第35卷 第24期 计 算 机 工 程 2009年12月
Vol.35 No.24 Computer Engineering December 2009
·软件技术与数据库· 文章编号：1000—3428(2009)24—0081—03 文献标识码：A 中图分类号：TP301.6

一种媒体流穿越NAT的算法设计与实现

魏立峰，刘丹斌，王庆辉
(沈阳化工学院信息工程学院，沈阳 110142)

摘 要：基于交互式连通建立草案协议，综合运用网络地址转换(NAT)会话穿越工具和中继穿越工具，设计一个媒体流穿越NAT的算法实例。使用请求/应答交互方式，探索通信双方NAT拓扑部署，通过排序算法找到并选择一条最优的传输路径。在Linux下进行编程测试，能使媒体流较好地穿越不同拓扑部署的NAT。

关键词：交互式连通建立；会话初始协议；网络地址转换；候选

Algorithm Design and Implementation of Traversing NAT for Media Streams

WEI Li-feng, LIU Dan-bin, WANG Qing-hui
(School of Information Engineering, Shenyang Institute of Chemical Technology, Shenyang 110142)

【Abstract】 An algorithm instance is designed about traversing Network Address Translator(NAT) for media streams, in which Session Traversal Utilities for NAT(STUN) and Traversal Using Relays around NAT(TURN) based on the Interactive Connectivity Establishment(ICE) are used synthetically. The algorithm explores the NAT topology for peer by the request/response interaction and finds the best path. The program test on Linux proves that media streams are able to pass through various topologies of NAT deployment.

【Key words】 Interactive Connectivity Establishment(ICE); Session Initiation Protocol(SIP); Network Address Translator(NAT); candidate

自提出会话初始协议(Session Initiation Protocol, SIP)起，穿越网络地址转换(Network Address Translator, NAT)问题就一直被关注[1]。目前解决该问题的方法很多，如ALGs, STUN, TURN等，这些方法应用于不同的网络拓扑时却分别有着各自的利弊，如经典STUN协议，该协议实现简单，可以穿越多重NAT，主要适用于非对称NAT的拓扑部署。TURN协议作为STUN的一个扩展，主要适合解决对称NAT的拓扑部署，但由于引入中继，容易出现丢包和延迟现象，因此需要根据不同的网络拓扑采取不同的穿越方法，从而给系统引入了许多复杂性和脆弱性因素。本文权衡利弊，针对此问题设计了一个基于交互式连通建立(Interactive Connectivity Establishment, ICE)[2]的算法实例。

1 媒体流穿越NAT与ICE算法

媒体流穿越NAT的过程是独立于SIP信令协议的。通信发生在2个peer端：主叫端和被叫端。ICE初始请求(Offer)包含了描述主叫端媒体流的配置与特征，并经过信令中继，最后到达被叫端。假设被叫端同意通信，产生应答消息(Answer)并反馈至主叫端，则媒体流建立成功。此外，信令协议还对媒体流参数修改以及会话终止消息等提供支持。对于SIP，会话发起者UAC，会话响应者即UAS，请求消息对应SDP[3]请求里面的INVITE，应答消息对应SDP应答里面的200 OK。

建立SIP呼叫连接的过程中，发送INVITE请求和返回200 OK响应时，通过ICE算法将SDP消息体*c*字段中的私网IP地址和*m*字段的端口号改写为用于RTP媒体流传输的有效候选地址，这些地址是可以在公网上路由的。这样，在SIP呼叫连接建立之后，双方就会根据协商好的地址和端口发送和接收媒体流。因此，RTP流可以顺利穿越NAT设备。

2 ICE方式穿越NAT的实例设计

2.1 拓扑及功能部署

在SIP通信中，当通信双方均处于NAT后，且处于不同NAT后，这种拓扑部署穿越最为复杂，本文以此作为实例来设计。在实验室本研究组将SIP用户代理A和B分别部署于2个不同的NAT背后，给主叫端A分配私网地址192.168.1.22，被叫端B分配私网地址172.16.10.102。NAT A拥有公网地址202.199.112.102，NAT B拥有公网地址202.199.112.87，且两者均为对称型NAT。同时在公网中部署了SIP服务器。为了实现ICE算法，在SIP用户代理上增加STUN Client/Server模块、TURN Client模块、ICE管理模块。还在公网部署STUN服务器、TURN服务器，如图1所示。

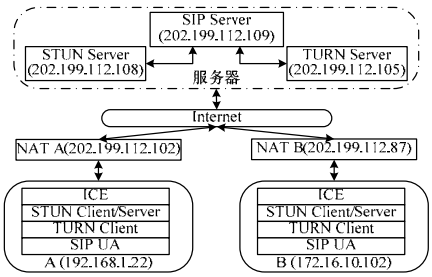

图1 拓扑-功能部署图

基金项目：沈阳市科学技术计划基金资助项目“无线网络视频监控系统关键问题研究及应用”(1081236-1-00)

作者简介：魏立峰(1962－)，男，教授，主研方向：网络体系结构与协议，多媒体通信；刘丹斌，硕士研究生；王庆辉，副教授

收稿日期：2009-07-06 **E-mail：**weilifeng62@sina.com

其中，STUN 服务器拥有公网地址 202.199.112.108，TURN 服务器拥有公网地址：202.199.112.105。

2.2 ICE 算法流程

ICE 是一种探索、学习和更新式的解决方案。在 ICE 算法的开始，通信的 2 个代理并不知道自己的拓扑部署——在 NAT 后还是不在 NAT 后。

2.2.1 初始请求的发送

为了探索本地拓扑，代理 A 执行如下操作：

收集 3 类候选地址：(1)A 从本地接口上获得主机候选地址 192.168.1.22: 8484；(2)发送 STUN 绑定请求[4]到 STUN 服务器获得服务器反身候选地址 202.199.112.102: 61866(图 2 消息 1~消息 4)；(3)发送 TURN 分配请求到 TURN 服务器获得中继候选地址 202.199.112.105: 5006，同时也获得了服务器反身候选地址 202.199.112.102: 62072(图 2 消息 5~消息 8)。这些候选地址是随后可能用于接收媒体流的地址。

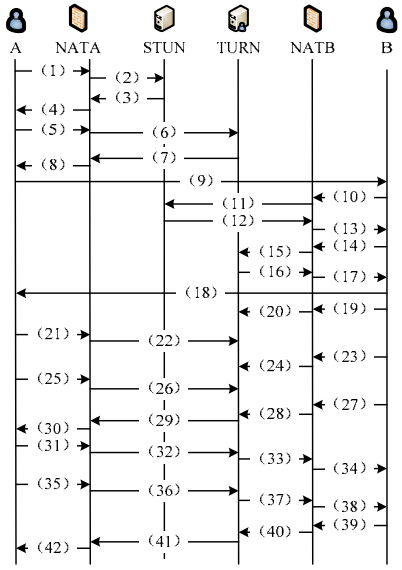

图 2　ICE 算法请求/应答交互图

计算候选的优先级。设置主机候选的类型优先参数为最高值 126，服务器反身候选的类型优先参数为 100，中继候选的类型优先参数为最低值 0。本地参数设为 65 535，分组 ID 为 1。经计算，主机候选的优先级为 2 130 706 431，服务器反身候选的优先级为 1 694 498 815，中继候选的优先级为 16 777 215。按候选优先级高低排序。分配主机候选的基金属性为 1，服务器反身候选的基金属性为 2，中继候选基金为 3。

按中继候选、服务器反身候选、主机候选次序选择默认候选(该候选包含了默认用于接收媒体流的地址和端口)，由于 A 获得了中继候选，因此优先选择连通概率较大的中继候选 202.199.112.105:5006 作为默认候选。

将默认候选的 IP 地址和端口编辑进 SDP 的 *c* 行和 *m* 行，并添加收集到的 3 个候选地址到 *a* 属性，形成发送请求 Offer(图 2 消息 9)，通过信令信道传给 B，请求消息内容如下所示，修改的参数和添加的属性值用粗体显示。

v=0
o=UserA 2890844526 2890842807 IN IP4 192.168.1.22
s=
c=IN IP4 **202.199.112.105**
t=0 0
a=ice-pwd:asd88fgpdd777uzjYhagZg
a=ice-ufrag:8hhY
m=audio **5006** RTP/AVP 0
b=RS:0
b=RR:0
a=rtpmap:0 PCMU/8000
a=candidate:1 1 UDP 2130706431 **192.168.1.22 8484** typ host
a=candidate:2 1 UDP 1694498815 **202.199.112.102 61866** typ srflx raddr 192.168.1.22 rport 8484
a=candidate:3 1 UDP 16777215 **202.199.112.105 5006** typ relay raddr 202.199.112.102 rport 62072

2.2.2 应答的发送

当 B 收到请求，就知道了 A 所处的拓扑环境(反身候选和主机候选地址不同，说明 A 处于 NAT 后)。B 执行和 A 相同的操作(图 2 消息 10~消息 17)，收集候选，计算候选优先级，设置基金，选择默认候选，进行 SDP 编码，并发送应答消息 Answer 给 A(图 2 消息 18)。这样 A 也知道 B 所处的拓扑环境了，反身候选和主机候选地址不同，说明 B 也处于 NAT 后。应答消息内容如下所示：

v=0
o=UserB 2808849004 2808849004 IN IP4 172.16.10.102
s=
c=IN IP4 **202.199.112.105**
t=0 0
a=ice-pwd:YH75Fviy6338Vbrhrlp8Yh
a=ice-ufrag:9uB6
m=audio **49152** RTP/AVP 0
b=RS:0
b=RR:0
a=rtpmap:0 PCMU/8000
a=candidate:1 1 UDP 2130706431 **172.16.10.102 8484** typ host
a=candidate:2 1 UDP 1694498815 **202.199.112.87 63756** typ srflx raddr 172.16.10.102 rport 8484
a=candidate:3 1 UDP 16777215 **202.199.112.105 49152** typ relay raddr 202.199.112.87 rport 63768

决定代理角色。由于 A 和 B 都是 Full 型代理，且 A 是请求的发起端，因此 A 充当控制代理，B 为被控制代理。A 和 B 开始对候选进行配对。A, B 各有 3 个候选，A, B 各选 1 个候选组成对，共有 9 个对。由于不能从服务器反身候选和中继候选发送请求，因此剪掉冗余对，A, B 每一方只剩下 3 个对，即从主机候选分别到对端的主机候选、服务器反身候选、中继候选。

计算候选对的优先权并对候选对排序。对于控制代理 A 而言，按优先级排序候选对，形成检查列表，结果如表 1 所示。

表 1　代理 A 的检查列表

本地候选	远程候选	对优先级
192.168.1.22:8484	172.16.10.102:8484	9.150 03e+18
192.168.1.22:8484	202.199.112.87:63756	7.277 82e+18
192.168.1.22:8484	202.199.112.105:49152	7.205 76e+16

对于被控制代理 B，同样也计算候选对的优先级，并按优先级排序，形成自己的检查列表，如表 2 所示。

表 2　代理 B 的检查列表

本地候选	远程候选	对优先级
172.16.10.102:8484	192.168.1.22:8484	9.150 03e+18
172.16.10.102:8484	202.199.112.102:61866	7.277 82e+18
172.16.10.102:8484	202.199.112.105:5006	7.205 76e+16

检查列表的次序决定了将来连通性检查的次序。设置检查列表中最高优先级对的状态为等待态，其余对为冷冻态。

2.2.3　连通性检查

B 开始它的连通性检查。B 依次从检查列表移出最高优先级对，对的状态由等待态迁移为进行态(这同时会触发次高优先级对转换为最高优先级对，状态由冷冻态变为等待态)，开始连通性检查。对第 1 个对从本地候选 172.16.10.102: 8484 到远程候选 192.168.1.22: 8484 发送绑定请求(图 2 消息 19~消息 20)，由于远程候选处于 NAT 后是私有的，不能被路由，检查失败。对第 2 个对执行连通性检查(图 2 消息 23~消息 24)，当数据包抵达 NAT A 时，NAT 会发现传输地址 202.199.112.102: 61866 已经映射 202.199.112.108: 3478 了。而此时 STUN 请求的源地址并非 202.199.112.108: 3478，所以数据包必然会被 NAT A 丢弃。

对第 3 个对执行连通性检查(图 2 消息 27~消息 34)。由于远程候选等于中继候选，为了有效利用带宽，应从本地候选 172.16.10.102: 8484 向远程候选 202.199.112.105: 5006 发送信道绑定请求[5]。请求中指出了信道号 0x4001 及通信对端 A 的地址，请求到达 TURN 服务器，绑定成功。该绑定的成功，激励其学习对端反身候选 202.199.112.102: 62072，经该反身候选到达对端 A，然后产生了一个成功的响应，A 的检查终于成功。B 产生了一个新的对(202.199.112.105: 49152, 202.199.112.105: 5006)，该对被增加到有效列表，媒体流分组的 ICE 处理迁移到完成态。至此 B 可以利用信道 0x4001 发送媒体流分组到 A 了，如图 3 所示。

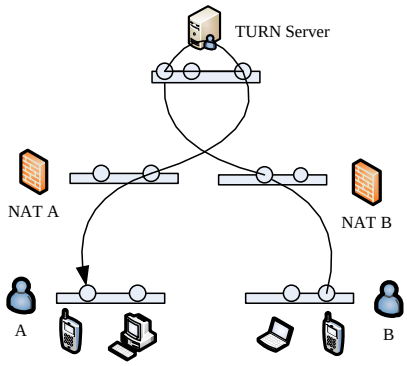

图 3　B 到 A 的连通性检查

当 A 收到应答(图 2 消息 18)后，也按照候选对的优先级次序开始自己的连通性检查(图 2 消息 21~消息 22，消息 25~消息 26)。和 B 类似，也失败了。当 A 一收到 B 检查成功的消息(图 2 消息 30)，马上开始触发检查(图 2 消息 35~消息 42)，在信道绑定请求中指定信道号 0x4002 以及对端 B 的地址。由于 A 是控制代理，在检查里可包含 USE-CANDIDATE 属性执行强制提名算法，结果检查也成功了。代理 A 产生了一个新的对(202.199.112.105:5006, 202.199.112.105:49152)，该对被增加到有效列表，并设置提名标志为 TRUE，媒体流分组的 ICE 处理迁移到完成态。A 可以通过信道 0x4002 发送媒体流到 B。

至此，通过该算法最终找到了媒体流传输的有效候选对，对应的最优路径也就随之确定了。由于有效候选是公网地址，因此通过该路径媒体流可顺利穿越 NAT。

3　测试结果

在 Linux 下利用 C/C++语言编程实现了 ICE 算法，对通信一方位于 NAT 后、双方位于同一 NAT 后、双方位于不同 NAT 后等拓扑部署进行了媒体流通信测试，通话正常。对称性 NAT 稍有延迟。表 3 是在 NATA 上捕获的关于代理 A (192.168.1.22: 8484)在 SIP 通信中穿越 NAT 及收到中继服务器 202.199.112.105 传回的应答包时的地址映射表。

表 3　NATA 的地址映射表

内容	映射 1	映射 2
通信协议	UDP	UDP
方向	出站	入站
专用地址	192.168.1.22	192.168.1.22
专用端口	8484	8484
公用地址	202.199.112.102	202.199.112.102
公用端口	62072	62072
远程地址	202.199.112.105	202.199.112.105
远程端口	5006	5006
空闲时间	10	29

4　结束语

本文设计了一个 ICE 算法实例，在算法的开始忽视拓扑，通过请求/应答交互，收集本地和通信对端尽可能多的候选信息，潜在地发现通信双方的拓扑，最终找到并选择一条或多条最优的媒体流传输的路径。从整体上分析可有效减少媒体延迟、丢包率和配置操作代价，实现负载均衡，提高网络的 QoS。

后续工作主要包括 2 个方面：(1)对算法进行优化，提高中继服务器的性能，减少穿越对称 NAT 的时延；(2)改进认证机制，增强网络的安全性。对本研究组而言，还有一个工作，即移植到嵌入式平台。相信 ICE 方案会有非常广阔的应用前景。

参考文献

[1] 刘春燕, 陈名松, 冼莉莉. 基于端口探测的 SIP 穿透 NAT 的设计与实现[J]. 计算机工程, 2008, 34(17): 114-116.

[2] Rosenberg J. Interactive Connectivity Establishment(ICE): A Protocol for Network Address Translator(NAT) Traversal for Offer/Answer Protocols[EB/OL]. (2007-10-29). http://tools.ietf.org/html/draft-ietf-mmusic-ice-19.

[3] IETF. SDP: Session Description Protocol[S]. RFC 4566, 2006.

[4] Rosenberg J, Mahy R, Matthews P, et al. Session Traversal Utilities for NAT(STUN)[EB/OL]. (2008-07-28). http://www.ietf.org/internet-drafts/draft-ietf-behave-rfc3489bis-18.txt.

[5] Rosenberg J, Mahy R, Matthews P, et al. Traversal Using Relays Around NAT(TURN): Relay Extensions to Session Traversal Utilities for NAT(STUN)[EB/OL]. (2008-07-12). http://www.ietf.org/internet-drafts/draft-ietf-behave-turn-09.txt.

编辑　顾逸斐