第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·网络与通信· 文章编号：1000—3428(2006)23—0116—03 文献标识码：A 中图分类号：TP393.09

SIP透明穿透NAT方案

蔡嘉勇，李 丹，陈 沫
(中国科学院计算技术研究所信息网络室，北京 100080)

摘 要：SIP是IETF提出的IP电话信令协议，应用于视频电话、即时通信等领域，而网络中大量存在的NAT成为SIP应用推广的最大障碍，因此SIP消息如何有效穿透NAT成为该领域的热点问题之一。文章分析了现有各类SIP穿透NAT的方案，发现其在网络拓扑和应用可扩展性上存在局限。提出了一种新的SIP透明穿透NAT方案，保持了SIP协议在应用方面的可扩展性和拓扑的灵活性，在NAT设备中也只需维护少量的地址映射信息，并对该方案的透明性予以实验验证。
关键词：SIP协议；SIP网络地址翻译；SIP应用层网关；IXP2400

Scheme for SIP to Traverse NAT Transparently

CAI Jiayong, LI Dan, CHEN Mo
(Lab of Information Network, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

【Abstract】 Session initiation protocol(SIP), which is delivered by IEFT for IP telephone signaling, is greatly used in video-phone, instant-messaging, and etc. recently. However what makes SIP difficult is the widely using of NAT devices in network, so how to traverse NAT efficiently becomes the SIP researching hotspot. All the existed approaches are reviewed for SIP NAT traversing, and found out their limitation in topology and flexibility. Basing on understanding on SIP, a new SIP NAT traverse approach is developed, which keeps the flexibility of SIP without assuming any topology and maintaining too much addresses mapping information. In the end, the transparency of the approach through a full test is demonstrated.
【Key words】 Session initiation protocol(SIP); SIP NAT; SIP ALG; IXP2400

会话(Session)是用户间的数据交换过程，Internet上大量应用都需要会话的创建与管理功能，这是IETF提出会话初始化协议SIP的初衷。在网络协议体系结构中，SIP协议位于传输层上的应用层，通过携带SDP(Session Description Protocol)载荷，可轻松地开/关会话、协商会话参数、建立数据交换流、管理会话。SIP定义了4类网络元素：用户代理(User Agent，UA)发送请求与响应；代理(Proxy)则转发SIP消息；注册服务器(Registrar)登记用户登录位置；重定向服务器(Redirect Server)管理并通知UA或Proxy用户的当前登录位置。在目前的SIP实现中UA通常作为通信客户端安装于PC，后3者则作为统一的服务端软件出现，因此本文中使用Proxy指代服务器端软件的统一体。

IETF在设计SIP协议时广泛借鉴已有的Internet协议，譬如HTTP、SMTP等，采用基于文本的编码。RFC3261[1]主要介绍SIP消息格式、通信方式及消息转发机制，SIP最大的特点是提供应用层定位、路由消息的能力，这是其灵活性的重要体现，而应用层数据中含有地址信息，却是造成SIP穿越NAT困难的根本原因。传统NAT设备只含传输层以下的转换，对应用层的信息分析则无能为力。

SIP协议提出伊始，人们就关注SIP穿透NAT问题。SIP消息的转换可分为两部分：SIP消息本身地址信息转换及其所携带SDP载荷中RTP地址信息转换。这必须建立在理解SIP语义的基础上，因此转换效率成为考虑的重点。关于SIP NAT的解决方案已有许多[2~5]，其主要思路可分为3类：(1)扩展NAT设备支持应用层解析——使用应用层网关(ALG)技术，如文献[2,5]；(2)使用SIP的可扩展性，对协议进行扩展以支持NAT应用，如文献[3]；(3)结合其它NAT协议，如STUN、ICE、MGCP，支持SIP NAT，如文献[4]等。

经分析，作者发现上述方案各有缺陷：文献[2]仅支持典型应用(网络内或外必须有Proxy)，文献[5]需为每个会话保存大量映射信息，存储利用率低；扩展SIP未成标准，不同厂商的SIP设备间无法通信；方案(3)扩展性虽不错，但客户端系统必须升级以支持该协议，且需专用服务器。最重要的问题是它们对SIP网络的拓扑作了假设：网络内或外必须有服务器(无论是Proxy还是STUN等服务器)，才能实现SIP的NAT穿越，甚至需要支持特定协议，这与SIP本身的灵活性与可扩展性原则相悖。

与此相反，SIP对网络拓扑不作任何假设，只需安装必要软件，就可选择任意可达路径与对方通信，这种灵活性也是其成为NGN核心协议的原因之一。因此SIP-NAT方案的设计必须保持其灵活性，基本要求是透明、高效。本文提出的新SIP NAT穿越方案，只简单计算并替换必要SIP头，无须在应用层保存地址映射信息，同时又适应各种SIP NAT拓扑环境。

1 SIP透明穿越NAT方案设计

SIP穿透NAT方案的基本要求是透明与高效。透明指SIP消息的内外转换全由NAT设备或特定服务器承担，SIP网络部署与软件安装不必考虑NAT的存在；高效是说存储要求低，执行效率高，不对网络设备造成负担。

1.1 设计思想

文献[1]定义了SIP协议的语法单位：消息头域(header)，

基金项目：国家自然科学基金资助项目(60273021)
作者简介：蔡嘉勇(1978－)，男，博士生，主研方向：大型网络安全与下一代互联网计算；李 丹，助研；陈 沫，博士生
收稿日期：2006-01-15 **E-mail：**jycai@mails.gucas.ac.cn

共 43 个，通常表示为“ name: value ”行的形式。消息以开始行(start-line)开始，请求的开始行格式为请求行(request-line)，响应则为状态行(status-line)。

达到高效目标要先缩小分析范围。以头域为单位分析，与 NAT 相关的有 Contact、Content-Length、Content-Type、From、Record-Route、Route、To、Via、CSeq、Expires 共 10 个，其中 Content-Length、Content-Type 与 SDP 转换模块相关；CSeq 用于判断消息所响应的请求类型；Expires 将影响建立的地址映射条目的存在时限，二者都无须修改；此外请求行包含被呼叫方的请求 URI(Request URI)，它是唯一标识通信主体的记号，可能包含主机的地址信息，也需转换。对于消息体(Message body)——SDP 载荷的转换，实现中是单独模块，不是本文的重点。因此 SIP 消息需转换的头域至多 7 个，其它头域直接跳过。

透明性目标要求对上述 7 个头域都进行处理。不同头域在应用层路由发挥的作用完全不同：Via 路由响应，Record-Route 在通信双方构造 Route 路径，Route 路由请求，Contact 与注册相关，请求 URI 用于首次呼叫中定位对方，From、To 用于验证消息的来源与目的。因此不同头域其转换逻辑必然不同。

头域是分析的基本单位，从协议定义的头域语义出发，面向 NAT 环境构造各头域的转换逻辑。在 SIP 路由中 Via、Record-Route、Route 发挥着重要作用，而其行为也极相似：首次定位过程中，SIP 将经过的每个中间元素(Proxy 或转发 UA)地址依次记录到某类头域，此后的实际路由中，中间元素每收到一条 SIP 消息，先检查某类头域的首地址是否指向自己，若是则删除，将消息转发给当前的第一个地址。这极似栈的先进先出操作，因此用“ 栈模式 ”设计分析替换算法。

1.2 实现过程

Record-Route 用于构造通信双方的 Route 路径：用户发出 INVITE 请求，消息在到达对方前，沿途愿意转发 SIP 请求的 Proxy，在收到消息后用本机的接收地址、端口构造一条新的 Record-Route 记录，并插入到所有 Record-Route 头域前，从而形成一个有序的地址列表。作者将消息中所有 Record-Route 头域按序设想为“ Record-Route 栈 ”。被呼叫方根据请求而响应，Record-Route 栈原封不动地拷贝至响应；同时将其倒置作为本次会话与对方通信的 Route 栈。当响应沿原路返回时，呼叫方直接把响应中的 Record-Route 栈作为 Route 栈。通信双方就同时拥有一条中间节点相同但顺序相反的路径，此后二者用各自的 Route 栈路由请求。

图 1 表示了用“ 栈模式 ”描述分析替换算法的设计过程。假设 4 个 Proxy 愿提供转发服务，分别为 RR0~RR3，数字表示其先后顺序。虚线为 NAT 定义的网域界限，由于呼叫未必始于内网，因此用 1、2 分别指代两个独立网络。

对于 NAT 接收的请求：当呼叫请求首次过 NAT 时，Record-Route 栈已按序记录 RR0 与 RR1，此时若不对消息转换，则根据 Record-Route 的语义，被呼叫方构造的 Route 栈将依次为 RR3-RR0，当被呼叫方发出请求时，消息到达节点 RR2 就会结束，因为 RR2 可能不识别网域 2 的节点地址 RR1。由于这种情况仅出现在网域 2 为内网时(内网能识别 Internet 地址)，因此 NAT 接收到 INVITE 消息时，检查 Record-Route 栈顶地址是否来自内网，若是则创建 NAT 映射条目 RR1→RR1’，并替换栈顶地址，来自外网则直接转发。

对于 NAT 接收的响应：被呼叫方发出响应，将 Record-Route 栈拷贝到响应沿原路返回。若呼叫始于内网，则当响应经 RR2 转发给 NAT 时，要对之前已替换的地址反向替换，否则呼叫方发出的请求将在节点 RR0 转发给外网 RR1’时错误；若呼叫始于外网，那么 NAT 在收到响应时应对栈中位于网域边缘的 RR2 构造映射 RR2→RR2’，否则呼叫方依据响应建立的 Route 栈将无法穿越 NAT。通过简单的内外地址辨别可得 RR1 与 RR2 位置——2 条连续 RR 记录分属不同域。

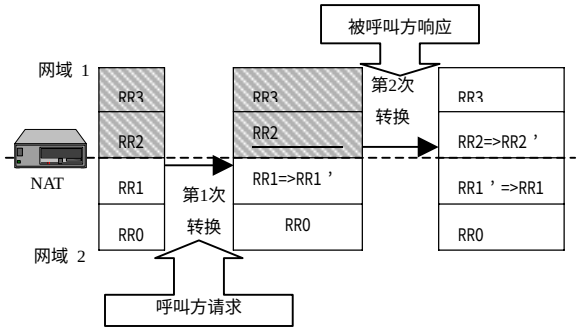

图 1 使用 Record-Route 栈设计分析替换算法

此外还应考虑特例：分界点前后仅有一个或无 Proxy 的情况。请求依然替换栈顶，对响应处理时分界点的判断则需调整。从呼叫方看，NAT 之前若仅有一个 Proxy(RR0 不存在)，且呼叫始于内网，则响应 Record-Route 栈中将无法发现分界点，但栈底地址为 NAT 分配地址，那么可确定分界点在栈底 RR1 与之后的 RR2 之间；若呼叫始于外网则判断法不变。若 NAT 之前未架设 Proxy(无 RR0、RR1)，呼叫来自内网，检查响应的 Record-Route 栈未发现内网地址或 NAT 分配地址，那么栈底必为内网地址，必须为其构造映射条目并替换；分界点在 NAT 之后的情况同理分析。每次至多处理一条 Record-Route 记录，剩下的 Record-Route 字段直接略过，以提高效率。图 2 是整理后的 Record-Route 头域处理流程。

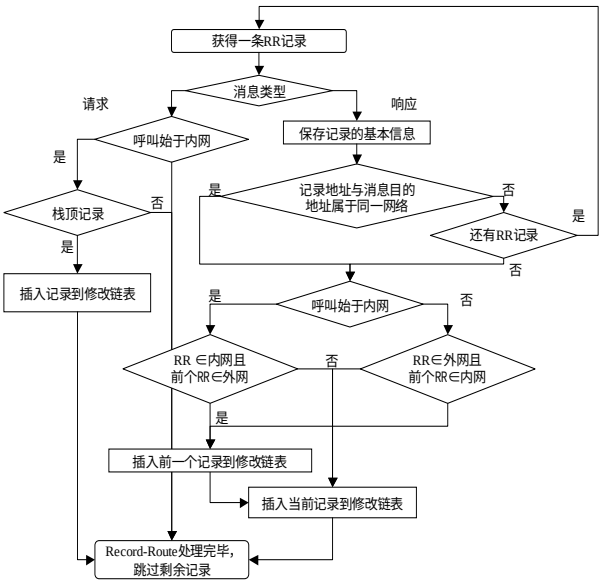

图 2 Record-Route 头域分析算法流程

按栈模式的思路，可构造 Via、Route 的转换逻辑，其处理简单得多，至多替换栈顶记录。分析中还发现，一次 SIP 会话最多生成两条 NAT 映射条目(分别用于 SIP、RTP)，因此消息中转换的头域地址，或源于现存 NAT 映射条目，或需新建映射条目，地址条目直接保存在 NAT 映射表中，避免了文

献[5]为每类头域耗费大量 NAT 存储空间的缺陷。

2 实验验证

为检验方案的透明性(也称完备性)，必须验证其对任何SIP拓扑，都无需SIP软件作任何修改、配置。为此需找出所有可能的SIP NAT拓扑环境。RFC3261[1]并未对SIP的拓扑做出任何规定，中间节点可任意部署，放入NAT环境将产生大量拓扑，不利完备性验证。因此采用约减法对所有拓扑进行归纳：两台UA通信时，若某中间节点的作用仅是在同一网域内的SIP路由，并不经过NAT，那么这些位于同一网域的Proxy就可视为一个Proxy节点。由此得到以下 5 类简化拓扑(见图3)。

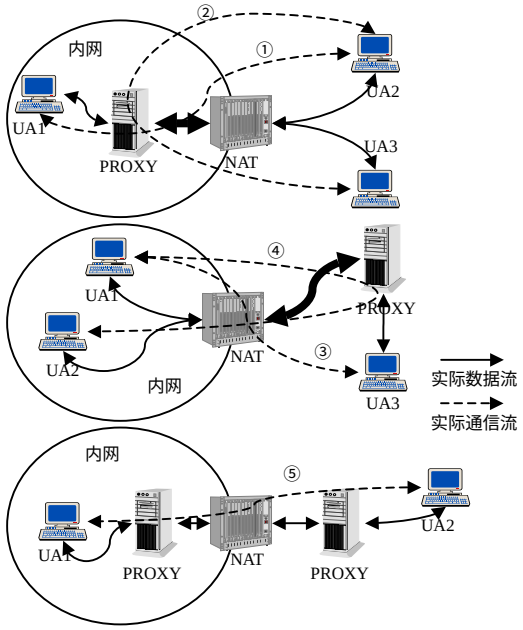

图 3 SIP NAT 的 5 种拓扑(圈中数字表示拓扑类型)

(1)拓扑中唯一的 Proxy 位于内网，分别处于内外网中的 UA1 与 UA2 通话；

(2)外网的 UA1、UA2 靠内网 Proxy 通话；

(3)Proxy 位于外网，分别处于内外网中的 UA1 与 UA2 通话；

(4)两台内网 UA 同时使用外网 Proxy 通话；

(5)两台 UA 分别位于内外网络，通过各自域内的 Proxy 通话；

以一个 SIP-ALG 模块，嵌入基于 IXP2400 的 IPv4-IPv6 互通网关，作为实验的研究对象。该网关已实现 IP 层、传输层及部分应用层协议，如 TCP、UDP、DNS 等的转换模块。实验中两台安装 Kphone-3.11 -ipv6(同时支持 Ipv4 与 Ipv6 的 SIP 客户端)的 PC 作 UA，服务器端安装 SER 与 BIND(SIP 必需的配套服务)，对照 5 类拓扑，测试 SIP 会话及其后音频通信情况，对于每类拓扑，还测试了任一方发起请求的情况。表 1 是实验结果，它证明了本文的 SIP NAT 方案的透明性。

表 1 透明性测试结果

测试项目	SIP 通信	音频通话	问题原因
拓扑 1	正常	正常	
拓扑 2	正常	正常	
拓扑 3	正常	正常	
拓扑 4	正常	正常	
拓扑 5	正常	正常,但若位于 IPv6 的 UA 发起邀请时，可能出现超时现象	DNS-ALG 解析域名超时，导致产生失败

3 总结与展望

本文从 SIP 头域的语义特点出发，以“栈模式”作为 SIP NAT 分析替换算法设计思路，实现了一种透明、高效的 SIP 穿透 NAT 方案。为证明透明性，还对 NAT 中 SIP 的所有可能拓扑进行归纳，提出 SIP 网络在 NAT 的 5 类拓扑模型，最后以实验结果验证该方案的透明性。虽然 SIP-ALG 是本文的实现手段，但其分析思想可用于各种 NAT 穿透技术中 SIP 分析算法的设计。

本文的方法虽降低了 NAT 存储要求，并简化了分析算法，但由于 SIP 属应用层协议，在语义分析所耗费的计算将不可避免地造成 NAT 效率下降，因此进一步提高 SIP 分析效率将是 SIP NAT 的研究重点。此外 NAT 本身的限制对 SIP 消息的安全提出了挑战，面对企业、个人大量安装的防火墙、设备，实现 SIP 的安全穿越也是目前的研究热点之一。

参考文献

1 Rosenberg J, Schulzrinne H, Schulzrinne G. SIP: Session Initiation Protocol[S]. RFC 3261, 2002.

2 Biggs B. A SIP Application Level Gateway for Network Address Translation[Z]. Internet Draft, 2000.

3 Rosenberg J, Weinberger J, Schulzrinne H. SIP Extensions for NAT Traversal[Z]. Internet Draft, 2001.

4 Martin M, Brunner M, Stiemerling M. SIP NSIS Interactions for NAT/Firewall Traversal[Z]. Internet Draft, 2004.

5 何永林, 林 浒. 一种 SIP NAT 应用网关的设计与实现[J]. 小型微型计算机系统, 2002, 23(8): 913-916.

（上接第 115 页）

参考文献

1 Poole C D, Wanger R A. Phenomenological Approach to Polarization Dispersion in Long Single Fibers[J]. Electronic Lett., 1986, 22(19): 1029-1030.

2 Sunnerud H, Karlaaon M, Andrekson P A, et al. Analytical Theory for PMD Compensation[J]. IEEE Photon Technology Lett., 2000, 12(1): 50-52.

3 叶会英, 常怡萍. 偏振模色散对波分复用系统性能影响的仿真分析[J]. 邮电技术设计, 2004, (9): 35-40.

4 刘秀敏, 杨伯君, 张晓光. 波分复用系统中偏振模色散特性的研究[J]. 中国激光, 2001, 28(12): 1103-1107.

5 陈 林, 张晓光, 张 茹等. 偏振模色散对多信道光纤通信系统信号的影响[J]. 光子学报, 2004, 33(4): 443-447.

6 杨红捷, 杨 名. PMD 对不同线路码型高速光纤通信系统影响的研究[J]. 光学与光电技术, 2003, 1(2): 6-9.

7 张慧剑, 左 萌, 孙学明. 40Gbps WDM 系统中 RZ&NRZ 调制格式的性能比较[J]. 线路传输技术, 2004, (12): 44-46.

8 胡辽林, 刘增基, 杨国庆. 40Gbps 非零色散位移光纤传输系统中四种调制格式的性能比较[J]. 光子学报, 2003, 32(10): 1181-1184.

9 Agrawal G P. 贾东方, 余震虹译. 非线性光纤光学原理及应用[M]. 北京: 电子工业出版社, 2002.