOpCancel：处理 SIP 线程接收的 Cancel 消息。

处理流程：

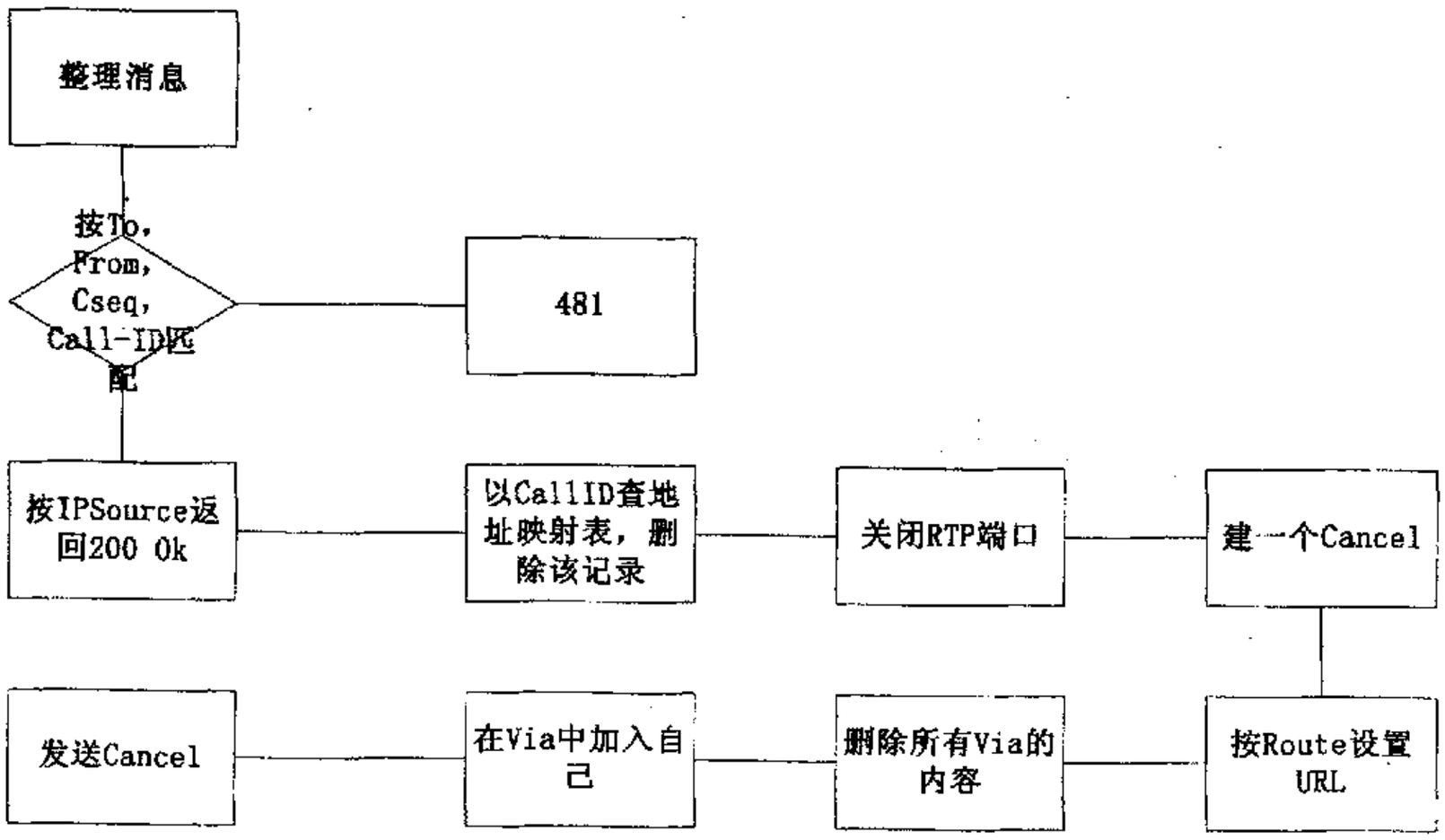


图 5－18：MrshlOpCancel 流程图

## 5.MPMS 对 180 Ringing ， 183Session Progress 的处理子模块

MPOpStatus：处理 SIP 线程接收的 180 Ringing ， 183Session Progress 消息。
处理流程：

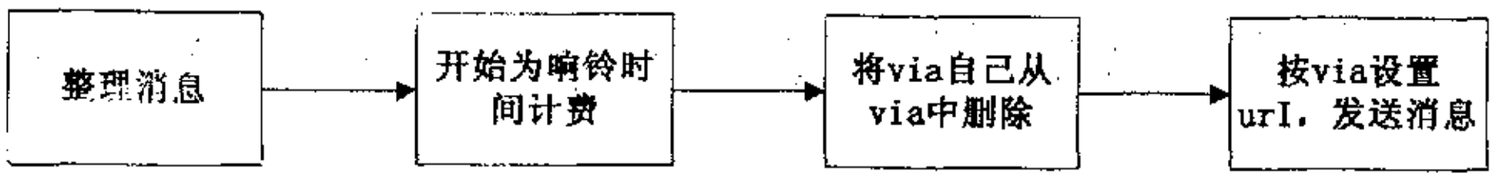


图 5－19：MPOpStatus，180 ringing 流程图

## 6.MPMS 对 200 OK 的处理子模块

MPOpStatus：处理 SIP 线程接收的 200 OK 消息。
处理流程：

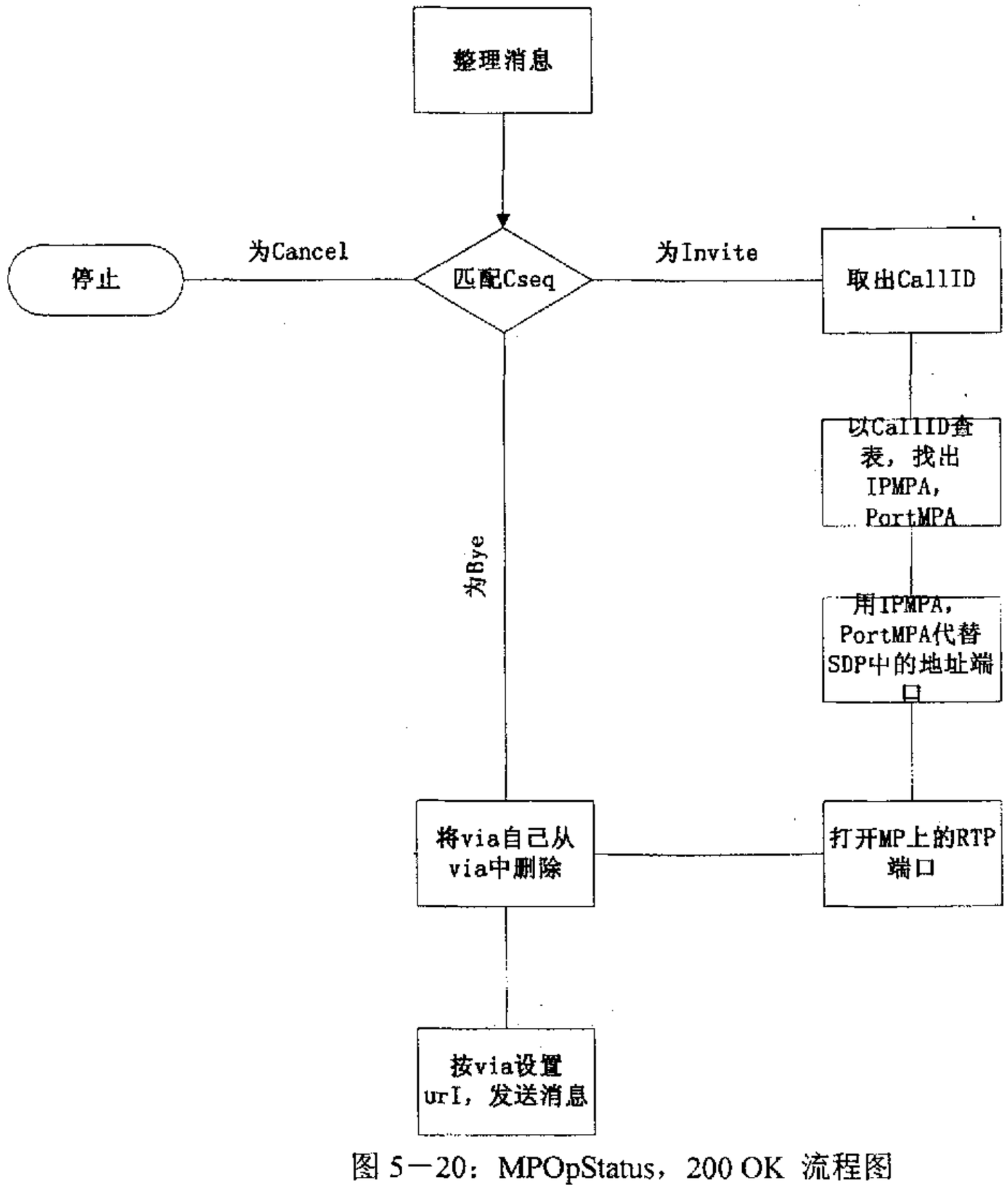


图 5－20：MPOpStatus，200 OK 流程图

## 7.MPMS 对 302 Moved Temporarily 的处理子模块

MPOpStatus：处理 SIP 线程接收的 302 Moved Temporarily 消息。
处理流程：

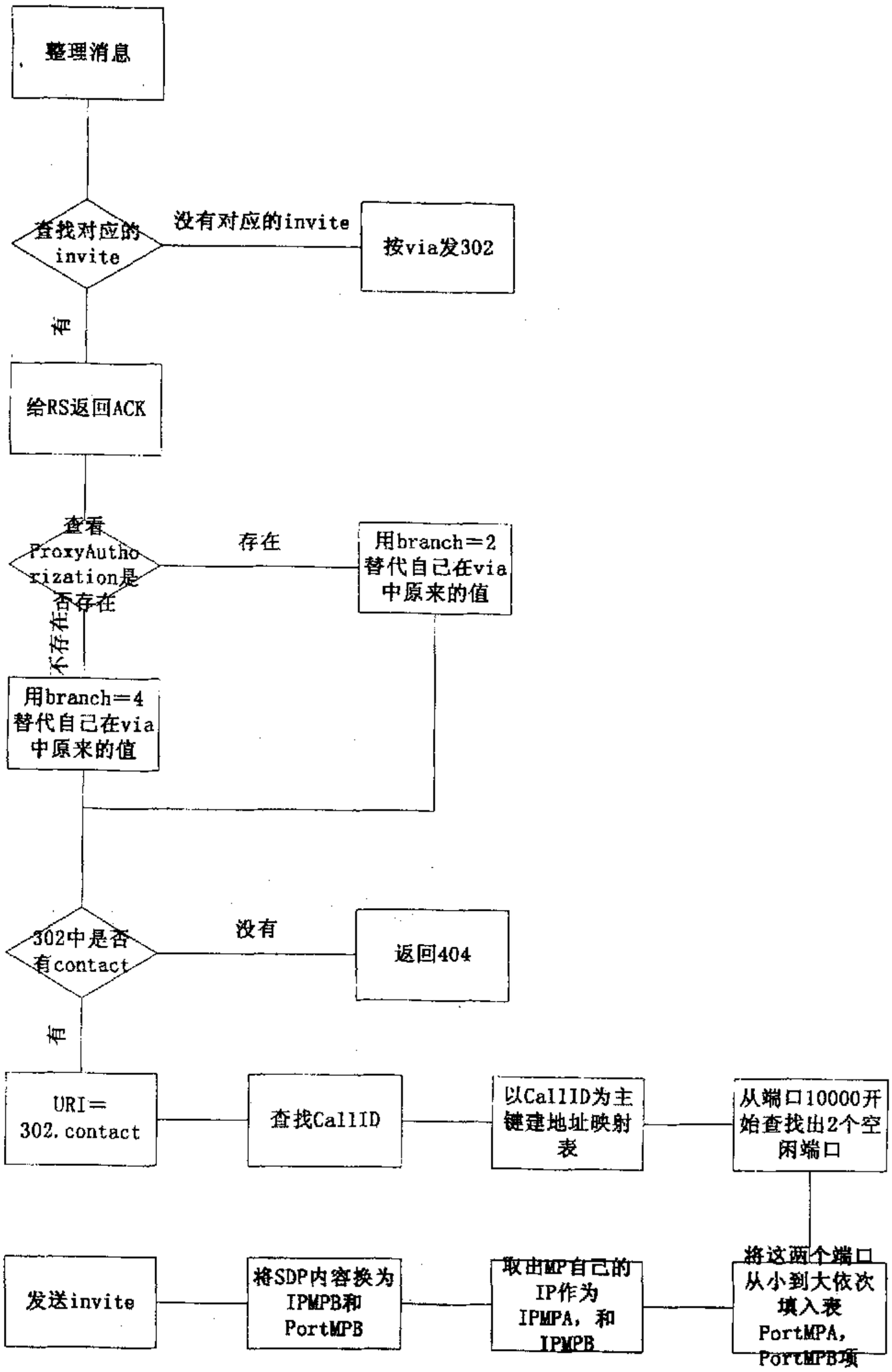


图 5－21：MPOpStatus，302 Moved 流程图

## 8.MPMS 通过 SIP 信令对 转发 RTP 流的呼叫资源的管理模块[22]

MP 在启动时建立一个线程池(进程太耗资源)，线程池的容量就代表了呼叫通路的个数。建立线程池时预分配呼叫资源.当有 Invite 时，就说明有呼叫要申请呼叫资源，每个呼叫资源包括的元素为:

```
        int fd_callingSocket;
        int fd_calledSocket;
        int rtcp_fd_callingSocket;
        int rtcp_fd_calledSocket;
//      string      *       callingBuffer;
        IPAddress           callingAddr;
        IPAddress           remoteCallingAddr;
        UDPSocket *         callingSocket;
        int                 CallingPort;

//      string      *       calledBuffer;
        IPAddress           calledAddr;
        IPAddress           remoteCalledAddr;
        UDPSocket *         calledSocket;
        int                 CalledPort;

        VThread* MPthread;
        vthread_t ThreadID;
//      VThread* RTCPThread;
//      vthread_t RTCPThreadID;
        int SourceID;
        SipCallId   CallId;
        int NodeStatu;
        string user_caller;
        string user_callee;
//      CallSourceNode();
        CallSourceNode(int ID);
        ~CallSourceNode() {};
        IPAddress           rtcp_callingAddr;
        IPAddress           rtcp_remoteCallingAddr;
        UDPSocket *         rtcp_callingSocket;
        int                 rtcp_CallingPort;

        IPAddress           rtcp_calledAddr;
        IPAddress           rtcp_remoteCalledAddr;
        UDPSocket *         rtcp_calledSocket;
        int                 rtcp_CalledPort;
```

这样在每个资源中都包括预留给主被叫的 MP 上的端口。

以下说明一下资源预留，分配和回收的过程。

1.MPMS 在启动后资源预留的结果:

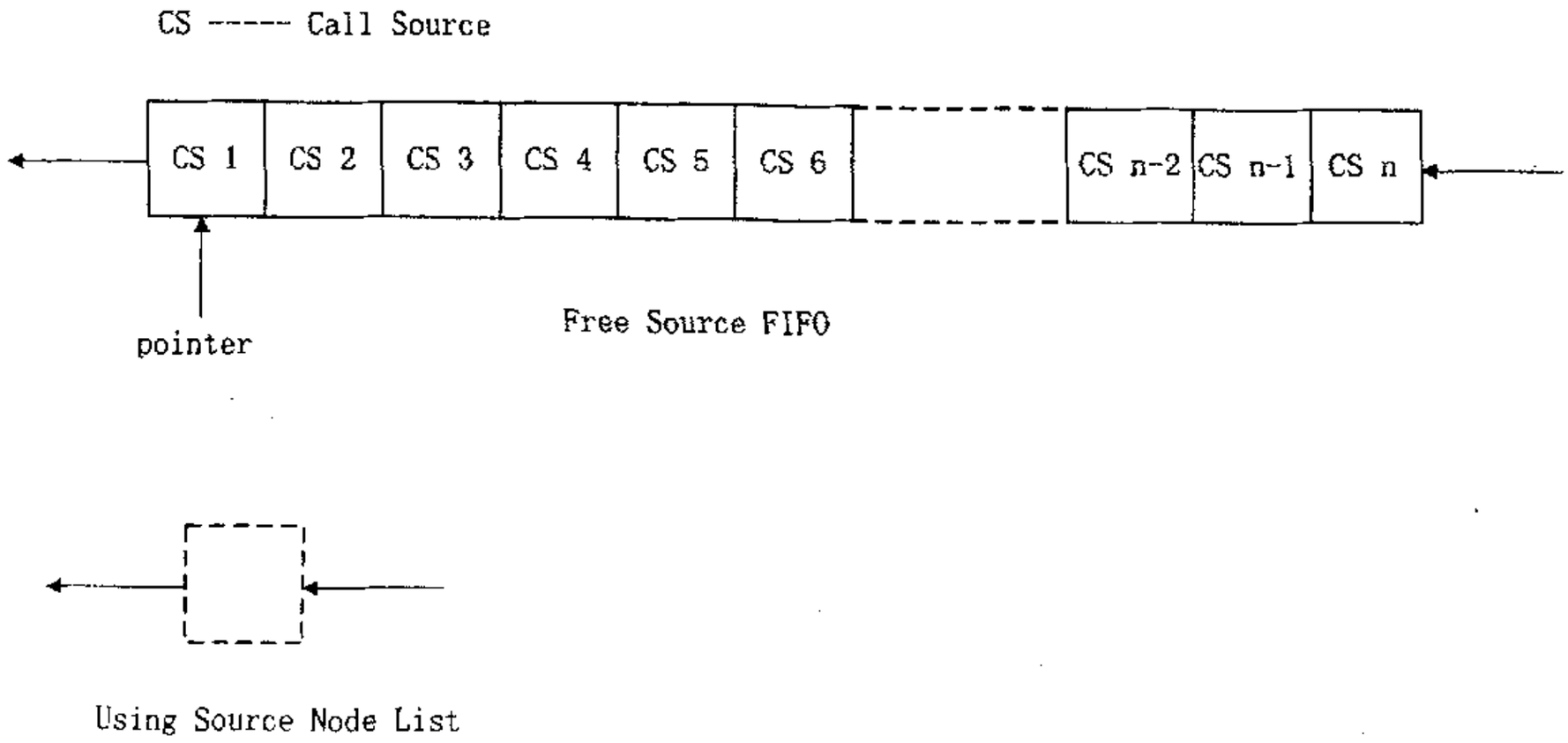


图 5—22：MPMS 资源分配（1）

2. Tel_A呼叫Tel_B 在MP收到INVITE后从Free Source FIFO的最前节点取出一个空闲资源CS 1，并讲CS 1 加入Using Source Node List中，然后取出CS 1资源的相应地址并修改INVITE的SDP的内容。如果Free Source FIFO为空 ，说明没有资源提供给通话，则回486 Busy Here。

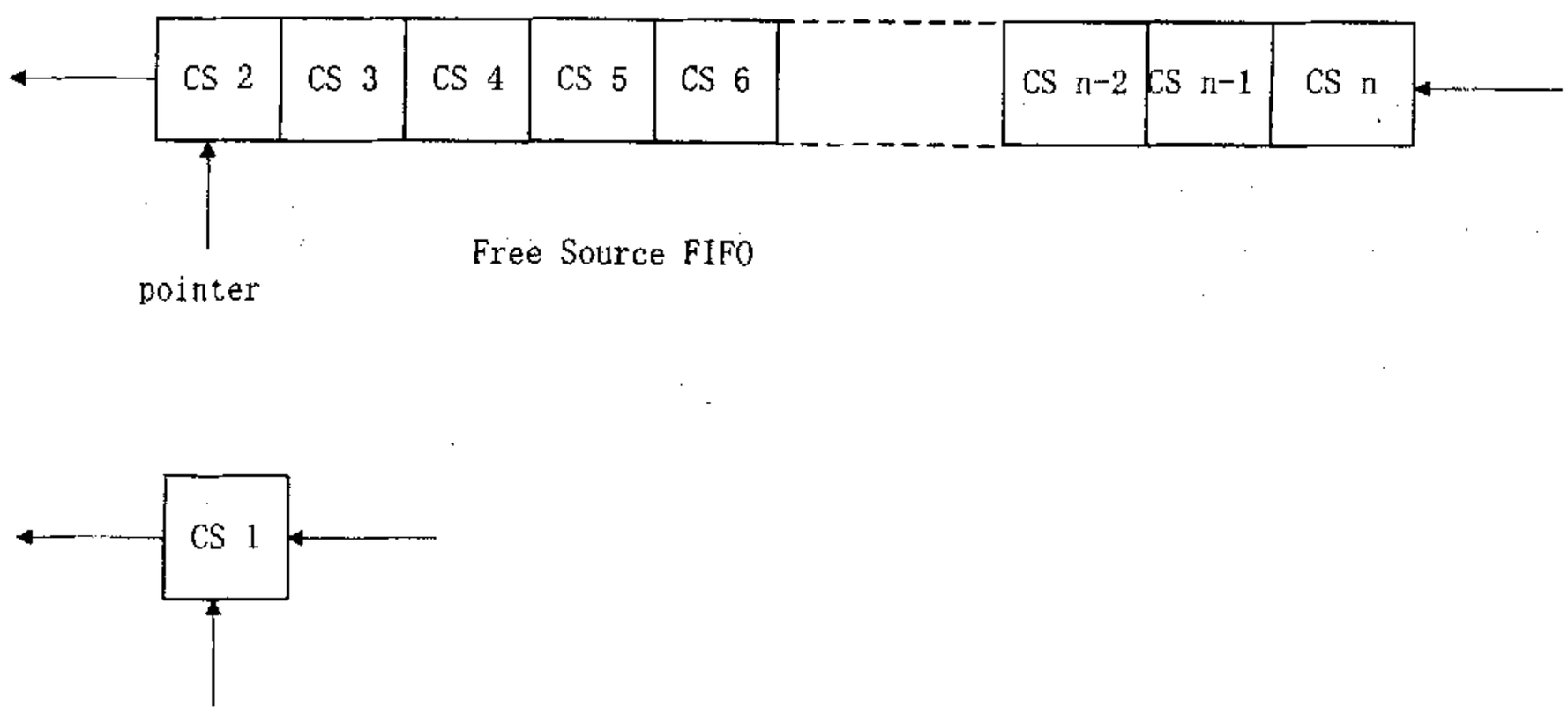


图 5—23：MPMS 资源分配（2）

3. 假设另外有路通话，Tel_C 呼叫 Tel_D 在 MP 收到 INVITE 后从 Free Source FIFO 的最前节点取出一个空闲资源 CS 21，并讲 CS 2 加入 Using Source Node List 中，然后取出 CS 2 资源的相应地址并修改 INVITE 的 SDP 的内容。如果 Free Source FIFO 为空 ，说明没有资源提供给通话，则回 486 Busy Here。

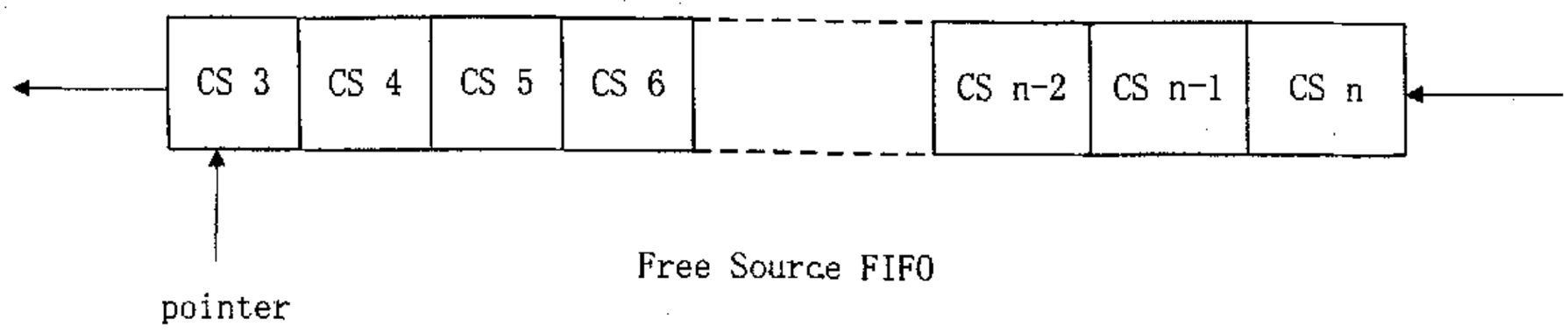


图 5—24：MPMS 资源分配（3）

4. 在收到200 OK后，MPMS会从Using Source Node List中以Call ID搜索分配给自己的呼叫资源，并取出对应的地址，修改200 OK的SDP内容，然后转发到RS，这个取出的地址是给主叫的MP的预留资源。

5. 在通话结束后，比如Tel_C发出了Bye，当Bye传到了MPMS后， MPMS会从Using Source Node List中以Call ID搜索自己的呼叫资源，然后释放资源，将资源从Using Source Node List中取出，并加入到Free Source FIFO 末尾。

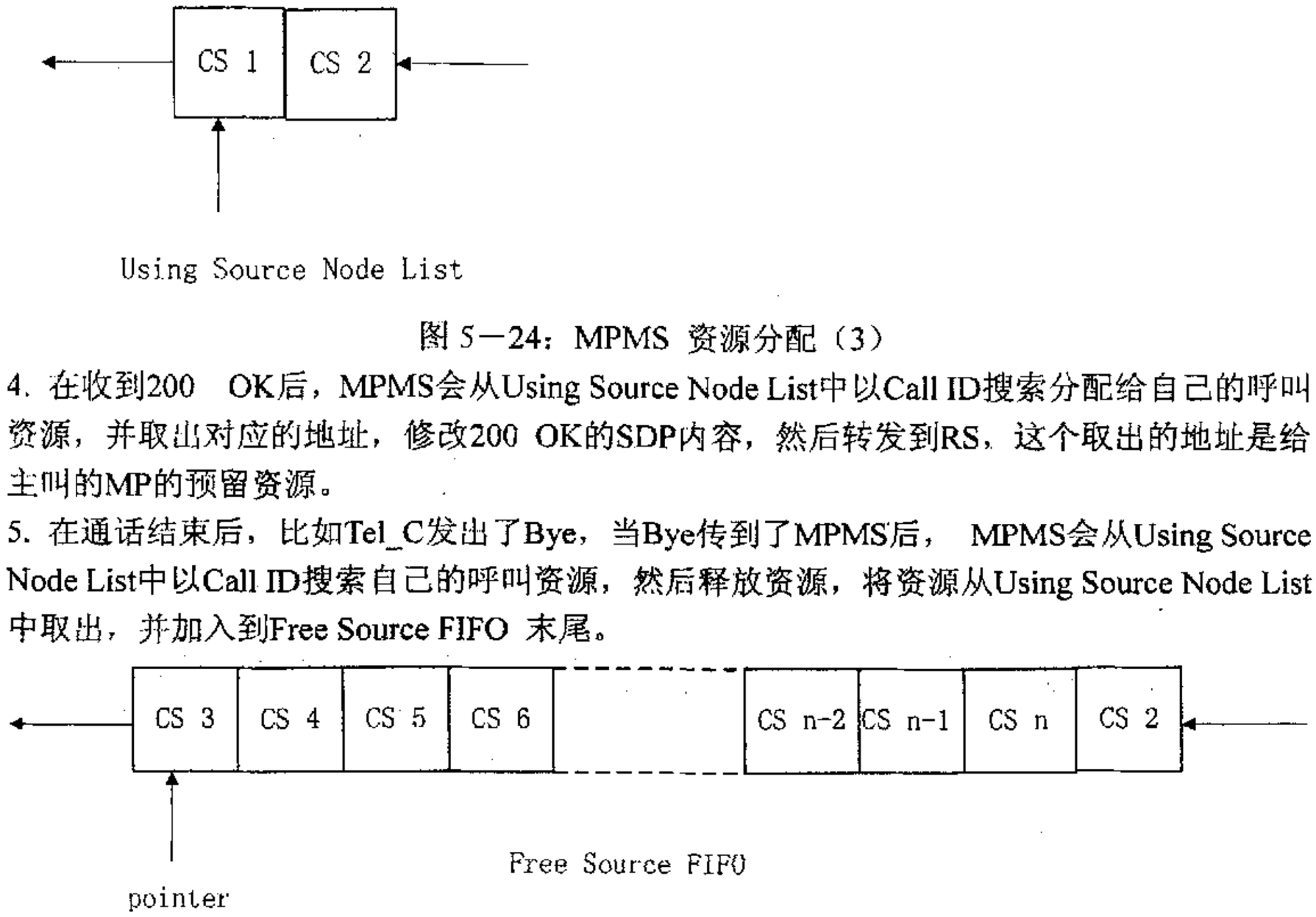


图 5—25：MPMS 资源分配（4）

### 5.2.3.3 RS 模块

RS 检查 REGISTER 消息中的 To 域来得到用户的信息。从 MS 的 Contact 域得到的信息存在 RS 中的用户终端的 Subscriber Container 中。通常这些信息是代理服务器和终端地址。如果终端处于 NAT 环境中，那么还应该含有 B2BUA Server 的地址信息。

当 INVITE 消息到来时，MS 或 MPMS 将 INVITE 发送到 RS 进行寻址。RS 需要进行以下几步来决定呼叫的下一跳：首先根据呼叫双方的用户的 Subscriber Container 中的信息来生成一个 Contact List；然后取出 INVITE 消息中的 via 域来和 Contact List 对比，决定下一跳的地址；如果下一跳地址有效，那么最后就返回下一跳地址。

MS 或 MPMS 接收来自 RS 的消息，该消息中的 contact 字段中的包含下一跳的地址信息。然后 MS 向下一跳继续发送 INVITE 请求。

# 第六章 测试环境与测试结果

## 6.1 测试环境

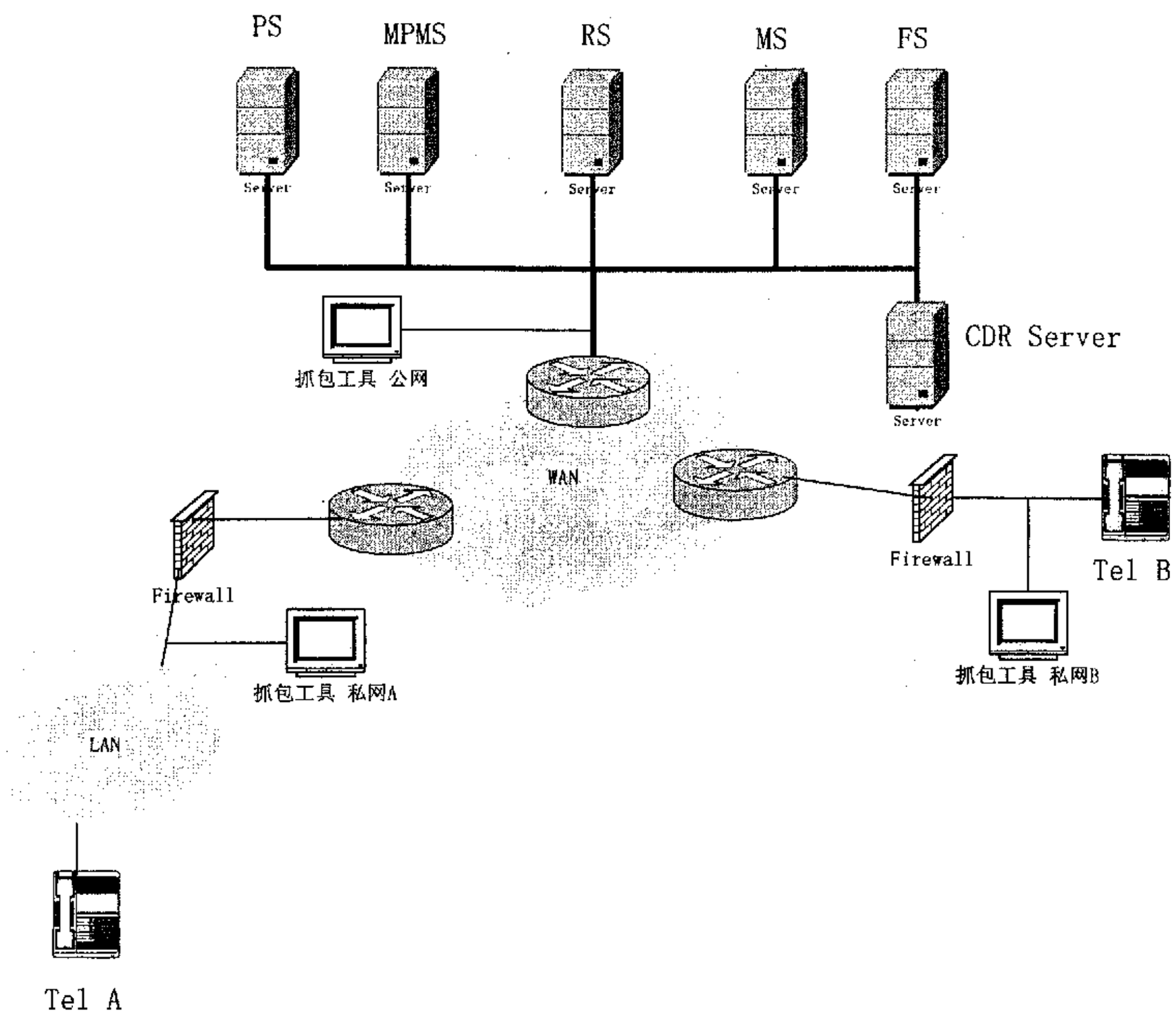


图 6—1：测试环境网络结构图

测试环境的结构图如上图所示，图中所示为涉及到的几个 Server， Marshal Server，Register/Redirect Server 和 MPMS。我们测试的重点是从 NAT 外部向内部以及 NAT 内部向外部发呼叫请求的情况。

| | MPMS 主机 | MS 主机 | RS 主机 | NAT 主机 |
|---|---|---|---|---|
| 操作系统 | Redhat Linux 7.1<br>Kernel 2.4.18 | Redhat Linux7.3<br>Kernel 2.4.18-3 | WindowsXP | Redhat Linux7.3<br>Kernel 2.4.18-3 |
| CPU | Intel PIII1G | Intel PIII1G | Intel PIII1G | Intel PIII1G |
| 内存（M） | 128 | 256 | 256 | 256 |

| 网卡速率（M） | 10/100 | 10/100 | 10/100 | 10/100 |
|---|---|---|---|---|
| IP 地址 | 10.0.0.2 | 211.68.68.61 | 211.68.68.28 | 双网卡<br>10.0.0.1<br>211.68.68.29 |
| 备注 | 处理信令和媒体流，协助穿越 NAT | 运行 Marshal Server， | 运行 NAT 外部终端，Register/Redirect | 采用 iptables 技术作 NAT |

表 6—1：系统配置表

终端采用了维信和科技的硬终端，北电网络的软终端，和几个其他公司的软终端.

## 6.2 测试结果

### 6.2.1 私网呼叫私网

为了表达简单，在这里我们把整个上端的几个服务器看成一个整体，这样转化成以下模型:

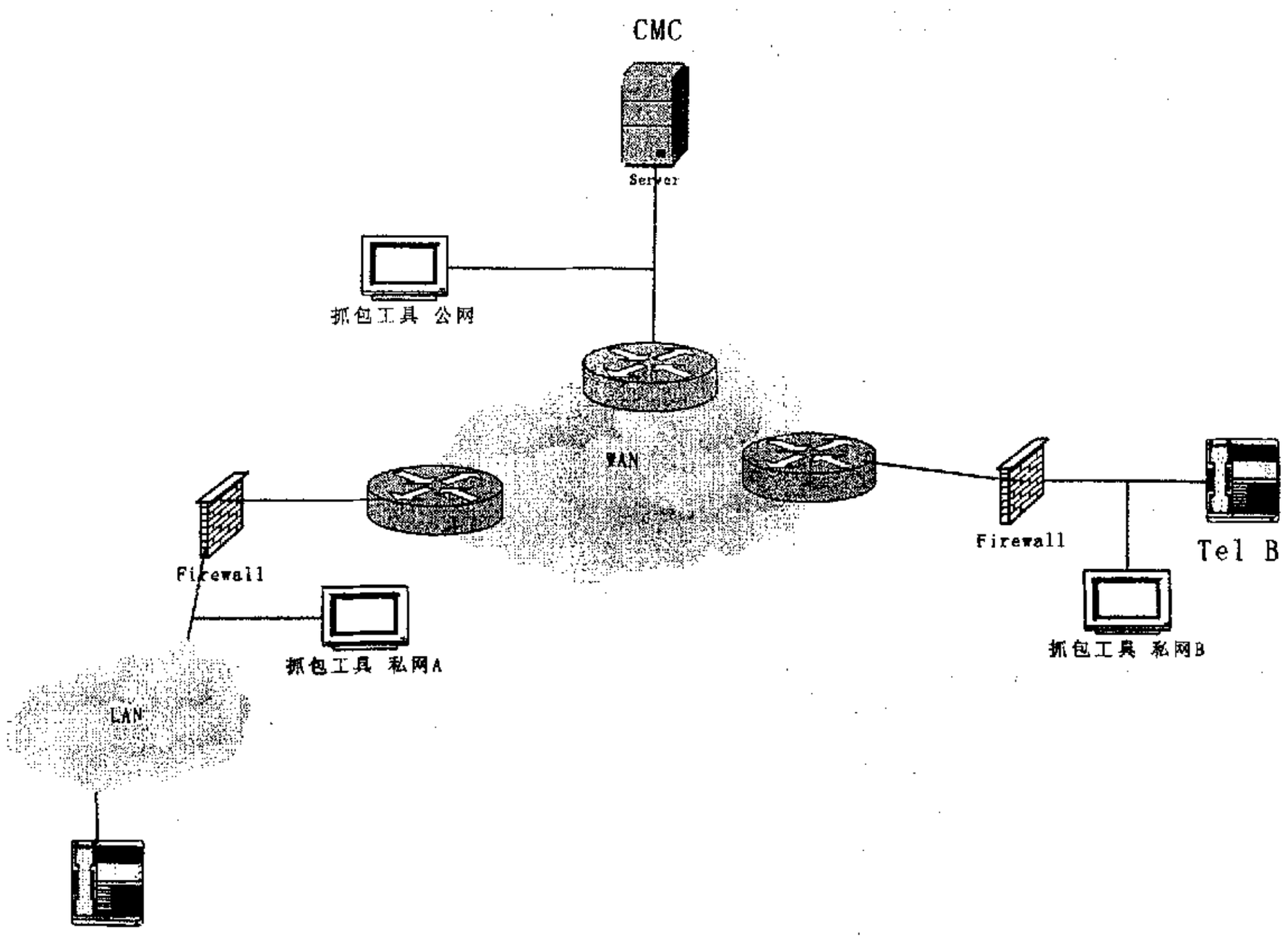


图 6—2：简化后的测试环境网络结构图

测试抓包流程:(为了方便理解，包的内容被简化)[39]

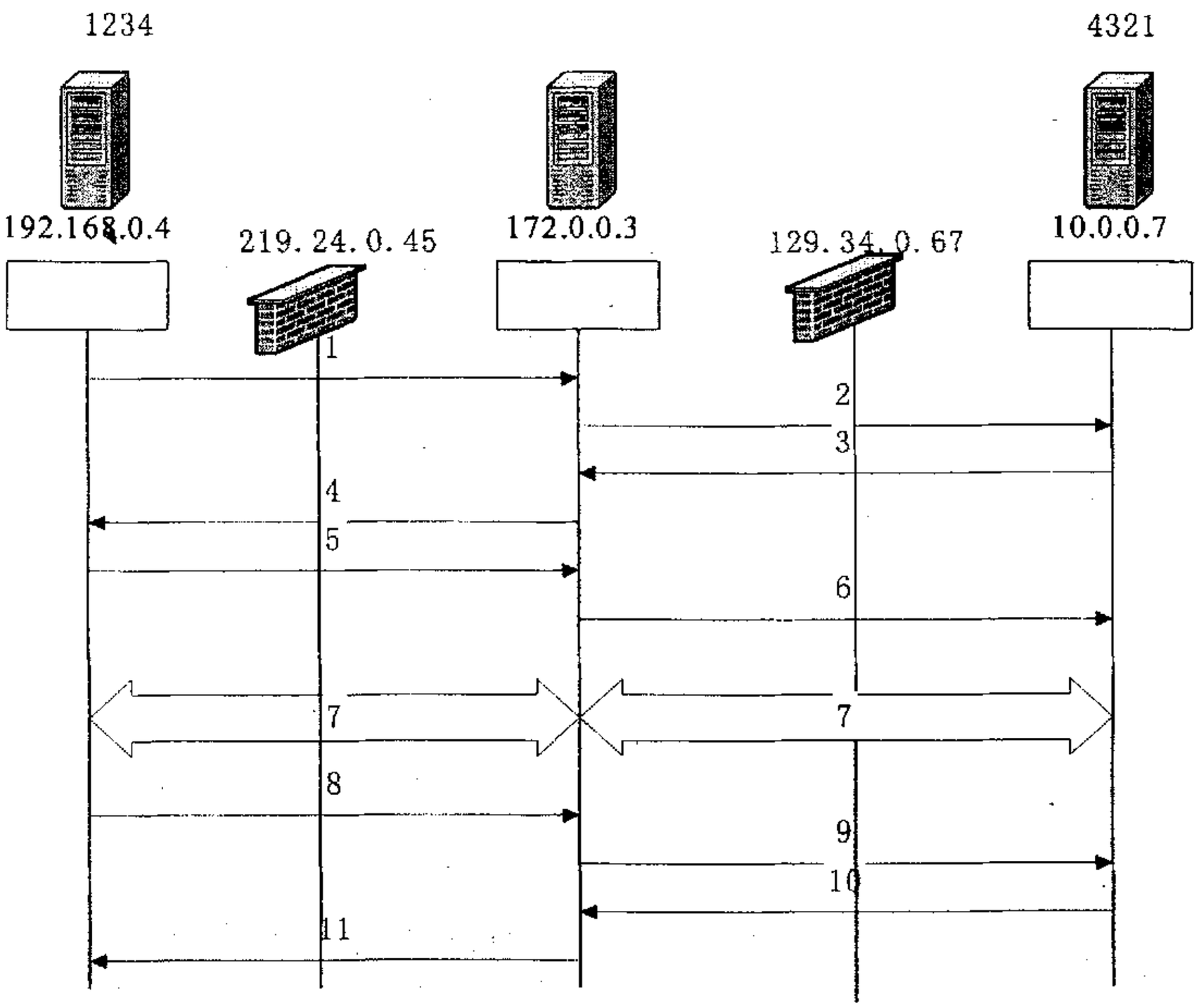


图 6—3：呼叫测试流程

1. 主叫发出 Invite 请求:

---

INVITE sip:4321@**172.0.0.3** SIP /2.0
Via: SIP/2.0/UDP **192.168.0.4**:5060
From: sip:1234@192.168.0.4
To: <sip:4321@172.0.0.3>
Call_ID: abcdefg@192.168.0.4
CSeq:10 INVITE
Exipres:180
Contact: <sip:1234@192.168.0.4:5060>
Content-Type:application/sdp
Content-Length: …
（SDP 地址为 **192.168.0.4**）

---

2 CMC 处理后转发主叫的 Invite 请求到被叫:

---

INVITE sip:4321@ 129. 34. 0. 67 SIP /2.0
Via: SIP/2.0/UDP 172.0.0.4:5060
Via: SIP/2.0/UDP 192.168.0.4:5060 **received:** 219. 24. 0. 45

Record-Route:<4321@**172.0.0.3**:5060;maddr=172.0.0.3>

From: sip:1234@192.168.0.4
To: <sip:4321@172.0.0.3>
Call_ID: abcdefg@192.168.0.4
CSeq:10 INVITE
Exipres:180
Contact: <sip:1234@192.168.0.4:5060>
Content-Type:application/sdp
Content-Length: …
（SDP 地址为 **172.0.0.3**）

---

这样可以看到 Invite 的 SDP 里描述媒体流地址被改为公网地址，而且在 via 中加入 received 已表示穿越过 NAT，而且这个 received 在下面就会被用到。

3.被叫回 200 OK

---

SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.0.0.4:5060
Via: SIP/2.0/UDP 192.168.0.4:5060 **received:** 219. 24. 0. 45
From: sip:1234@192.168.0.4
To: <sip:4321@172.0.0.3>
Call_ID: abcdefg@192.168.0.4
CSeq:10 INVITE
Contact:<4321@**10.0.0.7**:5060>
Record-Route:<4321@**172.0.0.3**:5060;maddr=172.0.0.3>
Content-Length:…
（SDP 地址为 **10.0.0.7**）

---

4 CMC 处理后转发被叫的 200 OK 到主叫:

---

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.4:5060 **received:** 219. 24. 0. 45
From: sip:1234@192.168.0.4
To: <sip:4321@172.0.0.3>
Call_ID: abcdefg@192.168.0.4
CSeq:10 INVITE
Contact:<4321@**129.34.0.67**:5060>
Record-Route:<4321@**172.0.0.3**:5060;maddr=172.0.0.3>
Content-Length:…
（SDP 地址为 **172.0.0.3**）

---

将 200 OK 的 SDP 里描述媒体流地址改为公网地址，并利用 received 里记录的主叫的经过

NAT 转换后的地址，将 200 OK 发送的 219.24.0.45. 另外注意一点 Contact 里的地址由原来的 10.0.0.7 转换成 129.34.0.67，这个在后面会用到。

5 主叫发 ACK。

```
ACK sip:4321@172.0.0.3:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.4:5060
From: sip:1234@192.168.0.4
To: <sip:4321@172.0.0.3>
Call_ID: abcdefg@192.168.0.4
CSeq:10 INVITE
Exipres:180
Contact: <sip:1234@192.168.0.4:5060>
Content-Type:application/sdp
Route:4321@172.0.0.3:5060;maddr=172.0.0.3
Route: <4321@129.34.0.67:5060>
Content-Length:0
```

这里我们可以看到，200 Ok 带来的 Contact 内容被加到了 Route 里，成为 ACK 最后一跳的目的地址。

### 6.2.2 私网呼叫公网，公网呼叫私网，公网呼叫公网

经过测试这三种情况下，通话也能够正常的建立，并能正常的结束。

## 6.3 存在的问题及解决方案

以上的测试主要是进行了功能上的测试，在放在公网上进行远程大话务量的通话后，发现了一些性能上的问题和功能上新的需求，以下就是发现的主要问题及对应的解决方案。

首先可以想到的是为了解决穿越 NAT 的问题，我们将媒体流原来的终端之间的点对点的通信方式改成了经由 MPMS 转发的方式，这样在解决了 NAT 问题的同时又引入了新的问题： MPMS 的瓶颈问题。

### 问题 1:在通话路数较多时 MPMS 对信令的响应变慢

经分析，发现由于线程池里资源数过多时，每次对 Invite，200OK，Bye，Cancel 的相应都要查找一遍线程池里的资源，这是占用系统的操作。

为此，可在分配资源时，以一定的标记对资源分类，这样每次查找资源时，可以通过分类而缩小查询的范围，加快查询速度。

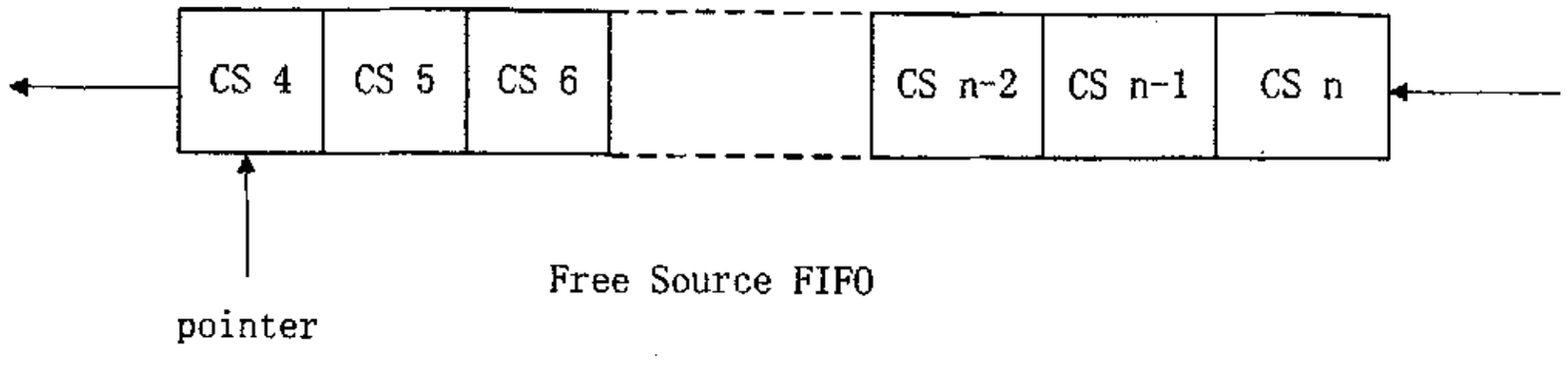


图 6—4：资源分配算法改进

在这里，因为 Call ID 的长度是经常变化的，而且得到一个字符串的长度不会占多少系统资源，所以系统中可以利用 Call ID 的长度对 3 求模，可以分出三个表示资源占用的链表. 经测试，这种算法在通话通路数量大的情况下，效果很明显。

## 问题 2:一个 MPMS 经测试大概只能够带 100 路通话，需要做负载均衡

这种情况是由于针对 RTP 协议的特点所做的转发算法造成的。如果 RTP 协议中能够包含通话 Call ID，或在发送 RTP 包前走个私有的协议就可以解决了。在这里，我们还是遵循了协议的标准，不采用上面的两个解决办法，而采用 MP 组，既 MP 负载均衡的处理方式。

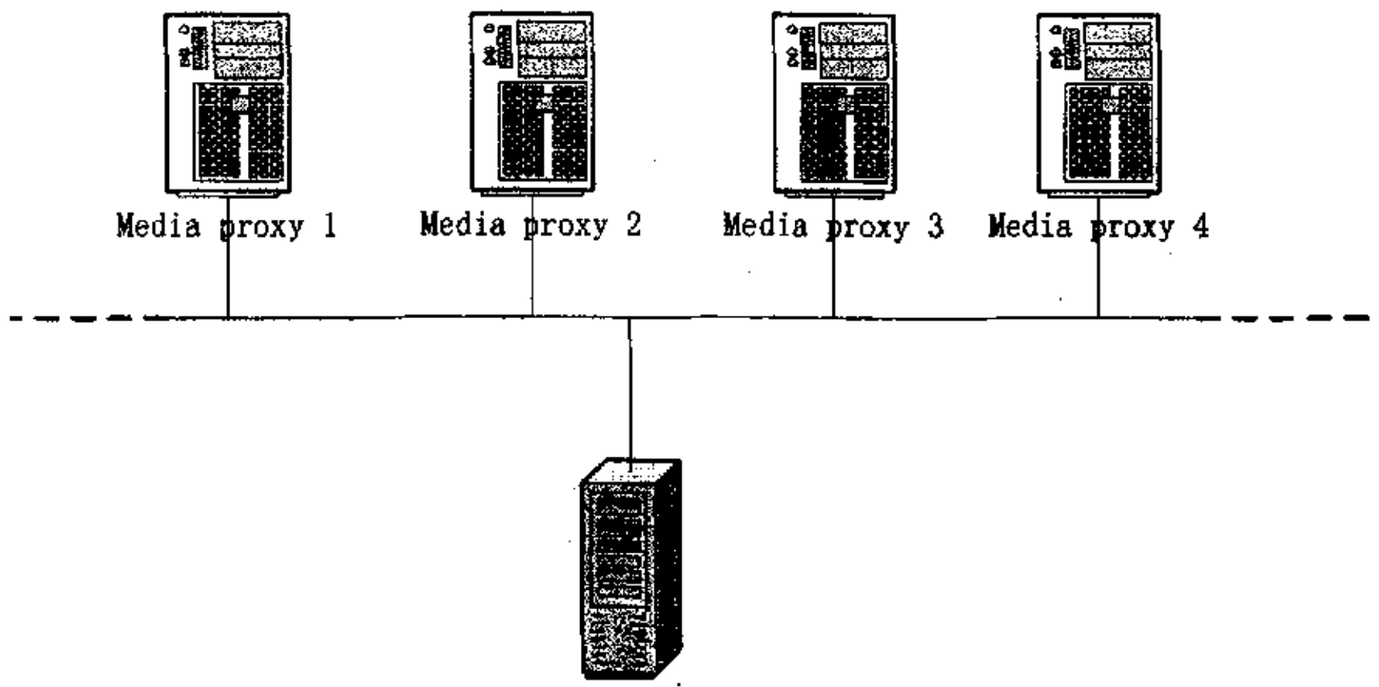


图 6—5：MPMS 负载均衡

将 MPMS 分为若干个 Media proxy 和一个 MP manger。前者专门用来处理转发媒体流，而后者负责处理信令，进行负载分配，控制通话到指定的 Media proxy 上。由于现实中每路通话的时长大多不同，而且还存在非正常结束通话的情况(这在网络状况差的地方更易发生，

如掉线等)，这就需要 Media proxy 和 MP manger 通过自己制定的私有协议通信来传送资源信息。

## 问题 3:在有视频通信的时候，同样有穿越 NAT 的问题.

1. 先了解一下终端如何在信令中描述视频信息，又是以何种形式发送和处理视频数据的。

对于 SIP 和 H.323 相比较而言，两者在视频通讯的概念上有很大的不同，SIP 把所有的媒体讯息理解成相同的 RTP 流，区别只是带宽不相同；而 H.323 则有一种专门的快速方式把两者区分开，首先打开语音通道传送音频，然后打开视频通道传送视频信息，两者用不同的媒体通道传输。后者的最大好处在于，如果带宽不足的话，至少可以传递语音信息到对方。

SIP 可以灵活的通过 SDP 来描述视频通信的信息，如:

---

Header: v=0
Header: o=- 1528076688 1528076688 IN IP4 192.168.66.1
Header: s=VOVIDA Session
Header: c=IN IP4 192.168.66.1
Header: t=3177769010 0
Header: m=audio 5068 RTP/UDP 0
Header: a=rtpmap:0 PCMU/8000
Header: a=ptime:20
Header: m=video 5070 RTP/UDP 31
Header: a=rtpmap:0 H261/90000

---

解释为:

媒体类型：Video 表示媒体类型是视频，5070 表示的是 RTP 端口号，这个端口号从资源管理上来说和音频的 5068 不相同。

传送协议：采用 RTP/UDP 传送，因为目前 SIP Stack 只支持 UDP 还不支持 AVP 的格式；

媒体格式：在 RTP 中定义的静态载荷类型文档号为 31；

数据算法为: audio(音频)用的是 PCMU，而 video (视频)用的是 H261。

2. 解决的方法:

了解了以上的原来，因为视频和音频都是通过 SDP 描述，通过 RTP 传送，不同处只在于对媒体流的编解码的算法上，所以与解决音频穿越 NAT 的方法是差不多的。在 MPMS 处理 Invite 和 200 OK 时，不光要修改 audio 的 IP 与端口，也要修改 video 的 IP 与端口。另外，还要在通话过程中为视频分配资源。

## 问题 4:为进一步提高通话质量，除了应用 RTCP，还可应用 RSVP.[8]

i. 资源预订协议（RSVP）是网络控制协议，它使 Internet 应用传输数据流时能够获得特殊服务质量（QoS），RSVP 是非路由协议；它同路由协议协同工作，建立与路由协议计算出路由等价的动态访问列表， RSVP 属 OSI 七层协议栈中传输层。

RSVP 一般工作机理如下图所示：

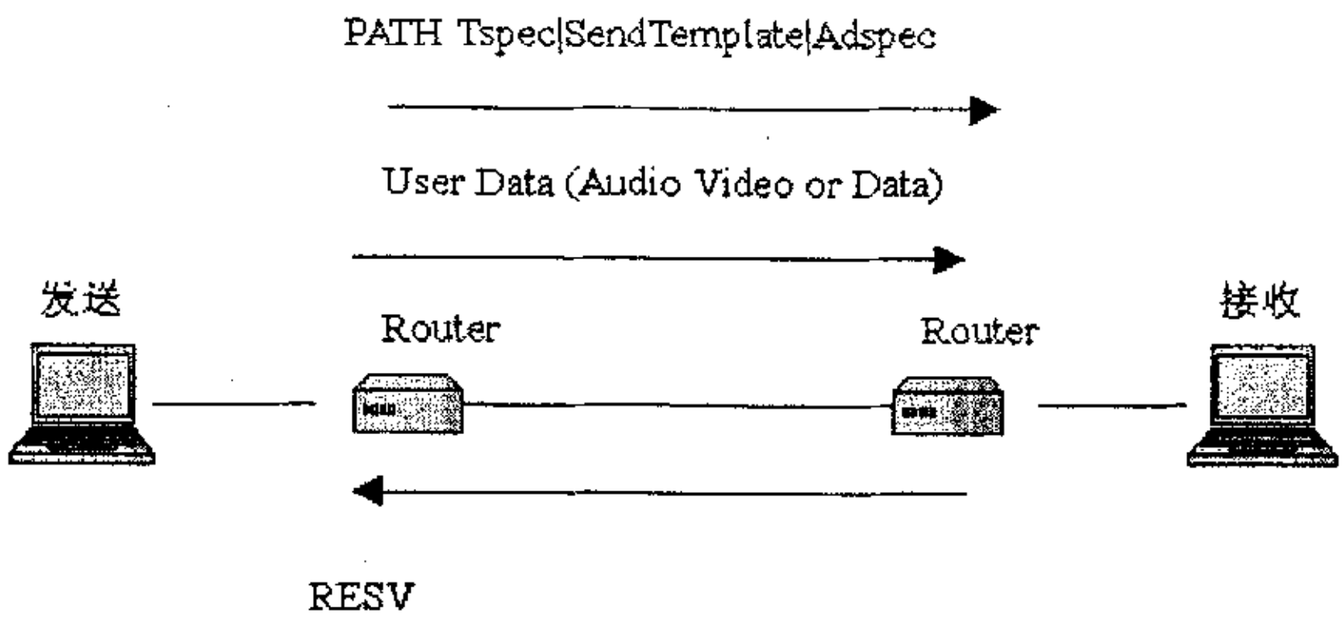


图 6—6：RSVP 工作原理

发送方发送 PATH 消息，消息中包含有数据业务特征，该消息沿所选的路径传送，沿途的路由器按照 PATH 准备路由资源，接收方接收到 PATH 消息以后，根据业务特征和所需要的 QOS 计算出所需要的资源，回送 RESV 消息，消息中包含的参数就包括请求预留的带宽，延 PATH 的原路途返回，沿途的路由器接收到 RESV 操作后才执行资源预留操作。发送方接收到 RESV 消息以后才发送用户数据。

而在 Vocal 中只不过是实现了一个简单 RSVP 构架，最重要的一点就是它不能够实现软状态，也就是定期刷新消息的 Tspec 和 Rspec，如果在音频，视频信号的时候这样的情况出现得特别频繁，由于音频，视频信号并不总是处于一种稳定的平缓的状态传输，可能会出现问题.

2. 解决上述问题的途径首先就是要在 RSVP 建立保证服务预定，也就是要根据接收端根据发送端的 AdSpec 消息计算预留的带宽(而在 Vocal 中基本上没有处理 AdSpec)，AdSpec 中参加带宽运算的主要是两个参数：Dtot 和 Ctot，第一个参数是最小路径延迟，第二个是路径带宽，通过这两个参数根据公式 D=(b(存储桶深度)+Ctot)/p + Dtot 计算出端到端之间的延迟:

例如：

PATH 流的初始特征：

Tspec(p=10mbps，L=2kbps，r=1mbps，b=32kbps) AdSpec(Ctot=0，Dtot=0)

经过第一个路由器：

Tspec(p=10mbps，L=2kbps，r=1mbps，b=32kbps) AdSpec(Ctot=11，Dtot=0.05s)

经过第二个路由器：

Tspec(p=10mbps，L=2kbps，r=1mbps，b=32kbps) AdSpec(Ctot=55，Dtot=0.1s)

现在我们来计算 Resv 中 Rspec 项目：

最长的延迟为 0.1s 的延迟，我们在 Rspec 中所计算的预留带宽必须符合这个要求，那么根据公式：

D=(b+Ctot)/p + Dtot

b：为存储桶深度

计算出的 D 为 0.185S 我们在根据这个公式来计算预留带宽

R=((p-r)（L+Ctot）+(b-L)p)/((t-Dtot)(p-r)+b-L)

r:业务流量

t:所需要的延迟

注意：所需要的延迟在 0.1-0.185 之间变化，这样我们通过上述公式得出一个比较确切的 R 值 R=1.66Mbps。所以 Rspec 为：R=1.66Mbps;松弛项(S)：用于指示 QoS 的富裕量，如果所有的路由器按照 R 预留，那么整个路径上的端到端的延迟会比要求的时延要少 S 毫秒：这里可以选择 0.05S，具体的松弛项计算可以参看 RFC2205 定义。[38]

3. 同样 RSVP 也面临者穿越 NAT 的问题

但经过分析，RSVP 描述的是媒体流的资源预留，就应该走媒体流的路径，也就是说对于终端来说要走媒体流的地址与端口，但对于 MPMS 来说对于来自终端媒体流端口的包解到传输层，从 MPMS 来看媒体流是 UDP 包，不同于 RSVP 包，.所以不能简单的直接利用 MPMS 为媒体流提供的资源转发.具体的方案还在研究中.

## 问题 5:系统会受到网络中恶意攻击的包而不能正常工作.

对于这个问题，在测试中发现过，目前能采用的比较经济的方式就是在系统前放一个过滤器[35]，只放行 SIP，RTP，RTCP 等包，但由于过滤器对包的分析，会影响包的传送速度，这对于媒体通信这个对实时性要求较高的工作影响较大，另外对于一些伪装包的攻击，这个方案也无能为力。

# 第七章 总结与技术展望

## 7. 1 总结

在公网上进行的二个月的国内和国际语音业务的测试通过，表明了我们的语音穿越NAT 的方案是切实可行的，整个系统在性能一般的 PC 机上运行也获得了良好的效果。

总的来说，本方案及实现具有以下特点

1. 不需要对 NAT 设备做任何修改，原有的集成 NAT 的防火墙设备也不需要升级。

2. 能完成 NAT 内部 SIP 终端和 NAT 外部标准终端之间以及双方都是 NAT 内部 SIP 终端之间的语音通信。

3. 能与其他现存的 SIP 终端结合使用。

4. 能透明穿透多层 NAT。

当然系统完善的过程中，我们也发现和引入了不少新的问题，这需要在今后的工作中去研究解决。

而通过前期的大量调研，中期的设计与实现，后期的测试与改善，系统越来越实用。同时在整个过程中，作者也经历和体验了一个项目的全过程，收获非常大。

## 7. 2 技术展望

随着以 DSL 技术和以太网技术为主的宽带接入业务的大规模展开，网络最后一公里的问题得以相对解决；另一方面 SIP 及其相关的协议的不断完善，让用户对通过网络提供更灵活，更稳定，更经济的多媒体通信业务提出更高要求。 这推动了 VOIP 的发展， 而 VOIP 也正是基于软交换系统的 NGN 的重要部分。但只要 NAT 和 Firewall 存在(而且会长期存在，不会因为 IPv6 的普及而消失)，VOIP 的发展就会受制约，毕竟绝大多数终端用户都是在私网里。在目前协议标准和 VOIP 发展水平的条件下，解决 NAT 问题的好的方案并不多。 但随着相关行业的发展，今后很有可能会有一个统一的，大家认可的穿越 NAT 的标准方案。这将大大加快 IP 网络上的多媒体业务的开展。[30]

另一方面，在调研和方案设计过程中感受最深的就是，如果企业有实力一定要加入到标准的制定者行列。 一些国外大企业的产品并不完全遵循协议的标准， 因为他们有整套的解决方案和从终端到系统的全套产品，又有很大的影响力和客户群。在我们处在既要符合并不完善的标准又要解决实际问题的矛盾路口时，这些大企业现在看来不标准的产品将来却有可能成为新的标准。

最后，由于作者的水平和时间的限制，论文中难免出现纰漏和错误，恳请各位专家和同行批评指正.

# 参考文献


[1] ITU-T Rec，H.323 Packet based multimedia Communication Systems，February 1998

[2] J. Rosenberg，H. Schulzrinne，G. Camarillo，A. Johnston，J. Peterson，R. Sparks，M. Handley，E. Schooler，SIP: Session Initiation Protocol，RFC3261，June 2002

[3] M. Handley，H. Schulzrinne，E. Schooler，J. Rosenberg，SIP: Session Initiation Protocol，RFC2543，March 1999

[4] IP 电话相关的国际标准化组织，中国 VoIP 论坛网技术文摘，http://www.chinagk.org/technology/thj03.htm

[5] H. Schulzrinne，S. Casner，R. Frederick，V. Jacobson，RTP: A Transport Protocol for Real-Time Applications，RFC1889，January 1996

[6] M. Handley，V. Jacobson，SDP: Session Description Protocol，RFC2327，April 1998

[7] ITU-T Rec，H.450.1 Generic functional protocol for the support of supplementary services in H.323，February 1998

[8] B.Rraden，L.Zhang et al，Resource ReSerVation Protocol(RSVP) – Version 1 Functional Specification，RFC2205，October 1997

[9] S. Deering，R. Hinden，Internet Protocol，Version 6 (IPv6) Specification，RFC2460，December 1998

[10] 平耀锋，简述 VoIP 技术，河北电信设计咨询有限公司，2002 年 8 月

[11] K. Egevang，P. Francis，The IP Network Address Translator (NAT)，RFC1631，May 1994

[12]阮帮秋，IP 网络的现状和发展趋势，www.bj.gs.cn

[13] Handley，Schulzrinne，Schooler，Rosenberg，“SIP: Session Initiation Protocol”，Internet-Draft，draft-ietf-sip-rfc2543bis-04.txt，July 20，2001

[14] SIP 协议概述，中国 VoIP 论坛网技术文摘，http://www.chinagk.org/technology/thj07.htm

[15] H. Schulzrinne，A. Rao，R. Lanphier，Real Time Streaming Protocol (RTSP)，RFC2326，April 1998

[16] 糜正琨，IP 网络电话技术，人民邮电出版社，2000 年 6 月

[17] 赵勇，曾珂，戴琼海，服务于流媒体的实时传输协议 RTP，清华大学信息学院多媒体中心，2002 年 5 月

[18] 陈维义，NAT——网络地址翻译，中国计算机报 768 期，1998 年 10 月

[19] M.Arango，C.Huitema et al，Media Gateway Control Protocol (MGCP)，IETF draft，February 1999

[20] P. Srisuresh，M. Holdrege，IP Network Address Translator (NAT) Terminology and Considerations，RFC2663，August 1999

[21] 计育青，VoIP 迈向主流应用，CTI 论坛 www.ctiforum.com

[22] 流媒体技术基础-流媒体传输协议，www.cninfo.com，2001.10

[23] ITU-T Rec，· H.248， Gateway control protocol， June 2000

[24] 袁帅，多媒体通讯中防火墙和 NAT 问题的解决，赛迪网，2002 年 12 月

[25] J. Rosenberg， J. Weinberger， C. Huitema， R. Mahy， "STUN - Simple Traversal of UDP Through Network Address Translators"， Internet-Draft， draft-ietf-midcom-stun-02.txt， August 22， 2002

[26] J.Rosenberg， J.Weinberger， H.Schulzrinne， "NAT Friendly SIP"， Internet-Draft， draft-rosenberg-sip-entfw-02.txt， February 2002

[27] D. Yon， "Connection-Oriented Media Transport in SDP"， Internet-Draft， draft-ietf-mmusic-sdp-comedia-04.txt， July 2002

[28] C.Rigney， RADIUS Accounting， RFC2139， April 1997

[29] David G. Kelly， Cullen Jennings， Luan Dang， Practical VoIP Using VOCAL ， O'Reilly ， July 2002

[30] Prince Mehta，Sanjay Udani, Voice over IP, Technical Report MS-CIS-01-31

[31] VOIP 的关键技术, 国信 VOIP 网

[32] Olivier Hersent，David Gurle, Jean-Pierre Petit 著，邝坚，戴志涛译，IP 电话—基于分组的多媒体通信系统，人民邮电出版社，2002.10

[33] 用户选购防火墙的十项注意，赛迪网，2002.06

[34] 文风，防火墙的分类，www.networkunion.org/suject/firewall/firewall2.htm

[35] Kevin Archer 等著，王堃，周毅等译，语音与数据安全，机械工业出版社，2002.07

[36] 谈路由器 NAT 功能的配置，www.ccw.com.cn，2001.01

[37] Vovida Open Communication Application Software Installation Guide, www.vovida.org

[38] 卢政，在 Vovida 的基础上实现自己的 SIP 协议栈，www.ctiforum.com, 2003.08

[39] Rusty Russell, Linux 2.4 Packet Filtering HOWTO, lists.samba.org, June 2006

# 附录

## 附录一：缩略语

VoIP: Voice over Internet Protocol(IP 承载语音)

IETF: The Internet Engineering Task Force (互联网工程任务组)

RFC : The Request for Comments(请求解释文档)

ISP : Internet Service Provider(因特网服务提供商)

QoS: Quality of Service（服务质量）

RSVP : Resource ReSerVation Protocol(资源预留协议)

SIP: Session Initiation Protocol（会话初始化协议）

SDP: Session Description Protocol（会话描述协议）

RTP: the Real-time Transport Protocol（实时传送协议）

RTCP: RTP control protocol（实时传送控制协议）

DMZ: Demilitarized zone（非军事化区）

UA: User Agent（用户代理）

UAC:User Agent Client（用户代理客户端）

UAS: User Agent Server（用户代理服务器端）

FS: Feature Server（特色服务器）

RS: Redirect Server（重定向服务器）

PS: Provision Server （规定者服务器）

MS: Marshal Server （招待员服务器）

MPMS: Media Proxy Marshal Server（媒体流代理招待员服务器）

CDR Server: Call Detail Recording Server（呼叫详细记录）

VPN: Virtual Private Network (虚拟专用网)

STUN: Simple Traversal of User Datagram Protocol Through Network Address Translators（用户数据报协议简单穿越地址转换）

NAT: Network Address Translation(网络地址转换)

PSTN: Public Switched Telephone Network（公共交换电话网络）

# 附录二：图表索引

# 致　谢

在论文行将定稿的时候，作者要十分感谢导师王安生老师，副导师罗宗贶先生，宋茂强老师，刘禾老师，他们在专业方向上的指点和工作方式上的指教让作者受益匪浅。不仅鼓励作者在一些理论上要有突破，还指导作者理论研究和实际项目结合起来，最后还要将实践过程中的收获再提高到理论，使我们的研究有延续性，这对我们自己和今后的研究者都是一笔财富。

作者感谢在维信和科技有限公司做课题的一年的时间里，公司的同事们，特别是马驹（总经理），柳少华等对作者的关心与帮助，他们给予了作者宝贵的锻炼机会，在项目上大力帮助和指导了作者。

作者感谢学院各位老师的关心和帮助。感谢同学王擎，王玉红，陈卓，孙建勇，马南鹏和刘东琦等人，他们和作者进行了大量的有益的探讨，对于作者的工作给予大量的帮助。

作者还要特别感谢家人的关心与支持。正是他们不断的鼓励自己跨越生活中遇到的各道障碍，克服前进中的一个又一个的困难。

最后，对百忙之中审阅我的论文和参加答辩会的老师们表示最诚挚的感谢！

# NAT环境下VoIP的解决方案与性能研究——SIP，RTP协议在VoIP中的应用

作者：刘涛
学位授予单位：北京邮电大学
被引用次数：2次

## 引证文献(2条)

1. 朱晓东 基于单DSP的模拟电话适配器关键技术研究与实现[学位论文]博士 2006

2. 张毅 基于SIP协议的IP电话穿透NAT/FW的研究和应用[学位论文]硕士 2005