文章编号: 1007- 2985(2006)06- 0077- 03

基于软交换与 Media Portal 的私网穿越方案

王融丽, 梁平原, 杨 喜
(吉首大学物理科学与信息工程学院, 湖南 吉首 416000)

摘 要: 介绍了用于解决软交换系统中的网络地址翻译穿越问题的几种技术, 分析它们各自的适用范围、适用对象和存在的缺陷, 提出了一种新的基于软交换与 Media Portal 配合的私网穿越方案.

关键词: 下一代网络; 网络地址翻译; VOIP; SIP 协议
中图分类号: TN911 文献标识码: A

下一代网络(Next Generation Network, NGN)以软交换为核心, 能够提供话音、视频、数据等多媒体综合业务, 采用了开放、标准体系结构, 能够提供丰富业务的下一代网络, 它的出现标志着新一代电信网络时代的到来. NGN 从传统的以电路交换为主的 PSTN 网络中逐渐迈向以分组交换为主的 PSTN 网络, 把大量的数据传输卸载到 IP 网络中以减轻 PSTN 网络的重荷, IP 技术的新特性增强了许多新老业务. 从这个意义上讲, NGN 是基于 TDM 的 PSTN 语音网络和 IP ATM 的分组网络融合的产物, 使得在新一代网络上语音、视频、数据等综合业务成为了可能.

网络地址翻译(Network Address Translation, NAT)技术解决日益枯竭的 IPV4 的地址资源, 隐藏企业私网内部的拓扑结构, 能保障一定程度的安全性[1]. 大量的基于 NAT 标准的内部网络的部署, 使得如何在 NAT 环境下成功的部署 VOIP 网络已成为在下一代网络领域研究方向.

1 NAT 对 NGN 私网用户 VOIP 应用的影响

以基于会话发起协议(Session Initiation Protocol, SIP)的 VOIP 应用为例进行分析, 基于 SIP 的呼叫可以分成 2 个部分: SIP 信令流和 RTP RTCP 语音媒体流. 信令流主要是为终端间的呼叫建立进行协商, 用户 Marry 想同 Bob 通信, Marry 首先要向软交换发送 SIP 请求, 软交换检查 Bob 状态, 如果 Bob 状态为待机, 那么软交换向 Bob 发送 SIP 请求. 在 Bob 向 Marry 发送连接确认消息之后, RTP 语音流才开始传输.

SIP 可以周期性的向软交换发送注册信息, 这样就可以使 NAT 设备为该 SIP 终端分配的公网地址映射保持不变, 这样私网的 SIP 终端就可以拥有不变的公网地址, 所以 NAT 设备对于信令流没有任何影响, SIP 本身就有穿越 NAT 设备的能力. 但对于 RTP 媒体语音流, 在 SIP INVITE 消息的会话描述协议(Session Description Protocol, SDP)消息中, 私网终端会将自己的私网地址写入, 作为主叫方的源地址, 在被叫方收到 INVITE 之后, 该地址被提取作为 RTP 媒体流的目的地址. 而这个地址为私网地址, 在公网中无法路由, 这样呼叫可以被建立, 但是没有语音流. 假设私网用户 Marry 在 NAT 设备下, Marry 向公网用户 Bob 发送呼叫请求, Bob 接受到的 SIP INVITE 消息如下:

001 INVITE sip: 12125551212@211.123.66.222 SIP 2.0
002 Via: SIP 2.0 UDP 211.123.66.223:5060; branch= a71b6d57- 507c77f2
003 Via: SIP 2.0 UDP 10.0.0.1:5060; received= 202.123.211.25; rport= 12345
004 From: < sip: 2125551000@211.123.66.223> ; tag= 108bcd14

收稿日期: 2006- 09- 23
作者简介: 王融丽(1982-), 女, 湖北荆门人, 吉首大学物理科学与信息工程学院助教, 硕士, 主要从事通信网中软交换技术研究.

005 To: sip: 12125551212@211.123.66.222
006 Contact: sip: 2125551000@10.0.0.1
007 Call-ID: 4c88fd1e-62bb-4abf-b620-a75659435b76@10.3.19.6
008 CSeq: 703141 INVITE
009 Content-Length: 138
010 Content-Type: application sdp
011 User-Agent: HearMe SoftPHONE
012
013 v=0
014 o=deltathree 0 0 IN IP4 10.0.0.1
015 s=deltathree
016 c=IN IP4 10.0.0.1
017 t=0 0
018 m=audio 8000 RTP AVP 4
019 a=ptime:90
020 a=x-ssrc:00aea3c0

SIP INVITE 消息中的第3行注明了该消息是从 Marry 的私网地址 10.0.0.1:5060 发送出来,并告诉 Bob 将反馈信息发往 202.123.211.25:12345 即是 Marry 在 NAT 上分配的公网地址.第16行和第18行注明了 RTP 媒体流的接收地址为 10.0.0.1:8000.这个地址为私网地址,所以语音流无法被接收.

2 现有的 VOIP 私网穿越解决方案

2.1 ALG(Application Layer Gateway)

一般NAT 设备仅仅修改UDP 或TCP 报文头部地址信息,对应用层消息中的地址却只是透传.对于大多数端到端业务,例如视频业务、会议业务等都是通过应用层中的地址信息携带连接信息,由于 NAT 设备的特性,造成该类业务在通过 NAT 设备时不能够被支持.[2-4] 为了解决这个问题,提出了应用层网关的概念.ALG 一般驻留在 NAT Firewall 中.当消息经过该设备时,设备除了修改 UDP 或 TCP 报文头部信息外,还会将应用层中的地址信息改成在 NAT 上对外的地址.

该方案的特点:(1) ALG 不能识别加密后的消息内容,所以必须保证明文传送消息;(2) 现在大量的NAT FW 不具备 ALG 能力,需要更换或升级;(3) 由于业务需要,而对 SIP 消息扩展时,可能需要对 ALG 进行相应升级.

2.2 STUN(Simple Traversal of UDP Through NATs)

STUN 方式就是 UDP 对 NAT 的简单穿越方式.由于 NAT 设备只对 UDP 的报文地址进行修改,因此在此种方案中,私网接入用户在发起呼叫前,需要预先通过某种机制得到其地址对应在出口NAT 上的对外地址,然后将应用层消息中的地址填上出口NAT 的对外地址.因此,当 SIP 消息经过 NAT 设备时,此时的 UDP 报文地址和 SIP 消息中的地址都将是 NAT 设备对外的地址.

该方案的特点:(1) 不需要对 NAT FW 设备做任何修改;(2) 需要 SIP 终端支持 STUN CLIENT 功能;(3) 不支持 TCP 协议;(4) 不适应对称式NAT.

2.3 MIDCOM

MIDCOM(Middle Box COMmunication) 技术现在仍然处于开发和完善阶段,一直被业界认为是 NAT 防火墙穿越的终极方案.该方案引入了一个可信任实体 Middle Box,该实体可以根据应用需求动态开启关闭 NAT、防火墙设备,从而达到NAT、防火墙的穿越.此方案的优势可将 NAT 和应用分离,对于不同应用可以与 NAT 防火墙存在不同的控制关系,因此扩展性强.但由于MIDCOM 仍然处于完善阶段,没有标准化,所以现在业界几乎没有这方面的产品.

3 RTP Media Portal 解决方案

RTP Media Portal 是专门针对 NAT、防火墙穿越的,它受软交换控制分别与主叫方和被叫方建立连接,并在 RTP Media Portal 内部进行 RTP 流的桥接,从而在不对现有 NAT 设备进行任何改动的前提下实现 NAT 穿越.

RTP Media Portal 方案对 NAT FW 的穿越分为呼叫信令对 NAT FW 的穿越和 RTP 流对 NAT FW 的穿越两方面.该方案来实现NAT FW 的穿越有以下特点:(1) 在 NAT FW 穿越过程中,由软交换来处理信令,RTP Portal 专门用作实现媒体的通道,完全实现了信令和媒体的处理相分离;(2) 对 NAT FW 没有任何特殊要求;(3) RTP Media Portal 还将用作不同运营商 NGN 网络之间互通的桥接设备,实现对本网的安全保护和媒体转换等功能.

3.1 信令对 NAT FW 的穿越

当呼叫双方中的任何一方在 NAT FW 的后面时, 终端与软交换的信令交互通路上将存在 NAT FW 的穿越问题:

(1) 对信令的处理由软交换完成而不引入其他设备来进行 NAT FW 穿越处理.

(2) IAD、IP Phone 的注册消息在 NAT FW 上产生私网和公网 IP 地址和端口的动态绑定.

(3) 从 IAD Phone 周期性地发出 Keep-Alive 消息保证维持 NAT FW 上的动态绑定, 使得信令通道畅通.

3.2 RTP 媒体对 NAT FW 的穿越

首先, 软交换系统将根据呼叫双方的信息判断是否需要引入 Media Portal 来完成对 NAT FW 的穿越:

(1) 同一个私网域内的用户将处在同一个 NAT FW 后面, 相互之间 IP 可达, 所以同一私网域内的用户之间的呼叫不需要引入 RTP Portal 来对 NAT FW 进行穿越.

(2) 当系统判断主叫方和被叫方之间存在 NAT FW 而使相互的 IP 地址不可达的时候, NGN 系统将启动 RTP Portal 来完成对 NAT FW 的穿越. 在以下场合中主叫方和被叫方之间存在 NAT FW 而使相互的 IP 地址不可达: 当企业内部 IP 电话用户和 PSTN 用户之间进行呼叫; 当不同的企业私网内的 IP 电话用户之间进行呼叫; 当 NAT FW 后面的个人用户终端与 NAT FW 外面的用户之间进行呼叫.

其次, 当系统判断需要进行 NAT FW 穿越的时候, 将通过软交换控制相应的 Media Portal, 启动相应的 NAT FW 机制, 将针对每一个需要穿越 NAT FW 的呼叫进行分别控制.

(1) 从 NAT FW 后面发往 RTP Portal 的 RTP 媒体流将在呼叫期间在 NAT FW 上生成 IP 地址和端口动态绑定.

(2) 从 IAD Phone 周期性的发出 Keep-Alive 消息保持维护 NAT FW 上的动态绑定.

(3) RTP Portal 在软交换的控制下将针对每一个需要穿越 NAT FW 的呼叫在 RTP Portal 上建立一个通道, 保证媒体流通过该通道, 在主被叫之间传送, 对 2 个通话端点的 IP 地址进行映射, 允许话务流在 2 个私网域之间通信; 对公网和私网中的 IP 地址进行映射, 允许私网用户能够通过运营商管理的中继网关如 PVG 来和 PSTN 网络用户互通; 呼叫结束时解除绑定.

4　结语

目前主流软交换制造商在解决私网穿越的问题上有各种不同的处理方法, ALG 方案简单, 但影响路由器性能, 不适合大规模部署; STUN 先进且适合各种协议, 但天生不支持防火墙和 Symmetric NAT; MIDCOM 是业界方向, 但还不成熟, 有待完善. 笔者提出的 RTP Media Portal 方案真正地解决了电信网的 VOIP 私网穿越难题, 很好地满足了运营商的各种需求.

参考文献:

[1] STEVEN M BELLOVIN. Problem Areas for IP Security Protocols [J]. AT & T Research, 1996, (5): 22- 25.

[2] 严　军. NGN 网络业务 NAT 穿越技术探讨 [J]. 通信世界, 2003, (12): 31- 32.

[3] 徐静华, 左冬红, 潘　鹏, 等. 多进程 VOIP 网关中 SIP 穿越 NAT 的实现 [J]. 计算机工程, 2006, (1): 145- 147.

[4] 杨　怡, 陶　军. 基于 NAT-PT 和 PROXY 的 HTTP 过渡方案的研究与改进 [J]. 计算机工程与应用, 2006, (4): 149- 151.

A Private Network Traversing Solution Based on Softswitch and Media Portal

WANG Rong-li, LIANG Ping-yuan, YANG Xi

(College of Physics and Information Engineering, Jishou University, Jishou 416000, Hunan China)

Abstract: Some technologies to resolve network address translation traversal problem in next generation network system are introduced. Through discussing those technologies available field, available object and limitation, a new solution based on coordination of Softswitch and Media Portal is presented.

Key words: next generation network; network address translation; VOIP; SIP protocol

(责任编辑　陈炳权)