

P2PSIP 系统中 NAT 穿越方案的研究与设计

王 南, 孙保锁, 王月平

(苏州大学 计算机科学与技术学院, 江苏省计算机信息处理技术重点实验室, 江苏 苏州 215006)

摘 要: P2PSIP 系统整合了 P2P 技术和 SIP 协议的优势, 是当今网络技术领域的热门应用之一。作为端到端的应用, NAT 穿越是 P2PSIP 系统所必须解决的关键问题之一。首先概述了 NAT 的由来、工作原理及 NAT 的各种常见类型; 然后阐述了系统中信令穿越 NAT 和媒体流穿越 NAT 所面临的问题; 随后分析了当前各种 NAT 穿越方法的优缺点, 在此基础上提出一种 P2PSIP 结点穿越 NAT 的方案: STUN + TURN 方式, 并在扩展会话描述协议 SDP 的基础上对该方案进行了详细设计。采用该方案的 P2PSIP 系统可以实现正常的 VoIP 通信。

关键词: P2PSIP; NAT 穿越; STUN; TURN; 会话描述协议

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2009)10-0066-04

Research and Design of NAT Traversal Scheme in P2PSIP System

WANG Nan, SUN Bao-suo, WANG Yue-ping

(Jiangsu Province Key Lab. of Computer IT, School of Computer
of Soochow University, Suzhou 215006, China)

Abstract: P2PSIP system is one of the most popular network application which integrates the advantage of P2P technique and SIP. As a Peer to Peer application, P2PSIP system must solve the problem of NAT traversal. Firstly outlines the origin, working mechanism and types of NAT; then analyzes the problem of NAT traversal in P2PSIP system; and proposes an STUN + TURN scheme based on the research of several NAT traversal methods, while describes it in detail on the foundation of extension of SDP. Finally provides a brief summary of this scheme. In this scheme, P2PSIP system can realize normal communication of VoIP.

Key words: P2PSIP; NAT traversal; STUN; TURN; SDP

0 引言

随着接入 Internet 的计算机数量的不断猛增, 公网 IPv4 地址变得日益紧张。使用私有网络地址和 NAT(Network Address Translation)技术, 可以使得私有 IP 地址映射到 Internet 所使用的公网地址, 从而减少了公网地址的使用。NAT 不仅解决了 IP 地址不足的问题, 而且还能够有效地避免来自网络外部的攻击, 隐藏并保护网络内部的计算机。虽然 NAT 技术已经得到广泛应用, 但是在带来节省 IPv4 地址空间等好处的同时, 破坏了 Internet 最基本的“端到端的透明性”的设计理念, 增加了网络应用的复杂性, 阻碍了业务的扩展和创新。

P2PSIP 系统^[1]整合了 P2P 技术和 SIP 协议^[2]的优势, 已成为互联网提供语音/视频会议、文本聊天等多媒体业务的首选系统结构。P2PSIP 电话系统如图

1 所示。它要求各终端之间能够直接进行端到端的通信。因此, 对于 P2PSIP 系统, 如何穿越 NAT, 从而使内网中的结点可以与公网中的结点或者其他内网中的结点进行通话, 成为其需要解决的关键问题之一。

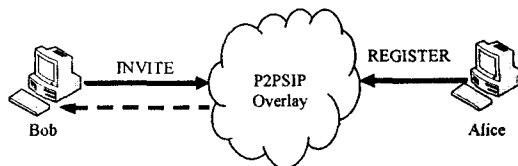


图 1 P2PSIP 系统

1 NAT 原理及常见类型

NAT 的实质是在路由器或代理服务器上维护一个映射表, 用来把内部的地址 (IP 地址、端口号) 映射到合法的外部地址上去。处于私网内的终端结点与外部进行通信时, 发起方的结点首先经过 NAT 设备向外发送数据包, NAT 设备会为该次通信建立 IP 地址和端口号的映射, 同时自动修改其 IP 包中的源 IP 地址和端口, 并且准备接收向该结点发回的数据包。其功

收稿日期: 2009-02-23; 修回日期: 2009-05-16

作者简介: 王 南 (1985-), 男, 硕士研究生, 研究方向为 P2PSIP 网络电话; 导师: 陆建德, 教授, 研究方向为网络技术与信息安全。

能简化如图 2 所示。

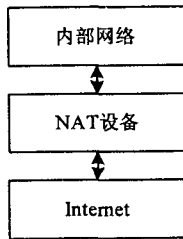


图 2 NAT 功能示意图

根据建立地址映射的方式不同,NAT 大致可以分为四种类型^[3]: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),对称型 NAT (Symmetric NAT)。前三种 NAT 也被称为非对称性 NAT,NAT 映射与目的地址无关,只要源地址相同,映射就相同;对称型 NAT 的映射则同时关联源地址和目的地址。

各种 NAT 类型说明如下:

(1) 完全圆锥型 NAT。

首先,把所有来自相同内部 IP 地址和端口的请求映射到相同的外部 IP 地址和端口。其次,任何一个外部主机通过把一个 IP 包发送给已得到映射的外部 IP 地址的方式,都能够把该包发送给该内部主机。

(2) 地址限制圆锥型 NAT。

地址限制圆锥型 NAT 也是把所有来自相同内部 IP 地址和端口号的请求映射到相同的外部 IP 地址和端口。但是与完全圆锥型 NAT 不同,只有当内部主机以前曾经给 IP 地址为 x 的外部主机发送过一个包时,IP 地址为 x 的外部主机才能够把一个 IP 包发送给该内部主机。

(3) 端口限制圆锥型 NAT。

端口限制圆锥型 NAT 与地址限制圆锥型 NAT 类似,只是限制中多了端口号。特别是,一个外部主机可以发送一个源 IP 地址和源端口号分别为 (x, P) 的 IP 包给内部主机,只有当内部主机以前曾经给 IP 地址为 x ,端口号为 P 的外部主机发送过一个包时,IP 地址为 x 的该外部主机才能够把一个源端口号为 P 的 IP 包发送给该内部主机。

(4) 对称式 NAT。

对称式 NAT 是指把所有来自相同内部 IP 地址和端口号到特定目的 IP 地址和端口号的请求映射到相同的外部 IP 地址和端口。如果同一主机使用不同的源地址和端口对,发送的目的地址不同,则使用不同的映射。只有收到了一个 IP 包的外部主机才能够向该内部主机发送回一个 IP 包。对称式的 NAT 不保证所

有会话中的(私有地址,私有端口)和(公开 IP,公开端口)之间绑定的一致性。相反,它为每个新的会话分配一个新的端口号。

2 P2PSIP 系统中的 NAT 穿越

在 P2PSIP 系统中,各结点间的通信包括两类数据包:SIP 信令和媒体流^[4]。SIP 信令通信的目的是建立呼叫连接,媒体流通信则是实现语音流的互通。所以,系统中各结点要实现通信,必须分别解决如下两个问题^[5]:

(1) SIP 信令穿透 NAT 的问题:分布在两个私网后的终端节点利用 SIP 信令建立呼叫连接时,被叫方 NAT 会丢弃主叫方发来的数据包,所以设法建立通信双方在本端 NAT 的映射,使得通信发起方的呼叫可以无碍到达对方结点,是终端节点所必须解决的问题。

(2) 媒体流穿透 NAT 的问题:媒体流通信包括媒体流的协商及媒体流的传输。媒体流协商通过在 SIP 协议层的 SDP 消息体中填入适当信息,并按照 SDP 协议进行协商来实现。当 SIP 信令穿透 NAT 并成功建立呼叫连接后,开始进行媒体流协商时,发起呼叫的终端 A 的 IP 地址和端口号会填入 SIP 信令数据包的 SDP 消息体中发往终端 B。终端 B 分析收到的数据包中的 SDP 消息体,从中提取终端 A 的 IP 地址和媒体流端口,并开始发送媒体流到此 IP 地址和端口。如果这个 IP 地址是私网地址,就无法路由该消息到达 B 终端。在这种情况下,虽然 SIP 呼叫已经建立,但终端 A 无法收到终端 B 的媒体流。由于在 SIP 协议层的 SDP 消息体包含通信结点的 IP 和端口地址,在媒体流协商时,需要把通信源结点的 SIP 层 SDP 消息体中的私网 IP 和端口地址转换为该结点的 NAT 映射后的公网 IP 地址和端口,随后才可以实现媒体流通信。

通过分析可知,SIP 信令穿越 NAT 可以通过信令中的 received 标记和 rport 标记分别记录接受返回包的 IP 地址和端口号。而媒体流穿越 NAT 需要媒体流通过 SDP 消息中的 c 行和 m 行来得到数据包的地址和端口。接下来根据 NAT 类型做具体分析。

3 NAT 穿越方案概述

目前已存在多种 NAT 穿越方案:ALG, MIDCOM, STUN, TURN 等。这几种穿越方式有如下特点:ALG (Application Level Gateway, 应用层网关) 方式,实现简单,但需要对现有 NAT 设备升级同时需要 NAT 设备对所有数据包进行监控和解析,其性能、可扩展性和可实施性较差;MIDCOM (Middlebox Communications, 中间盒通信)^[6]方式,性能较好但实现复杂,

需要对所有 NAT 设备升级,投入大,实现周期长;STUN(Simple Traversal of UDP over NATs, NAT 的 UDP 简单穿越)^[7]方式,协议简单,采用 C/S 架构,支持多级 NAT,但不支持 TCP,无法在对称型 NAT 下工作;TURN(Traversal Using Relay NAT,中继方式穿越 NAT)^[8]方式,采用 C/S 架构,私网用户发出的报文都要通过 TURN 服务器进行 Relay 转发,可以解决所有 NAT 穿越问题,但是 TURN 服务器负担重,容易出现延时和丢包问题。

因此,对于不同的 NAT 类型,可以采用不同的穿越方式,可是不同的穿越方法只适用某种特定类型的 NAT 设备,至于如何充分利用这些针对各种不同 NAT 的解决方案,应该综合考虑。文中采用 STUN+TURN 方式来实现 NAT 穿越;其中,使用 STUN 方式穿透非对称性 NAT,使用 TURN 方式穿透对称性 NAT,具体描述如下。

3.1 STUN 方式穿越非对称性 NAT

对于上文中提到的前 3 种 NAT 类型,即非对称性 NAT,可以采用 STUN 方式穿透,具体描述如下:

在 P2PSIP 系统中的结点内置 STUN 客户端,结点通过 UDP 方式向 NAT 外的 STUN 服务器发送请求消息,服务器在收到请求后,生成响应消息,响应消息中携带了 STUN 客户端在 NAT 设备上对应的外部端口,然后将响应消息发送给 STUN 客户端,后者通过响应消息体中的内容得知其在 NAT 上对应的外部地址,并且将其填入呼叫协议以后的 UDP 报文负载中,告知目的端节点自己的接收地址和端口号。

这样报文负载中的内容在经过 NAT 时就无须修改了,只需按普通 NAT 流程转换报文头的 IP 地址即可,并且负载中的地址信息和报文头地址信息是一致的。

采用 STUN 方式无须改动现有的 NAT 设备,同时 STUN 方式可在多个 NAT 串联的网络环境中使用,支持 NAT 的多级穿越。对于非对称性 NAT,只要知道了内网主机对应的公网 IP 和端口,那么在 SDP 消息中填上这些地址信息就可以了。但是 STUN 无法在对称型 NAT 下工作,因为用户到 STUN 服务器所映射的 IP 地址与用户到通话方所映射的 IP 地址将不一样。另外,STUN 并不适合支持 TCP 连接的穿越。

3.2 TURN 方式穿越对称性 NAT

因为在对安全性要求较高的企业网中,出口 NAT 通常采用的是对称型 NAT,故而在一定程度上限制了 STUN 方式穿越 NAT 的应用范围。对于对称型 NAT,可以采用 TURN 方式穿越。TURN 方式解决

NAT 问题的思路和原理类似于 STUN 方式。不同之处在于,STUN 方式发送给用户的是它所看到的对应公网地址,TURN 方式则是通过 TURN 服务器分配一个 IP 地址和端口号发送给用户,采用 TURN 服务器的地址和端口作为私有网客户端对外的接收地址和端口,即内网用户发出的报文都要经过 TURN 服务器进行中继转发。

采用 TURN 方式可以解决 STUN 方式无法穿透对称型 NAT 的问题,同时 TURN 还支持基于 TCP 的应用。其局限性在于所有报文都必须经过 TURN 服务器转发,增大了包的延迟和丢包的可能性。

4 NAT 穿越方案的实现

根据上述分析,采用 STUN+TURN 方式来实现 NAT 穿越,即在 PSBDK 系统中的每个结点中同时配置 STUN 和 TURN 客户端,应用程序优先采用 STUN 方式进行通信。以媒体流穿透 NAT 为例,分析如下:

进行媒体流通信时,结点首先连接公网上已存在的 STUN 和 TURN 服务器,并把得到的地址放在 SDP 消息中进行发送至会话对应端,会话对应端收到并解析此 SDP 消息,按照 STUN 优先的规则尝试连接所给出的地址,直到找到可以互通的地址为止。

为实现这一目标,需要扩展 SDP 协议,加入一个新的 SDP 头域,描述如下:

plus= IP Address;Port number

其中,IP Address 和 Port number 分别指本地客户端通过查询 STUN 服务器所得到的 IP 地址和端口号。

假设通话的双方是 A 和 B,且 A 和 B 都处于 NAT 之后,A 和 B 的 IP 地址分别为 192.168.150.1 和 192.168.151.1;在公网上架设 STUN 和 TURN 服务器,服务器 IP 地址分别为 202.195.1.1 和 202.195.2.1。服务器均使用默认设置,STUN 监听 3478 端口,TURN 监听 5556 端口。

假设 A 为这次会话所分配的端口为 1234,A 接着连接 STUN 和 TURN 的服务器,然后得到所返回的端口号。分配的端口号分别为 8000 和 9000。A 端收集到 STUN 和 TURN 所返回的地址后,把查询 TURN 服务器得到的 IP 地址和端口号放入 SDP 的 *c* 和 *m* 中。而新加的 SDP 属性中放 STUN 的地址。消息体如下所示:

c = IN IP4 202.195.2.1

m = audio 9000 RTP/AVP 0

plus = 202.195.1.1:8000

消息到达 B 端后,B 端首先也进行与 A 相同的操作,连接 STUN 和 TURN 服务器。B 端得到的 STUN

和 TURN 服务器分配的端口号分别为 8100 和 9100。B 端得到地址后就开始用 STUN 从本地的地址(192.168.151.1:2345)来尝试连接 A 端所提供的地址。B 端的应答消息体中 SDP 地址结构与 A 类似。消息体如下所示:

$c = \text{IN IP4 } 202.195.2.1$

$m = \text{audio } 9100 \text{ RTP/AVP } 0$

$\text{plus} = 202.195.1.1:8100$

以下对 A 分两种 NAT 情况讨论:

(1) 若 A 为非对称性 NAT: 因为 A 处于非对称性 NAT 之后, A 的 STUN 地址可以连通, 那么 A 端送来的 c 和 m 的地址在 B 端就可以不去测了。这时 B 端发应答给 A, 同时可以向测通的 A 端的这个地址发送音频流。A 收到应答后, 同样从本地地址(192.168.150.1:1234)发送 STUN 请求来尝试连接 B 应答中所给出的地址直到有一个可以连通为止。同样的如果 B 端在非对称型 NAT 之后, 那么 B 的 STUN 地址将可以通信。

(2) 若 A 为对称型 NAT: 首先 B 端也会去尝试连接 A 端的 STUN 地址, B 端的 STUN 消息到达 A 端的 NAT, 因为 A 端是对称型 NAT, 这个包会被丢掉, A 没有应答, 那么 STUN 地址将不会通。这个时候 B 端会测 A 的 TURN 地址。B 端连接 A 端的 TURN 地址会成功。B 端在收到 A 应答时就可以用地址向 A 发送语音流, 连通成功。

该节主要讲述的是媒体流数据的 NAT 穿透。进行媒体数据传输的前提是已经建立信令连接, 关于

SIP 信令的穿透也可以用类似的方法处理。

5 结束语

文中分析了应用 P2PSIP 系统时面临的 NAT 穿越的问题, 在分析各种 NAT 穿越方法的基础上提出一种 STUN + TURN 方式穿越 NAT 的方案。同时通过对会话描述 SDP 进行扩展(增加头域)以实现该方案。采用该方案的 P2PSIP 系统可以实现正常通信。

参考文献:

- [1] Bryan D, Matthews P, Shim E, et al. Concepts and Terminology for Peer to Peer SIP[S]. draft-ietf-p2psip-concepts-01, 2007.
- [2] Rosenberg J, Schulzrinne H, Camarillo G, et al. SIP: Session Initiation Protocol[S]. RFC 3261, 2002.
- [3] 何宝宏. 浅析 NAT 的类型[J]. 电信网技术, 2004, 8(8): 427-430.
- [4] 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.
- [5] 王健婷, 赵 霞, 刘 杰, 等. 基于 P2PSIP 的 NAT 穿透方法的研究[J]. 北京工商大学学报, 2008, 5(5): 615-618.
- [6] Mart P A, Sijben P, Brim S, et al. Middlebox Communications (midcom) Protocol Requirements[S]. RFC3304, 2002.
- [7] Rosenberg J, Weinberger J, Huitema C, et al. Simple Traversal of User Datagram Protocol Through Network Address Translators[S]. RFC 3489, 2003.
- [8] Rosenberg J, Mahy R, Huitema C. Traversal Using Relay NAT[S]. Internet - Draft, 2005.

(上接第 65 页)

在服务注册中心注册后, 即可通过与其他服务模块的组合实现新的功能。

5 结束语

文中把 SOA 模块化整合思想引申到 Web 软件系统的建设过程中。采取与整合相反的方式, 把系统进行模块化划分, 设计了用户交互中心(UIC)、虚拟处理中心(VCPU)等媒介以协调各个系统各个模块的组合, 提高了系统的可扩展性和灵活性, 增强了系统的适应能力。同时, 本事务处理模型通过引入进程, 可以对用户某项业务的使用状态加以监控。后续的工作要把用户的业务使用偏好引入到模型中, 在统计用户业务偏好的基础上改进服务组合, 对不同的客户提供准确的服务。

参考文献:

- [1] Jeng J J, An Lianjun. System Dynamics Modeling for SOA

Project Management[J]. Proceedings of the IEEE, 2007(7): 286-294.

- [2] 杨象驰, 李鹏飞. 基于 SOA 的邮政物流信息系统规划[J]. 计算机工程与设计, 2007, 28(19): 4825-4827.
- [3] 王一宾, 张玉州, 程一飞. 几种新型软件体系结构风格的分析[J]. 计算机技术与发展, 2008, 18(8): 39-42.
- [4] Wu Jian, Wu Zhaohui. Similarity-based Web Service Match-making[J]. Proceedings of the IEEE, 2007(1): 287-294.
- [5] 周 煜, 成 斌, 童维勒. 基于 QoS-Ontology 的 Web 服务选择 Broker 模型[J]. 计算机应用与软件, 2008, 25(9): 10-16.
- [6] Chang Fu-chun, Hung Tai-chang, Chiou Young-jang, et al. Design and implementation of web service integration Tool [J]. Proceedings of the IEEE, 2005(10): 91-96.
- [7] 李 磊, 牛春雷, 陈宁江, 等. 一种高效的 Web 服务性能优化策略[J]. 计算机研究与发展, 2007, 44(7): 1191-1198.
- [8] 惠敏顺, 朱国进. 基于 SOA 的分布式程序设计竞赛系统的研究[J]. 计算机技术与发展, 2008, 18(10): 123-126.