采用 PCP 协议实现 TCP NAT 穿越①

Implementation of TCP NAT Traversing Based on the PCP Protocol

杨晓波 （浙江财经学院 信息学院 浙江杭州 310012）

摘 要: 本文提出了一种可靠的 TCP NAT 穿越方法,有效解决了 P2P 传输过程中 NAT 穿越的问题。具体的实现方法是:首先研究 NAT 穿越的关键技术,接着对 TCP NAT 穿越的实现原理进行分析,最后提出基于 PCP 协议的 TCP NAT 实现过程。研究结果表明:本文提出的基于 PCP 协议的 TCP NAT 穿越方法是可行的,能够较好的满足 P2P 技术的应用,如果进一步提高穿透率,则必须保证端口的连续性。

关键词: PCP 协议 NAT 打洞 NAT 穿洞 NAT 穿越服务器

目前,许多 P2P 视频播放软件是基于 Peercast 开发并实现的,如 PPlive、Tvants 等视频播放软件。Peercast 是一种开源 P2P 流媒体软件,自身定义了 PCP 协议,即 Peercast Protocol,Peercast 之间的媒体数据和控制消息均通过 PCP 协议传递,PCP 协议是建立在 TCP/UDP 基础之上的应用层协议,目前该协议使用 TCP 协议[1,2]。

在当前 Internet 网络环境中存在大量的 NAT 设备,这些 NAT 设备形成了逻辑上分离的区域,使得处于 NAT 后的对等节点不能直接进行连接和通信。因此,基于 Peercast 上开发的视频播放软件都会面临 TCP NAT 穿越的问题。

1 关键技术

1.1 NAT 类型检测和端口预测

Network Address Transform（网络地址转换）简称 NAT,是一个 IETF 标准,能将一个 IP 地址域映射到另一个 IP 地址域,从而为终端主机提供透明路由,并能较好解决当前公网 IP 地址紧缺和网络安全问题[3-7]。NAT 按 STUN 方式可分为四种类型:完全圆锥型(Full Cone)、地址限制圆锥型(Address Restricted Cone)、端口限制圆锥型(Port Restricted Cone)以及对称型(Symmetric)。前三种统称为 Cone 型 NAT,其特点是映射与目的地址无关,只要源地址相同,映射就相同;后一种类型的特点是映射同时关联源地址和目的地址。

实现 TCP NAT 穿越的关键步骤就是要进行 NAT 类型检测和端口预测。NAT 类型检测方法如图 1 所示。

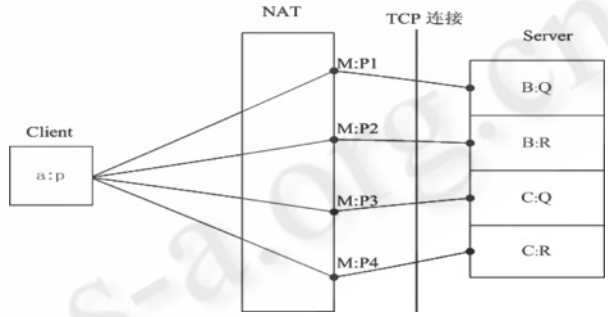

图 1 NAT 类型检测

图 1 中的 Server 是 NAT 穿越服务器,该服务器有二个 IP 地址 B 和 C,每个 IP 地址绑定两个端口 Q 和 R;NAT 映射的 IP 地址和 Port 端口号分别为 M 和 P,不同的连接会分配不同的端口号;客户端有一个 IP 地址 a 和端口号 p。

客户端连续向服务端发起四次 TCP 连接,在客户端每次发起 TCP 连接后,由服务器返回 NAT 映射的 IP 地址和 Port 端口号给客户端,使用不同类型的 NAT 设备重复进行。所有返回的结果如表 1 所示:

① 基金项目:高等学校校级重大课题(课题编号 2007YJZ05)

表 1　NAT 映射结果

客户端	服务端	NAT1	NAT2	NAT3	NAT4	NAT5	NAT6
a	B	M P	M P	M P	M P1	M P	M P
a	B	M P	M P +1	M P +1	M P2	M P +1	M P
a	C	M P	M P +2	M P +2	M P3	M P	M P +1
a	C	M P	M P +3	M P +3	M P4	M P +1	M P +1

表 1 中 NAT1 ~ NAT6 表示不同类型的 NAT 设备。从表中可看出不同类型的 NAT 设备的端口映射分配策略也不尽相同。

通过对表 1 进行分析，可以预测下次连接时 NAT 分配的端口号。对于 NAT1 ~ NAT4 类型，可以计算出 NAT 分配的端口间距为 （P1 为第一次分配的端口号，P2 为第二次分配的端口号），这样可预测下次连接的 NAT 端口号为 （P3 为第三次分配的端口号）；对于 NAT5 和 NAT6 类型，也可按前述方法预测下次连接的 NAT 端口号。

1.2 NAT 穿越服务器的设计

NAT 穿越服务器是一个中介服务器，在实现 TCP NAT 穿越的过程中起着非常重要的中介作用。NAT 穿越服务器主要实现客户端的注册、协助客户端检测 NAT 类型以及为两客户端交换各自的 NAT 映射 IP 地址和 Port 端口号等功能。为了能顺利实现这些功能，在 NAT 穿越服务器上驻留着四种服务：即注册服务、回响服务、通信服务和交换服务，如图 2 所示。

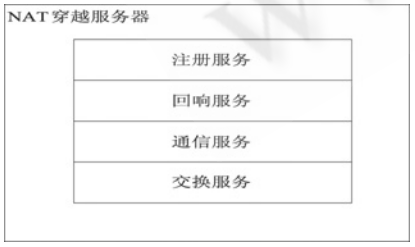

图 2　NAT 穿越服务器结构图

从图 2 可知，注册服务提供客户在服务端的注册功能；回响服务协助客户端完成 NAT 类型检测；通信服务接收客户端的注销、查询、连接等请求，并做出相应的响应；交换服务是核心服务，它帮助两客户端互换各自的 NAT 映射 IP 地址和端口号。这四种服务负责监听和接收客户的连接请求并分别建立四个通道，分别是注册通道、回响通道、通信通道以及交换通道。客户端通过这四个通道来完成注册、NAT 类型检测和端口预测以及交换 NAT 映射 IP 地址和 Port 端口号。

1.3 PCP 协议扩展

PCP 协议是 Peercast 用来在节点间传送媒体数据包和各种控制消息所自定义的协议，该协议是建立在 TCP/UDP 协议上的应用层协议，具体协议栈如图 3 所示。

为实现基于 PCP 协议的 TCP NAT 穿越，需要对 PCP 协议进行扩展，扩展后的 PCP 协议栈如图 4 所示。PCP 扩展协议引入了 ESTP 概念，ESTP（Expand Stunt Protocol）是自定义的 NAT 穿越协议[8-10]，它对 HTTP 协议进行扩展后形成 HTTP 协议的两个变种：一个是 HTTPMT（HTTP Multicast over TCP），另一个是 HTTPT（HTTP over TCP），前者用于广播穿洞消息，该消息包含组号、跳数、延时、目地主机 ID 号、源主机 ID 号、频道 ID 号以及版本号；后者用于单播打洞消息，该消息包含对方主机 ID 号和频道 ID 号；这两条消息被封装在 HTTP 协议中，HTTP 协议和其扩展协议是 PCP 协议的核心组成部分。

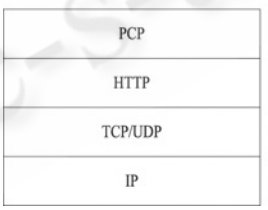

图 3　PCP 协议栈

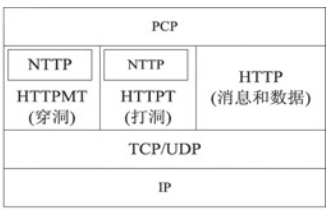

图 4　扩展后的 PCP 协议栈

2　TCP NAT 穿越实现

2.1 基于 PCP 协议的 TCP NAT 实现过程

将 TCP NAT 实现穿越方法应用到 PCP 协议之中，其实现过程如图 5 所示：

从图 5 可知，节点 A 和节点 B 是分别位于 NAT M 和 NAT N 之后两私网内的主机，S 是流媒体服务器，节点 B 与流媒体服务器 S 已经建立连接，并能够正常发

送和接收消息和媒体数据。

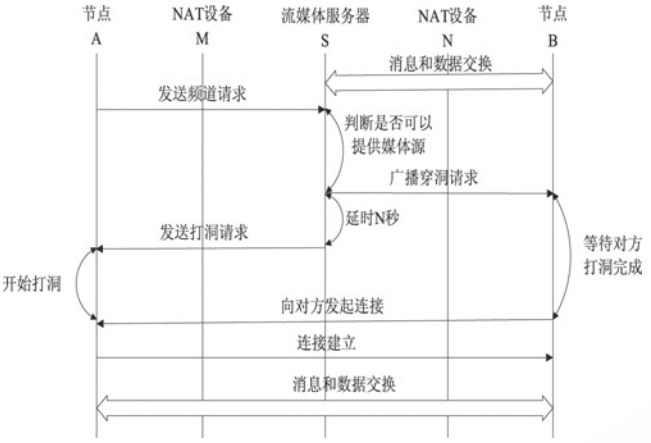

图 5 基于 PCP 协议的 TCP NAT 穿越实现过程

当节点 A 要播放某一频道时，首先向流媒体服务器 S 发送频道请求，服务器 S 收到该请求后，会判断节点 A 是否存在防火墙或处于 NAT M 之后，同时判断本机是否可以为该节点提供媒体源，如果服务器 S 不能提供媒体源，则从服务器 S 保存的节点列表中选择一节点，如果选中的该节点也处于 NAT 或防火墙之后，则向节点 B 等发送广播穿洞请求，随后，延时 N 秒后向节点 A 单播打洞请求消息。

节点 B 接收到广播穿洞请求消息后，首先会判断该消息是否发送给本机，如果是，则借助 NAT 穿越服务器完成注册和 NAT 类型检测，随后等待对方完成打洞。

同样道理，节点 A 接收到打洞请求消息后，借助 NAT 穿越服务器完成注册、NAT 类型检测、端口预测、与节点 B 互换 NAT 映射 IP 地址和 Port 端口号等工作，随后开始打洞，成功之后在本地进行监听。节点 B 在节点 A 打洞完成后开始穿洞，即向节点 A 发起连接，连接建立后，两节点之间就可以开始传输 PCP 消息和媒体数据。

3 结束语

本文详细论述了实现 TCP NAT 穿越的关键问题、TCP NAT 穿越实现原理以及应用该原理在 PCP 协议中实现 TCP NAT 穿越的过程，并得出以下结论：

1）实现 TCP NAT 穿越的关键在于要进行 NAT 类型检测和端口预测。

2）在不同的网段使用视频播放软件进行测试，测试结果表明本文提出的 TCP NAT 穿越方法是一种可靠的方法，可以应用到目前流行的 P2P 应用软件之中。

3）目前采用 TCP NAT 穿越方法的穿透率只能达到 80% －90%，如果要进一步提高穿透率，

必须保证端口号的连续性，可以考虑采用新型的 NAT 设备，如华为或思科产品等。

参考文献

1 Eppinger JL. TCP connections for P2P apps: A software approach to solving the NAT problem. Technical Report CMU－ISRI－05－104, Carnegie: Carnegie Mellon University, 2005. 51－63.

2 Biggadike A, Ferullo D, Wilson G, Perrig A. NATBLASTER: Establishing TCP connections between hosts behind NATs. In: ACM SIGCOMM Asia Workshop. Beijing, China, 2005. 42－48.

3 Clark D, Bragen R, Falk A, Pingali V. FARA: Reorganizing the addressing architecture, In : ACM SIGCOMM FDNA Workshop. Marina: MIT Lab for Computer Science, 2003. 62－71.

4 Guha S, Francis P. Characterization and Measurement of TCP Traversal through NATs and Firewalls. Tech. Rep. CMU－ISRI－05－104, Ithaca: Cornell University, 2004. 37－45.

5 Guha S, Takeda Y, Francis P. NUTSS: A SIP－based Approach to UDP and TCP Network Connectivity. In Proceedings of SIGCOMM04 Workshop, 2004, 8(5): 43－48.

6 Francis P, Gummadi R. IPNL: A NAT－extended Internet architecture. In ACM SIGCOMM, 2001,8(1): 69－80.

7 吴新龙. 端到端通信中 TCP 穿越 NAT 的解决方案. 电力系统通信, 2006, 27(159): 10－12.

8 谢镇宇，夏清国. 在 NAT 后的主机之间建立 TCP 连接的研究. 科学技术与工程, 2006, 6(8): 1091－1094.

9 王止戈, 彭宇峰, 张苏灵, 高传善. 一种基于预测的 Symmetric NAT 穿越解决方案. 计算机工程, 2005, 31(11): 122－210.

10 曹玉琳, 吴力文. P2P 网络中利用 JXTA 穿越 NAT 的方法研究. 计算机工程与设计, 2006, 27(19): 3619－3621.