基于STUN协议的NAT路由器穿越算法设计与实现

刘胜辉[1]，刘油锤[2]
(1.哈尔滨理工大学 软件学院，黑龙江 哈尔滨 150080；
2.哈尔滨理工大学 计算机科学与技术学院，黑龙江 哈尔滨 150080)

摘 要：NAT穿越是多媒体传输技术中的一个重要研究课题，STUN解决方案能解决部分NAT的穿越问题，但是还有一定的弊端。在STUN技术的基础上，介绍了NAT路由器的识别方法，详细分析并设计一种解决NAT路由器穿越问题的算法，并对处于不同NAT路由器环境下的直接通信给出一种解决方案。既提高了NAT路由器的识别效率，也改善了通信质量。

关键词：NAT；STUN；直接通信；穿越
中图分类号：TN915.05 文献标识码：A

Design and achievement of traversal NAT router based on STUN protocol

LIU Sheng Hui[1], LIU You Chui[2]
(1.College of Software, Harbin University of Science and Technology, Harbin 150080, China;
2.College of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China)

Abstract: Network access translator(NAT) traversal solution is an important research project in transportation technology of multimedia. STUN (simple traversal of UDP through network address translators) can afford solutions for NAT traversal, but it has some drawbacks. A solution about traversal NAT Router designs and research in detail. It can improve the efficiency of identifying NAT and reform the quality of communication.

Key words: NAT; STUN; connect directly; traversal

NAT是为了解决网络IP地址资源紧缺而出现的一种技术，由于其具有隐藏内网IP的功能，增加了内网的网络安全性，所以得到了广泛的应用。但是，由于外网主机不能首先发起对处于NAT后主机的访问，特别是处于两个内网主机不能直接进行通信，这对一些应用程序的部署造成一定的困难。比如说网络视频会议系统和VoIP系统。为了解决这个问题，也就是处于内网的主机之间能够穿越它们之间的NAT建立直接通信，已经提出了许多方法，STUN(Simple Traversal of UDP Through NetWork Address Translators)技术就是其中比较重要的一种解决方法，并得到了广泛的应用。

本文主要是基于STUN协议，对NAT路由器识别问题进行研究，对NAT类型的判断方法做了改进，详细分析并提出一种算法来解决NAT路由器穿越问题，对处于NAT路由器后的主机设计了直接通信方案。

1 NAT(Network Address Translator) 介绍

1.1 NAT简述

NAT即网络地址转换，是一个IETF(Internet Engineering Task Force)标准，它允许一个整体的组织或机构用一个公用的IP地址出现在网络上，归根到底，NAT就是把内部私有的IP地址翻译成公网上合法的IP地址的一种技术。

NAT负责把内部主机的数据包的源地址(私有IP地址)按照一定的规则翻译成合法的、唯一的公网IP地址，源数据包的端口转换成NAT的一个端口，目的IP地址和端口不变，最终数据包经过路由器发送到目的地址。同时，NAT也负责把外部主机返回的数据包的目的地址和端口转换成内网的私有地址和端口，源地址和端口不变。这种变换的本质是在NAT内部维护着一张转换表，负责由内到外和由外到内的IP地址与端口的转换。

对于视频会议和 VoIP 软件来说，对位于不同 NAT 内部的主机通信需要靠服务器来转发完成，这样就会增加服务器的负担。为了解决这种问题，要尽量使位于不同 NAT 内部的主机建立直接通信，其中，最重要的一点就是要判断出 NAT 的类型，然后才能根据 NAT 的类型，设计出直接通信方案。

1.2 NAT 类型

根据 STUN 协议，把 NAT 分为以下几种类型

(1) 完全锥形(Full Cone)NAT：所有内部 IP 地址和端口的请求都被映射到相同的外部地址和端口，任何外部主机都可以通过映射的外部地址向内部主机发送数据包。

(2) 受限锥形(Restricted Cone)NAT：所有从相同内部 IP 和端口的请求都被映射为相同的外部地址和端口，与 Full Cone 不同的是，必须是内部主机已经向外部主机发送过数据包，外部主机才能通过 IP 地址向内部主机发送数据包。

(3) 端口受限锥形(Port Restricted Cone)NAT：和 Restricted Cone 类似，但是包括对端口的限制，外部主机(IP 地址 X，端口 P)向内部主机发送数据包当且仅当满足内部主机先前已经向(X,P)发送过数据包。

(4) 对称(Symmetric)NAT：限制最严格的 NAT，所有来自同一内部 IP 地址和端口发送到某一特定目的 IP 地址和端口的请求，都会映射为同一个目的地址和端口。若同一台内部主机从同一个端口发送数据包，只是目的地址和端口不同，那么映射关系也是不同的。并且，只有曾经收到过内部主机请求的外部主机才能向内部主机发送数据包。

2 NAT 路由器

2.1 STUN 技术简介

STUN 技术能使客户端应用程序发现它和公共互联网之间存在的 NAT 和防火墙及其类型，还能获得路由器分配给它的公网 IP 地址和端口号。它主要由三部分组成：STUN 客户端、STUN 服务器端、NAT 路由器。如图 1 所示。

STUN 客户端通过向服务器端发送不同的消息类型，根据服务器端不同的响应来判断客户端 IP 地址类型，如果是内部网络地址，还可以判断所经过的 NAT 类型，同时可以得到路由器分配给它的公网 IP 地址和端口(映射过的)。

STUN 服务器端根据客户端不同的动作(客户端发送不同的消息类型)作出不同的处理，可以获得客户端的源地址与端口(映射过得公网 IP 地址和端口)并返回给客户端。根据客户端发送的消息类型，按照要求用不同的 IP 地址和端口返回给客户端。

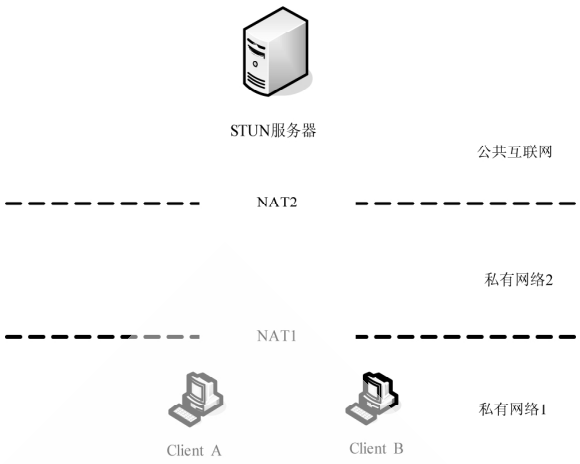

图 1 STUN 配置

2.2 NAT 路由器类型判断

2.2.1 测试方案设计

根据 RFC3489 提供的解决方案，NAT 类型的判断由客户端来完成。设计了下面两种测试方法。

测试 1：客户端(IP:A，PORT:A)向服务器(IP:B，PORT:B)发送消息，服务器响应客户端的请求，做出动作，服务器(IP:B，PORT:B)发送 Response 给客户端(IP:A，PORT:A)。

测试 2：客户端(IP:A，PORT:A)向服务器(IP:B，PORT:B)发送消息，服务器(IP:B，PORT:C)发送 Response 给客户端(IP:A，PORT:A)。

2.2.2 NAT 路由器类型判断

由图 2 可以得到客户端所处的网络环境有以下几种：

- 阻塞 UDP 的防火墙；
- 公开的互联网上(有公网 IP)；
- 对称型 UDP 防火墙；
- 完全锥形或受限锥形 NAT；
- 对称 NAT；

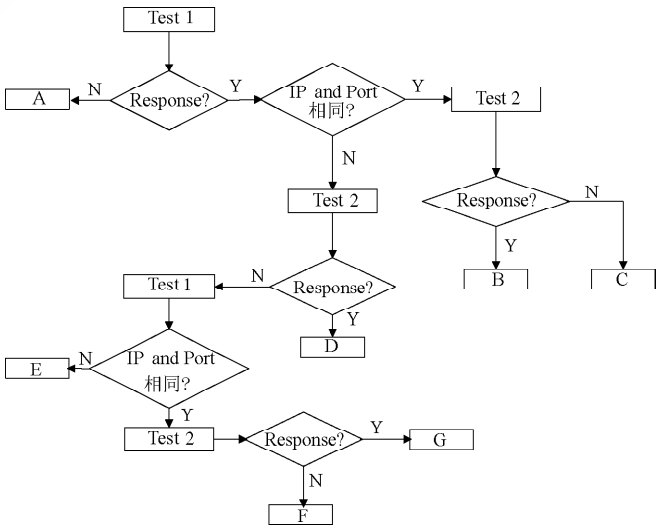

图 2 NAT 类型判断流程图

・端口受限锥形 NAT;

・受限锥形。

2.3 NAT 路由器类型判断改进

RFC3489 给出了判断 NAT 路由器类型的解决方案，它需要在公网上部署两台服务器才能对 NAT 路由器进行判断，这就需要两个 IP 地址才能完成测试，这在 Windows 环境下比较难实现，对于当今 IP 地址比较缺乏的情况下，往往要花费的成本比较大。本文对 RFC3489 所给的解决方案进行了改进，在同一台服务器上用不同的端口对客户端的消息进行响应，设计出以上的测试方案，来判断出 NAT 的类型。但是有些情况不能具体识别出固定类型，但是这并不影响后续工作，本文研究目的是为了在客户端之间建立直接联系。所以这种方法还是很有应用价值的。

3 NAT 路由器穿越算法设计

3.1 NAT 路由器穿越概述

通过以上的分析，很容易看出，对于处于不同网络环境的客户端来说，想进行直接通信，首先需要判断出 NAT 的类型，根据 NAT 路由器的类型来决定处于路由器后面的主机双方是否可以进行直接通信。以某个公司的网络为例，公司通过 NAT 路由器连接到公网上，公司内部通过 NAT 路由器建立了三个局域网。网络环境(见图 1)处于路由器后面的主机双方要直接通信需要有 STUN 服务器的配合。根据判断的 NAT 路由器的类型确定路由器后面的双方客户端是否可以建立直接通信。

3.2 NAT 路由器穿越算法

根据前面分析，NAT 路由器的穿越算法可以描述如下：

(1) 终端 A、B 分别登录服务器，判断自己所处的网络环境，即各自所处网络中 NAT 的类型。

(2) 从服务器获得终端 B 所处的网络 NAT 的类型，确定是否可以建立直接通信。

(3) 不能建立直接通信的情况，程序直接退出

(4) 对于可以建立直接通信的网络，确定具体的解决方案。有下面几种情况

a. 终端 A、终端 B 处于同一网段时，终端 A 直接向终端 B 发送 Message 消息。终端 B 响应 Message 消息，回复 Message 消息给终端 A。

b. 对于不同网段，分为两种情况。终端 B 为对称 NAT 的情况，终端 A 首先向终端 B 发送 Message 消息，然后终端 A 往服务器发送 Message2 消息。服务器收到 Message2 消息后，服务器再向终端 B 发送 Message3 消息，终端 B 根据收到的消息类型做出响应，往终端 A 发送 Message 消息；对于终端 B 为非对称 NAT 的情况，终端 A 首先向服务器发送 Message2 消息，然后再发送 Message 消息给终端 B。

(5) 终端 A、终端 B 退出服务器。建立直接通信成功。

在发送消息时，要建立消息来源信息库，如 IP 地址，端口号，以及映射关系。方便处理消息时使用相关资源。算法流程如图 3 所示，终端 A(图中用 A 标识) 与

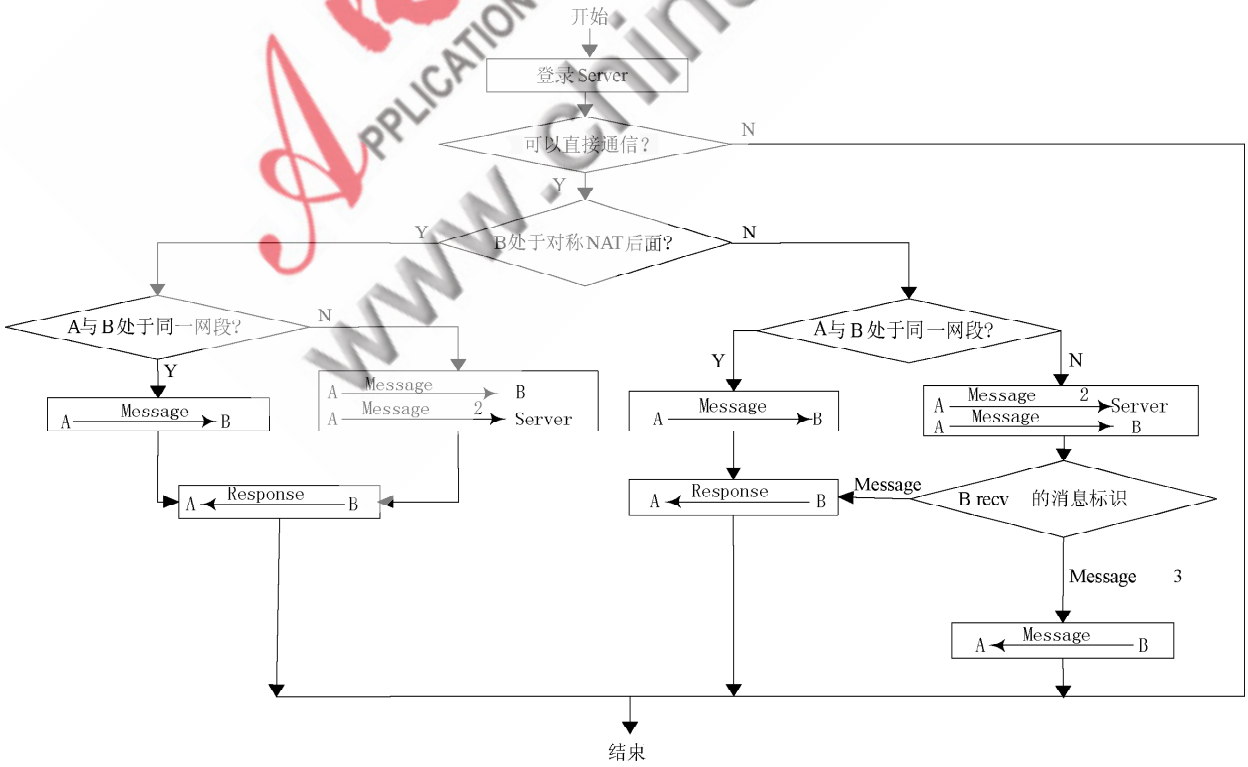

图 3 直接通信算法流程图

终端 B(图中用 B 标识) 建立直接通信，STUN 服务器为 Server。消息类型有 Message、Message 2、Message 3 三种消息类型。

这里以终端 B 所处的 NAT 类型为对称 NAT 为例，终端 A 的 IP 为 172.22.2.9，其公网 IP 为 210.80.43.104，Server 的 IP 为 202.120.58.178，终端 B 的 IP192.168.101.6，终端 B 的公网 IP 是 222.191.255.68。图 4 为终端 A 在与终端 B 建立直接通信的时序图。

图 4 中，只对终端 A 与终端 B 处于不同的网段内作了一个分析。对于二者处于同一个网段内的情况，比较容易解决,终端 A 直接向终端 B 发送 Message 消息即可建立直接通信。

对于终端 B 处于非对称 NAT 的情况，解决方案的差别之处就在于发送的消息顺序不一样。非对称 NAT 的情况下，终端 A 首先发送 Message 2 消息和服务器通信，然后在发送 Message 消息与终端 B 进行通信。这与对称 NAT 的情况刚好相反。

为了能够顺利的建立直接通信，在建立直接通信成功后，让客户端双方在相互通信 3 次，确认直接通信是否成功，在下面的仿真实验中可以体现出来。

有三种情况现在还没有找到比较好的解决办法：双方处于阻碍 UDP 防火墙的 NAT 路由器；双方都是对称 NAT 的防火墙；一方为对称 NAT，另一方为端口受限 NAT。

3.3 算法仿真结果

对于 NAT 路由器穿越算法，进行了实验测试，仿真中，发送的消息类型(TRANS，MESSAGE，Message3)，客户端实验结果如图 5、图 6 所示。

此外，对于双方客户端处于同一局域网内不同级别的 NAT 后面理论上是可以直接通信的，但是要取决于最外层的 NAT 是否支持 Loopback translate 功能，也就是内网主机 A 向内网主机 B 的最外层 NAT 外网地址和端口发送数据，最外层的 NAT 是够能够将数据转发给主机 B，如果最外层 NAT 支持此功能，则 A 和 B 可以建立直接通信，否则不能。

4 NAT 路由器穿越算法的优缺点

NAT 技术的优点决定了它的应用广泛性，但是根据 STUN 协议来实现 NAT 路由器的穿越问题往往需要的开销比较大，本文提出了一种比较方便的算法，在不增加成本的基础上能够准确地判断出来 NAT 路由器的类型，对 NAT 路由器穿越问题进行了详细的研究、设计。这对于中小型的企业来说，不仅节省了成本预算，而且达到了实际的效果。但是对于有些公司部署对称 NAT 路由器，该算法还有一些不足之处，还需要进一步研究，

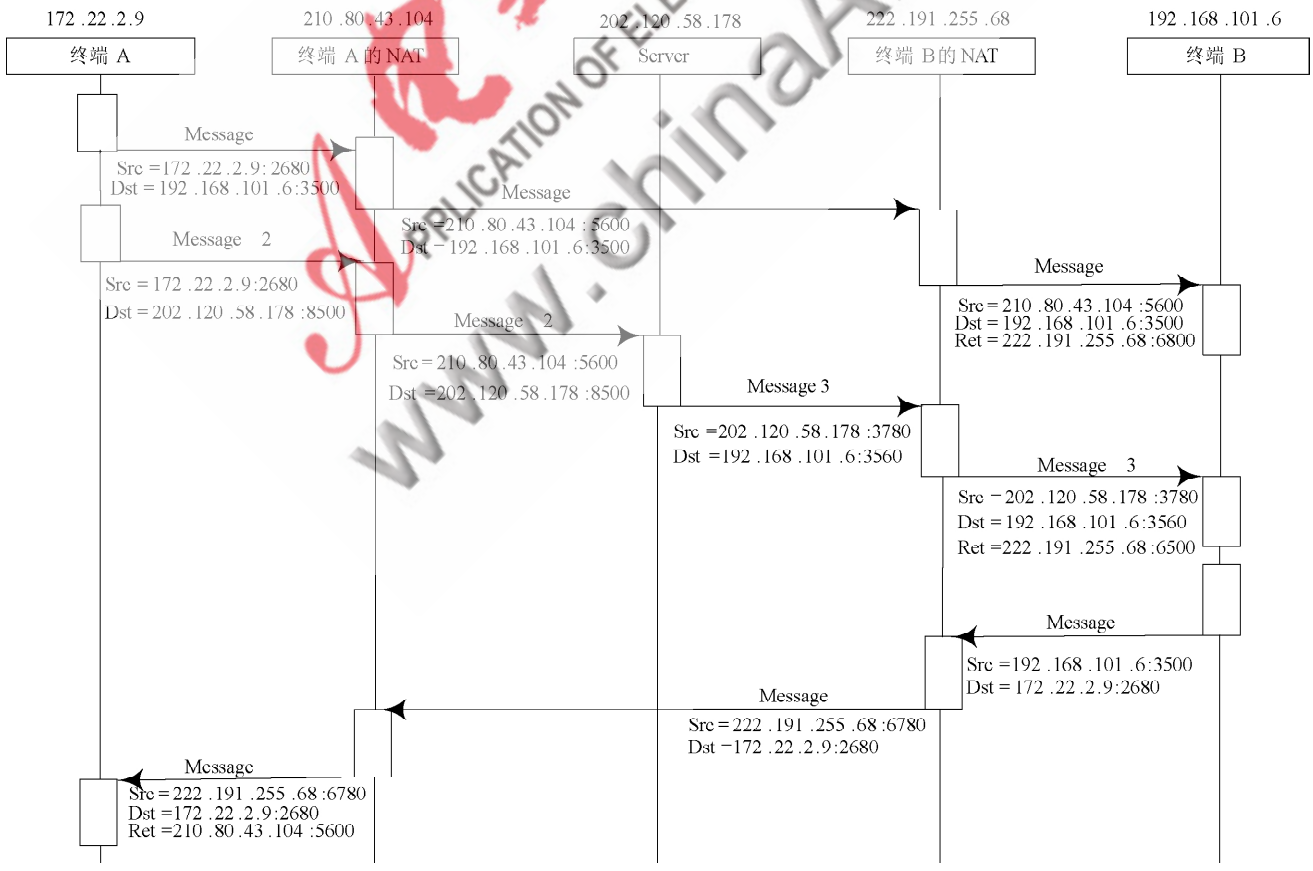

图 4 直接通信时序图

(下转第 52 页)

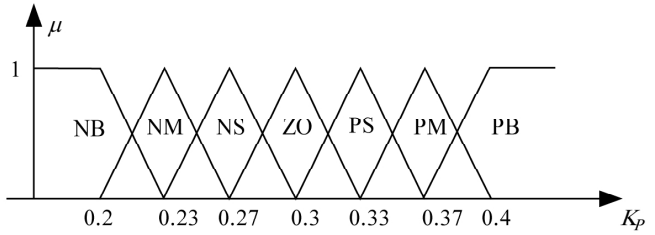

图 7 K_p 隶属度函数曲线

根据 K_p 的调整规则模型进行算法合成，求得响应的控制表如表 1 所示。其他参数依此类推。

表1 参数的Fuzzy调整控制

EC \ E	-3	-2	-1	0	1	2	3
-3	0.4	0.4	0.4	0.4	0.37	0.33	0.3
-2	0.4	0.4	0.4	0.4	0.38	0.3	0.3
-1	0.37	0.37	0.37	0.37	0.33	0.3	0.27
0	0.37	0.33	0.33	0.3	0.27	0.27	0.27
1	0.33	0.3	0.27	0.23	0.23	0.23	0.23
2	0.3	0.3	0.23	0.2	0.2	0.2	0.2
3	0.3	0.27	0.23	0.2	0.2	0.2	0.2

模糊控制器和传统控制器相比，具有更快的响应和更小的超调，而且具有很强的鲁棒性，能够克服非线性因素的影响。

本系统采用 AT89C52 单片机为核心来进行温度的测控，在环境温度下，使用同一个单元进行加热或制冷，减小了箱体的体积。配上所选的各种硬件，最大限度地减少了元器件的数量，资源也得到了充分的利用，一方面大大减少了开发成本，并使得控温精度达到 ± 0.5℃，另一方面本设计中由于引入温控的制冷作用，使得整个温控过程响应速度快，在较少的时间内能够完成控制目标，达到工业监控的要求。模糊 PID 算法的引入，消除了到工作现场来回设定参数的麻烦，能在较短的时间内实现温度的自动调节，是一种较好的设计方案，在箱体温控设备上有很好的应用前景。

参考文献

[1] 赵东辉. 单片机89C52在加热炉测控温度中的应用[J]. 电气开关，2002(5):10.

[2] 杨定安. 89C52单片机在可控硅调功温控系统中的应用[J]. 机电工程技术，2002,31(3):23.

[3] 戴佳，戴卫恒. 51单片机C语言应用程序设计实例精讲[M]. 北京：电子工业出版社，2006.

[4] 李军，王孙安. 模糊控制器在温度控制系统中的应用[J]. 机床与液压，2003(4).

[5] 王丽娟. 单片机在锅炉温度控制系统中的应用[J]. 微计算机信息，2007(2).

(收稿日期：2009-01-06)

(上接第48页)

图 5 客户端 A 实验结果

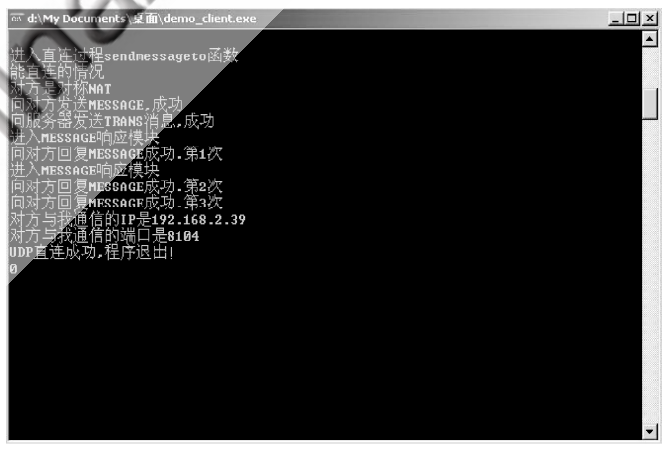

图 6 客户端 B 实验结果

对算法进行改进。

本文对 STUN 协议提出的 NAT 识别方法进行了有效地改进，并对 NAT 路由器的穿越问题进行了详细地研究，并设计出比较合理的算法。提高了效率，节省了成本。并指出了该算法的优点和不足。

参考文献

[1] ROSENBERG J, WEINBERGER J. STUN-Simple Traversal of user Datagram Protocol (UDP) Trough Network Address Translators (NATs). RFC3489, 2003.

[2] EGEVANG K. The IP Network Address Translator (NAT). RFC1631, 2001.

[3] HITEMA C. Short Term NAT Requirements for UDP Based Peer-to-Peer Applications. IETF Draft, 2001.

[4] P SRISURESH, M HOLDREGE . IP Network Address Translator (NAT) Terminology and Considerations. RFC2663, 1999.

(收稿日期：2008-12-29)