

P2P 中 NAT 穿越问题的研究

孙卫喜, 席少龙

(渭南师范学院 数学与信息科学学院 计算机网络工程技术中心, 陕西 渭南 714000)

摘要:针对目前常用的几种 NAT 穿越技术存在的需要改变网络环境、不支持 Symmetric NAT 与 TCP 的穿越、延时、丢包等问题,在对 P2P 网络环境下 NAT 穿越原理认真分析的基础上,以穿越原理为基点,对目前 NAT 穿越技术存在的问题进行了研究。给出了‘采用端口预测穿越 NAT 的新方案’,该新方案在不需要改变现有网络设备的情况下实现了 TCP 对各种 NAT 的穿越,减少了延时和丢包等 NAT 穿越常见的问题。通过大量的实验表明该新方案更适合于对网络安全需求更高而使用对称型 NAT 的企业。

关键词:对等网络;网络地址转换;ICMP;生存时间;穿越

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2014)02-0242-04

doi:10.3969/j.issn.1673-629X.2014.02.060

Research on NAT Traversal Problem in Peer-to-Peer

SUN Wei-xi, XI Shao-long

(Center of Computer Network Engineering Technology, College of Mathematics and Information Science,
Weinan Normal University, Weinan 714000, China)

Abstract: Due to several problems in the common technology of the NAT traversal at present, such as the need of changing the environment, non-supporting the Symmetric NAT and TCP traversal, delaying, the lost of data and so on, after carefully analyzing the theory of the NAT traversal in P2P, based on the traversing theory, studied the appearing problems of the NAT traversal, then give a new method of using port to predict the NAT traversal. This new method achieves the way of TCP crossing all kinds of NAT in no need of changing the original equipment of the Internet, which reduced the common problems in the field of NAT traversal such as delaying and the lost of data. Some experiments which has been verified present that the method can adapt to the enterprises which have higher requirement of network security and using a class of symmetry NAT.

Key words: P2P; NAT; ICMP; TTL; traversal

1 NAT 技术

网络地址转换 (Network Address Translator, NAT) 是 IETF (Internet Engineering Task Force) 为了缓解 IPv4 地址紧缺而提出的一种解决方案^[1]。NAT 的基本思想是:把网络分成局域网和 Internet 两部分,其中用于局域网的 IPv4 地址 (私网地址或内网地址) 主要包含: A 类 IP 地址中的 10.0.0.0 ~ 10.255.255.255 及 B 类 IP 地址中 172.16.0.0 ~ 172.31.255.255 和 C 类 IP 地址中的 192.168.0.0 ~ 192.168.255.255; 局域网内部主机间的通信只用私网地址,私网地址不会在因特网上被分配,但可以在局域网内重复使用,不同子网的内网地址可以相同;公网 IP 地址是指能在 Internet 上使

用的 IPv4 地址,公网 IP 地址包含除私网 IPv4 地址外的 IPv4 地址,当局域网内部主机与 Internet 通信时,需要通过 NAT 将公网 IP 地址分配给内网主机, NAT 可以使同一局域网的多个内部地址共享单个或多个公网地址与外网连接。

NAT 是一种将私网地址转化为公网 IP 地址的转换技术,它缓解了 IPv4 地址紧缺的问题,实现了内网地址的复用,同时因其有私网地址不能直接被外网用户所访问的特点,而提高了私网内部的安全性和可管理性^[2]。

因此 NAT 被广泛应用于各种类型的 Internet 接入方式和多种类型的网络中。

收稿日期:2013-05-20

修回日期:2013-08-24

网络出版时间:2013-11-29

基金项目:2012 年地方高校国家大学生创新训练项目 (201210723020); 陕西省自然科学基金基础研究计划资助项目 (2012JM8048); 陕西省渭南市科技创新扶持资金项目 (2012KYJ-6); 渭南师范学院 2012 大学生创新计划项目 (12XK041)

作者简介:孙卫喜 (1965-), 男, 高级工程师, 研究方向为网络安全、网络技术应用。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0826.009.html>

2 NAT 对 P2P 的影响

点对点技术(Peer-to-Peer, P2P)也称对等联网或对等网络,对等网络中用户地位是平等的,也就是说每个用户既能通过访问其他用户获得资源,也能为用户提供资源服务,这也是对等网络区别于传统 Client/Server 网络最显著的特征^[3]。对等网络克服了传统网络中存在的“服务器瓶颈”问题,因而被广泛使用于电子业务、新闻、电视、教育、广告、医疗等行业中。

对等网络中用户间实现的是对等服务,而内网用户使用的私网 IP 地址是不能被 Internet 上用户所识别的,内网用户可以通过 NAT 共享外网地址的方式访问外网,但外网用户不能通过直接穿越大多数 NAT 的方式访问内网用户,且外网用户欲建立与内网的通信时,需由内网用户先发起连接请求,内网用户拒绝来自外网用户的主动连接。这都有悖于互联网公平、资源相互共享等思想,也与互联网上流行的 P2P“相互服务”的思想所不容。显然网络中 NAT 设备的大量使用给视频、音频、网络下载等 P2P 中流行软件的使用带来障碍。可见网络中要实现对等服务的前提是:解决好如何让信息有效地穿越 NAT。

3 ICMP 在 NAT 中的处理方式

ICMP(Internet Control Message Protocol)是一种面向连接的 Internet 控制报文协议,是 TCP/IP 协议族的一个子协议,用于在 IP 主机及路由器间传递:网络不通、主机是否可达、路由是否可用等网络本身的控制消息。从技术角度来说,ICMP 就是一个“错误侦测与回报机制”,其目的是检测网络的连线状况,确保连线的准确性。功能主要有:侦测远端主机是否存在、建立及维护路由资料、重导资料传送路径、资料流量控制。

生存时间(Time To Live, TTL),是 IP 协议包中的一个值,它表示网络中数据包的生存时间。TTL 值随着网络环境的不同而变化,不同的网络环境下会初始化一个不同 TTL 值,当数据包经过路由器时 TTL 值就会被减去 1,当 TTL 值被减为 0 时还没到目标用户,则数据包就会被丢掉,TTL 也用来表示包在被丢弃前最多能经过的路由器个数。当数据包被丢掉时会给发送者发送一个 ICMP 报文,发送者在获得所发数据包没能到达目标的信息后再确定数据包是否需重发^[4]。

ICMP 错误消息的例子之一是 TTL 值过期。每个路由器在转发数据报的时候都会把 IP 包头中的 TTL 值减 1。如果 TTL 值为 0,“TTL 在传输中过期”的消息将会回报给源地址。通常在:IP 数据报无法访问目标、IP 路由器无法按当前的传输速率转发数据报、IP 路由器将发送主机重定向为使用到达目标的更佳路由时,会自动发送 ICMP 消息。

在信息包的穿越中,依赖于 NAT 设备对收到的公网发往私网的 ICMP 消息的处理。如 NAT 内的某主机向一个公网传输层地址发 SYN 消息,若 IP 包在到达目的地址前 TTL 值就已超时,则产生 ICMP 消息并将消息发往源地址,若 NAT 设备不丢弃该消息而把此 ICMP 消息发送到 NAT 内欲发起连接的某主机,此次连接就会失败。

目前,大多数 NAT 设备忽略 ICMP 消息,而不将其转发到私网中的主机^[5]。在文中所介绍的穿越方法中,默认 NAT 设备忽略 ICMP 消息。

4 划分 NAT 类型

按照信息包穿越不同类型 NAT 时穿越方式不同的特征将 NAT 分成 4 类。

(1)Full Core NAT(全克隆 NAT)。该类型的 NAT 将内网中从某一用户发出的连接请求都映射为外部同一端口与同一 IP,外网用户均可以通过该映射与该用户连接。

(2)Restrict Cone NAT(限制性克隆 NAT)。该类型的 NAT 将内网中从某一用户发出的连接请求都映射为外部同一端口与 IP,只有该内网用户访问过的外网用户才可以用不同的端口与该内网用户连接。

(3)Port Restricted Cone NAT(端口限制性克隆 NAT)。该类型的 NAT 将内网中从某一用户发出的连接请求都映射为外部同一端口与 IP,只有该内网用户访问过的外网用户且用内网连接该外网用户时映射过的端口才能连接该内网用户。

(4)Symmetric NAT(对称型 NAT)。该类型的 NAT 与前 3 种 NAT 的映射方式不同,内网某一用户连接外网时随连接目标或所用的端口不同映射关系将不同,也可以说用对称型 NAT 连接的内外网用户在发生连接时,源用户使用的 IP 与端口号及目标用户使用的 IP 与端口号四者任一发生变化则映射关系将改变。

5 P2P 穿透 NAT 的解决方案

5.1 TTL 的确定

客户端 A 与 B 连接时,TTL 值的确定采用 NAT A 后的客户端 A 在连接请求前,先发出 SYN 包的 TTL 值为 1,当捕获到 TTL 超时的 ICMP 报文后,再次发送 TTL 值为 2 的数据包,依次增加 SYN 数据包的 TTL 值,直到接收不到 ICMP 数据报为止,这时的 TTL 值就是数据包 SYN 刚好穿过自己 NAT 的最小值。只有选择好 TTL 值,才能确保主机 A 发出的 SYN 数据报刚好穿过 NAT A,在 NAT A 上建立映射,而不能到达目的地址 NAT B,防止 NAT B 产生 RST 数据报,导致 NAT A 后的主机 TCP 连接失败。

5.2 NAT 设备的 Hairpin 特性

当 NAT 后的主机 A 把数据包发往某 IP, 而该 IP 又是同在一个 NAT 后的主机 B 经 NAT 映射后的 IP, 这就是 Hairpin(或称 loopback), 目前, 大多数 NAT 设备并不支持 Hairpin。

依据局域网域名唯一性的原则, 在同一 NAT 后的主机网域名是相同的。连接双方在服务器 S 上注册时, 客户端所在的网域名被记录在注册信息中, 连接双方从 S 中获得对方的信息后, 检查网域是否相同, 相同时就向对方的内网地址发起连接, 不同时就按下文中给出的新方案发起连接, 以避免不支持 Hairpin 情况发生, 使得同一 NAT 后主机间的通信顺利实现。

5.3 STUN 方案

IETF 制定了 UDP 数据包穿越 NAT 的简单协议 STUN, STUN 支持 NAT 分类中克隆型 NAT(即前 3 种 NAT)的穿越, 其基本思想是: STUN Client 向 NAT 外的 STUN Server 发请求消息, STUN Server 收到请求消息产生的响应消息中携带 STUN Client 在 NAT 上映射的外部端口。STUN Client 通过响应消息得知其在 NAT 上映射的外部地址, 然后在其报文负载所描述的地址信息中直接填写经 NAT 映射后的对外地址, 这样报文负载中的内容在经过 NAT 时就无需改动, 按普通 NAT 流程转换报文头的 IP 地址即可, 显然负载中的 IP 地址信息和报文头地址信息是一致的, 故媒体流能顺利穿越 NAT^[6-7]。

STUN 的优点是无需改变现有 NAT 网关设备, 缺点是终端需有 STUN 代理功能, 不支持 TCP 及对称型 NAT 的穿越^[8]。

5.4 TURN 方案

TURN(Traversal Using Relay NAT)是针对 STUN 无法穿越对称型 NAT 提出的穿越协议。TURN 穿越对称型 NAT 的思路与 STUN 类似, TURN Client 向 NAT 外的 TURN Server 发出连接要求后 TURN Server 产生的应答信息中携带 TURN Server 的外部端口, 然后在其报文负载所描述的地址信息中直接填写 TURN Server 的对外地址。STUN 与 TURN 的区别在于 STUN 得到的是 NAT 的出口地址, TURN 得到的是 TURN Server 的地址, 其实际应用原理也是一样的^[9]。TURN 是通过分配 TURN Server 的地址和端口作为客户端对外的接收地址和端口, 使内外网通信时报文都要经过 TURN Server 进行 Relay 转发。

TURN 继承了 STUN 无需改变现有 NAT 网关设备的优点, 解决了 STUN 应用无法穿透对称 NAT 的问题, 支持基于 TCP 的应用(如 H323 协议), 实现了各种 NAT 的穿透。TURN 的缺点是其终端需要支持 TURN Client, 再是所有报文都必须经过 TURN Server 转发, 增

大了包的延迟和丢包的可能性^[10]。

6 NAT 穿越的新方法

STUN 不支持 TCP 及对称型 NAT 的穿越, TURN 因所有报文都必须经过 TURN Server 转发, 增大了包的延迟和丢包的可能性^[11-12]。

为使穿越方案更具有普遍性, 文中改进了 STUN 穿越方式给出了‘采用端口预测穿越 NAT 的新方案’, 该方案成功实现了对所有 NAT 的穿越, 克服了 STUN 与 TURN 穿越 NAT 存在的缺点, 具有极高的应用和推广价值。特别适合于对内网安全需求更高, 使用 Symmetric NAT 的企业用户。

STUN 之所以不能穿越 Symmetric NAT 其原因在于, 发起连接的客户端在连接不同的目的地址时得到 Symmetric NAT 的映射地址是不同的^[13]。如当客户端 A/B 一方或双方处于 Symmetric NAT 后, 客户端 A 向客户端 B 发连接请求时, 客户端 A 与客户端 B 发起会话的映射地址与客户端 A 注册时的映射地址已不同, 因而 NAT A 会拒绝来自客户端 B 的连接请求, 因为这属于不请自来的连接请求, 而采用端口预测新方案就能使应答端 B 准确地得到发起连接的客户端 A 此时的端口映射值, 实现对 Symmetric NAT 的穿越^[14-15]。

NAT 的穿越结构如图 1, 若 NAT 为任意类型的 NAT, 客户端 A 与 B 是处于 NAT A 与 NAT B 后的用户, STUN Server 是处于 Internet 中有两个端口号 (Port 1 和 Port 2) 和两个公网 IP 地址 (IP1 和 IP2) 的客户端服务器 S。

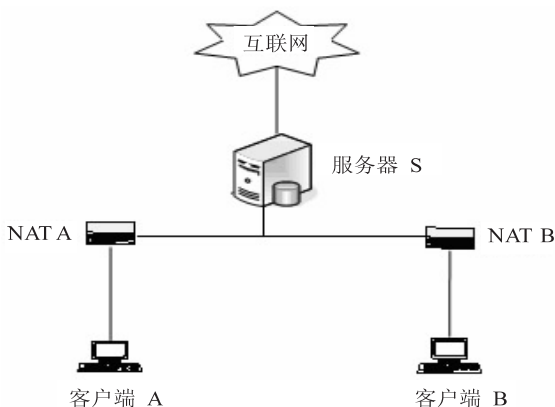


图 1 网络布局示意图

客户端 A 与 B 的 TCP 连接流程如图 2 所示。

(1) 客户端 A/B 向处于 Internet 中有两个端口号 (Port 1 和 Port 2) 和两个公网 IP 地址 (IP1 和 IP2) 的客户端服务器 S 发出第一次 (Port 1、IP 1)、第二次 (Port 2、IP 1)、第三次 (Port 1、IP 2)、第四次 (Port 2、IP 2) 共四次连接, 计算出相邻两次连接所得到的端口增量, 如果各次的增量值相同 (或都是 0) 则说明是获得

固定增量就转入(2)。若各次的增量不尽相同,说明 NAT 给新建连接分配端口是随机的,若将获得的随机增量值记为 ΔT ,经过大量的实验发现 NAT 在分配随机端口号时仍存在着某种相关性或函数关系,若 NAT 分配给用户 B 第一次连接的端口号是 P_1 ,第二次分配的端口号是 P_2 ,则会发现 $P_2 = P_1 + \Delta T$,其中 $\Delta T = f(p)$ 。实验证明依据网络特性对 ΔT 值的范围进行分析与预测,然后用试探法来确定端口的增量值也是一种获得随机端口地址好的方法。

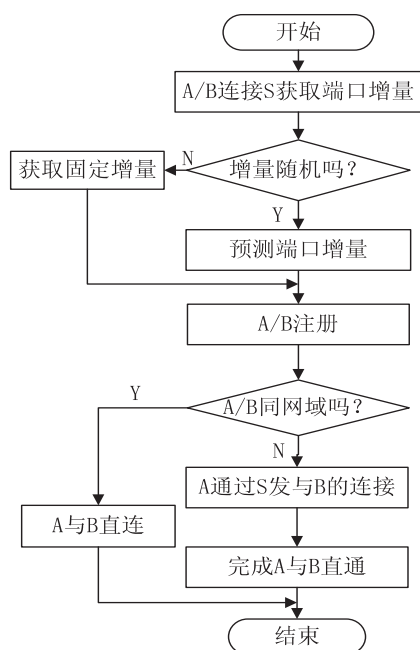


图2 A与B的TCP连接流程图

(2)客户端 A 与 B 通过连接服务器 S 完成在 S 上的注册,S 在映射表中记录下客户端 A 与 B 的网域名、内网 IP 地址、映射后的 IP 地址、端口增量。

(3)检查客户端 A 与 B 在 S 上注册的网域名,若客户端 A 与 B 在同一网域内,则 A 直接向 B 的内网地址发起 TCP 连接完成通信,转入(8)。若客户端 A 与 B 不在同一网域内转入(4)。

(4)客户端 A 按照前面 TTL 的确定方法获得 TTL 值,并侦听返回的 ICMP 消息,获得 TCP 的连接序号 SYN 及端口映射增量,把 SYN 和端口增量发给 S,并请求服务器 S 与客户端 B 连接。

(5)服务器 S 告知客户端 B 客户端 A 的连接请求,且将客户端 A 的预测 IP 地址及 SYN 发送给客户端 B,同样服务器 S 也将 B 的预测值发给 A。客户端 A 用前面的 SYN 发送连接要求到 B 的预测地址使 SYN 正好穿越 NAT A 以建起来自客户端 B 的映射。

(6)B 向 A 的预测地址发送 SYN+ACK,由于之前 NAT A 设备已建好映射规则,故客户端 B 发出的连接要求能顺利经过。

(7)客户端 A 收到连接要求,发出确认包 ACK 完

成三次握手,建立了 TCP 连接通道。

(8)A 与 B 间建立了连接,实现了 P2P 通信,就不再需要与 S 交换信息了。

7 结束语

‘采用端口预测穿越 NAT 的新方案’能穿越所有类型的 NAT,克服了目前常用的几种 NAT 穿越技术存在需要改变网络环境、不支持 Symmetric NAT 与 TCP 的穿越、延时、丢包等问题,特别适合于对网络安全需求更高,使用 Symmetric NAT 的企业用户。具有极高的应用和推广价值。

参考文献:

- [1] 陈明东. OpenH323 网络视频会议中微量化穿越技术研究[J]. 计算机与现代化,2012(2):120-123.
- [2] 韩小燕,曾桂根,李敏. SIP 中 NAT 穿透技术的研究及实现[J]. 计算机技术与发展,2011,21(1):193-196.
- [3] Srisuresh P, Ford B, Kegel D. State of peer-to-peer (p2p) communication across network translators (NATs) [EB/OL]. 2008-03-15 [2008-11-16]. <http://www.ietf.org/rfc/rfc5128.txt>.
- [4] 朱光,张云华,卢娟. 基于 ICE 的 VOIP 穿越 NAT 方案的研究[J]. 计算机应用与软件,2011,28(10):222-224.
- [5] 畅巨峥,汪滢,王庆辉. 利用 ICE 实现 VOIP 媒体流穿越[J]. 现代电子技术,2010(6):105-108.
- [6] Rosenberg J, Weinberger J, Huitema C, et al. STUN-Simple traversal of user datagram protocol (udp) through network address translators (nats) [EB/OL]. (2003-03-11) [2008-11-16]. <http://www.ietf.org/rfc/rfc3489.txt>.
- [7] Jennings C. NAT classification results using STUN [EB/OL]. [2005-10-21]. <http://www.ietf.org/internet-drafts/draftjennings-midcom-stun-results-02.txt>.
- [8] Huston G. A look inside network address translators[J]. The internet protocol journal,2004,7(3):2-32.
- [9] Newrong Inc. NAT traversal SDK [EB/OL]. [2005-10-25]. <http://www.newrong.com/en/product/index.html>.
- [10] 孙名松,段志鸣,王湛昱. 混合式 P2P 网络 UDP 下 NAT 穿越方案的研究与设计[J]. 计算机与数字工程,2010,38(4):104-107.
- [11] 黄桂敏,朱晓姝. 基于 UDP 协议穿透 NAT 设备的对等网络模型研究[J]. 计算机工程与设计,2010,31(2):317-320.
- [12] 彭李超,谭兵. 基于 STUNT 的 Symmetric NAT 穿越[J]. 微计算机应用,2010,31(10):31-35.
- [13] 郑少仁. 现代交换原理与技术[M]. 北京:电子工业出版社,2010.
- [14] 刘娟娟,陶加祥. 一种基于第三方服务器的 P2P 穿透 NAT 的实现方法[J]. 软件导刊,2010,9(1):121-122.
- [15] 王秀欣,臧宇林,王鼎. 基于 NAT 协议的 NAT 穿越技术的设计与实现[J]. 电力系统通信,2009,30(4):60-63.

P2P中NAT穿越问题的研究

作者：[孙卫喜](#)，[席少龙](#)，[SUN Wei-xi](#)，[XI Shao-long](#)

作者单位：[渭南师范学院 数学与信息科学学院 计算机网络工程技术中心, 陕西 渭南, 714000](#)

刊名：[计算机技术与发展](#)



英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(2)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201402061.aspx