面向 NAT 用户的 IPv6 隧道技术研究

吴贤国[1),2)] 刘 敏[1),2)] 李忠诚[1)]

[1)](中国科学院计算技术研究所，北京 100080)

[2)](中国科学院研究生院，北京 100049)

摘 要 目前只有 Teredo 协议是专为 NAT 用户设计的一种 IPv6 隧道技术.但是,该协议不能为用户分配固定的 IPv6 地址,不支持对称类型的 NAT 用户,并且不能有效防御源地址欺骗攻击.针对这些不足,文章基于客户端-服务器隧道模式和服务器的有状态特性,提出一种新的 IPv6 隧道技术 Silkroad. Silkroad 协议在网络中引入隧道服务器,负责为 NAT 用户分配 IPv6 地址,然后作为中继器转发用户和 IPv6 网络之间的数据流.针对客户端-服务器隧道模式的不足,对 NAT 用户之间的通信进行优化,有效降低了通信开销. Silkroad 协议支持所有类型的 NAT 用户和 IPv6 网络进行互连,能为用户分配固定不变的 IPv6 地址,并且具有更高的安全性.

关键词 IPv6;过渡;NAT;隧道;Teredo

中图法分类号 TP393

Research on the IPv6 Tunneling Technology Designed for Network Address Translator Users

WU Xian-Guo[1),2)] LIU Min[1),2)] LI Zhong-Cheng[1)]

[1)](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100084)

[2)](*Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract Teredo is the only one tunnel mechanism designed for NAT users. However, Teredo does not support symmetric NAT users and cannot allocate stable IPv6 addresses for the users, and also has security problems. Based on client-server tunnel mode and servers' statefule characteristic, a new tunnel mechanism named Silkroad is proposed to resolve Teredo's problems. The mechanism makes use of tunnel servers, which assign IPv6 addresses to users and then act as relays to transmit the packets between NAT users and IPv6 networks. In addition, an adaptive communication optimization scheme is presented to reduce the time cost of communication between two clients. Silkroad supports all types of NAT users to connect with IPv6 networks, can assign stable IPv6 addresses to the users and has high security.

Keywords IPv6; transition; NAT; tunnel; Teredo

1 引 言

在广泛力量的推动下,IPv6 即将取代 IPv4 已是不争的事实.但 IPv4 网络的基础设施十分广泛,从 IPv4 到 IPv6 的过渡不可能一蹴而就,新旧网络的彻底更换需要一个渐进的过程.在相当长的时间里,两者将相互共存.因此,研究如何实现平滑过渡,对加快整个过渡进程、推动 IPv6 的部署和运营具有十分重要的现实意义.

收稿日期:2005-08-10;修改稿收到日期:2006-10-18.本文得到国家自然科学基金(60273021,90604016)资助.**吴贤国**,男,1978 年生,博士研究生,研究方向为下一代互联网与无线网络. E-mail: xgwu@ict.ac.cn. **刘 敏**,女,1976 年生,博士研究生,副研究员,研究方向为移动切换与网络测量. E-mail: liumin@ict.ac.cn. **李忠诚**,男,1962 年生,博士,研究员,博士生导师,研究领域为计算机网络和测试等.

隧道是一种重要的过渡技术.它的实质是封装,即将一种协议类型的分组封装在另一种协议类型的分组中[1],前者将后者看作它的数据链路层.因为对封装和被封装的协议类型没有具体要求,所以隧道具有很好的灵活性.利用隧道可以在不建设网络基础设施的情况下扩展新的网络.因此在 IPv4/IPv6 过渡时期,隧道技术被广泛采用.

目前,用于过渡的绝大多数隧道基于 IPv6-in-IPv4 封装方式,也就是将 IPv6 分组封装在 IPv4 分组中,利用已有的 IPv4 路由体系进行传输,从而解决被 IPv4 网络分离的两个 IPv6 网络或节点之间如何通信的问题.但是,IPv6-in-IPv4 报文无法通过 IPv4 网络中大量存在的 NAT 设备,因此这类隧道不能在有 NAT 的环境中使用.微软公司提出的 Teredo 协议[2]是目前唯一面向 NAT 用户设计的隧道技术,但是存在不能为用户分配固定的 IPv6 地址、不支持对称类型的 NAT 用户、不能有效防止非法用户利用 Teredo 服务和 IPv6 网络互连等不足之处.

本文在分析 Teredo 不足的基础上,基于客户端-服务器隧道模式和服务器的有状态特性,提出了一种新的面向 NAT 用户的 IPv6 隧道技术,称之为 Silkroad. Silkroad 协议在网络中引入隧道服务器,负责为 NAT 用户分配 IPv6 地址,然后作为中继器转发用户和 IPv6 网络之间的数据流.另外,针对客户端-服务器隧道模式的不足,对 NAT 用户之间的通信进行优化,有效降低了通信开销. Silkroad 协议支持所有类型的 NAT 用户和 IPv6 网络进行互连,能为用户分配固定不变的 IPv6 地址,并且具有更高的安全性.

2 现有技术分析

2.1 NAT 用户的过渡场景

NAT 是解决 IPv4 地址不足的一种临时性技术[3].由于 IP 地址资源短缺的现象十分严重,因此 NAT 技术的使用非常普遍. NAT 用户在网络内部采用私有地址进行通信,并通过 NAT 公用一个或若干个公有地址与外部互联网进行通信.由于私有地址的非全球唯一性,外部互联网的节点不能主动访问 NAT 用户,可见 NAT 用户是 IPv4 地址不足真正的受害者,因而它们更迫切需要 IPv6.为 NAT 用户提供一种有效的过渡机制,成为目前十分紧迫的一项任务.

目前,终端设备的主流操作系统如 Windows, Linux, Symbian 等都已实现 IPv4/IPv6 双协议栈.本文在接下来的描述中,假设 NAT 用户都是双栈节点,具备作为隧道端节点的条件.如图 1 所示, NAT 用户的过渡场景可以分为两种:(1)将 NAT 设备升级成 IPv6 路由器,并采用手工配置隧道或 6to4 隧道等方式和 IPv6 网络相连,然后向 NAT 内网广播 IPv6 路由宣告, NAT 用户根据路由宣告获得 IPv6 地址,从而获得端到端的 IPv6 连接;(2)NAT 用户直接通过隧道方式和 IPv6 网络建立通道,这种方式不需要对现有的网络作任何改造.

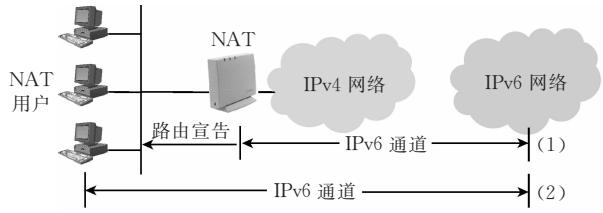

图 1 NAT 用户的过渡场景

升级 NAT 设备解决的是整个 NAT 子网如何接入 IPv6 网络的问题,而非针对分散的 NAT 用户.即使子网内只有少数用户希望获得 IPv6 连接,也必须对整个网络进行改造,因此这种方式缺乏灵活性.实际上,在运营商或管理员有足够充分的理由之前,升级网络边缘设备的可能性很低.在现阶段,有必要设计一种面向分散用户的隧道技术,在不改造现有网络基础设施的情况下,该技术能够为 NAT 用户提供 IPv6 接入服务.

从图中可以看出,这样的隧道必须具备一个基本的特征:允许隧道主体也就是两个隧道端节点之间的路径上存在 NAT 设备.

2.2 现有隧道技术及其不足

IETF 在制定 IPv6 协议的同时也制定了几种用于过渡的隧道机制,如手工配置隧道[4]和 6to4[5]、ISATAP[6]、Tunnel Broker[7]等自动隧道.它们无一例外地采用了 IPv6-in-IPv4 封装方式,但由于绝大多数 NAT 设备只支持 TCP, UDP, ICMP 等常见报文的转发, IPv6-in-IPv4 数据包(IP 头部类型字段值为 41)无法通过 NAT,因此这些隧道都不允许隧道主体上存在 NAT 设备.另外,6to4 等隧道机制要求端节点必须具有公有 IP 地址, NAT 用户显然无法满足这样的要求.

Teredo 是微软公司专为 NAT 用户设计的一种隧道技术.它采用 IPv6-in-UDP 封装方式来解决上述隧道存在的问题.然而, Teredo 协议存在以下一

些不足.

首先，Teredo 不能为用户分配固定不变的 IPv6 地址. 为了达到自动封装的目的，Teredo 分配给用户的 IPv6 地址中内嵌隧道参数，也就是用户的私有地址和 UDP 源端口经 NAT 转换后的外部地址和外部端口. 用户的 IPv6 地址在初始化过程中由服务器分配，由于外部地址和外部端口的随机性，用户每次和服务器初始化通信时往往被 NAT 转换成不同的外部地址或外部端口，所以通常情况下总是获得和上次不同的 IPv6 地址. 如果只访问 IPv6 网络上的服务，而不希望其他 IPv6 节点主动和它通信，地址的变化对用户来讲没有什么影响. 但 IP 网络的一个重要优势在于通信的端到端特征，特别是对不具备这种特征的 NAT 用户来讲，端到端更是一种需要，是推动过渡的有力因素. 在地址经常变化的情况下，另一方很难主动向 NAT 用户发起连接，使 NAT 用户丧失了这种端到端的优势. 采用 IPv6 动态域名解析系统是一种解决方案，但在过渡时期，IPv6 网络基础设施很不完善，这种方案的可行性很小.

其次，Teredo 不支持对称类型的 NAT 用户. Teredo 协议采用客户端-客户端隧道模式，通信端点就是隧道端点，NAT 用户若要和不同的节点通信，意味着要建立不同的隧道，因此隧道另一端的 IPv4 地址随着通信目的地的变化而变化. 对称类型 NAT 根据数据包目的地址来转换它的私有地址和端口，如果目的地址不同，那么转换后的外部地址和外部端口也不同. 这样，隧道另一端 IPv4 地址的变化，引起了 NAT 用户本身隧道参数的变化. 而 Teredo 协议一个隐含的假定是，用户配置了 IPv6 地址后，内嵌其中的隧道参数是不会发生变化的. 显然，存在对称类型 NAT 的情况下，从用户 IPv6 地址中获得的隧道参数是不正确的，这是 Teredo 不支持对称类型 NAT 用户的根本原因.

最后，Teredo 不能有效阻止非法用户利用 Teredo 中继器和 IPv6 网络互连. Teredo 中继器是一个和 IPv4 网络、IPv6 网络都相连的双栈节点，负责转发 NAT 用户和 IPv6 网络之间的数据流，它是无状态的，不维护任何有关用户的信息. 由此引起的问题是，如何保证从 IPv4 接口接收的数据包确实来自合法的 NAT 用户？ Teredo 采取了一定的安全措施，比如验证数据包的源 IPv4 地址是否和 Teredo 地址内嵌的外部地址一致，若一致，则认为是合法的. 但是，只要构造出符合 Teredo 格式的源 IPv6 地址就可以通过这样的验证. Teredo 中继器的无状态特性，使得没有经过身份认证的非法用户只要花很少的代价就可以享用中继器提供的数据转发服务，这对合法用户来讲是不公平的，甚至是危险的，非法用户通过这种方式获得 IPv6 连接后，进一步可对 IPv6 网络上的节点实施攻击.

3　Teredo 问题的解决方法

针对 Teredo 协议的不足，本文提出一种新的自动隧道机制，称之为 Silkroad. Silkroad 采用客户端-服务器隧道模式并利用服务器的有状态特性来解决 Teredo 存在的问题.

3.1　客户端-服务器模式

按隧道两端节点是否是通信节点来划分，隧道模式可以分为三种：客户端-客户端模式、客户端-服务器模式和服务器-服务器模式. 第一种模式中隧道的两个端节点都是通信节点，一般应用于被 IPv4 网络分离的两个双栈主机之间的 IPv6 通信；第二种模式中隧道的两个端节点中有一个是通信节点，一般应用于被 IPv4 网络分离的双栈主机和双栈路由器之间的 IPv6 通信；第三种模式中隧道的两个端节点都不是通信节点，一般应用于被 IPv4 网络分离的两个双栈路由器之间的 IPv6 通信.

Teredo 采用的是第一种隧道模式，如前所述，客户端-客户端模式下 NAT 用户的隧道端节点随着通信目的地的变化而变化，如果隧道主体上存在对称类型的 NAT，隧道端节点的变化又将引起客户端隧道参数的变化，导致通信不能正常进行. 因此客户端-客户端模式不适用于对称类型的 NAT 用户.

和客户端-客户端模式不同，客户端-服务器模式下 NAT 用户作为客户端一旦在初始化过程中确定选择接入的隧道服务器，此后不管和普通 IPv6 节点通信还是和其他 NAT 用户通信，和它建立 IPv6-in-UDP 隧道的始终是隧道服务器. 用户向目的节点发送的 IPv6 数据包必须经过封装后先发送给隧道服务器，再由隧道服务器解封装后转发给目的节点；来自目的节点的数据包也必须先到达隧道服务器，经服务器封装后再发送给 NAT 用户，然后由 NAT 用户进行解封装.

可见客户端-服务器模式能够保证 NAT 用户的隧道端节点在整个接入期间都是固定的，不会因为 IPv6 通信目的地的不同而改变. 根据 NAT 原理可知，由于用户发出的 IPv6-in-UDP 数据包中 IPv4

目的地址的固定,不管它和隧道服务器之间的路径上存在何种类型的 NAT 或者多少个 NAT,其隧道参数也就是经 NAT 映射后的外部地址和外部端口总是固定的.服务器利用 NAT 用户固定的隧道参数对发往该用户的 IPv6 数据包进行封装,封装后的数据包就可以通过 NAT 到达目的地.这说明客户端-服务器模式下隧道的通信和 NAT 的类型数量没有关系,因此客户端-服务器模式允许隧道主体上存在任何类型和任意数量的 NAT 设备.

3.2 服务器的有状态特性

服务器作为隧道的一端,必须获得客户端的隧道参数后才能对目的地是该客户端的 IPv6 数据包进行封装并发送.现有的自动隧道机制往往将隧道参数嵌入到客户端的 IPv6 地址中,这样就可以根据客户端地址自动获得隧道参数.由于简单有效,该方式被 6to4,ISATAP,Teredo 等自动隧道机制广泛采用.然而,在客户端和隧道服务器之间存在 NAT 的情况下,由于隧道参数的随机性,导致了客户端地址的频繁变化.

为了解决这个问题,本文采取的方法是由隧道服务器维护一组状态信息,其中包含客户端 IPv6 地址和隧道参数之间的映射关系,在已知客户端 IPv6 地址的情况下,通过查找映射关系来获得它的隧道参数.映射关系的创建可以在客户端初始化过程中完成,隧道服务器收到客户端 A 的请求报文后,从报文中获得它的隧道参数,即报文的源 IPv4 地址 IP_A 和源 UDP 端口 UDP_A,然后根据一定的配址机制为 A 构造一个 IPv6 地址 $IP6_A$,建立 $IP6_A$ 和 IP_A、UDP_A 之间的映射关系 $\{IP6_A:IP_A+UDP_A\}$,作为状态信息以表的形式保存在隧道服务器上.如图 2 所示,在接下来的数据转发过程中,隧道服务器从 IPv6 接口收到数据包后,以数据包的目的 IPv6 地址为入口,查表得到对应的 IPv4 地址和 UDP 端口,然后对数据包进行封装,再将封装后的报文发送给客户端.如果客户端在下一次接入时隧道参数变为 $IP'_A+UDP'_A$,只需要将映射表的 $\{IP6_A:IP_A+UDP_A\}$ 更新为 $\{IP6_A:IP'_A+UDP'_A\}$,客户端的 IPv6 地址可以保持不变,仍为 $IP6_A$.

在客户端 IPv6 地址和隧道参数相互独立的情况下,隧道服务器可以灵活引入各种配址机制,如有状态地址自动配置[8]或无状态地址自动配置[9],为客户端分配固定不变的 IPv6 地址.

服务器的有状态特性不仅可以解决客户端 IPv6 地址不固定的问题,还可用来检查流经服务器的数据包是否合法.利用如图 2 所示的映射表,隧道服务器采取下述措施来检查数据包的合法性:一是从 IPv6 接口收到数据包后,以目的 IPv6 地址为入口查找映射表,如果没有这个入口,则表明是一个非法数据包,作丢弃处理;二是检查从 IPv4 接口收到的数据包,以源 IPv6 地址为入口查找映射表,如果没有这个入口,或者这个入口对应的隧道参数和数据包的源 IPv4 地址、源 UDP 端口不一致,则表明数据包非法,作丢弃处理.只有源或目的是合法用户的情况下,数据包才能通过上述检查.即使恶意主机采用源 IPv6 地址欺骗手段,也会因为数据包的源 IPv4 地址、源 UDP 端口和服务器上保存的隧道参数不一致而被拒绝转发.

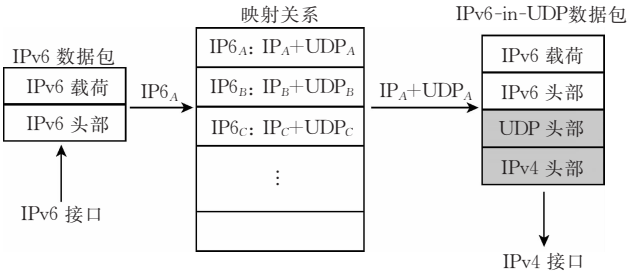

图 2 基于映射关系的封装

当然,数据包合法性检查的前提是必须确保存储在隧道服务器上的映射关系的合法性.做到这一点并不困难,在客户端初始化过程中,隧道服务器收到客户端的请求报文后可以采取一定的身份认证机制对其合法性进行认证,通过认证的情况下才向客户端分配 IPv6 地址并建立映射关系,从而保证映射关系的合法性.在对客户端进行身份认证的基础上,通过数据包合法性检查,可防止非法用户利用隧道服务器和 IPv6 网络互连,并能有效防御源 IPv6 地址欺骗攻击,从而提高了系统安全性.

服务器的有状态特性解决了 Teredo 存在的一些问题,同时也带来了一个新的问题,那就是如何对状态信息进行管理.维护信息需要消耗系统资源,特别是在接入用户很多映射表很大的时候,对状态信息的管理不当可能会造成服务器运行效率的下降甚至系统崩溃,可见状态信息的管理十分重要.因此有必要采取一定的措施删除那些不再使用的映射关系,使得服务器维护的都是处于活动状态也就是用户正在使用的映射关系,以减少信息维护对系统资源的占用.本文将在 4.4 节介绍如何对隧道服务器的状态信息进行管理.

4 Silkroad 协议设计

4.1 系统结构

如图 3 所示，Silkroad 协议定义了 3 种通信实体：客户端、隧道服务器和导航器. 客户端指 NAT 域内的双栈节点，它通过一个初始化过程来获得 IPv6 地址并建立 IPv6-in-UDP 隧道，在此基础上向应用程序提供透明的 IPv6 连接，另外还负责维护隧道的有效性. 隧道服务器是和 IPv4、IPv6 网络都相连的双栈节点，负责对客户端进行身份认证并为合法客户端分配 IPv6 地址，然后作为中继器转发客户端和 IPv6 网络之间的数据流，同时对自身的状态信息进行管理. 导航器位于 IPv4 网络，拥有客户端的注册信息和隧道服务器的部署情况，它的主要功能是为客户端选择一个就近的隧道服务器进行接入，并对各个服务器的运行状况进行监视.

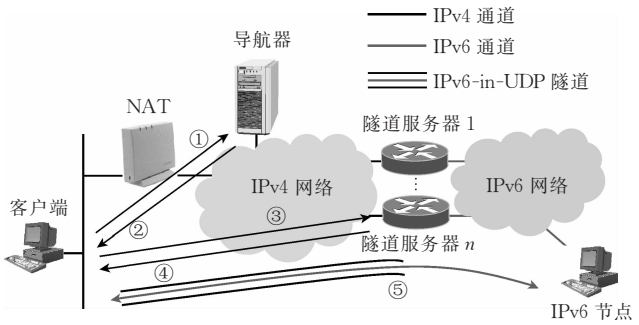

图 3　Silkroad 系统结构

初始化过程中，客户端首先向导航器发送接入请求报文，导航器为其选择一个路由距离最近的隧道服务器，将它的 IPv4 地址返回给客户端. 客户端然后向指定的隧道服务器发送地址请求报文，报文内容为身份认证信息以及创建 IPv6 地址所需的接口标识符，服务器收到请求报文后首先对客户端的身份进行认证，通过认证后为其构造一个 IPv6 地址，在映射表中添加该地址和隧道参数之间的映射关系，然后将地址和更新过的身份认证信息作为响应报文的内容返回给客户端. 客户端对服务器的身份进行认证，通过认证后配置 IPv6 地址，并建立另一端为服务器的 IPv6-in-UDP 隧道. 在这之后，客户端就可以通过该隧道和 IPv6 网络上的其他节点进行端到端的通信，服务器在数据转发过程中，按 3.2 节所述规则对数据包的合法性进行检查. 需要指出的是，初始化过程中所有的交互报文均为 UDP 类型.

单个隧道服务器的性能总是有限的，从图 3 可以看出，本文采用了分布式的多服务器结构来解决系统因用户增多引起的可扩展性问题. 在网络中部署多个隧道服务器，各个服务器之间是状态无关的，都可以独立为用户提供接入服务，它们位于不同的地方，具有地理位置上的分布式特征. 服务器在运行过程中，周期性地向导航器报告负载信息如 CPU 利用率、带宽利用率、用户数目等，导航器则负责对这些信息进行统计和分析，以便系统管理员动态掌握服务器的运行状况. 由于身份认证、地址分配、数据转发等功能都集中在隧道服务器上，导航器的负载相对来讲要轻得多，因此这样的结构具有良好的可扩展性.

4.2 客户端 IPv6 地址构造

客户端的 IPv6 地址由 64 位的地址前缀和 64 位的接口标识符组成，地址前缀由隧道服务器确定，接口标识符由客户端确定. 只要初始化过程中地址前缀和接口标识符都能保持固定，客户端就可以获得永久不变的 IPv6 地址.

每个隧道服务器在部署的时候都会分配一个全球唯一的 64 位地址前缀用于构造客户端 IPv6 地址，同时将 IPv6 网络中目的为该前缀的路由指向对应的服务器. 客户端只要确定了选择接入的隧道服务器，64 位的地址前缀也随之确定而不再发生变化，所以客户端 IPv6 地址是否固定，取决于由它本身确定的接口标识符是否固定. 为了生成固定的接口标识符，需要以固定的信息作为基础，客户端机器的硬件信息满足这些要求. IEEE 定义了 64 位的 EUI-64① 编码，用来表示网络适配器的地址，如图 4

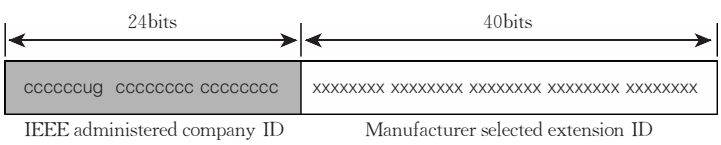

图 4　EUI-64 编码格式

① IEEE. Guidelines for 64-bit global identifier (EUI-64) registration authority. http://standards.ieee.org/db/oui/tutotials/EUI64.html, 1997

所示.参考 PPPv6[10]生成接口标识符的方法,如果客户端有 EUI-64 地址,只要将它的"u"位取反,就可以得到接口标识符;如果有 EUI-48 地址(目前的网络适配器地址都采用传统的 48 位 EUI-48 编码),在其中间添加值为"0xFFFE"的 16 位比特,成为一个 EUI-64 地址后,再将"u"位取反便可得到接口标识符;如果没有 EUI-48 或 EUI-64 地址,就将机器序列号等数值转换成 64 位编码.采用这种方式生成的接口标识符不仅具有固定性,而且具有唯一性,从而保证了 IPv6 地址的唯一性.

值得一提的是,客户端虽然通过上述方式能够获得固定不变的 IPv6 地址,但是如果要被其他节点主动访问,还是有必要注册一个域名,在 IPv6 DNS 服务器中设定一个 AAAA 或 A6 记录,这样其他节点就可以采用域名的方式更方便地向客户端主动发起通信.

4.3 身份认证机制

前面讲到,Silkroad 之所以提高了安全性,在于它利用服务器的有状态特性对数据包的合法性进行检查,有效起到了防御源 IPv6 地址欺骗攻击的作用.隧道服务器对数据包的检查是建立在映射关系的合法性基础之上的,而映射关系的合法性则通过初始化过程的身份认证机制来实现.

身份认证是双向的,不仅隧道服务器认证客户端的合法性,客户端也认证服务器的合法性.如图 5 所示,认证信息包括客户端标识符、哈希值、随机数和确认值等.确认值在客户端设为 0,如果通过认证,服务器返回的确认值仍为 0,非 0 则表示认证失败.随机数由客户端确定,并由隧道服务器原封不动返回,客户端通过检查返回的随机数是否和初始值一致来防止遭受数据包重放攻击.哈希值采用 SHA1[11]散列函数计算,对于请求报文,输入数据包括客户端标识符、口令、随机数、确认值和接口标识符,对于响应报文,输入数据除了将接口标识符改为客户端的 IPv6 地址外,其余保持不变.隧道服务器通过验证客户端的哈希值,可以防止非法用户享用 Silkroad 服务;客户端通过验证隧道服务器的哈希值,可以防止恶意用户假冒隧道服务器实施中间人攻击.

图 5 身份认证信息

4.4 隧道维护和状态信息管理

客户端在初始化过程中向隧道服务器发送地址请求报文时,NAT 建立起一个 UDP 会话(不妨称之为 Silkroad UDP 会话),并在后继的数据传输中以该会话为依据转发 IPv6-in-UDP 数据包.因此,隧道有效的前提是 NAT 上的 Silkroad UDP 会话是存活的,一旦会话因超时而中断,即 NAT 维护的映射关系被删除,隧道便不再有效.NAT 删除 UDP 会话的原因是在规定的时间内没有收到会话数据流,认为用户已经不再使用该会话,为节省资源,NAT 设备将不再维护对应的映射关系.对于一般的 UDP 会话,删除对应的映射关系只意味着 NAT 用户的某个应用程序失去了 UDP 连接;对于 Silkroad UDP 会话,情况要严重得多.因为 IPv6-in-UDP 隧道的作用好比是一条虚拟的 IPv6 链路,删除映射关系相当于切断了连接 NAT 用户和外部 IPv6 网络的通道,因此所有的 IPv6 应用程序都将中断.

为使隧道在接入期间始终有效,就必须对 Silkroad UDP 会话进行维护.隧道服务器具有较重的负荷,因此比较而言由客户端负责维护更为合适.客户端完成初始化过程后以一定的时间间隔周期性的向隧道服务器发送 IPv6-in-UDP 报文,发送周期默认为 30s.为了节省带宽资源,报文的 IPv6 头部中下一个头部类型字段值为 59,表示一个空包,没有 IPv6 数据载荷.

管理状态信息的目的是为了尽可能多地删除那些不再使用的信息,从而降低因维护信息对系统资源的消耗.服务器对状态信息的管理通常采用客户端显式通知的方式,比如客户端在下线之前向服务器发送一个中断连接请求,服务器收到请求后删除对应的映射关系.但是,这种方式不能较好地处理客户端异常下线的情况.本文利用客户端维护 UDP 会话的过程来管理状态信息.服务器为每个映射关系设定一个计时器,超时时间为 61s,一旦收到来自客户端的数据包就刷新计时器重新计时.如果收到的是空包,服务器除了刷新计时器外不作任何其他处理.计时器一旦超时,服务器认为客户端已经下线,将删除对应的映射关系.采用这种方式可使隧道服务器上维护的都是处于活动状态的映射关系,有效达到了管理的目的.

4.5 不 足

Silkroad 在解决 Teredo 问题的同时也付出了一定的代价.它的不足在于两个客户端之间通信时,

从一个客户端 A 发出的数据包，必须先到达隧道服务器，再由隧道服务器转发给另一客户端 B；从 B 返回的数据包也必须经过隧道服务器的中转，才能到达客户端 A. 这种三角路由方式一方面增大了客户端之间通信的时间开销，另一方面也增加了隧道服务器的通信负载.

5　NAT 用户之间的通信优化

5.1　基本原理

为了解决 Silkroad 协议存在的不足，本文对 NAT 用户之间的通信进行优化. 通信优化的基本原理是在两个客户端之间建立 IPv6-in-UDP 隧道，从而绕开服务器进行直接通信. 客户端之间能够建立隧道的一个前提是通信双方都有另一方的隧道参数. 如何获取对方的隧道参数，是实现直接通信首先需要解决的问题.

由于客户端的隧道参数保存在服务器上，因此在直接通信之前，客户端必须在隧道服务器的参与下通过一个交互过程来获得对方的隧道参数. 另外，由于 NAT 对外网数据包的转发有一定的限制规则，交互过程的另一目的是在 NAT 处打开一个缺口，以便另一方发出的数据包能够进入本方所在的 NAT 内网.

5.2　交互过程

不同类型的 NAT 对外网数据包的转发有着不同程度的限制，因此交互过程和 NAT 类型有关. NAT 类型可分为锥形、受限锥形和对称 3 种，在通信双方都不是全锥形 NAT 用户并且至少有一方是对称 NAT 用户时，通信优化不可能实现，其余情况下均可对通信进行优化. 限于篇幅，具体原因不再阐述.

不同类型 NAT 用户之间的交互过程如图 6 所示，图中 CSC，RSC，SSC 分别表示全锥形、受限锥形和对称类型 NAT 用户，SAR 表示隧道服务器. 以图 6(d)为例说明如何完成交互过程：RSC 首先向 SAR 发送一个请求报文，内容为通信另一方也就是 CSC 的 IPv6 地址；SAR 以该地址为入口查找映射表，得到 CSC 的隧道参数 $IP_{CSC}+UDP_{CSC}$ 并返回给 RSC；RSC 获得 CSC 的隧道参数后，建立映射关系 $\{IP6_{CSC}:IP_{CSC}+UDP_{CSC}\}$，然后向其发送一个 Hello 报文(即空包)，目的有两个，一是告知 CSC 它的隧道参数，二是在自身所在的受限锥形 NAT 处打开一条通路，以便来自 CSC 的报文能够通过 NAT. CSC 收到 Hello 报文后，建立映射关系 $\{IP6_{RSC}:IP_{RSC}+UDP_{RSC}\}$，然后向对方发送一个 Hello 报文作为响应；RSC 收到 Hello 报文后，说明对方已经获得隧道参数，接下来就可以进行直接通信了.

从图 6(a)～图 6(f)，不同情况下，交互过程有 3～6个步骤不等，完成所有步骤需要花费一定的时间，可见通信优化是需要付出代价的. 对于长数据流，付出这样的代价是值得的，因为一旦完成交互过程以后，后继的大量数据传输不再经过隧道服务器，

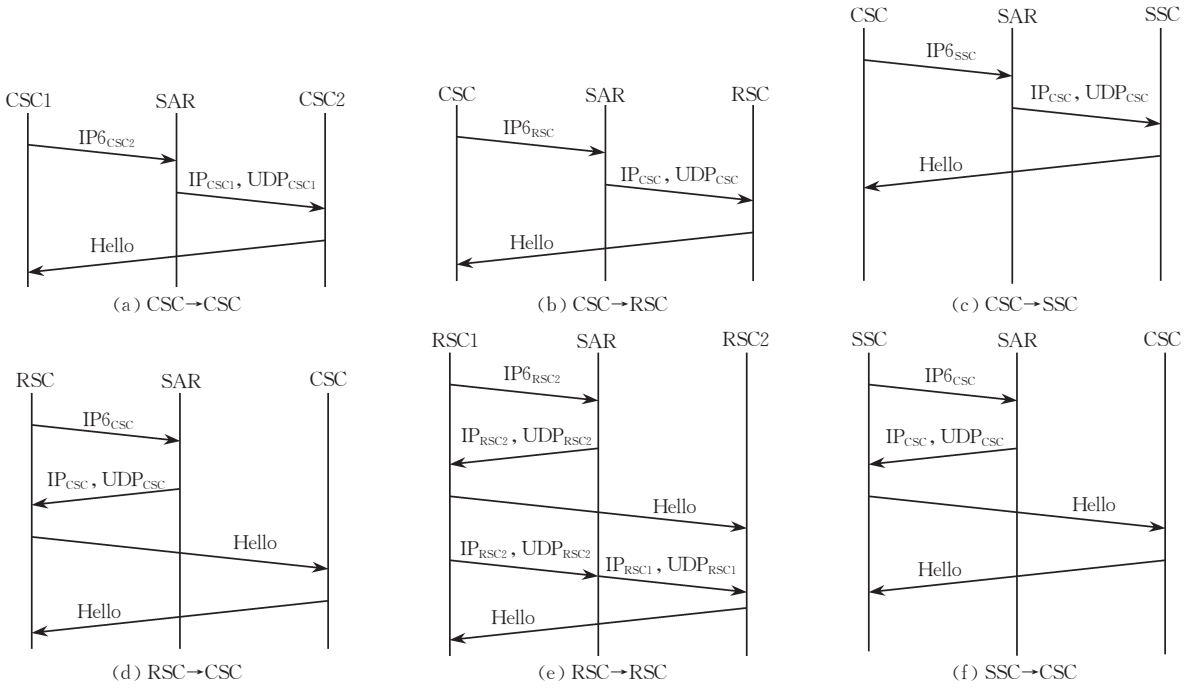

图 6　交互过程

因此缩短的时间超过了交互过程花费的时间;但是对于来回只传输少量数据包的短数据流,通信优化未必合算.因此,实际应用中客户端之间的通信是否需要优化应根据不同的情况进行判断.针对这个问题本文提出一种自适应优化方法.

5.3 自适应优化方法

显然,通信优化与否和通信的长度直接相关.自适应优化方法根据客户端之间的会话长度来确定是否对通信进行优化,最终目的是减少通信花费的时间开销,使各种类型的网络应用都能获得尽可能好的服务质量.

在自适应优化方法中,如果客户端和另一客户端之间的会话长度大于预先定义的一个阈值,客户端选择通信优化,在正式通信之前启动交互过程,向隧道服务器发送一个空包,待收到另一方的空包后,开始和对方进行直接通信;如果会话长度小于阈值,客户端放弃通信优化,将数据包发送给隧道服务器,再由隧道服务器转发给另一方,返回的数据包同样如此.通过分析不难得出,在服务器和客户端以及客户端和客户端之间的链路时延相对交互报文的处理时间和数据包发送时间而言比较大的情况下,会话长度阈值近似等于交互过程的步骤数目.实际情况往往如此,因此可以根据双方的 NAT 类型获得阈值大小.

图 7 显示了在典型的网络状况下,以 RSC 或 SSC 向 CSC 发起会话为例,不同优化策略下通信开销的比较情况,图中 NCO 表示不优化,CO 表示优化,ACO 表示自适应优化.会话长度较小时,数据传输的开销占总开销的比重较小,因通信优化节省的开销不足以弥补交互过程的开销,因此通信优化反而增大了会话总的时间开销.随着会话长度的增大,因优化节省的开销越来越多,CO 的开销比 NCO 的开销越来越小.ACO 和 CO 的主要区别在于当会话长度较小时,它的开销和 NCO 一致,小于 CO 的开销.

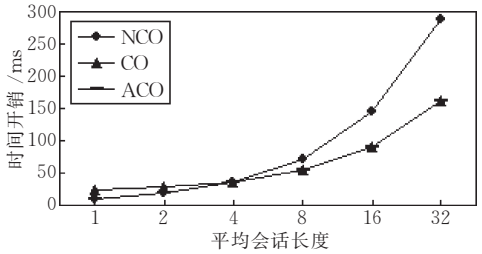

图 7 不同优化策略下通信的时间开销

6 Silkroad 原型系统

本文在 Linux 平台上实现了 Silkroad 原型系统,其中客户端软件在 Windows 2000,Red Hat 8.0,Familiar Linux 7.1 以及 Symbian 7.0 上都有相应的实现版本.目前,隧道服务器运行于中国科学院计算技术研究所,IPv4 地址为 159.226.39.108,可分配的 IPv6 地址前缀为 2001:250:f007:8::/64.

为了展示 Silkroad 系统的功能,设计了如图 8 所示的演示网络.演示的内容是 NAT 用户通过隧道服务器接入 IPv6 网络,然后和网络中的 IPv6 节点进行端到端通信的过程.NAT 用户是一个 Sony-Ericsson P802 智能手机,操作系统为 Symbian 7.0,安装了客户端软件.IPv6 节点是一个 HP H3905 掌上电脑.两个节点均安装基于 IPv6 协议的网络五子棋游戏软件.

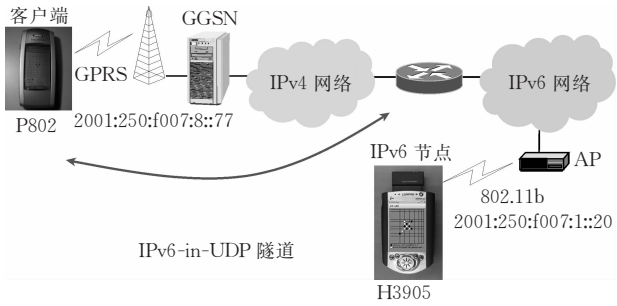

图 8 Silkroad 系统演示网络

客户端通过 GPRS 拨号获得一个私有 IPv4 地址 10.*.*.*,通过 GGSN 的 NAT 功能访问 IPv4 网络.运行客户端程序,使其通过隧道服务器接入 IPv6 网络,服务器为其分配的 IPv6 地址为 2001:250:f007:8::77.IPv6 节点通过 802.11b 无线局域网直接接入 IPv6 网络,设置 IPv6 地址为 2001:250:f007:1::20.双方启动五子棋程序,然后输入对方的 IPv6 地址,就可以开始端到端的网络游戏.

7 结束语

本文分析了现有 IPv6 隧道技术尤其是 Teredo 协议存在的不足.在此基础上,基于客户端-服务器隧道模式和服务器的有状态特性,提出了一种新的面向 NAT 用户的 IPv6 隧道技术 Silkroad.Silkroad 协议在网络中引入隧道服务器,负责为 NAT 用户分配 IPv6 地址,然后作为中继器转发用户和 IPv6 网络之间的数据流.针对客户端-服务器隧道模式的

不足，对 NAT 用户之间的通信进行优化，有效降低了通信的时间开销. Silkroad 协议支持所有类型的 NAT 用户和 IPv6 网络进行互连，能为用户分配固定不变的 IPv6 地址，并且具有更高的安全性.

参 考 文 献

[1] Hanks S, Farinacci D, Traina P. Generic routing encapsulation (GRE). RFC 1701, October 1994

[2] Huitema. Teredo: Tunneling IPv6 over UDP through NATs. draft-huitema-v6ops-teredo- 04. txt, January 2005

[3] Egevang K, Francis P. The IP network address translator (NAT). RFC 1631, May 1994

[4] Gilligan R, Nordmark E. Transition mechanisms for IPv6 hosts and routers. RFC 2893, August 2000

[5] Carpenter B, Moore K. Connection of IPv6 domain via IPv4 clouds. RFC 3056, February 2001

[6] Templin F, Gleeson T, Talwar M, Thaler D. Intra-site automatic tunnel addressing protocol (ISATAP). draft-ietf-ngtrans-isatap-24. txt, January 2005

[7] Durand A, Fasano P, Guardini I, Lento D. IPv6 tunnel broker. RFC 3053, January 2001

[8] Droms R et al. Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315, July 2003

[9] Narten T, Thomson S. IPv6 stateless address autoconfiguration. RFC 2462, Dec. 1998

[10] Haskin D, Allen E. IP version 6 over PPP. RFC 2472, Dec. 1998

[11] Eastlake D, Jones P. US secure hash algorithm 1 (SHA1). RFC 3174, Sept. 2001

WU Xian-Guo, born in 1978, Ph. D. candidate. His research interests include next generation Internet and wireless networks.

LIU Min, born in 1976, Ph. D. candidate. Her research interests include mobile handoff and network measurement.

LI Zhong-Cheng, born in 1962, Ph. D., professor, Ph. D. supervisor. His research interests include computer networks and measurements.

Background

Research on mechanisms of transition from IPv4 to IPv6 is very important. Nowadays, many methods have been proposed to support connections between IPv4 users and IPv6 users. Unfortunately, there is only one tunnel mechanism named Teredo, which is designed for NAT users. However, Teredo does not support symmetric NAT users and cannot allocate stable IPv6 addresses for the users, it also has security problems. This paper focuses on resolving the problems of Teredo, and the proposed Silkroad protocol supports all types of NAT users to connect with IPv6 networks, can assign stable IPv6 addresses to the users and has high security.

This research is sponsored by National Natural Science Foundation of China under contract number 60273021 & 90604016.