第34卷 第12期 计 算 机 工 程 2008年6月
Vol.34 No.12 Computer Engineering June 2008
·网络与通信· 文章编号：1000—3428(2008)12—0112—02 文献标识码：A 中图分类号：TP393.02

一种 UDP 穿越 NAT 的新方案

张国印，叶在伟，曲丽君
(哈尔滨工程大学计算机科学与技术学院，哈尔滨 150001)

摘 要：网络地址转换是解决 IPV4 地址紧缺的有效方法，但对 P2P 技术的应用产生了负面影响。该文分析网络地址转换对 P2P 网络产生的负面影响，研究 NAT 端口映射类型及其检测方法，给出了一种用于 P2P 网络的穿越 NAT 协议。该协议可以解决 P2P 网内私网计算机之间建立直接 UDP 通信的问题，从而改善了 P2P 网络连通性。

关键词：P2P 网络；网络地址转换；端口映射

Novel Solution of Using UDP to Traverse NAT

ZHANG Guo-yin, YE Zai-wei, QU Li-jun
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)

【Abstract】 Network Address Translation(NAT) is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. It is an efficient solution for the lack of IP address. However, it has negative impact on P2P. The negative impact on P2P caused by the NAT is pointed out. And a method of testing NAT port mapping is presented. A new NAT traversal protocol under P2P network environment is designed. The protocol describes how to establish direct UDP communication between two NAT computers. The performance of the network connectivity is improved.

【Key words】 P2P network; Network Address Translation(NAT); port mapping

1 概述

网络地址转换(Network Address Translation, NAT)是用于将一个地址域映射成另一个地址域的国际标准方法，也是一种解决IPV4 地址紧缺的有效方法，因此，得到了大规模的应用和部署[1]。然而，这对P2P技术的应用产生了负面影响，综合起来主要有以下几点原因：

(1)P2P 技术的应用范围越来越广，可能涉及不同的场所与不同的计算平台。

(2)现有的很多计算机都是通过 NAT 设备接入互联网的。

(3)通过 NAT 设备联网的计算机只能发起到公网计算机的“出境”会话，而不能接收“入境”会话。因此，2 台私网计算机之间不能进行直接的 UDP/TCP 通信，这是阻碍 P2P 应用与推广最根本的原因。

如何穿越 NAT 在 2 台私网计算机之间建立 UDP/TCP 通信是 P2P 软件研发工程师所面临的首要问题。本文在实践经验的基础上，总结与设计了一种 UDP 穿越 NAT 的新方法。与现有的方法相比，该方法在性价比、安全性、可靠性、可扩展性与可移植性等方面具有明显的优势。

2 NAT 设备端口映射类型的检测

当若干台计算机通过NAT设备接入互联网时，这些计算机就构成了一个私有网络。它们共享同一个公有IP地址，同时NAT为网内每台计算机分配了一个私有IP地址。当私有网络中某台计算机需要与互联网通信时，它将会通过NAT将数据包发送出去，当相应的应答数据包返回时，NAT会根据端口映射列表来决定数据包的转发。例如，当NAT接收到来自于私网计算机A:Q上的数据包时，它会为A:Q分配一个端口U，并通过NA:U将该数据包发送到目标地址(D:P)，同时建立A:Q<->NA:U<->X:X(X表示未知的IP和端口，需要根据NAT的端口映射类型来决定)的映射记录，同时更新端口映射列表。当NA:U接收到外部的UDP数据包时，NAT会根据该数据包的源IP和端口信息进行处理。具体的处理方式由NAT的端口映射类型决定。NAT端口映射类型主要分为 4 种：全双工锥型，受限制锥型，端口受限制锥型和对称型。各种NAT对数据包的具体处理方式[2-3]如下：

(1)在全双工型时，NAT(NA:U)接收到 UDP 数据包后，会将该数据包转发到 A:Q，而不考虑该数据包的源 IP 和端口。

(2)在受限制锥型时，NAT(NA:U)接收到 UDP 数据包后，首先检查该数据包的源 IP 地址是否为 D，如果是，那么将该数据包转发给 A:Q，否则丢弃。

(3)在端口受限制锥型时，NAT(NA:U)接收到 UDP 数据包后，不仅检查该数据包的源 IP 地址是否为 D，还要判断该数据包的源端口号是否为 P，如果是，那么将该数据包转发给 A:Q，否则丢弃。

(4)在对称型时，NAT 的处理方式可能是随机的。

由于本文提出的方法仅仅针对锥型 NAT，因此对于对称型 NAT 不做过多的探讨。

据统计，80%以上的NAT所采用的端口映射类型均为前 3 种，这类NAT统称为锥型NAT[4]。为了实现UDP穿越NAT，检测NAT的端口映射类型十分重要。

NAT 端口映射类型的检测是 UDP 穿越 NAT 的关键和基础，只有清楚地知道 NAT 的端口映射类型，才能提出相应的穿越方法。图 1 给出了具体的检测流程。

基金项目：黑龙江省自然科学基金资助项目(F2004-06)
作者简介：张国印(1962－)，男，教授、博士生导师，主研方向：网络与信息安全，嵌入式系统；叶在伟、曲丽君，硕士研究生
收稿日期：2007-06-30 **E-mail：**zhangguoyin@hrbeu.edu.cn

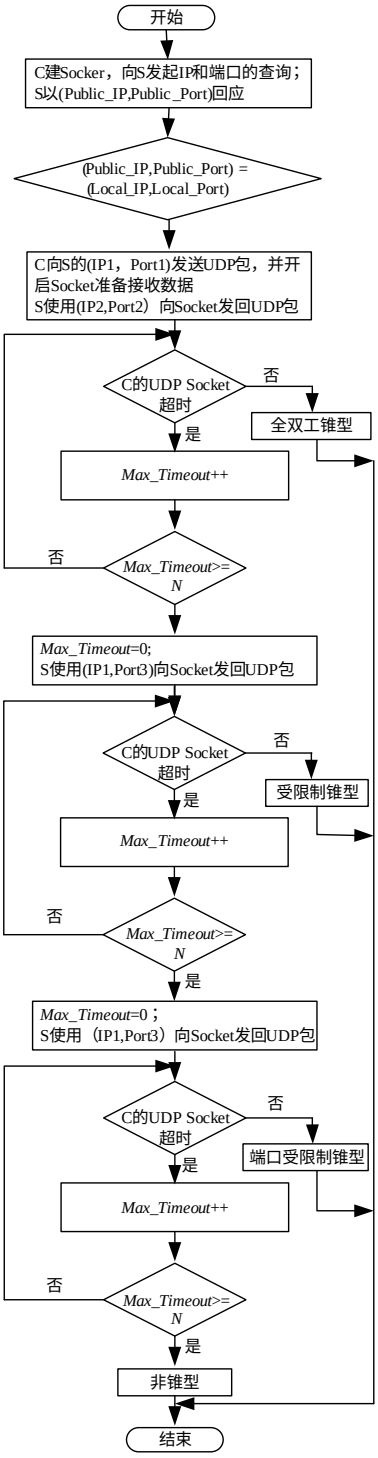

图 1　NAT 端口映射类型的检测流程

通过图 1 的检测流程，最终可以检测出 NAT 的端口映射类型是否为锥型。相对于其他类型的 NAT，UDP 数据包穿越采用锥型映射方式的 NAT 的复杂度很小而且成功率很高，因此，本文所提出的穿越方案均针对锥型 NAT 而言。另外在锥性 NAT 中，只要解决了端口受限制的锥型 NAT 的 UDP 数据包穿越问题，就能成功地实现 UDP 数据包穿越所有锥型 NAT，包括全双工锥型、受限制锥型和端口受限制锥型。

3　UDP 穿越 NAT 协议的设计

为了穿越 NAT 而在 2 台私网计算机之间建立直接的 UDP 通信，需要设置一台中间服务器，该中间服务器必须是一台公网计算机，它主要用于辅助 NAT 类型检测和 UDP 通信的建立，其结构如图 2 所示。

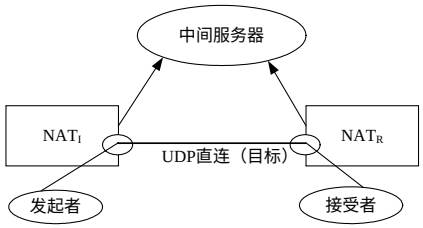

图 2　UDP 穿越 NAT 结构

在图 2 中，接受者和发起者分别是 2 台通过NAT接入互联网的私网计算机，NAT_I和NAT_R分别对应接受者和发起者的 2 个锥型NAT。在此结构上，本文设计了一种UDP穿越NAT的协议，该协议共分为 3 部分：接受者注册，发起者查询和接受者打洞，其细节见图 3。

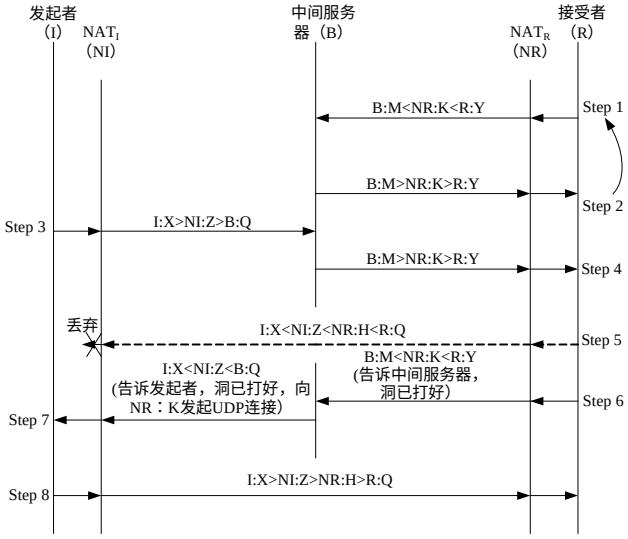

图 3　UDP 穿越 NAT 协议

接受者注册——接受者通过向中间服务器发送UDP数据包的方式向中间服务器进行注册(Step1)。注册信息包括接受者的外网IP和端口(NR:K)。由于NAT映射端口的存在受到时效性的影响，因此接受者应该间歇性地通过R:Y向中间服务器发送注册信息，保持NR:K与R:Y的端口映射关系(Step 2)。

发起者查询——发起者通过向中间服务器发送UDP数据包的方式向中间服务器进行查询，请求和一个NAT节点进行UDP连接(Step 3)。中间服务器收到该查询请求之后，便会遍历自身的注册节点列表。如果该列表中存在满足查询条件的节点，那么中间服务器就会向该节点(接受者)转发UDP连接请求消息，告诉接受者，转发者(I)想要和它建立UDP通信，并将转发者的外网IP和端口发送给接受者(Step 4)。此时，接受者启动打洞程序，开始打洞操作。

接受者打洞——接受者使用第 4 步获得的发起者的外网IP和端口号信息(NI:Z)试探性地向该目标地址发送UDP数据包(Step 5)。但是该操作必然以失败告终，因为都会被当成“ 不请自来 ”的非法数据包而被丢弃。虽然此次试探性的操作失败了，但这对于下一步的操作是关键的一步，因为接受者已经在其NAT_R上打好了一个洞，今后所有发送到NR:H上的UDP数据包都会被成功地转发到内网主机R:Q上。在Step 6，接受者会将“ 打洞完毕 ”的消息告诉中间服务器。在Step7，中间服务器会告诉发起者，立即向NR:K发送UDP数据包进

(下转第 131 页)