SIP应用层网关探讨及设计

■ 广州大学松田学院：郑昌波　张汉杰　陈小亮　刘翠芳

摘　要：基于SIP协议构建的网络如智能家居在进行私网和公网间通信时，由于SIP协议由于本身具有的特点，导致了基于SIP构建的私网穿透NAT/FW的难题。通过分析SIP协议特点，本文提出利用“应用层网关（ALG）”方法来实现SIP网络穿透NAT/FW，文中详细的介绍了SIP应用层网关的原理和实现方法，并利用SIP应用层网关技术实现SIP对NAT/Firewall的穿越。

关键词：会话初始化协议；私网；公网；应用层网关
中图分类号：TP393.08　　文献标识码：B

DISCUSSING AND DESIGN OF SIP ALG

ZHENG Chang-bo[1], ZHANG Han-jie[1], CHEN Xiao-liang1, LIU Cui-fang1

(1.Guangzhou University SonTan College, Guangzhou, China 511370)

Abstract: It's hard for the network based on SIP like digtal home network to pass NAT/FireWall, this paper has analyze the characteristic of SIP, it's give the method "Application Layer Gateway (ALG)" based on SIP to pass NAT/Firewall. This paper discussing and analyzing the ALG, and accomplish it at last.

Key words: SIP; private network; public network; ALG

引言

SIP（Session Initiation Protocol)称为会话初始协议[1][4]，是一个与HTTP和SMTP类似的、基于文本的协议，SIP独立于传输层协议和其它会话控制协议，可以与其他协议（如RSVP，RTSP等）一起构建多媒体通信系统如智能家居网络、视频会议[2]等。

NAT/防火墙（FW）为私网提供统一的对外出口，从而隐藏内部网络的拓扑结构，提高了私网的安全性[3]。但这也给私网的远程控制应用带来很大的麻烦。对于NAT，其功能是在公网IP地址及端口和私网IP地址及端口间进行映射，工作在传输层，它只对TCP/UDP包头中的地址、端口进行修改，而SIP协议需要在信令消息中内嵌IP地址和端口号[5]，这些地址、端口在应用层上才可见，因此NAT不会对其中的地址信息进行修改，导致信令消息中的IP地址和端口不能指向正确的地址，因而通信也不能正常进行；对于FW，对公网打开的端口通常是固定的(Fw不会在运行过程中动态的打开或者关闭这些端口)，且数目有限。而基于SIP构建的私网的远程控制应用要求FW不但能够提供对信令协议的代理功能，而且要求FW能够在通信过程中动态的打开一些端口进行媒体流数据的交流，现有的FW难以满足这个要求。

鉴于上述原因，本文提出了“SIP应用层网关”技术，并将其应用于网络通信中来建立相对合理、完善的SIP网络，以解决SIP私网远程控制中穿越NAT/FireWall的难题。

SIP私网穿越NAT/防火墙方法分析

由于所有NAT和Firewall都是对于TCP/IP层以下进行处理和过滤的，而SIP是应用层控制信令协议，SIP与下面的传输层和网络层协议无关。所以必须采用其他的途径来解决基于SIP的私网穿越NAT/防火墙这一问题，主要有以下不同的解决方案：1.UpnP（通用即插即用）；2.TURN(Traversal Using Relay NAT)；3.STUN(Simple Traversal of UDP Through network Address Translators)；4.ALG(Application Layer Gateway，应用层网关)。

其中前3种都是由SIP Client(包括UA和Proxy)通过某种手段或协议在INVITE之前获取自己的公网地址和端口。需要SIP Client提供额外支持，并且也不适应所有的NAT方式。ALG(Application Layer Gateway)[2]适应所有NAT方式，并不需要SIP Client做任何额外的支持。它对Application层的SIP信令进行处理和修改，从而做到透明转换地址。该思想的基本思路是通过在NAT/FW中加入协议认知(Protocol Awareness)能力，使NAT/FW能够在SIP信令消息通过时修改其内容中的地址信息，ALG修改SIP消息里面的SIP地址和端口，并为分配给呼叫双方的地址和端口进行绑定，这样，以后的媒体流数据能够通过NAT/FW指定的端口穿过。本文主要讨论的是基于SIP的应用层网关方法。

SIP应用层网关原理分析

“ SIP应用层网关 ”是为解决基于SIP的私网控制应用穿越NAT/FW的问题，实现私网内的SIP用户代理与公网上的SIP用户代理之间的互连而提出的解决方案，从功能上来说，SIP应用层网关是一种为私网内的SIP终端提供连接到公网的代理功能的SIP设备或软件。下文中提及的“ 应用层网关 ”和ALG(Application Level Gateway)都是指SIP应用层网关。

为了实现SIP应用层网关的功能，同时保持与已有SIP应用的兼容性，必须把ALG设计成一个SIP兼容的应用。但是对于私网上和公网上的SIP应用而言，ALG提供的功能并不完全相同：对于私网的SIP终端，SIP应用层网关的角色是一个SIP意义上的代理服务器(Proxy)，它不但需要为通往公网上的呼叫提供代理，同时还需要为私网内部不同SIP终端之间的呼叫提供代理；另一方面ALG必须允许私网内部SIP终端进行注册，因为只有通过注册才能使SIP终端明白ALG是它们的代理服务器，因此，SIP应用层网关同时也是私网上的SIP注册服务器。而对于公网上的SIP终端而言，私网内部是不可见的，唯一可见的是处于公网上的SIP应用层网关，因此对它而言，ALG只是一个SIP终端，公网上的SIP设备就能够直接对它进行呼叫或者接收它的呼叫。

综上所述，SIP应用层网关功能在私网和公网上是非对称的，可划分为：1.对内功能：SIP应用层网关是私网上的SIP注册服务器和代理服务器，同时，对于跨网呼叫的情况，SIP应用层网关除需为私网终端提供SIP消息的代理，还须提供媒体流数据的代理，这种媒体数据的代理功能对通信双方是透明的；对外功能：在公网上，SIP应用层网关作为一个普通的SIP终端而存在，它能够与公网上的其它SIP应用建立互连关系，并隐藏ALG与私网内部SIP应用之间的关系。

SIP应用层网关的实现

本节前面部分详细的介绍了SIP应用层网关实现的理论基础，本节介绍ALG的软件实现方式，软件开发平台是Windows2000，开发工具是Visua1C++ 6.0，采用的是OSIP协议栈，开发的语言主要是C。

结构及工作流程

图1是SIP应用层网关的结构框图，从图中可以看到，按照各部分功能上的差异，可以将ALG划分成“ 信息数据库接口 ”、“ 基于SOCKET的消息接收与应答 ”、“ 媒体会话 ”、“ 信息管理 ”和“ SIP消息处理及对话维护 ”五个模块。

这里ALG被分成两个部分：ALG主体部分和SIP URI信息管理系统部分，这两部分被设计成是两个相互独立的程序。ALG主体部分的功能是处理各种流向上的SIP消息、管理呼叫环境以及跨网络呼叫时，在通信双方之间进行RTP数据包的转发；SIP URI信息管理系统部分的功能是负责私网内部SIP URI及其绑定信息的管理和维护，该系统及其维护的数据库放置在私网内部的其它主机上运行。两部分之间通过UDP/TCP进行通信，这样可以减小来自外网上攻击的风险，从而提高数据信息的安全性。 由于ALG主体无法直接对SIPURI的数据信息进行访问，因此必须在这两部分之间提供访问的接口，“ 信息数据库接口 ”模块就是为 ALG访问SIP URI信息管理系统的接口。

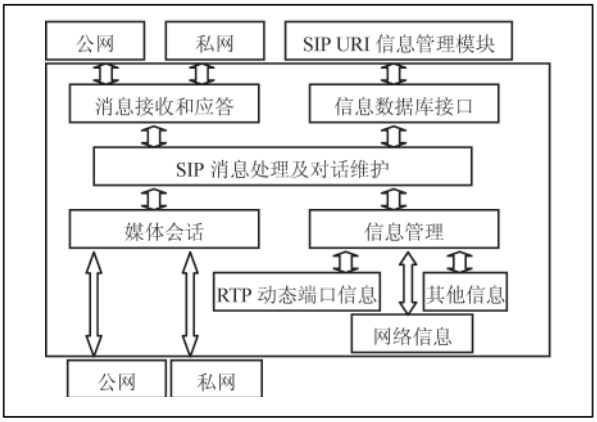

图1: SIP应用层网关的结构框图

SIP应用层网关的主要工作由一个SIP消息的监听线程、一个与SIP URI信息管理系统进行通信的线程、一个SIP消息处理线程(包括对话的管理和维护)和数量不定的RTP数据包转发线程完成。RTP数据包转发线程能够根据需要而动态的生成和释放，因此数量不定。

SIP应用层网关的基本工作流程如下：

应用程序初始化完毕以后，启动SIP消息监听线程、URI信息数据库访问线程和SIP消息处理线程。SIP消息监听线程对ALG的所有SIP端口(包括私网和公网)进行监听，如果收到SIP消息，它把消息连同其源IP地址和端口以及消息本身的长度封装成一个简单的数据结构放入一个先入先出的队列(FIFO)当中，然后继续监听，它不对消息进行进一步的处理。

一旦FIFO中有了SIP消息，SIP消息处理线程就被唤醒，并投入运行，它从FIFO中取走消息，然后开始对这个消息进行处理：首先它对消息进行解析以及例行的语法检查，然后根据SIP消息的源地址和目的地址将其分成四类：

（1）内部消息，其源地址和目的地址都在私网内部。

（2）对外消息，其源地址是私网地址，目的地址是公网地址。

（3）对内消息，其源地址是公网地址，目的地址是ALG的公网地址。

（4）外部消息，其源地址和目的地址都是公网地址。

SIP消息被分成以上四类后，ALG对它们进行不同的处理。第(1)类消息称为“内部消息”，第(2)类和第(3)类消息统称为“跨网络消息”；第(4)类消息称为“外部消息”，它会被无条件丢弃，ALG不对其作进一步的处理。SIP消息处理线程在对“跨网络消息”消息进行处理的同时，对呼叫的上下文环境进行管理和维护，并在必要的时候，启动新的RTP数据包转发线程，使其完成对跨网络通信的RTP数据包的转发工作。

基于SOCKET消息接收与应答功能模块

由于UDP包的接收是异步的，ALG无法预测何时会有SIP消息到来，因此在SIP应用层网关的设计中，用单独的线程对SIP端口进行监听。由于SIP应用层网关处在两个网络的边界上，并在两网之间转发数据，因此ALG的SIP端口也相应的分为私网和公网两部分，在任何一边的网络上，都可以打开一个或者多个与套节字(SOCKET)相联系的SIP端口。并且每隔一定时间试图从所有监听的SIP端口相关联的SOCKET上读取数据，如果读到了数据，就对数据做简单的封装，然后把它放入应用层网关的SIP消息FIFO当中。

信息数据库接口模块

出于安全性的考虑，SIP URI信息管理系统从SIP应用层网关中分离出去，这个系统的功能并不复杂，一方面它接受来自ALG的访问；另一方面，它必须对自身的信息数据库进行维护。ALG本身必须通过信息数据库接口模块对其进行访问。

ALG需要从SIP URI信息管理系统得到的信息有两类：一类是用户信息，包括用户名和密码；另一类是SIP URI绑定信息，这一类信息的交互是双向的，不同的REGISTER请求会要求ALG添加、修改、删除或者仅仅是获取SIP URI的绑定信息。本文用统一的数据结构来表示这两类信息，这样只需要一次访问就能够获取所需全部信息，可以缩短ALG处理SIP消息所需的时间。

信息管理模块

SIP应用层网关需要很多信息才能完成工作，有些信息是动态的，例如SIP URI的绑定信息，不同用户不同时间的绑定信息是不同的，因此只有在需要的时候应用层网关才从数据库中进行动态的访问；而另外一些信息则是相对稳定的，如ALG本身的域名、IP地址等等。这些信息很多，但并不复杂，大多是字符串、数值或者布尔型的变量，信息管理模块的功能就是维护和管理它们。

“媒体会话”模块

当SIP应用层网关为跨网络呼叫的终端之间建立起媒体会话(视频、音频)的连接后，双方之间主要的交互将是RTP数据流(媒体数据被打包成RTP数据包)的交互，“媒体会话”模块的功能主要就是在通信双方之间进行RTP数据包的转发工作，每一个RTP数据包转发器能够为多路RTP连接提供数据包转发服务。

当ALG需要为一路RTP连接提供数据包转发服务时，它试图从转发器环境中得到一个空闲的RTP数据包转发器，如果环境中的转发器都已经被占用，环境会试图创建一个新的RTP数据包转发器，并把它加入到环境当中，并将它返回给ALG使用。另一方面，当一个转发器不再为任何RTP连接提供转发服务时，环境会把它删除，并释放相应的资源。

“消息处理及对话维护”模块

这是SIP应用层网关的核心模块，它的功能是对收到的SIP消息进行解析和处理，完成对SIP消息的代理，对跨网络呼叫的上下文环境进行维护以及在必要时启动对话的RTP代理。这些功能之间是相互关联的，统一由SIP消息处理及对话的维护线程完成。图2是SIP消息处理线程的工作流程图。

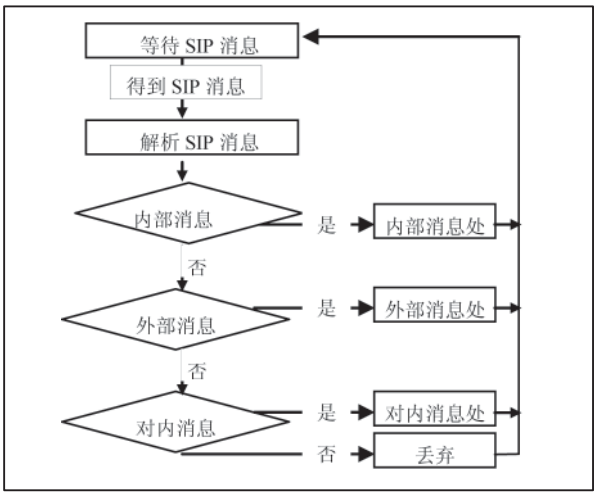

图2：SIP消息处理线程的工作流程图

本文小节

SIP协议凭借其简单、易于扩展、便于实现等诸多优点越来越得到业界的青睐，越来越多的基于SIP协议的网络如VOIP、视频会议、智能家居系统被开发实现，本文实现的SIP应用层网关正是SIP网络对NAT/Firewall的穿越的关键技术，但这一方案仍存在着不足之处，由于SIP应用层网关必须对跨网络的所有SIP消息进行解析，导致这些消息须以明码的形式传输，降低了SIP应用的安全性，进一步研究表明：这要求我们对SIP协议进行适当扩展来实现信息的加密。

本文创新点：综合分析了基于SIP的网络如何穿越公网私网技术，提出并实现了基于SIP协议的ALG方法。

参考文献

[1] 储泰山，基于SIP的服务器的研究与实现[D]，浙江大学硕士学位论文，2004.3。

[2] 叶德谦，基于SIP集中式多媒体视频会议系统中对私下会议问题的研究[J]，微计算机信息 2006.1-3 P78-79、P268。

[3] William R.Cheswick,Steven M.Bellovin 著，罗万伯译．防火墙与因特网安全[M],戴宗坤．北京：机械工业出版社，2002.31-39。

[4] Garcia-Martin M, Henrikson E, Mills D. Private header (P-Header) extensions to the session initiation protocol (SIP) for the 3rd-generation partnership project (3GPP)[S]. Internet RFC3455, 2003.

[5] Arkko J, Torvinen V, Camarillo G, Niemi A, Haukka T. Security mechanism agreement for the session initiation protocol (SIP)[S]. Internet RFC 3329, 2003.

作者简介：郑昌波（1977－），男，湖北松滋人，广州市广州大学松田学院讲师，硕士（毕业于武汉大学），主要研究方向：多媒体通信与传输技术。

联系人：郑昌波

广州大学松田学院电子系，邮编：511370 ，电话：020-35579011； E-mail: zcbqxy2004@21cn.com

新闻

飞兆半导体的 HDMITM 多媒体开关获厦华电子选用于其最新型的 LCD TV 中

飞兆半导体公司 (Fairchild Semiconductor) 的FSHDMI04高分辨率多媒体接口(HDMI) 开关获厦华电子公司 (XOCECO) 选用于其新型的42英寸LCD TV (型号LC-42FY27) 中。厦华电子作为主要的消费电子产品跨国制造商和出口商，选择了FSHDMI04来实现其业界领先的保护功能、高带宽及低功耗特性；加上飞兆半导体提供的HDMI预测试支持，使到厦华电子的TV产品轻易取得HDMI认证，而这正是他们选用飞兆半导体产品的另一个重要原因。

当用于带有双接口的媒体系统时，FSHDMI04 HDMI开关能够连接至两个其它的视频源，如DVD、游戏总台及机顶盒等。通过在单个器件中提供HDMI功能，设计人员可利用FSHDMI04在现有应用的电路中方便地添加第二个HDMI输入，而无需昂贵的升级费用。与那些需要独立接收器添加HDMI连接的传统设计相比，FSHDMI104能降低设计的复杂性而大幅缩短了设计时间。