# 基于 STUNT 的 TCP 穿越 NAT 技术研究

庄霄，邓中亮
北京邮电大学电子科技学院，北京 (100876)
E-mail: craymails@gmail.com

**摘 要：**NAT(Network Address Translation)技术已经被广泛应用,得到了多数防火墙/网关设备的支持。但目前穿越 NAT 的方法都是大多是基于 UDP 来实现的。而 TCP 由于连接的建立需要经过三次握手并且存在状态转换,相比 UDP 在穿越 NAT 时存在更大的困难。本文首先研究了 NAT 技术的基本原理以及分类方法，并对目前基于 UDP 穿越 NAT 技术的实现方法以及 TCP 穿越 NAT 遇到的困难进行了分析。之后基于 STUNT 协议提出了一种 TCP 穿越 NAT 的方案，这个方案主要是利用发送一个低生命周期的信号来引发本地 NAT 返回一个 ICMP 错误消息，以获得 TCP 连接序号等信息，然后利用这些信息来伪造一个 TCP 连接的方法来实现穿越的。在本文的最后部署并测试了这一方案，证实了其可行性。

**关键词：**TCP； NAT； STUN； STUNT

## 1. 引言

NAT : (Network Address Translators;网络地址转换) [1]是在IP地址日益缺乏的情况下产生的,它的主要目的就是为了能够地址重用。NAT是一个IETF标准,它可以将局域网中的内部地址节点翻译成合法的IP地址在Internet上使用(即把IP包内的地址域用合法的IP地址来替换),或者把一个IP地址转换成某个局域网节点的地址,从而可以帮助网络超越地址的限制,合理的安排网络中共有Internet地址和私有IP地址的使用。

但NAT的存在将给通信双方建立会话连接带问题。比如:当主叫对处于NAT后的被叫发起会话请求时,由于此时被叫用户尚未在其NAT上留下端口映射关系,因此主叫不知道目的的端口号,NAT设备也不知道该往内网何处转发外来的请求。这种接连是不能建立成功的。如果通信双方都在NAT之后,建立会话连接将会更加困难。

目前基于UDP穿越NAT的技术已经发展的比较成熟，而且已经运用到了实际产品中，如Skype(一款著名的VOIP软件)。而由于TCP连接的特殊性,在穿越NAT时要比UDP困难的多。

## 2. 穿越NAT的原理

### 2.1 NAT的分类

主要的NAT可以分为下面四种[2]

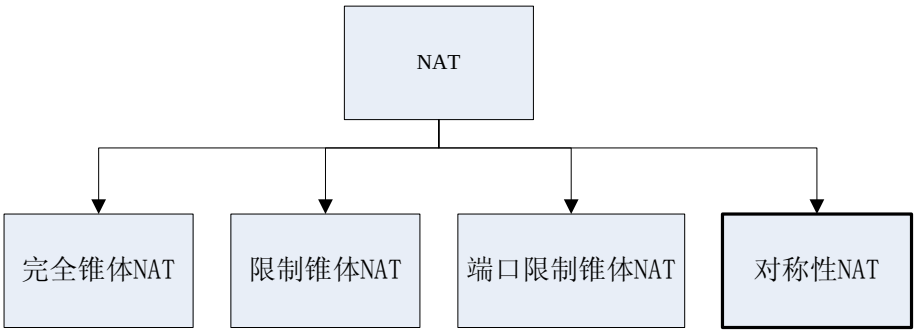


图1 NAT的分类

完全锥体(Full cone) NAT: 是指所有来自相同内部 IP 地址和端口的请求都映射到某一个相同的外部 IP 地址和端口上。此外,任意的外部主机可以通过发送信息包到内部主机对应的外部 IP 地址上来发送信息包。

限制锥体(Restricted cone) NAT: 是指所有来自相同内部 IP 地址和端口的请求都映射到某一个相同的外部 IP 地址和端口上。与完全锥体(Full cone) NAT 不同的是,一个外部主机只能在内部主机曾经发送过信息包给它的情况下,才能发送信息包到该内部主机(IP 必须一致端口号可以不同) 。

端口限制锥体(Port restricted cone )NAT: 类似于限制锥体(Restricted cone) NAT。但是限制还包括端口.也就是说,只有在内部主机(通过 IP 和端口号)给外部主机发送过信息包的情况下,该外部主机才可以发送信息包给内部主机,并需要明确的表明原来接收内部主机信息时的 IP 地址和端口号。

对称性(Symmetric) NAT:指的是所有来自相同内部 IP 地址和端口到同一目的地的请求都映射到某一个相同的外部 IP 地址和端口上。加入相同的主机使用相同的源 IP 地址和端口号发送信息包到另一目的地,哪么将会映射到另一外部地址上。而且,只有当外部主机接收到内部主机的信息包后才能发送信息包回给该内部主机。

## 2.2 UDP穿越NAT的方法

现在主流的UDP对NAT的穿越都是以STUN[3](Simple Traversal of UDP through NATs)协议为基础，采用打洞（Hole Punching)的方式来实现的。 原理如图2。

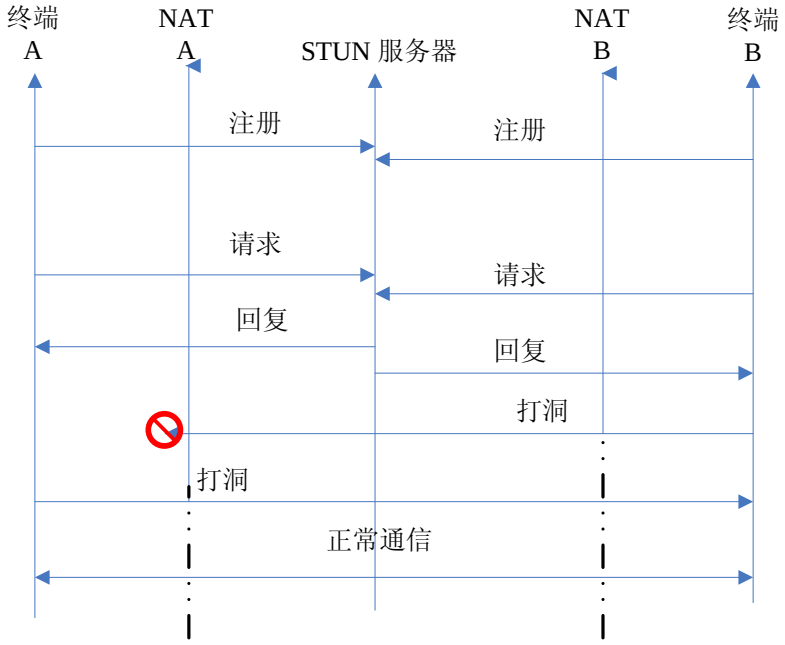


图2 STUN工作原理

要穿越NAT进行通信，首先要知道对方在其NAT上对应的外网端口号，这需要一台拥有公网地址的STUN服务器，NAT后的终端向STUN服务器发送消息，终端发出的IP包通过NAT的转换后发送往服务器，服务器接收到这个包后就可以解析出其中的地址信息，并记录下来。这一过程我们称之为注册。

假设终端A和终端B需要通讯，他们各发送连接请求到STUN服务器，服务器会把对方所映射的公网地址告诉双方。这样终端A,B就知道对方所映射在公网上的地址了。

接着通知终端B发送一个数据包到终端A,由于终端A前NAT A的存在，这个消息包是无法到达终端A的，但对于终端B前的NAT B会认为此次会话的发起方为终端B,从此不会阻挡

从终端发送给终端B的消息包，我们称这在NAT B上打了一个洞。之后终端A发送一个数据包到终端B,由于之前打洞的存在这个消息可以穿越NAT B,到达终端B,同时在NAT A上打了一个洞。此后就可以脱离服务器进行正常的通信了。NAT穿越至此完成。

### 2.3 TCP穿越NAT时遇到的问题

而TCP就不像UDP这么简单了，UDP是无连接 无状态的，其会话建立只是简单的从第一个数据包开始，不需要维持连接和状态的转换。TCP是面向连接的，其连接过程的实现需要经过三次握手，完成相应的状态转换。

另外UDP是对等的，双方的NAT可以同时认为自己是此次对话的发起方而不会阻挡后续的通信穿越NAT。而TCP是不对等的，一次通信必然是由发起者发送SYN包开始，被叫方只用等待SYN并做出回应。哪么发往被叫方的后续数据会被NAT所拦截，造成穿越失败。

## 3. 基于STUNT的TCP穿越方案

从上面一节我们可以看到TCP穿越NAT主要的问题在于如何让三次握手顺利完成，以及如何让两方都认为自己是会话的发起方。

康奈尔大学的NUTSS项目组提出了一种STUN的改进协议STUNT(STUN with TCP) [4]，这个协议利用发送一个低生命周期的信号来引发本地NAT返回一个ICMP错误消息，以获得TCP连接序号等信息，然后利用这些信息来伪造一个TCP 连接的方法来实现穿越的。

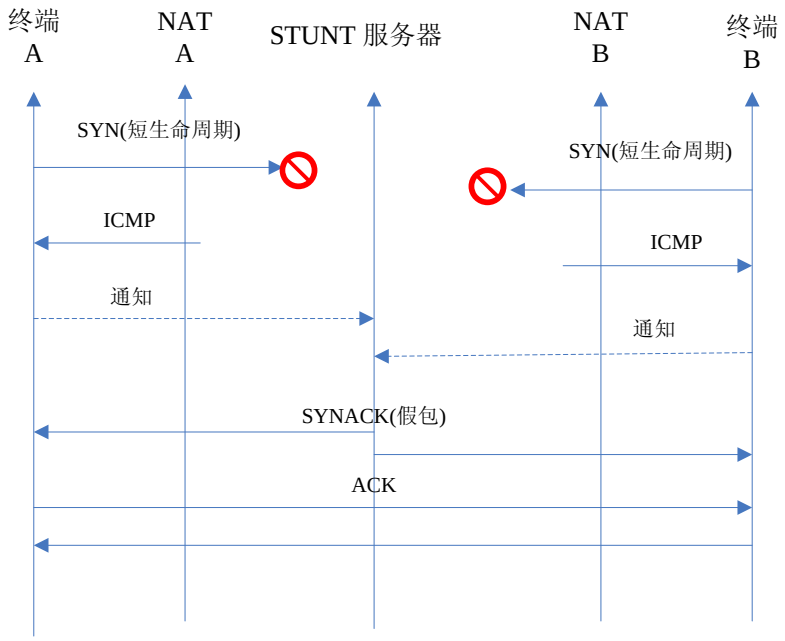


图3 STUNT #1

如图 3 所示，终端双方都主动发送低生命周期（TTL）的 SYN，且 SYN 的生命周期要足够大，大到 SYN 包能穿过他们各自的 NAT，但生命周期又要足够小，小到穿过各自的 NAT 后就过期而被网络丢弃。这样发起终端一方的 NAT 就会返回一个 ICMP 消息，通过侦听经过 RAW-socket 或 PCAP 返回的 ICMP 消息，终端可以得知初始 TCP 的序号。终端双方把各自的序号告诉都能抵达（连接）的 STUNT 服务器，紧接着 STUNT 服务器通过设置匹

配的序号构造一个 SYNACK 来欺骗双方（双方都认为该 SYNACK 是对方回应的）。完成 TCP 握手任务的 ACK 按照正常方式穿过网络。这种方法最大的缺点在于，它需要一个第三方为一个任意地址产生一个欺骗包，而该欺骗包很可能被网络中各种各样的进出过滤器丢弃。

为了解决这个问题提出了另一种解决方案[5]

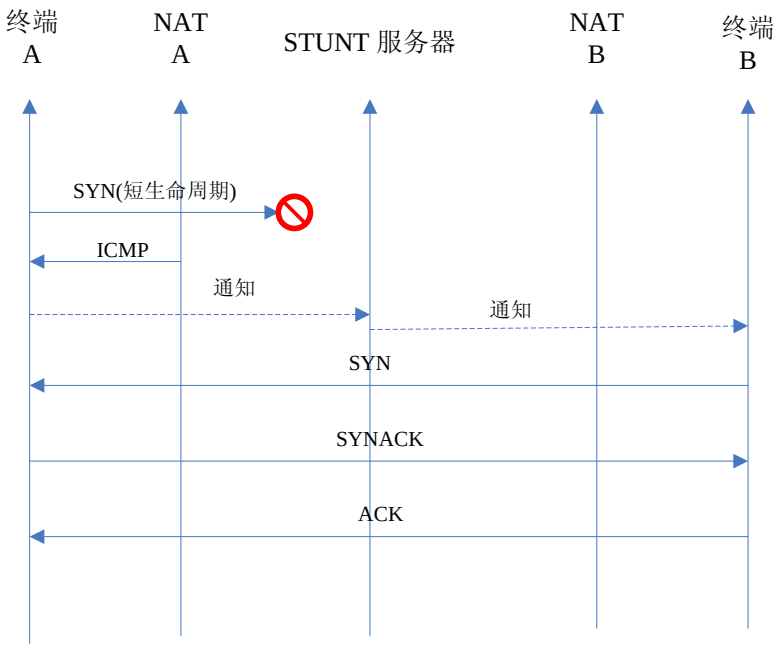


图4 STUNT #2

如图4所示，终端A 发出一个低生命周期(TTL)的SYN包，同样这个SYN的生命周期要足够大，大到SYN包能穿过他们各自的NAT，但生命周期又要足够小，小到穿过NAT A后就过期而被网络丢弃。这样NAT A就会返回一个ICMP消息，终端A通过侦听经过RAW-socket或PCAP返回的ICMP消息，可以得知初始TCP的序号。终端A 把自己的序号告诉的STUNT 服务器，接着终端A取消该连接企图，并在相同的地址和端口创建一个被动的TCP套接字。然后STUNT服务器会通知另一个终端初始化一个正常的TCP连接。终端B经过终端A第一次尝试连接留下的洞，进行三次握手最终和终端A建立TCP连接。

## 4. 实验及结果分析

我们编程实现了上述NAT穿越方案中的第二套，并部署了测试环境来进行测试其实际效果。如图5:

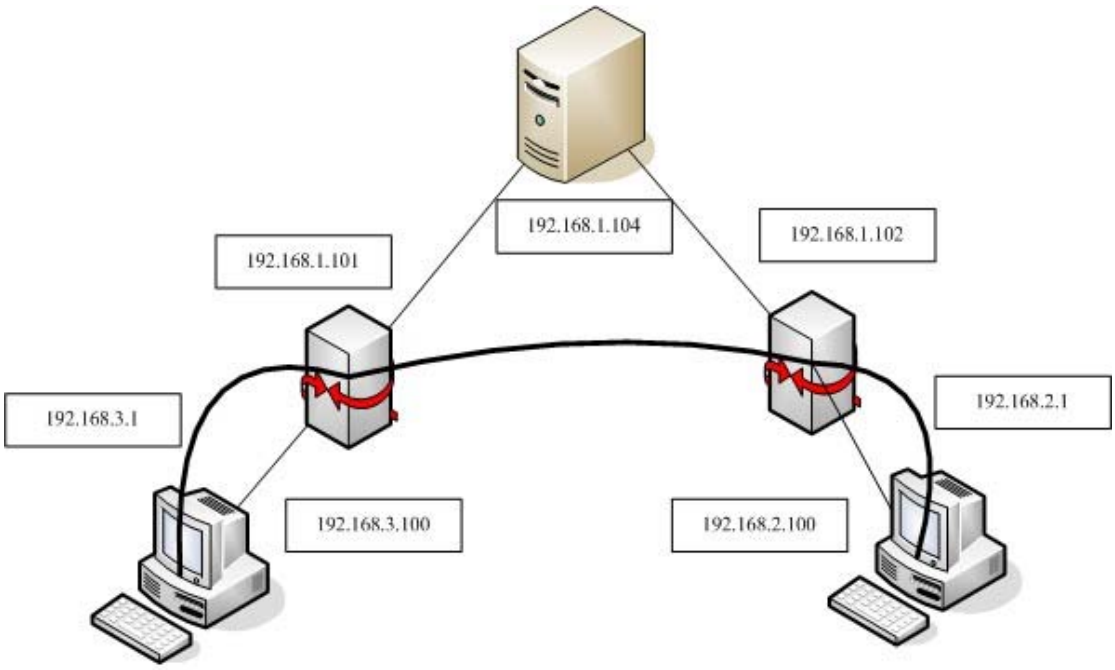


图 5 测试部署

STUNT 服务器地址为 192.168.1.104.

而终端 A 192.168.2.100 和终端 B192.168.3.100 分别属于两个 NAT 后，其中 192.168.2.100 所在的 NAT 的公网 IP 为 192.168.1.102，而 192.168.3.100 所在的 NAT 的公网 IP 为 192.168.1.101

图 6 为经过 NAT 穿越后终端 A 的连接情况，可以看出，它同 192.168.3.100 所在的 NAT 的公网 IP：192.168.1.101 建立了 TCP 连接

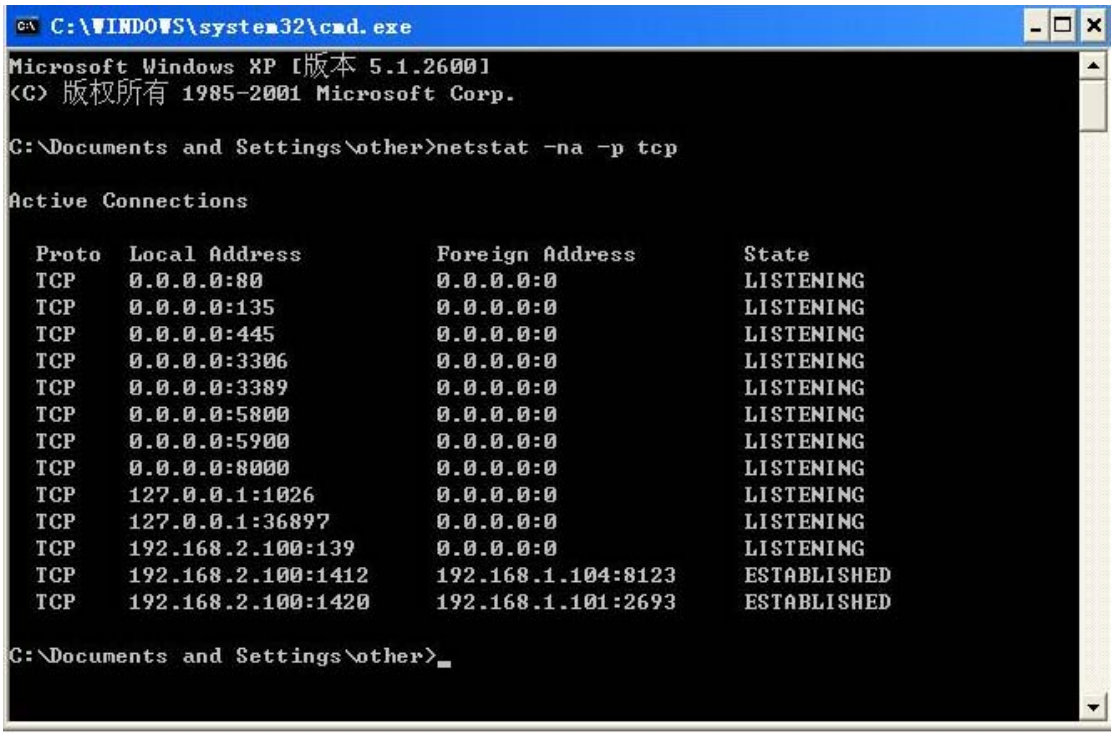


图 6 终端 A 连接状态

图 7 为终端 B 的连接情况，可以看出，它同 192.168.2.100 所在的 NAT 的公网 IP：192.168.1.102 建立了 TCP 连接。

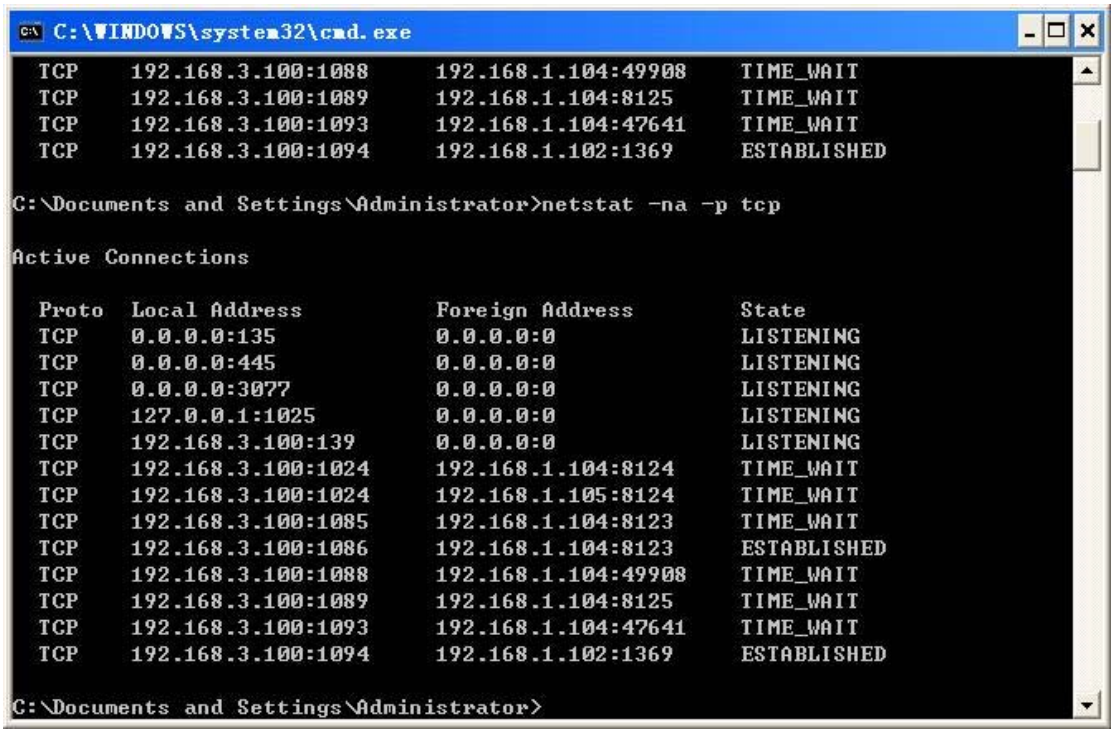


图 7 终端 B 连接状态

从上述实验可以看到使用这种方案使得两台位于各自 NAT 后的终端成功建立的 TCP 连接，证明这个方案是可行的。

## 5. 总结

NAT 设备的广泛应用打破了原有的网络模型，使得很多应用在穿越 NAT 时遇到了问题。目前基于 UDP 穿越 NAT 的技术已经发展的相当成熟，本文通过分析 UDP 穿越 NAT 穿越的原理，TCP 穿越 NAT 与 UDP 的不同，及 TCP 穿越 NAT 遇到的问题,提出了一种基于 STUNT 协议的 TCP 穿越 NAT 的方法。并通过实验证明了其可行性

但是这个方案也存在一些问题，比如需要准确的预测信号生命周期，过低则会导致无法到达本地 NAT，过长则会导致到达对方 NAT 并获得一响应而不是获得本地 NAT 的 ICMP 消息使得穿越无法完成。在这一方面还有待改进。、

### 参考文献

[1] Srisuresh P,et,al.IP Network Address Translator(NAT) Terminology and Considerations[S] RFC 2663,IETF issue Aug.1999.
[2] Doyle J.TCP/IP 路由技术(第 2 卷)[M].北京:人民邮电出版社,2003.
[3] Rosenberg, J., Weinberger, J., Huitema, C., and Mahy, R. RFC 3489: STUN — Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), Mar. 2003.
[4] Eppinger, J. L. TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem. Tech. Rep. CMU-ISRI-05-104, Carnegie Mellon University, Pittsburgh, PA, Jan. 2005.
[5] Guha, S., Takeda, Y., and Francis, P. NUTSS: A SIP-based Approach to UDP and TCP Network Connectivity. In Proceedings of SIGCOMM'04 Workshops (Portland, OR, Aug. 2004), pp. 43—48.

# TCP NAT-Traversal based on STUNT

Zhuang Xiao，Deng Zhongliang
Beijing University of Posts and Telecommunications, Beijing (100876)

**Abstract**

NAT(Network Address Translation) is becoming increasingly prevalent, and supported by many firewall devices. Now most solution implement base on UDP. Unfortunately, compared to UDP, establishing TCP connection is more complicated. Because TCP need a three-way handshake to establish a connection. This paper investigate the rationale and taxonomy of NAT, analyzes the current methods used for UDP Traversal, proposes and implements a TCP Traversal solution based on STUNT. This solution first send a low TTL syn to get a ICMP error message from local NAT. then fake a TCP connection use the TCP sequence number and other information from that ICMP message. At last,we implement and test this solution. Prove it is feasible.

**Keywords:** TCP; NAT; STUN;STUNT;

**作者简介：**庄霄，男，1983 年生，硕士研究生，主要研究方向 NAT 穿越。