文章编号: 1001- 9081(2003) 02- 0120- 03

针对 SIP 的 ALG 解决方案及实现

罗 强[1], 许 鲁[1], 常致全[2]
(1. 中国科学院 计算技术研究所, 北京 100080; 2. 四川大学 计算机学院, 四川 成都 610064)

摘 要: SIP 是一个很有潜力的基于文本的应用层协议。由于 SIP 协议本身不能保证 SIP 信令能安全地穿过 NAT 和防火墙, 从而限制了其在现有广域网上的使用和发展。文中归纳了对该问题的解决方案, 重点介绍了 ALG 的解决方案, 并根据 SIP 的特点提出了 SIP ALG 的具体实现框架。

关键词: SIP 协议; 网络地址翻译; 应用级网关; 防火墙
中图分类号: TP393.08 文献标识码: A

Solution and Implementation of ALG Based on SIP

LUO Qiang[1], XU Lu[1], CHANG Zhi-quan[2]
(1 *Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *Computer College, Sichuan University, Chengdu Sichuan* 610064, *China*)

Abstract: SIP is a promising text-based application-layer protocol. It can't be used in NAT or firewall environment, which deeply cumbers its development on WAN. This paper proposes some relative ways to resolve the problem, mainly focuses on ALG and provides a detailed framework for SIP ALG.

Key words: session initiation protocol; network address translation; application level gateway; firewall

SIP(Session Initiation Protocol) 是一个应用层控制信令协议, 用于建立、更改和终止多媒体会话或呼叫, 其特点是简单、便于扩展和扩充, 而且 SIP 的概念与 Internet 的出发点一致, 借鉴了许多已有的 Internet 协议, 是实现增值综合业务的理想手段, 具有很好的发展潜力。针对 SIP 对 NAT 防火墙的局限性, 本文介绍了相关解决方案, 其中重点描述了 SIP ALG (Application Level Gateway) 及其实现。

对于 SIP ALG, B Biggs 在文献[2] 中对其实现做了一定分析, 对报文修改提出了一些建议, 但提出没有具体实现框架。本文根据 SIP 和 ALG 的具体特点, 进一步给出了一个 SIP ALG 的详细实现框架。

1 问题的提出

NAT(Network Address Translation, 网络地址翻译) 是一种将一个 IP 地址域映射到另一个 IP 地址域技术, 目前广泛用于私有地址域与公用地址域的转换以解决 IP 地址匮乏问题。NAT 可以分为 SNAT(Source NAT, 源网络地址翻译) 和 DNAT(Destination NAT, 目的网络地址翻译) 两种类型, 分别完成对向外的源地址和向内的目的地址的翻译。

SIP 主要借鉴了 HTTP 和 SMTP, 是一个基于文本的应用层协议, 会话建立的有关地址信息的描述信息在 SIP 消息内。当 NAT 存在时, 会导致 NAT 外和 NAT 内的用户之间无法从 SIP 消息中得到有效的地址信息, 无法完成正常的会话建立过程。

如图 1 所示, 以两个 UA(User Agent 用户代理) 间的直接呼叫建立 SIP 连接的简单情况为例, 当 NAT 内的客户 B 向 Internet 上的 SIP 客户 A 发送 INVITE 请求时, 请求的消息头为:

```
INVITE: UserA@159.226.39.2 SIP/2.0
Via: SIP/2.0/UDP 10.10.1.2:5060
……(略)
```

INVITE 消息的源 IP 地址在经过 NAT 后, 被翻译为 159.226.39.3:6000, 然而在 SIP 协议中, 这里的客户 A 不会按此地址返回 100(Trying) 回答, 而是按 Via 中的 10.10.1.2:5060 返回。由于这是个私有地址, 因此相应的回答不会被发送到 B 中去, 连接无法建立。

同样地, 对于 SIP 所控制的媒体流的传输, 有关的地址和参数信息的传送在 SIP 消息的 SDP 消息体内。因此, 除了消息本身, SIP 所控制的媒体流的传输也无法完成。

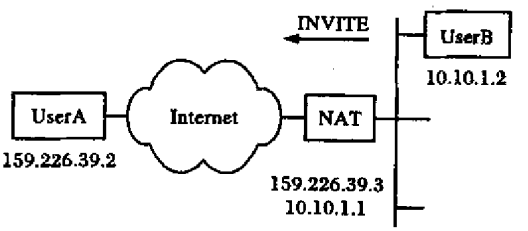

图 1 有 NAT 情况下的 SIP 连接

2 针对 NAT 的 SIP 解决方案

对于 SIP 穿越 NAT 的问题 RFC2543 中提出了一些解决方法, 定义了一些相关的头和参数, 例如专用来标识出消息中有私有地址的使用 Via 头域中的 Receiver-tagged 等。就目前所提出的对 NAT 的 SIP 解决方案来看, 主要集中在以下几个

收稿日期: 2002- 08- 12

作者简介: 罗强, (1975-), 男, 硕士研究生, 主要研究方向: 计算机网络及应用技术; 许鲁(1962-), 山东长青人, 男, 研究员, 主要研究方向: 操作系统、网络系统; 常致全(1947-), 男, 四川中江人, 副教授, 主要研究方向: 数据与信息系统.

方面:

1) RSIP 技术

RSIP (Real Specific IP)是 IETF NAT 工作组提出的一个新的协议, 用于解决 NAT 防火墙网络地址翻译带来的问题。RSIP 客户端位于内网, 但采用外网地址与外部主机发生联系建立端到端通信。任何一方发起呼叫所构造的呼叫建立控制信令包中所包含的地址都是外网中唯一的公有地址。采用 RSIP 协议后, 进行地址转换时不需要对控制数据包的内容进行解析和变换, 这样简化了地址变换的复杂度。

RSIP 等类似的技术的问题在于, 目前协议尚未成为标准。要求所有主机都能支持相关协议。因此, 这是一个很有前景的解决方案, 但对解决目前存在的问题不太实用。

2) SIP Proxy

另一种办法是对 SIP 系统作相应扩充, 具体如 Fredrik 在文献[6]中提出的使用 MGCP(media gateway control protocol, 媒体网关控制协议) , 来控制防火墙打开/关闭端口完成 NAT 的穿越。又例如使用 midcom[4] , 也就是使用一个用户代理或代理服务器来控制防火墙。这一类的解决方案实际上都是在现有的 SIP 系统之外构造一个 SIP proxy 来控制 NAT 和防火墙, proxy 根据 SIP 消息做相应的动作, 从而实现 NAT 的穿越。

这种解决方案可操作性较强, 同时也能较好地解决相应的问题, 但缺点是需要构造额外的服务器来实现系统的穿越, 此外同样需要增加对相关协议的支持, 代价较高。

3) SIP ALG

ALG 是解决 NAT 带来的局限问题的一个比较常用的手段。SIP ALG 内置于 NAT 网关上, 分析和修改进出 NAT 的 SIP 报文, 根据报文内容在 NAT 防火墙上打开相应的端口, 使相关 SIP 消息和媒体流能进入 NAT 内部。同时修改报文中的相关消息头和参数的值, 从而完成一个完整的 SIP 会话。

SIP ALG 最突出的特点是 ALG 和具体的 SIP 系统无关。NAT 外的 SIP 客户将不会知道 NAT 的存在, NAT 内的客户能自由地穿越 NAT 防火墙, 完成到 Internet 上的注册或 SIP 呼叫连接等。对于一个 SIP 系统不需要做任何修改, 只要在相应的 NAT 网关上加载 SIP ALG, 就能完成私有网络到公共 Internet 甚至私有网络之间的两个客户之间的 SIP 连接。

由上面的分析可以看出, 透明性和通用性是 ALG 相对于前面两种方案的最大优点。虽然在 NAT 防火墙上内置 ALG 会一定程度上降低 NAT 网关的效率, 但几种方法相比较, 我们仍认为 SIP ALG 是目前性价比最好的 NAT/ firewall 的 SIP 解决方案。

3　SIP ALG 的实现

从逻辑上看, 一个 SIP ALG 可以分成两个主要的部分, 一部分实现对向外报文的修改, 将对应私有地址修改为 NAT 网关上对应的 Internet 上的公共地址, 一部分控制 NAT 完成对向内的消息和相关媒体流的转发。ALG 通过这两个部分完成不同 NAT 间的 SIP 连接。因此, 一个基本的 SIP ALG 的实现框架应包括转发模块和消息修改模块两个模块的内容。

下面以一个典型的两个不同 NAT 内的客户通过 Register Server 完成连接的过程为例来说明 SIP ALG 的两个功能模块具体实现。本文主要讨论 SIP 以 UDP 实现时的情况。

如图 2 所示, User1 和 User2 分别位于不同的私有网络中, 在公共 Internet 上设置了注册服务器, User1 和 User2 的 NAT 防火墙上分别配置 SIP ALG。

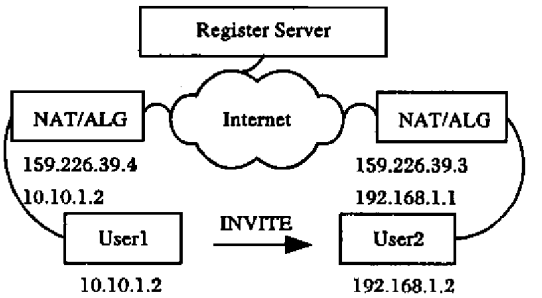

图 2　NAT 间通过 ALG 实现SIP连接

3.1　相关实现条件

RFC2543 中规定了 30 多个头, 但一个基本的 SIP 呼叫过程可以只包含其中的几个。比较重要的主要的几个头域为: Request-URI、Via、From、To、Call-ID、Cseq、Content-Type、Content-Length 和 Contact。大部分 SIP 系统提供的 UA 都支持这几个头, 这几个头中携带了会话过程中的基本地址信息, 通过它们基本上已经能完成一个较完整的 SIP 呼叫, 因此本文中 ALG 主要分析这几个头。

RFC2543 中对 SIP 请求(Request)定义了 INVITE、ACK、OPTIONS、BYE、CANCEL 和 REGISTER6 个方法。其中, INVITE、ACK、BYE 和 REGISTER 这几个方法基本上能完成一个相对完整的 SIP 呼叫建立过程。本文主要讨论这 4 个重要的方法的处理过程。

同样地, 协议中对 SIP 回答(Response)定义了相关的回答, 本文主要分析的几个和基本连接直接相关的状态码为 100(Trying), 180(Ringing), 200(OK)。

3.2　对消息和媒体流转发模块的实现

ALG 的一个重要的功能就是在 NAT 防火墙上打开相应端口, 完成对相应的 SIP 消息和媒体流向 NAT 内的转发, 即实现相应的 DNAT 的功能。转发模块在 ALG 中建立并维护一个地址映射信息表来记录相关的地址映射信息。消息修改模块通过该表来确定对经过 ALG 的报文的具体修改。

表 1　地址映射信息表

User	Source IP	Sport	Destination IP	Dport
User1	10.10.1.2	5060	159.226.39.4	6000
		.....		

上表中的数据表示所有目的地址为 159.226.39.4:6000 的 SIP 包都会被 NAT 网关转发到主机 10.10.1.2:5060 上处理。消息修改模块在作修改前, 要首先查询 ALG 内记录的地址映射信息表, 如果表内已经建立了该用户的信息, 则按此信息对向 NAT 外的 SIP 消息做相应的修改, 否则丢弃该消息。

为了生成相关地址映射信息表, ALG 首先需要分析向外的 SIP 消息, 主要分析其中的 REGISTER 消息。ALG 记录 REGISTER 中的 To 和 Contact 头域, 按它们的值在 NAT 防火墙上打开一个未用端口, 然后 ALG 记录生成的映射信息并填入地址映射信息表。生成地址映射信息表后, 消息修改模块再按映射信息修改向外的 INVITE 和 REGISTER 等报文, 使后面向内的 SIP 消息能进入 NAT 内部。

此外, 对 SIP 控制的向内的媒体流的转发, ALG 分析向

外的 INVITE 和 200(OK) 消息的 SDP 消息体中“m=”和“c=”行,对应这两行中描述地址在 NAT 防火墙上打开未用端口,完成向内接收媒体流的目的地址翻译,从而实现媒体流通信的建立。

ALG 记录会话状态,当 SIP 呼叫结束后,ALG 关闭媒体流 DNAT 端口。当用户取消注册后,关闭 SIP 消息 DNAT 端口,删除记录的对应地址映射信息。在具体实现上,DNAT 的实现会因不同的 NAT 实现类型而有所不同。

3.3 对消息的修改模块的实现

ALG 对 SIP 消息的修改,在转发模块完成 DNAT 并填写地址映射信息表后,NAT 内 SIP 消息向外通过 ALG 时发生。ALG 先查询地址映射信息表的有关的映射信息,然后按地址映射信息对 SIP 消息做相应的修改。对消息的修改具体地可以分为下面几种情况,以图中的 INVITE 请求为例:

1) 对 Via 头域的修改

Via 记录请求所通过的路径。

Via: SIP/2.0/UDP 10.10.1.2:5060

改为:Via: SIP/2.0/UDP 159.226.39.4:6000

其中,地址 159.226.39.4:6000 由地址映射信息表得到。User1 发出的 INVITE, ACK, BYE 和 REGISTER4 个请求消息和 100(Trying), 180(Ringing) 以及 200(OK) 3 个回答的 Via 头在向外穿越 NAT 时都需要进行相似的修改。

2) 对 Contact 头域的修改

Contact 通常标明能到达用户的下一个 URL,和注册、重定向等密切相关。

Contact: <sip: User1@10.10.1.2:5060>

改为:Contact: <sip: User1@159.226.39.4:6000>

对 User1 和 User2 的 REGISTER 中的 Contact 头,ALG 同样要做和上面 INVITE 相同的修改。

3) 对 SDP 消息体的修改

SDP 消息体中描述了和会话及相关媒体特性的有关内容。其中,在 SDP 消息体中和连接直接相关的几个比较重要的域是:

“Connection c=”,描述主机地址。

“Media m=”,在这里主要关心的是参数中接收媒体流端口的信息。

图 2 中 NAT 内主机 User1 发出的 INVITE 请求的 SDP 消息体内相应的部分如下所示:

c= IN IP4 10.10.1.2

m= audio 49172 RTP/AVP 0

SDP 消息体中的这两行被 ALG 修改为:

c= IN IP4 159.226.39.4

m= audio 60012 RTP/AVP 0

其中,“c=”行中的主机地址由私有地址改为 NAT 网关地址,“m=”行中的 60012 表示在该端口上接收到的媒体流在 DNAT 后将被转发到 User1。User2 中返回的 200(OK) 的 SDP 消息体中的相应部分同样要完成相似的修改。

4) Content-Length 头的修改

由于经过 ALG 后 SIP 消息体被修改,消息体的长度发生了变化,因此 User1 的 INVITE 和 User2 中返回的 200(OK) 消息头中的 Content-Length 都要做相应的修改。

综上所述,ALG 的具体转发和报文修改处理流程如下:

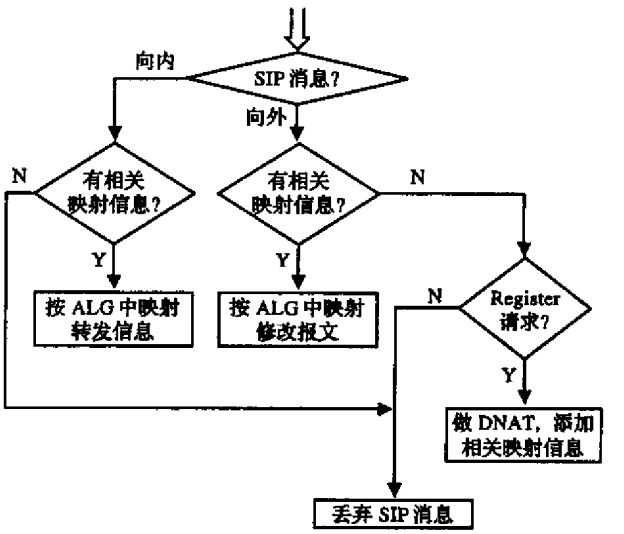

图 3 ALG 的处理流程

需要强调的是,在这种 NAT 间的 SIP 客户连接建立的情况下,要求在公共 Internet 上必须有 Register Server 来完成对 NAT 内客户的注册和重定向。图 2 中的 Register Server 逻辑上实际上集成了 SIP 协议中的 Location, Registration 和 Redirect 三个逻辑服务器的功能。

另外,Proxy Server 是 SIP 协议定义的一个重要的服务器,主要负责 SIP 消息的转发。在 NAT 网关上配置了 Proxy Server 时,上面处理流程中消息修改模块的内容应加以修改。此时通过 NAT 内外的消息都由 Proxy Server 转发,ALG 只需要对 SDP 消息体中对媒体流描述的部分进行修改,消息头部分不需再改动。这样就使 ALG 完全地对 SIP 系统透明。

此外,本文的 ALG 以连接为重点,没有考虑 SIP 的安全和认证等内容。

4 结语

本文描述了不同 NAT 间的 SIP 客户通过 Register Server 建立 SIP 连接的 ALG 实现。通过内置于 NAT 上的 ALG 映射 IP 地址,修改报文以及完成转发,不需要修改 SIP 或添加其它协议,NAT 间的客户就可以实现透明地建立 SIP 会话。在此框架上的消息修改模块部分略加扩充,就可以支持相关的 4XX, 5XX 等 SIP 消息,从而实现功能相对更加完善的 SIP ALG。

参考文献

[1] Handley M, Schulzrinne H, Schooler E, *et al*. SIP: session initiation protocol[S]. RFC 2543, Internet Engineering Task Force, March 1999.

[2] Biggs B. A SIP Application Level Gateway for Network Address Translation[S]. Internet Draft, Internet Engineering Task Force, March 2000.

[3] Srisuresh P, Kuthan J, Rosenberg J. Middlebox communication architecture and framework[S]. Internet Draft, Internet Engineering Task Force, Feb. 2001.

[4] Rosenberg J, Weinberger J, Schulzrinne H. SIP Extensions for NAT Traversal[S]. Internet Draft, Internet Engineering Task Force, November 21, 2001.

[5] Themelius F. SIP Firewall Solution[S]. Internet Draft, Internet Engineering Task Force, July 2000.