IPv4/IPv6 网间的 SIP 通信的解决方案*)

李献礼
(长江师范学院网络中心　重庆 408003)

摘　要　在分析 SIP 协议和的 IPv4/IPv6 转换机制的基础上，提出了一种应用层网关与 NAPT-PT 相结合的解决方案并且实现了在不改动终端和原有设备的情况下实现了异类网之间 SIP 通信。

关键词　SIP，IPv6，NAPT-PT，ALG

A Solution for SIP Communication between IPv6 and LPv4

LI Xian-Li
(Network Center, Yangtze Normal University, Chongqing 408003)

Abstract　After analyzing SIP messages and several common mechanisms of translating between IPv4 and IPv6, then a solution based on the cooperation of SIP_ALG and NAT-PT is proposed. At last communications based on SIP in the heterogeneous network without changing application programs on client hosts is inplemented.

Keywords　SIP, IPv6, NAPT-PT, ALG

1　引言

SIP 协议是下一代网络多媒体通信的信令协议。协议提出时只考虑了 IPv4 的网络环境。面对 IPv4 地址分配越来越紧张的局面，IETF 提出新的协议规范：IPv6。与此同时，SIP 的应用也在迅速地发展着。SIP 最大的特点是充分利用已定义的头域，对其进行简单必要的扩充就能很方便地支持各项新业务和智能业务，有利于与 Internet 的各项应用集成开发增值业务。在 IPv6 将要逐步代替 IPv4 的过程中，网络环境的变化必然会对上层的应用协议产生影响。因此，SIP 是否能够顺利穿越异类网，是它未来发展中不可忽略的问题。

1.1　SIP 协议[1,2]概述

总体来说，SIP 协议支持多媒体通信中以下几个方面的功能：

(1)用户定位：确定通信中终端的位置；

(2)用户可用性：确定被叫方是否愿意参与通信；

(3)性能协商：确定通信中所用媒体及媒体参数；

(4)会话建立：呼叫双方会话参数的建立；

(5)会话管理：包括会话转移和中止、会话参数变更、调用新业务等内容。

SIP 协议是一个客户服务器协议，用于发起和管理用户间的会话。SIP 终端系统称为用户代理(UA)，含用户代理客户机(UAC)和用户代理服务器(UAS)两部分。中间单元称为代理服务器。它的消息分为两大类：从客户端到服务器的请求(Request)和从服务器到客户端的响应(Response)。无论请求消息还是响应消息都是由起始行(Start-Line)、消息头部(Message-Header)和可选的消息体(Message-Body)构成。

SIP 协议支持 3 种呼叫方式：用户代理客户机(UAC)向对方用户代理服务器(UAS)直接呼叫；由代理服务器代表用户代理向客户服务器发起代理呼叫；由用户代理客户机在重定向服务器的辅助下进行重定向呼叫。呼叫方式 2 需要代理服务器转发用户的呼叫信令，因而加大了信息处理量。为了有效地将网络设备的压力推向网络边缘，呼叫信令 3 只指明目的地的方向，不保留每一呼叫状态，从而为组建大规模的 IP 网奠定基础。

1.2　使用 IPv6 后的变化

SIP 使用 IPv6 的一个显著原因就是有巨大的可用地址。尤其在 3G 系统中，基于 SIP 的 IP 电话需要数量巨大的 IP 地址，这在 IPv4 网络中是无法满足要求的，NAT 技术虽然可以在一定程度上满足 IP 地址的要求，但增加了网络结构的复杂度，并且使信令穿越 NAT 网关的过程变得困难。尤其是在终端的地址自动配置和负载平衡方面矛盾更为突出。

2　动态地址配置

IPv6 地址配置可以分为手动地址配置和自动地址配置 2 种方式。自动地址配置方式又可以分为无状态地址自动配置和有状态地址自动配置 2 种。在无状态地址自动配置方式下，网络接口接收路由器宣告的全局地址前缀，再结合接口 ID 得到一个可聚集全局单播地址。在有状态地址自动配置的方式下，主要采用动态主机配置协议(DHCP)，需要配备专门的 DHCP 服务器，网络接口通过客户机/服务器模式从 DHCP 服务器处得到地址配置信息。

3　任播

任播[3]是 IPv6 的一种专用的通信模型。与组播不同的是，共享组播地址的所有节点都将收到发给该地址的包，而共享任播地址的所有节点最终将只有一个节点收到发给该地址的包。发给任播地址的包，总是发送到具有该地址并按照选路协议测得距离为最近的节点。任播地址是从单播地址空间分配出来的，可用任何一种规定的单播地址格式，当一个单播地址被分配给多个接口时，该单播地址就转化为任意点播地址。对于任何已分配的任播地址，有一个最长的地址前缀用于标识一个拓扑地区，所有属于该任播地址的接口均位于该地区内。当一个用户开始通信会话时，他将会发送 SIP

*)基金项目：重庆市教委科学研究项目(项目合同号：KJ071306)。**李献礼**　副教授，研究方向：计算机网络应用，下一代网络。

包到注册服务器或是外部 SIP 代理。注册服务器和外部 SIP 代理服务器可以在 UA 中手动设置。更灵活的方式是使用任播功能对所有代理设置同样的任播地址。这样消息可以直接发到最近的实体。当有超过一个用户注册时，由于基于负载平衡机制的路由选择原因，UA 可以发送注册信息到注册服务器的任播地址，在矢量路由最近的注册服务器注册。这样不但简化了 UA 的配置，而且使各节点自动实现负载平衡，这对于有较大通信量的多媒体通信来说，是一个巨大的优势。

经过了多年的发展，IPv4 已经遍布到了世界的各个角落。如果要将整个网络完全变为 IPv6 的，需要更换数量巨大的终端设备、路由器和服务器。这一庞大的工程不会在短期内完成，IPv4 和 IPv6 的混合环境必将在相当长的一段时间内存在。在这种混合网络条件下的通信会有如下几种结构：

(1)双协议栈

即同时运行 IPv4 和 IPv6 两套协议栈，同时支持两套协议。在网络中同时运行 IPv4 和 IPv6 两套路由协议，终端系统可以接收发送 IPv4，IPv6 数据包，使用 IPv4，IPv6 地址。当收到一个带 IPv4 地址的数据包时，终端系统会将数据包回复到该 IPv4 地址去。收到一个 IPv6 数据包时也同样。一个 DNS 查询到一条 AAAA 记录返回 IPv6 地址，若没有找到 AAAA 记录，则将寻找 A 记录返回 IPv4 映射 IPv6 地址。双协议栈主机将从返回结果列表中选择最佳地址作为目的地址。当返回的是纯 IPv6 地址时使用 IPv6，返回的是 IPv4 映射 IPv6 地址时使用 IPv4，这一过程由双栈传输协议控制。

(2)隧道技术

当 2 个 IPv6 的“岛”通过一个 IPv4 的网络相连接时要用到隧道技术。在隧道的两端是运行双协议栈的路由器，分别连接 IPv4 和 IPv6 网络。当 IPv6 的数据包到达隧道一端时会被封装为 IPv4 数据包通过 IPv4 网络。到达隧道的出口时，该封装包会被解封装，还原 IPv6 数据包发往原目的地址。隧道技术提高了网络的复杂性，增大了管理难度。

(3)协议转换[5](NAT-PT)

这种结构要求在 IPv4 和 IPv6 网络之间设立网关。网关的功能就是协议地址转换网关管理一张 IPv4 和 IPv6 的地址表，当 IPv4 接口收到要进入 IPv6 网络的数据包，网关将用 IPv6 地址头替换原来的 IPv4 地址头。它能较好地解决 IPv4 和 IPv6 的互通问题，其最大优点是原有的各种协议不加改动就能与新的协议互通。但该技术在应用上有一些限制：首先在拓扑结构上要求一次会话中所有报文的转换都在同一个路由器上，因此地址/协议转换方法较适用于只有一个路由器出口的 STUB 网络(存根网络)；其次，一些协议字段在转换时不能完全保持原有的含义。

4 系统结构

该项目采用 NAPT-PT 和应用层网关(ALG)合作的机制，完成对纯 IPv4 站点和纯 IPv6 站点之间的 SIP 消息包和多媒体数据的传送。为了接收和发送两种 IP 消息包，系统所在主机应支持 IPv4 和 IPv6 两种协议。当纯 IPv6 站点发送的 SIP 消息包到达该网关时，NAPT-PT(地址管理器)为发送站点匹配临时 IPv4 地址，同时 ALG 改写 SIP 消息包的 IP 地址，使消息包符合纯 IPv4 接收站点的语法和语义标准。这样，终端应用程序不做任何修改就可以跟异类网中的所有用户通信。按照功能划分，整个系统由呼叫监视器、消息修改器、地址管理器和流量监视器组成。系统结构如图 1 所示。

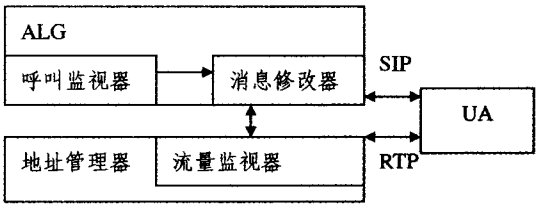

图 1 系统结构

呼叫监视器用于监督呼叫流程是否遵守 SIP 的标准。因此，它需要每个会话的当前状态和 SIP 呼叫状态机。消息修改器是系统的重点所在。它为呼叫双方匹配多媒体数据通信的地址和端口，将 SIP 消息包中的 IP 地址替换成系统匹配的临时地址，并将那些与路由有关的原始数据记录在 SIP_NAT 表中。改写后的消息包记录着 ALG 的地址信息，这使得 ALG 接续呼叫如同自己发起或响应 SIP 消息。地址管理器有两个主要功能：匹配 IP 地址和管理呼叫双方的多媒体数据传送通道，流量监视器主要用来防止 RTP 攻击。攻击者通常发送超大的 RTP 包或者多个具有相同 RTP 序号的包，造成网络阻塞。我们利用消息修改器读取呼叫双方设定的多媒体数据传输带宽(Bandwidth)。在多媒体通道建立时，该记录被送到流量监视器。如果某个通道的传输速率超过预先的设置，系统将判断这是 RTP 攻击，从而及时采取应对措施。另外，当某个通道在一定时间间隔内没有收到多媒体流时，流量监视器会通知消息修改器，以判断该会话是否需要关闭。

本项目选择 NAT-PT 模式，这样对于终端设备来说会比较简单，只需要支持一种网络模式。其模式如图 2。

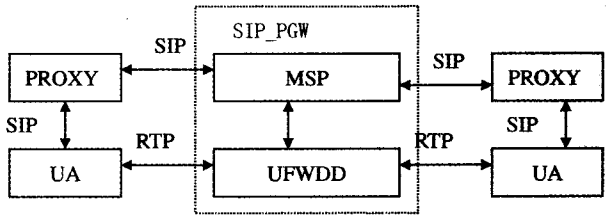

图 2 NAT-PT 模式

图 2 中的 PGW 是 SIP 协议转换器(SIP Protocol Gateway)，位于 IPv4 网络和 IPv6 网络的边界。PGW 运行双协议栈，可以看作是一个代理，把从一方收到的 IPv4/IPv6 数据包转发到另一端的 IPv6/IPv4 主机。

SIP PGW[6,7]包括 3 个部分：

(1) MSP(Mini SIP proxy)

MSP 接收 SIP 消息，经过修改以后，建立 RTP 连接的 UDP 映射将 SIP 消息转发到其他代理处。每个 MSP 必定有 2 个相连接的外部代理：一个位于 IPv4 网，一个位于 IPv6 网。MSP 本身并不具备路由功能。对于一个来自 IPv4 端口的 SIP 请求信息只会被简单的转发到 IPv6 端口，反之亦然。SIP 响应消息的路由由 VIA 字段头来定义。只有以下几种 SIP 消息字段会被修改：

①Contact 字段 Contact 字段给出一个 URI，在 SIP_PGW 中原 Contact 字段会被修改为有对应的原地址映射的连接地址(real_uri 实 URI 参量)。在随后发送的请求(如 BYE) 会按这个修改后的 Contact 字段发送。即 SIPPGW 会增加一个 real_uri 参量。

②Request URI 这种修改只在请求 URI 中有一个实 URI 参量时使用，real_uri 会被原 URI 代替。

③SDP headers 字段 位于消息体中的：

originato r (o=)

contact (c=)

media_description (=)

这些与 IP 地址或端口联系的字段必须被修改得与目标协议簇一致。这些地址包括在发送到 UFWDD 的映射请求的 SDP 部分。

④ Content_length 当一个消息体(SDP) 被修改后，包长也要重新计算。

⑤VIA VIA 头会插入到请求消息，从响应消息里删除。

(2) UFWDD (UDP 域转发)

这个功能实体管理 IPv4 和 IPv6 地址空间，进行网络地址翻译。从 IPv4/IPv6 收到的数据包使用由网关管理的 IPv6/IPv4 地址表分配的 IPv6/IPv4 地址转发给相应的 IPv6/IPv4 主机。接收到的 UDP 包请求格式如下：

MAPPED 0.0.0.0：0 0.0.0.0：0

[：：]：0[3ffe：3ff：1be0：273：3e0e：1bcf：0ace：86ab]：10003 2

这里有 5 个字段参量：源地址/端口，入地址/端口，出地址/端口，目标地址/端口，相邻端口数。UFWDD 用“MAPPED”格式回答源映射请求：

MAPPED 0.0.0.0：0 210.41.35.199：70001

[3ffe：4ff：1be0：273：18d0：6568：a9bc：1f00]：7005

[3ffe：3ff：1be0：273：3e0e：1bcf：0ace：86ab]：10003 2

在这个例子中，UFWDD 从 210.41.35.199：70001 收到数据包，属于 IPv4 地址/端口，将这个数据包通过 IPv6 输出地址/端口[3ffe：3ff：1be0：273：3e0e：1bcf：0ace：86ab]：10003 转发到 IPv6 目标地址[3ffe：4ff：1be0：273：18d0：6568：a9bc：1f00]：7005，并忽略被请求的源地址/端口。为了使接收到的目标地址返回的数据包可达，同时还要建立一张反向映射表，这样，从出地址收到的来自目标地址的数据包就可以通过入地址发到源地址。只有当来自源地址的第一个数据包被接受后，反向映射表才会被建立。

(3) 控制协议

为了请求分配地址，在协议簇间映射都通过 UDP 进行。这就允许不同结构下的组件相互通信。在图 1 中，除了网关还有 SIP 代理。每个代理都表示了混合 I 网络中一边的 SIP 服务提供商。例如，一个 SIP 服务提供商如 iporg，一个来自 IPv4/IPv6 网络的请求，目的为 iporg 的用户，会被定向到 IPv4/IPv6 网络中的 iporg 代理，当代理在呼叫发起的网络(如 IPv4) 中时，不能确定用户位置，将会向网关转发请求，在经过修改转换之后，会再次转发到位于 IPv6 网络中的 iporg 代理，这些功能模块被统一放置于 SIP_PGW 中。当然，这样的结构无疑会增加网关的复杂性和网关的负载，尤其在处理大量的 SIP 消息和可能执行的诸如 CPL 一类的服务时，或是类似的翻译和路由数据之外服务。但是这样的结构可以使网关的生产商独立提供信令与媒体数据包的转接设备，减轻 SIP 服务商的压力，使他们专注于处理媒体业务，而不必考虑网络间的接口问题。

结束语 本文提出了一种有效连接 IPv4 和 IPv6 网络之间的通信方法。这种解决方案是基于用户域的，而不是核心域，可以有更高的执行效率，但是需要 2 个 SIP 代理，这增加了管理的开销。下一步我们将代理服务器和网关融合，使用更底层的 NAT-PT 进行 IP 头的转换，以取得更高的效率。

参 考 文 献

1 Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol. RFC3261, IETF, 2002-06

2 Holdrege M, Srisuresh P. Protocol Complications with the IP Network Address Translator (NAT). RFC3027, 2001-01

3 Deering S, Hinden R. Internet Protocol (Version 6). RFC 2460, IETF, 1998-10

4 Handley M, Jacobson V. SDP: Session Description Protocol. RFC2327, 1998-04

5 Gilligan R E. Nordmark: Transition Mechanisms for IPv6 Hosts and Routers. RFC2893, 2000-08

6 RFC3303: Middlebox communication architecture and framework

7 RFC2824: Call processing language framework and requirement

(上接第 46 页)

二是沿传输路径计算的转发模式，在这种转发模式中，封装体报文按照指定的每到一个中间节点时，就要在该节点执行其携带的程序。通过这种执行方式，管理节点可以把集中的任务分发到沿整个传输路径上去执行。

(2)One-Multi 模式：在这种转发模式中，多个同样的封装体报文同时从一个节点发出，这些封装体报文发向不同的目的节点并且在该节点执行。这种转发模式可以用于信息的广播(如拥塞位置的检测)、子网的控制。

(3)BFST(Breadth First Search Traversing)转发模式：这是一种并行控制模式。当封装体报文到达一个主动节点后，它被转发到与当前节点直接相连的邻居节点。到达下一个节点时同样按照将该报文直接转发给相邻的节点。显然，经过一次转发后，网络中将出现很多该封装体报文的副本。当这些副本到达下一个节点后，它们又被复制，并转发到它们的邻居节点，报文副本依次转发下去，直到遍历完整个网络。

(4)DFST(Depth First Search Traversing)转发模式：这是一种串行控制模式。在该模式中，封装体报文到达一个主动节点后，它被转发到与当前节点直接相连的一个邻居节点。当它到达这个邻居节点后，它又被转发到该邻居节点的一个邻居节点，依次转发下去，直至遍历完整个网络。

结束语 主动网络管理体现了主动网络的思想，将一部分网络管理功能动态地分布在主动节点上，充分利用了主动节点的计算能力，使节点能够自动发现、解决问题，从而极大地优化了网络管理。本文讨论了一种主动网络的管理模型，该模型中各个模块相互独立、任务明确，而且在每个层都可以动态更新以适应主动网络中主动节点的易变性和主动应用的扩展性，因此网络管理的稳定性和扩展性都大为提高，适应了现代网络管理的需要。

参 考 文 献

1 Moore O T, Nettles S M. [EB/OL]. Towards Practical Programmable Packets: [Technical Report]. MS-CIS-00-12. University of Pennsylvania, May 2000

2 Di Fatta G, Lo Re G. Active Networks [J]: an Evolution of the Internet. In: Proc of AICA2001 - 39th Annual Conference, Cernobbio, Italy, Sept 2001

3 Marshall I W, et al. Active management of multiservice networks. In: Proc IEEE NOMS, 2000. 981～983

4 Al Shaer E. Active Management Framework for Distributed Multimedia Systems [J]. Journal of Networks and Systems Management, 2000, 8: 49～72

5 Brunner M, Stadler R. Service Management in Multi-Party Active Networks [J]. IEEE Communications Magazine, March 2000, 38(3): 281～286

6 Kiwior D, Zabele S. Active Resource Allocation in Active Networks [J]. IEEE JSAC, March 2000, 19(3): 452～459