NGN业务穿越NAT/FW的解决方案

吴 伟
(中国电信集团公司 100032)

摘 要 主要探讨了NGN软终端和IAD的NAT问题,介绍了ALG、MidCom、STUN、协议修改、Proxy等几种私网穿越方法,并分析了方案的可行性和适用性。

关键词 NGN 软终端 IAD NAT私网穿越

1 引言

目前NGN(软交换)技术已逐步从试验走向商用,在应用过程中遇到了很多实际问题,特别是NGN用户的接入问题。NGN是一个基于分组网承载的网络,用户接入都是通过IP地址来寻址的。由于IP地址紧缺以及安全等各种原因,所以大量的企业网和驻地网都采用私有IP地址通过出口的NAT/FW接入公网。

NGN网络最大的好处就是能为用户提供丰富的业务,特别是为企业用户提供语音、数据、视频融合的IP Centrex业务,但是像H.323、SIP、MGCP、H.248等在IP上承载语音和视频的协议的控制通道/媒体通道难以穿越传统的NAT/FW 设备与公网进行互通,或者说目前的NAT/FW大多只是支持HTTP的数据应用协议穿透,而无法支持这种会话型业务的控制与媒体的NAT/FW穿透,因此私网穿越问题的解决显得更加迫切,成为目前NGN网络业务开展的最大障碍。目前,解决这一问题的主要方案有ALG、STUN、MidCom和Proxy等。

聚层的压力,例如:

(1) 加强用户管理

接入层交换机可利用流量控制、地址数量限制等功能对互联网用户、VPN用户的流量和用户数进行控制,尽可能减轻网络的负担,防止非法用户接入。在上层发现可疑数据时,可利用端口镜像功能实现对数据的采样分析,进行迅速的定位和处理,保证上层网络的稳定性。

(2) 分布式PE功能

接入层交换机和汇聚层VPN PE设备之间可利用VLAN技术建立用户汇聚通道,VPN用户通过接入交换机与PE设备通信。接入交换机完成对VPN用户的汇聚,并通过VLAN ID区分用户,以减少PE设备端口的占用,从而实现VPN业务的扩展。

(3) 基于802.1p划分服务等级

接入层交换机在上行端口可对用户进行基于802.1p CoS的业务等级划分,从而为汇聚层设备提供初步的服务等级依据,以减轻汇聚层的工作压力。

4 经济欠发达地区的特殊考虑

当然,中国现阶段还存在一些经济发展相对较缓慢的地区,这些地区目前还不具备在城域网核心层和汇聚层大量部署路由器的能力和条件。另一方面,这些地区的用户数和业务量相对较少,网络负载较轻,因此可以考虑仍采用三层交换机来组建城域网的核心层和汇聚层。

用于核心层的交换机应具有高速路由转发能力,并支持10GE以太网端口及多GE端口绑定功能,以提供充足的骨干链路带宽,并通过轻载来保证服务质量;同时必须加强对网络的监控,一旦发现设备资源消耗过大的情况,能够及时采取措施加以分析和解决。在汇聚层交换机的选择上,仍应以设备的业务提供能力作为主要衡量指标,以配合运营商全国范围业务的开展。建议在汇聚层部署部分路由器,以提供对3G、NGN等实时语音业务和金牌大客户的接入和承载。

2 穿越技术介绍

2.1 ALG方案

NAT和NAPT只能对IP报文的头部地址和TCP/UDP头部的端口信息进行转换，对于报文的数据部分可能包含IP地址或端口信息的特殊协议（如H.323、SIP、MGCP等），则无法实现有效的转换，这就可能导致问题发生。例如，一个使用内部IP地址的FTP服务器可能在和外网主机建立会话的过程中需要将自己的IP地址发送给对方，而这个地址信息是放在IP报文的数据部分，NAT无法对它进行转换，当外网主机接收到这个私有地址并使用它，这时FTP服务器将表现为不可达。

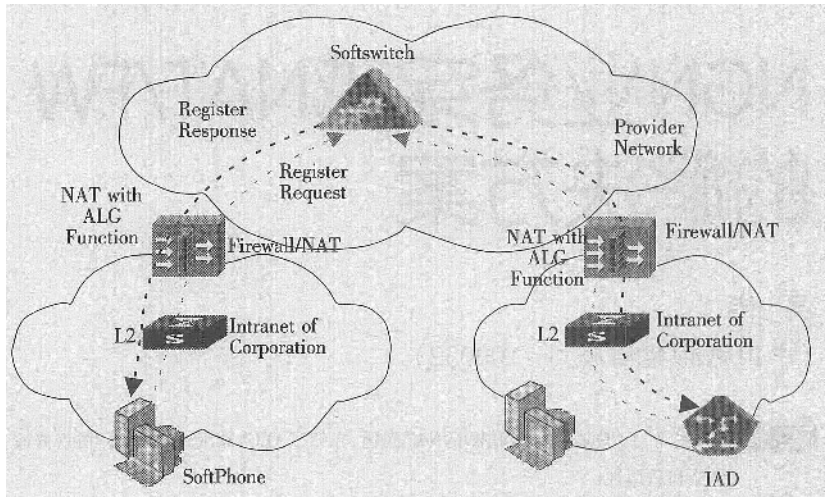

图1 ALG组网示意

解决这些特殊协议的NAT转换问题的一个方法就是在NAT实现中采用ALG（Application Level Gateway，应用级网关）功能。ALG是能够识别指定IP协议（如H.323、SIP或MGCP）的设备。它通过与NAT交互以建立状态，使用NAT的状态信息来改变封装在IP报文数据部分中的特定数据，并完成其他必需的工作以使应用协议可以跨越不同范围运行。例如，一个“目的站点不可达”的ICMP报文，该报文数据部分包含了造成错误的数据报A的首部（注意，NAT在发送A之前进行了地址转换，所以源地址不是内部主机的真实地址）。如果开启了ICMP ALG功能，在NAT转发ICMP报文之前，它将与NAT交互，打开ICMP报文并转换其数据部分的报文A首部的地址，使这些地址表现为内部主机的确切地址形式，并完成其他一些必需工作后，由NAT将这个ICMP报文转发出去。

ALG可以是单独的连接于外网和内网之间的设备，也可以是内置于NAT内的插件。ALG典型的组网方式如图1所示。

ALG是支持NGN应用最简单的方式，但由于目前网络中已大量部署了不支持NGN业务应用的NAT/FW设备，因此不推荐采用这种方式，理由如下：

（1）目前网上大量的NAT/FW设备因不具备ALG能力而需要更换或升级；

（2）NGN业务的ALG生产厂商少，没有一套产品特性需求基线；

（3）NAT/FW设备厂商一般不是IP业务领域的专业厂商，难以支持业务的变化（如SIP的扩展多种多样）；

（4）用户普遍希望运营商在不改变已有网络设备（NAT）的情况下就可以提供新的IP业务，用户不愿意重新购买NAT/FW设备，更无法判断各种ALG的可行性。

2.2 MidCom方案

MidCom（Middlebox Communications）方案是通过在第三方实体和FW/NAT之间建立中间盒来通信，使FW/NAT设备变为可控的一种新的概念。如图2所示，MidCom包括MidCom Agent和Middlebox，Agent通过MidCom协议通知Middlebox建立相应的NAT映射表项。

一般情况下，Middlebox集成在NAT或FW设备

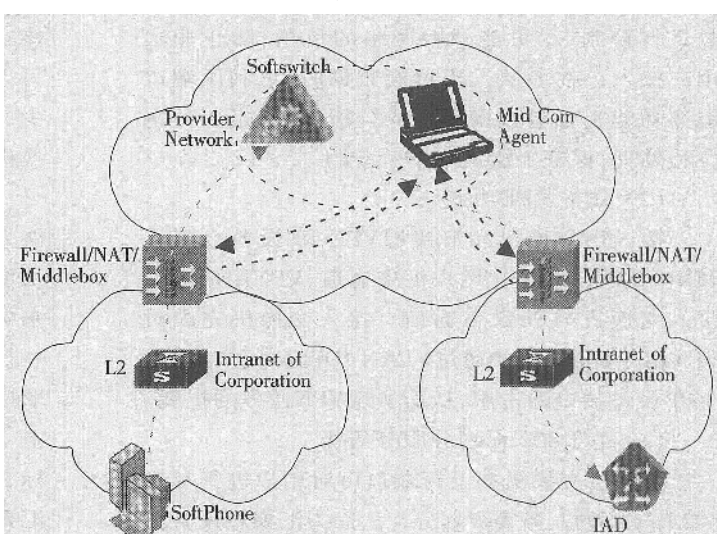

图2 MidCom方式组网示意

中，Agent可在软交换、代理服务器或终端上实现。

由于应用业务识别的智能从Middlebox移到外部的MidCom Agent上，因此，根据MidCom的架构，在不需要更改Middlebox基本特性的基础上，通过对MidCom Agent的升级就可以支持更多的新业务。这是相对于NAT/ALG方式的一个很大的优势。

从安全性考虑，MidCom方式支持控制报文和媒体流的加密，因此安全性比较高。

2.3 协议修改

由于目前的多媒体应用协议无法穿越NAT/FW，因此可以考虑通过修改协议以适应NAT/FW。

对于H.323，SIP，MGCP，H.248等协议，为支持NAT/FW穿越而做的修改尚未形成标准，还在起步研究阶段，因此本文不做详细探讨。

2.4 STUN方案

STUN（Simple Traversal of UDP Through NATs）是由IETF研制的一种UDP流协议穿透NAT的协议。如图3所示，位于内部网络的STUN client（NAT内）通过UDP发送请求STUN消息给外部网络的STUN Server（NAT外），STUN Server收到请求消息后产生响应消息（响应消息中携带请求消息的源端口，即STUN Client在NAT上对应的外部端口），响应消息通过NAT发送给STUN Client，STUN Client通过响应消息体中的内容得知其在NAT上对应的外部地址，然后将该地址填入以后的呼叫协议的UDP负载中，并且告知对端，本端的RTP接收地址和端口号为NAT外的地址和端口号。由于通过STUN协议已在NAT上预先建立媒体流的NAT映射表项，因此媒体流可顺利穿越NAT。

需要注意的是，终端设备需要集成STUN Client功能，STUN Server可以集成在相应的应用所属的部件上（如在NGN应用中可以集成到SoftSwtich上）或者是由独立的设备提供。

STUN协议最大的优点是无需现有NAT/FW设备做任何改动。目前，网络中已有大量的NAT/FW，而且这些NAT/FW并不支持VoIP应用。如果采用MidCom或NAT/ALG方式，则需要替换现有的NAT/FW，实施起来难度较大，且MidCom方式无法实现对多级NAT的有效控制。如果采用STUN方式，不但无需改动NAT/FW，而且能够很好地适应多个NAT串联的网络环境。

但STUN也有以下几个方面的局限性：

（1）需要应用程序支持STUN Client的功能，即NGN的网络终端需具备STUN Client功能；

（2）STUN不支持TCP连接的穿越，也就表示不支持H.323协议；

（3）STUN方案不支持NGN业务对FW的穿越，不能穿越对称NAT（Symmetric NAT）类型（在安全性要求较高的企业网中，出口NAT通常就是采用这种类型）。

2.5 Proxy方案

Proxy方案是指通过对私网内用户呼叫的信令和媒体同时做Relay来实现出口NAT/FW的穿越。对于NGN网络的私网穿越问题，目前业界已基本倾向Proxy方式，并且在Proxy方案中还增加了网络安全、防止终端漫游等特性。

Proxy设备是在原来网络结构的基础上，采用网络叠加方式，部署在IP网络的边缘或汇聚层，是会话信令和媒体的聚合点。信令Proxy与媒体Proxy可以在一个设备上实现，也可以分离实现，当在同一个设备上实现时称为Full Proxy。NGN终端通过Proxy设备连接到软交换上，如图4所示。

在网络中，信令Proxy和媒体Proxy各自担负着不同的工作。

（1）信令Proxy：Proxy设备对NGN用户而言，可看作是软交换系统，即用户的注册和呼叫消息

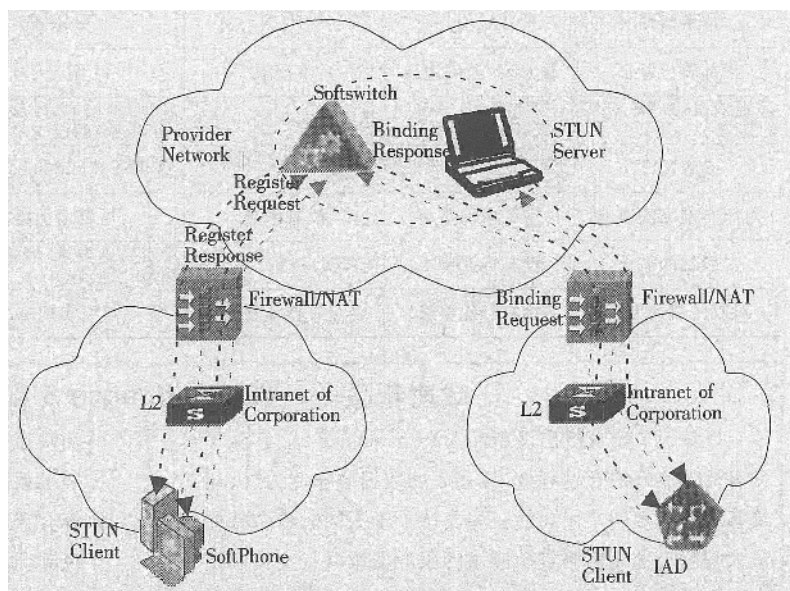

图3 STUN方式组网示意

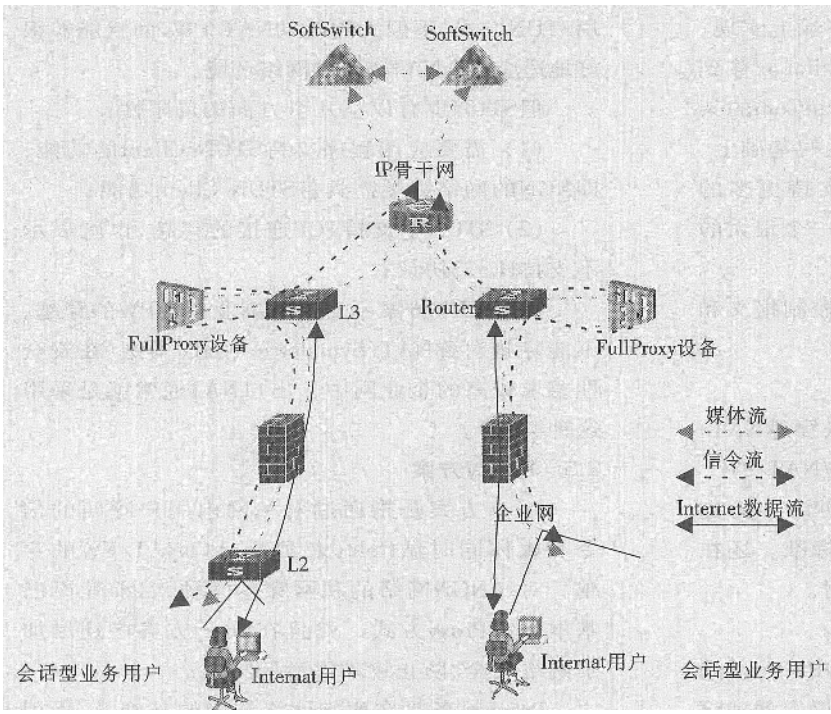

图4 Proxy组网示意

都会发给Proxy设备，Proxy设备经过信令处理后再转发给软交换系统。同时，Proxy设备对软交换系统又可看作是用户，软交换系统首先将呼叫被叫的请求发给Proxy设备，Proxy设备经过信令处理后再转发给真正的被叫用户。Proxy设备通过对信令进行处理和分析，得到本次会话的地址变换状况、带宽需求等信息，并根据当前网络资源占用情况等信息来决定媒体流是否通过Full Proxy设备网关，从而起到网络保护、防止带宽盗用等作用。

（2）媒体Proxy：Proxy设备是媒体流的必经之处，所有域内用户与外界互通的媒体流都经过Proxy设备进行处理和转发。Proxy设备网关首先检查报文的合法性，并根据信令处理结果来制定媒体流转发策略（如FW、QoS和地址转换策略），通过指定内网/外网用户RTP流的接收地址和端口这种方式来确保无论采用何种组网方案，媒体流都能得到正确转发和严格的QoS保证、安全控制。

Full Proxy方式由于不用对运营商和客户端的现有网络设备进行任何改造，具有很强的适应性，组网灵活，可满足NGN初期多样化的组网和用户接入。除了解决NAT问题外，功能还可以大大扩展，同时可在接入层实现对会话业务QoS和安全的处理，可以发展成为NGN网络的用户接入平台。

3 方案的简单对比

上述几种穿越技术的简单对比见表1。

表1 穿越技术对比

技术类型	ALG	STUN	MidCom	协议修改	Proxy
部署位置	在私网/公网边缘	不受限	不受限	不受限	不受限
对现有NAT/FW设备的需求	需要替换或升级为具备ALG的设备	不支持对称NAT方式	需要替换或升级为具备Middlebox的设备	不需要修改	不需要修改
多级NAT	每一级的NAT都需支持ALG	每一级的NAT都不能是对称NAT	需要支持Middlebox或ALG	支持	支持
对原有网络的影响	需要增加路由	没有影响	需要增加路由	没有影响	没有影响
对终端的需求	没有特殊要求	需要实现STUN客户端	没有特殊要求（考虑Agent在Server上实现）	需要修改协议	终端收发端口应一致
对服务器的需求	没有特殊要求	没有特殊要求	需要实现Agent	需要修改协议	没有特殊要求