

混合式 P2P 网络 UDP 下 NAT 穿越方案的研究与设计^{*}

孙名松¹⁾ 段志鸣¹⁾ 王湛昱²⁾

(哈尔滨理工大学网络信息中心¹⁾ 哈尔滨 150080)(哈尔滨工业大学机电工程学院工程训练中心²⁾ 哈尔滨 150001)

摘 要 随着 P2P 网络技术的迅速发展,它给用户带来了巨大的便利和效益, P2P 充分利用了网络带宽,大大提高了带宽的利用率。 NAT 技术的广泛应用主要是为了解决公共 IP 地址不足的问题, 却对 P2P 的深入应用造成障碍, 基于 P2P 的 NAT 穿越问题已经成为当今的热点议题。 该方案根据混合式 P2P 网络中特殊结构的特点, 借鉴 skype 的成功经验, 改进超级节点 UDP 下 NAT 穿越的设计, 利用超级节点记录用户信息帮助 P2P 应用实现非对称 NAT 的穿越, 利用超级节点中继来解决 P2P 下对称 NAT 的穿越, 最终实现 P2P 的正常通信。

关键词 P2P; NAT; 穿越
中图分类号 TP393

Research and Design of NAT Travsering Scheme Based on Composite P2P Network on UDP

Sun Mingsong¹⁾ Duan Zhiming¹⁾ Wang Zhanyu²⁾

(Network Information Center, Harbin University of Science and Technology¹⁾, Harbin 150080)
(Engineering Training Center, Harbin Institute of Technology²⁾, Harbin 150001)

Abstract In recent years, the application based on P2P network technology has developed rapidly. It has brought the users tremendous convenience and efficiency, and P2P make full use of the network bandwidth, greatly increasing the bandwidth utilization. NAT technology handicaps the further P2P application, although it is widely used to solve the problem that caused by public IP addresses lackness. NAT traversing based on P2P has become a hotspot of VoIP application and the relevant technology of traversing are various. The special construction characteristic is used to implement P2P communication by utilizing skype experience and improving the NAT travsering scheme of super nodes on UDP. With the help of informations that recorded by super node, dissymmetry NAT travsering can be implemented by P2P applications, symmetry NAT travsering under P2P can be resolved by the relay of super nodes, and P2P communication can be archieved finally.

Key Words P2P, NAT, traversing
Class Number TP393

1 引言

NAT 被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单, NAT 不仅完美地解决了 IP 地址不足的问题, 而且还能够有效地避免来自网络外部的攻击, 隐藏并保护网络内部的计算机。但是随着 P2P 技术的广泛应用,

NAT 带来的实际问题也引起了人们的重视。 NAT 技术虽然缓解了 IPV4 地址匮乏的危机, 但却给互联网上的主机, 特别是处于不同内网的主机之间的 P2P 通信带来了障碍, 限制了 P2P 的深入应用。 NAT 阻碍主机进行 P2P 通信的主要原因是 NAT 使得内部网络主机的 IP 地址对外部网络不可见; 不允许外部主机主动访问内部主机; 内部

^{*} 收稿日期: 2009 年 12 月 20 日, 修回日期: 2010 年 1 月 25 日
作者简介: 孙名松, 男, 教授, 研究方向: 网络应用, 网络安全。 段志鸣, 男, 硕士, 研究方向: 网络应用, 网络安全。
王湛昱, 男, 硕士, 助理工程师, 研究方向: 网络应用。

©1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

主机可以作为客户机访问外部网络,但却不能作为服务器向外部网络提供服务。而在 P2P 的应用中,每个节点既是客户机又是服务器,他们是对等的,如果不能穿越 NAT, P2P 网络就无法实现真正的对等。本文利用混合式 P2P 网络中特殊结构的特点,借鉴 skype 的成功经验^[1],改进超级节点 UDP 下 NAT 穿越的方案^[2],利用超级节记录用户信息帮助 P2P 应用实现非对称 NAT 的穿越,利用超级节点中继来解决 P2P 下对称 NAT 的穿越,最终实现 P2P 的正常通信。

2 相关性研究

2.1 混合式 P2P 网络

Kazaa 模型是 P2P 混合网络的典型代表,它在纯 P2P 分布式模型基础上引入了超级节点的概念,综合了集中式 P2P 快速查找和纯 P2P 去中心化的优势。Kazaa 模型将节点按能力不同(计算能力、内存能力、连接带宽、网络滞留时间等)区分为普通节点和搜索节点两类。其中搜索节点与其临近的一些普通节点之间构成一个“自治簇”,簇内采用基于集中目录式结构的 P2P 模式,而整个 P2P 网络的各个不同的簇之间再通过纯 P2P 模式将搜索节点连起来,还可以在各个搜索节点之间再次选取性能最优的节点或者另外引入一个新的性能最优的节点,作为索引节点(也就是超级节点)来保存整个网络中可以利用的搜索节点信息,并且负责维护整个网络的结构。由于每个簇中的超级节点监控着所有普通节点的行为,可以非常有效的消除纯 P2P 结构因采用泛洪算法而带来的网络拥堵、搜索迟缓等不利影响。同时也能使一些恶意攻击行为在网络局部得到有效控制,而且超级节点的存在也在一定程度上提高了整个网络的负载均衡^[3~4]。

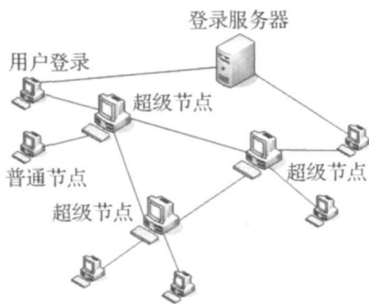


图 1 混合式 P2P 网络-skype 的系统结构示意图

2.2 NAT 技术

NAT(Network Address Translator)^[5] 又称地

址代理,用来实现私有地址和公有地址之间的转换。私有地址是指内部网络的主机 IP 地址,而公有地址是指内部网以外的可路由的公共地址(在 Internet 上全球惟一的 IP 地址)。按照地址转换的方式,可以将 NAT 分为 3 类,静态 NAT、动态 NAT 和网络地址端口转换(NAPT)。其中 NAPT 方式是企业网常用的 NAT 类型,通过同时改变内部主机的 IP 地址和端口号完成地址转换。按照地址映射的实现方式,可以将 NAT 分为 4 类,全锥型 NAT(full cone NAT)、受限锥型 NAT(restricted cone NAT)、端口受限锥型 NAT(port restricted cone NAT)和对称 NAT(symmetric NAT)。前 3 种 NAT 均可实现某内部(IP: 端口)对与多个外部(IP: 端口)对之间的映射转换,区别在于 NAT 的激活以及端口的限制。第 4 种则要求每一对内外(IP: 端口)对对应惟一的映射绑定,即根据目的地址不同而映射为不同的公网地址。

2.3 基于 NAT 穿越的解决方案

目前基于 NAT 穿越主要分为 UDP 下和 TCP 下,由于 UDP 是面向无连接的,因此应用较为广泛,我们主要研究 UDP 下 NAT 穿越的技术。现在主要有以下几种办法:ALG(Application Layer Gateway)、MIDCOM、STUN(Simple Traversal of UDP through NAT)、TURN(Traversal Using Relay NAT)、完全代理(Full Proxy)、ICE(Interactive Connectivity Establishment)、SBC(session border controller)、UPnP(Universal Plug and Play)、RSIP(Realm specification Internet Protocol)等,这里我们简单介绍一下 STUN 和 TURN,因为后面的方案会用到这两个技术。

2.3.1 STUN(Simple Traversal of UDP through NAT)

STUN 是一种网络协议,它允许位于 NAT(或 多重 NAT)后的客户端找出自己的公网地址,查出自己位于哪种类型的 NAT 之后以及 NAT 为某一个本地端口所绑定的 Internet 端端口。这些信息被用来在两个同时处于 NAT 路由器之后的主机之间建立 UDP 通信^[6~7]。

2.3.2 TURN(Traversal Using Relay NAT)方式

TURN 方式解决 NAT 问题的思路是私网中的终端通过某种机制预先得到公网上的服务地址(STUN 方式得到的地址为出口 NAT 上外部地址,TURN 方式得到地址为 TURN Server 上的公

网地址), 然后在报文净载中直接填写 TURN Server 上的公网地址, 由 TURN 服务器做中继转发实现穿越^[9]。

3 混合式 P2P 网络 UDP 下的 NAT 穿越方案

为了更好地研究混合式 P2P 网络 UDP 下的 NAT 穿越, 方案设置两种情况, 第一种情况是同一个超级节点下的两个终端的通信, 第二种情况是不同超级节点下的两个终端的通信。

首先, 介绍第一种情况(如图 2)。

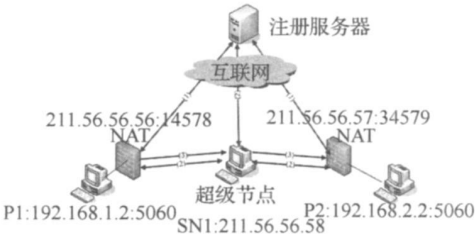


图 2 混合式 P2P 网络同一超级节点内 NAT 穿越示意图
设定用 $P1$ 、 $P2$ 代表终端, $SN1$ 代表超级节点。
第一步, $P1$ 、 $P2$ 加入到 P2P 网络, 首先需要到

表 1 $SN1$ 内用户记录

用户 ID	验证码	内网 IP	内网端口	外网 IP	外网端口	NAT 类型	临时分配中继端口
$P1$	XXX	192.168.1.2	5060	211.56.56.56	14578
$P2$	YYY	192.168.2.2	5060	211.56.56.57	34579

第三步, $P1$ 要与 $P2$ 进行通信, 因为超级节点内保存着节点下所有用户的记录, 所以通过对超级节点的搜索, $P1$ 很快知道 $P2$ 与自己是 在 同一个超级节点下。

如果 $P1$ 、 $P2$ 都是全锥型的 NAT, 因为 $SN1$ 与 $P1$ 、 $P2$ 均保持联络的状态, 而且全锥型 NAT 的特点决定了任何外部主机都可以通过 NAT 上已经激活的映射访问内网的主机, $P1$ 可以通过查询 $SN1$ 内的用户记录, 发现 $P2$ 是全锥型, 进而通过访问其在记录内的外网映射与 $P2$ 进行正常通信;

如果 $P1$ 是全锥型、 $P2$ 是限制锥型时, 因为限制锥型只允许被内部主机访问过的外部主机进入 NAT, 因此需要 $SN1$ 协助, 具体步骤是 $P1$ 通过查询 $SN1$ 的用户记录, 发现 $P2$ 是限制锥型, 要求 $SN1$ 通知 $P2$ 主动向 $P1$ 的外网映射发起连接, 因为 $P1$ 是全锥型, $P2$ 可以与 $P1$ 取得连接, 随后双方可以正常通信;

如果 $P1$ 是全锥型、 $P2$ 是端口限制锥型时, 仍然可以用上面的方法实现正常的通信;

如果 $P1$ 是全锥型、 $P2$ 是对称型时, 就需要

注册服务器进行注册, 获得各自的身份 ID 和验证码。随后 $P1$ 、 $P2$ 请求注册服务器用 STUN 技术对自己进行 NAT 类型判断, 判断结果由用户自己保存。同时注册服务器标示 $P1$ 、 $P2$ 没有加入任何超级节点, 因此未正式进入网络。

第二步, $P1$ 、 $P2$ 用收到的身份 ID 和验证码向附近的超级节点 $SN1$ 发起加入请求, $SN1$ 将收到的信息送注册服务器认证, 注册服务器收到超级节点验证请求进行验证, 验证通过后通知 $SN1$, 同时将 $P1$ 、 $P2$ 划到 $SN1$ 下, 解除 $P1$ 、 $P2$ 标示。 $SN1$ 收到通知后接受 $P1$ 、 $P2$ 申请, 并需要与 $P1$ 、 $P2$ 交互得到 NAT 地址映射及 NAT 类型等信息, 最后建立用户记录。如果是对称的 NAT 类型, $SN1$ 会采取 TURN 式的策略, 为其分配临时中继端口, 同时为每个连结的节点设立定时器, $P1$ 、 $P2$ 要定时与 $SN1$ 进行联系, 延时就会被标记下网离线, 并收回临时分配的中继端口。 现在我们为了深入研究 NAT 穿越, 将 $P1$ 、 $P2$ 均设置在 NAT 之后。 STUN 探测过程和 TURN 方式有很多文献介绍, 这里不详述, 用户记录如表 1 所示。

$SN1$ 进行中继, 具体步骤是 $P1$ 通过查询 $SN1$ 的用户记录, 发现 $P2$ 是对称型, 记录下 $P2$ 的临时中继端口, 要求 $SN1$ 通知 $P2$ 主动激活其在 $SN1$ 上的临时中继端口, 然后 $P1$ 向 $P2$ 的临时中继端口发起连接, 由 $SN1$ 中继到 $P2$, 双方可以正常通信。

如果 $P1$ 是限制锥型或端口限制锥型、 $P2$ 是全锥型时, 那么 $P1$ 主动发起连接不会存在障碍。

如果 $P1$ 、 $P2$ 都是限制锥型时, $P2$ 主动连接 $P1$ 的方法就行不通了, 因为 $P2$ 主动向 $P1$ 的外网映射发起连接时, 会遭到 $P1$ 外部 NAT 的拒绝, 因为 $P1$ 还没有主动访问过 $P2$, 这时就要“打洞”, 具体步骤是 $P1$ 通过查询 $SN1$ 的用户记录, 发现 $P2$ 是限制锥型, $P1$ 要求 $SN1$ 通知 $P2$ 主动向 $P1$ 的外网映射发起连接, 然后 $P1$ 再去连接 $P2$, $P2$ 向 $P1$ 的连接会遭到 $P1$ 外部 NAT 的拒绝, 但稍后 $P1$ 向 $P2$ 的连接会因为 $P2$ 主动连接 $P1$ 时在 NAT 上留下的映射而顺利通过, 双方可以正常通信;

如果 $P1$ 是限制锥型、 $P2$ 是端口限制锥型及 $P1$ 、 $P2$ 都是端口限制锥型时, 打洞的方法依然有

效, 双方可以实现正常通信;

如果 $P1$ 是限制锥型或端口限制锥型、 $P2$ 是对称型时, 因为 $P1$ 会主动连接 $P2$ 在 $SN1$ 上的中继端口, 所以通过 $SN1$ 中继, 双方通信不存在障碍;

如果 $P1$ 、 $P2$ 都是对称型时, 双方通过 $SN1$ 中继, 通信不存在障碍。虽然双方在 $SN1$ 上均有临时中继端口, 但此时只会用 $P2$ 的中继端口进行中继。

现在, 介绍第二种情况(如图 3)。

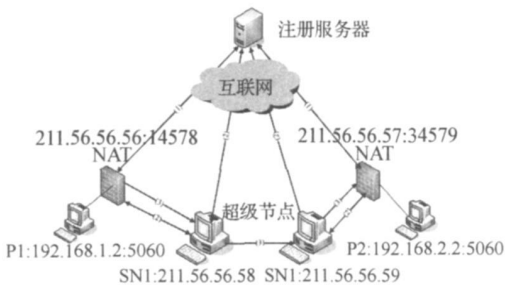


图 3 混合式 P2P 网络不同超级节点间 NAT 穿越示意图
设定用 $P1$ 、 $P2$ 代表终端, $SN1$ 、 $SN2$ 代表超级节点。

第一步和第二步, 在两种情况下并没有多大分别, 只是 $P1$ 、 $P2$ 要分别向自己附近的超级节点 $SN1$ 、 $SN2$ 发起加入请求, $SN1$ 、 $SN2$ 各自维护自己的用户记录, 并决定是否分配临时中继端口。同样 $SN1$ 、 $SN2$ 也要设置定时器以监测终端的在线状态。

第三步, $P1$ 要与 $P2$ 进行通信, 通过对超级节点的搜索, $P1$ 很快知道 $P2$ 是在超级节点 $SN2$ 下; $P1$ 、 $P2$ 是不同 NAT 类型时的穿越步骤与同一超级节点下的步骤基本类似, 只是 $P1$ 此时查找 $P2$ 的 NAT 类型和映射记录需要在 $SN2$ 上进行, 并且要求 $P2$ 主动连接和“打洞”操作需要 $SN2$ 的协助, 在穿越对称类型时, 需要用 $SN2$ 分配给 $P2$ 的临时中继端口进行中继。

4 结语

该方案利用超级节点记录用户信息, 帮助 P2P 实现非对称 NAT 穿越; 利用超级节点的中继, 解决了对称 NAT 下的 P2P 穿越问题。方案虽然解决了 UDP 下 P2P 通信障碍的问题, 却给超级节点带来了比较大的负担, 尤其是穿越对称 NAT 类型时, 需要超级节点做为中继服务器代价太大。所以继续研究改良 P2P 结构, 优化 P2P 网络及传输技术仍是今后需要深入研究的重要课题。

参考文献

[1] Salman A. Baset, Henning G. Schulzrinne. Analysis of the Skype Peer-to-Peer Internet Telephony Protocol [S]. INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, 2006, 4: 1~11

[2] 蔡祖恋, 刘克剑, 甘春娇, 等. 无结构 P2P 系统中一种 UDP 协议穿透 NAT 技术的研究[J]. 西华大学学报, 2009, 28: 58~61

[3] 邢小良. P2P 技术及其应用[M]. 第一版. 北京: 人民邮电出版社, 2008, 2: 32~33

[4] 杨天路, 刘宇宏. P2P 网络技术原理与系统开发案例 [M]. 北京: 人民邮电出版社, 2007, 6: 20~21

[5] Egevang K, Francis P. The IP Network Address Translator(NAT)[S]. IETF, RFC1631, 1996

[6] 郭长清. 针对 SIP 的 STUN 解决方案的设计与实现 [J]. 科学技术与工程, 2006, 6: 1556~1660

[7] Rosenberg J, Weinberger J. STUN Simple Traversal of User Datagram Protocol(UDP) Through Network Address Translators (NATs) [S]. RFC3489, IETF, 2003, 3

[8] Rosenberg J, Mahy R, Hutiema C, et al. Traversal using relay NAT (TURN). IETF Internet draft [EB/OL]. [2007-05-10]. <http://www.jdrosen.net/papers/draft-Rosenberg-midcom-turn-08.txt>