基于 SOCKS5 的 IPv4 和 IPv6 通信方案*

段晓东,凌晓峰,沈金龙
(南京邮电学院 计算机科学与技术系,江苏 南京 210003)

摘 要:随着 Internet 的不断发展,当前的 IPv4 已经日益暴露出它的缺陷。向下一代的 IP 技术 IPv6 过渡已经成为一种迫切的需要。论述了一种通过 SOCKS5 代理进行 IPv6 和 IPv4 网络通信的方案,最后阐述了支持双协议 SOCKS5 代理服务器软件的实现和应用。

关键词:IPv4,IPv6,SOCKS5,代理
中图分类号:TN919.21 文献标识码:A 文章编号:1004-5694(2002)02-0046-05

A Communication Scheme Between IPv4 and IPv6 Based on SOCKS5 Proxy

DUAN Xiao-dong, Ling Xiao-feng, SHEN Jin-long
(*Department of computer Science & Technology, NUPT, Nanjing* 210003, *China*)

Abstract: With the rapid development of Internet, the old Internet Protocol IPv4 is getting out of date. It is necessary to shift to a new generation Internet protocol IPv6 with IP technology. This thesis discusses a scheme for communication between IPv6 nodes and IPv4 nodes with SOCKS5 proxy. In the end, the realization and application of the software supporting dual protocol SOCKS5 proxy is introduced.

Key words: IPv4, IPv6; SOCKS5; proxy

0 引 言

在过去几年里,以 IP 技术为代表的网络互联技术给传统的通信网络和计算机网络带来很大的冲击。目前使用的 IP 协议是 IPv4,但是随着网络技术的飞速发展,现行的 IPv4 协议存在着很多问题,地址短缺、设计上的性能安全性,配置复杂性和不支持移动网络等各种问题日益突出。尤其是地址短缺问题成为突出的矛盾,由此产生了下一代的 IP 协议。IPv6 是下一代因特网想采用的协议。与现行的 IPv4 相比,IPv6 在很多方面作了改进,扩大了地址空间,提高了处理速度,增强了安全保密性等。

IPv6 协议的应用越来越引起各方的关注。目前 IPv6 的发展非常迅速,IPv6 的试验网络 6bone 已经在许多国家中建立起节点,Cisco 和 Nokia 等厂商也开始推出试验产品,。很多实验网络已经建立起来了。虽然 IPv6 有明显的优势,但是如何从现在 IPv4 网络过渡到将来的 IPv6 网络是一个涉及到整个互联网的问题。目前的过渡方案有很多种。本文提出了一种通过 SOCKS5 代理来实现 IPv4 和 IPv6 网络之间通信的方案。

1 SOCKS5 代理

随着企业网络对安全性要求的提高和网络中防火墙的普遍使用,与外界相对隔离的企业 Intranet 也日益增多。内部网络要访问外部网络则需通过代

* 收稿日期:2001-11-16
作者简介:段晓东(1977-),男,山东临沂人,南京邮电学院 99 级硕士研究生,研究方向为计算机通信与网间互联技术;凌小峰(1976-),江苏吴江人,硕士生;沈金龙,教授。

理服务器。除了有一般针对各种应用服务的代理服务器外，还有 SOCKS5 这样一种通用代理协议，它可以支持各种基于 TCP 和 UDP 的应用。

一般的代理服务器，比如 HHTP 代理、FTP 代理、Telnet 代理等都是应用层级别上的代理软件，是和某种应用层协议密切相关的。SOCKS 代理与应用层代理、HTTP 层代理不同，也是一种工作在传输层的代理，并和传输层的 TCP，UDP 协议密切相关。SOCKS 代理只是简单地传递数据包，而不必关心上层是何种应用协议。所以，SOCKS 代理服务器比应用层代理服务器要快得多。

SOCKS 是 David Koblas 在 1990 年开发的。此后，就一直作为 RFC 中的开放标准。最新的功能版本 SOCKS5 协议由 RFC1928 定义。SOCKS 作为一种开放标准，与 Winsock 不同的是，SOCKS 具有平台无关性，也就是说应用程序不一定要遵循特定的操作系统平台。目前在各种操作系统上面都有 SOCKS 服务器的实现。也有很多的应用程序支持 SOCKS 代理。

SOCKS5 是 SOCKS 协议的最新版本，它在 SOCKS4 的基础上增加了支持 UDP，有效认证，以及支持域名等新功能。SOCKS5 支持 IPv6 协议栈，这对我们开发的转换网关是一个非常有利的因素。图 1 给出了一种 SOCKS5 代理常见的应用结构。其

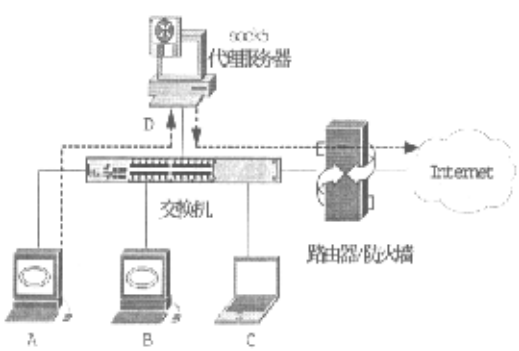

图 1　典型的 SOCKS5 代理服务器应用连接图

Fig. 1　Diagram of application connection of typical SOCKS5 proxy

中用防火墙对内网和外部 Internet 进行屏蔽。在 A、B、C、D 这 4 个主机中只有充当代理服务器的主机 D 是可以和外界直接联通的。以 A、B、C 主机为任何源地址或目的地址为 A、B 的 IP 包都被防火墙挡住。A、B、C 想要和外界通信必须经过代理服务器 D。当 A、B、C 需要访问 Internet 时便向 D 机发出请求，由 D 机和外部主机建立连接，转发请求。SOCKS5 协议本身基于 TCP。SOCKS5 代理服务器开设一个端口（缺省是 1080）作为监听，等候客户请求。客户机要访问受防火墙限制的外部站点，就要先和 SOCKS 服务器建立 TCP 连接，通过认证后，发出请求命令，然后 SOCKS 服务器和目的站点建立连接，转发传送的内容。图 1 中的虚线表示了主机 A 经过 SOCKS 服务器和外界建立连接时的数据流的走向。

2　SOCKS5 的 IPv4 和 IPv6 互联方案

利用 SOCKS5 代理服务器建立 IPv4 和 IPv6 主机通信的一种方式是将代理服务器配置成支持 4、6 双协议栈的连接主机。我们可以利用 SOCKS 协议使访问 4、6 两个网络的服务器进行两者的通信。

2.1　SOCKS5 代理基本过程

当客户需要通过 SOCKS5 代理访问外部时，要向代理发送连接请求。首先是客户连上来之后的认证方法协商过程。客户连上 SOCKS5 服务器后，进入认证方法协商。由客户端先发一个版本标志/方式选择消息，格式如下。

版本（Ver）	支持的方法数	方法列表
← 1 Byte →	← 1 Byte →	← 1－255 Byte →

其中的方法列表是客户提供的各种供选择的方法。然后服务器选择一种客户给出的方法，返回一个应答消息，格式如下。

版本（Ver）	所选方法
← 1 Byte →	← 1 Byte →

如果返回的方法为 xFF，则表示客户所列出的方法服务器一种也不支持，客户必须关闭连接。SOCKS 所支持的方法常用的如表 1 所示。

表 1　SOCKS 支持的各种方法列表

Tab. 1　List of different ways supported by SOCKS

00	01	02	80-FE	FF
无需身份认证	GSSAP I 方式	用户名/口令方式	为私有方法保留	不支持的方法

认证协商结束后，客户发送请求消息包，格式如表 2 所示。

表 2　客户请求消息结构

Tab. 2　Message from clients structure

字段名	所占字节	表示意义	值域
VER	1	版本号	x05
CMD	1	请求命令	x01-x02
RSV	x00	保留字段	
ATYPE	1	地址类型	
DST. ADDR	可变	目的地址	地址域
DST. PORT	2	目的端口号	网络字节序

其中 CMD 字段为请求命令，如表 3 所示。

表 3　CMD 请求命令字段

Tab. 3　Byte of CMD request

CONNECT	BIND	UDP ASSO.
x01	x02	x03

ATYPE 字段标识了地址类型，它的值表示了其后所含内容为下列之一：

x01　IPv4 地址，长度 4 个字节；

x03　域名，后面字段第一个字节为域名长度，然后是域名字符串，无需以 0 结尾；

x04　IPV6 地址，长度 16 个字节。

SOCKS5 服务器收到请求后进行处理，然后返回一个应答消息，格式如表 4 所示。

表 4　服务应答消息结构

Tab. 4　Structure of message reply by servers

字段名	长度	表示意义	值域
VER	1	版本号	x05
REP	1	请求命令	x00-x08
RSV	1	保留字段	
ATYPE	1	地址类型	
BND. ADDR	可变	目的地址	地址域
BND. PORT	2	目的端口号	网络字节序

其中最关键的是 REP 字段，它是服务器返回给用户的状态信息。只有在返回值为 x00 时候才表示请求处理成功。其它字段分别表示不同的返回错误。用 16 进制表示的意义如下：

x01　一般性 SOCKS 服务失败

x02　连接被规则禁止

x03　网络不可达

x04　主机不可达

x05　连接拒绝

x06　TTL 超出

x07　命令不支持

x08　地址类型不支持

x09-xFF　保留值

对于一般的 TCP 连接要求，客户端只要发一个 CMD 为 CONNECT 的请求报文就行了。对客户软件来说，它会根据自己的需要在请求报文里填上目的主机的 IP 或域名。可以从上面的连通过程中看到 SOCKS5 对 IPv6 协议的支持。在请求消息结构和应答消息结构中都已经定义了 ATYPE 为 x04 即 IPv6 地址这种地址类型。而且其后的地址字段已经为 IPv6 地址预留了空间。对于 IPv6 的地址可以同等对待。

基于上述的基本过程，我们利用 SOCKS5 协议可以设计一种 IPv6-IPv4 双协议支持 sock5 代理服务器互联方案。

2.2　IPv6-IPv4 的代理服务器通信方案的设计

运行 SOCKS5 代理的服务器必须支持 IPv4/IPv6 双协议，也就是说服务器的协议栈中必须带有 IPv4 和 IPv6 的协议支持，可以同时访问 IPv6 子网和 IPv4 子网。只有这样它才能在内外网的 IPv4 与 IPv6 之间转化。我们设计的通信网关同样要符合考虑 SOCKS5 协议的协商机制。

客户和代理服务器之间首先是一个认证的过程，这个过程和一般的 SOCK5 代理没有什么区别。认证协商之后，客户就要发送请求数据包。这个时候就要考虑到 IPv4 和 IPv6 地址的问题了。客户首先要把目的站点的地址和端口发给 SOCKS5 服务器。这里考虑 2 种情况。

(1) 发送域名和端口。域名解析过程由 SOCKS 代理服务器完成，对于客户机来说，并不知道目的站点是 IPv4 站点还是 IPv6 站点，SOCKS 代理要根据域名解析情况来判断。如果是 IPv6 地址，则通过 IPv6 协议栈和目的机器建立连接；如果是 IPv4 地址，则通过 v4 协议栈和目的机器建立连接。这也就是为什么要双协议栈支持的原因。

(2) 直接发送 IP 地址和端口。SOCKS 代理可以根据请求中的地址格式，判断地址类型，然后和上面一样通过不同协议栈和目的机器建立连接。

可以定义 SOCKS5 代理的几种方式工作，比如，只对 IPv6 节点提供代理服务，即只以 IPv6 协议栈作监听，接受连接，也可以双向工作，同时为 IPv6 节点和 IPv4 节点提供服务，作为 IPv6 节点和 IPv4 节点通信的桥梁。这时 SOCKS 代理服务器可以作

为一台双穴主机，同时加上防火墙的地址过滤、授权访问、安全记录日志等功能。

全面考虑，我们定义 SOCK5 代理是支持 IPv6/IPv4 双协议的服务器。IPv6 客户可以通过此代理访问 IPv6 服务器，同时 IPv4 客户也可通过此代理访问 IPv4 服务器。如果进行交叉访问，则需要通过域名来访问。在许多情况下，往往只能给出 IP，例如很多 Web 页面中内嵌了 IP 地址，则需要客户端也显式地支持。也就是说，IPv6 的客户端软件必须能够识别 IPv4 的目的地址，而 IPv4 客户端则需能识别 IPv6 地址。因此我们还要考虑给 SOCKS5 代理增加一个 IPv6 地址和 IPv4 地址的转换功能。我们也可以利用与 IPv4 兼容的 IPv6 地址来提供 IPv6 主机到 IPv4 主机的访问。还要在 SOCKS 服务器中建立静态映射表，来静态的完成 IPv4 和 IPv6 地址的转化。SOCKS5 代理工作流程如图 2 所示。

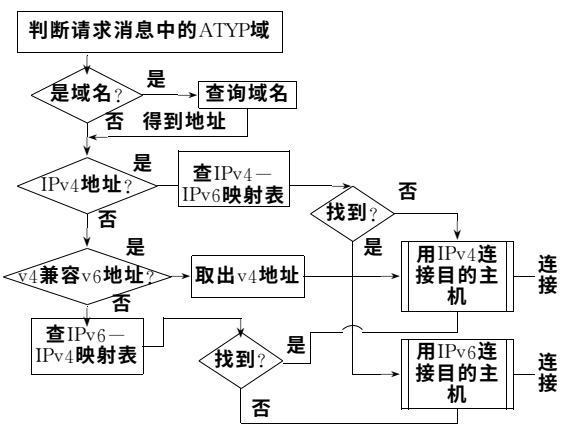

图2 IPv6－IPv4SOCKS5代理服务器地址解析流程

Fig. 2 Flow chart of address decoding by IPv6－IPv4 SOCKS5 proxy

SOCKS5 服务器首先产生 2 个 Socket 对象，分别用于 IPv4 和 IPv6 的连接和监听。当判断到不同地址的客户连接的时候，不同的对象要分别处理。对于每一对连接，都将产生 2 个 Socket 对象实例。客户来源和请求目的地址的不同产生的对象也不同。产生 2 个对象的可能情况有：都是 IPv4 Socket 对象，当源和目的都是 IPv4 主机的时候；都是 IPv6 Socket 对象，当源和目的都是 IPv6 主机的时候；一个是 IPv4，一个是 IPv6，当要建立起 IPv4 和 IPv6 节点之间连接的时候。

处理完 SOCK5 协议后，下面就交给新建立的对象来处理。这将建立起对象实例之间的对应关系。对于从网络接口接收到的数据，发送到不同的对象进行处理，再经过不同的对象发送出去。SOCKS 代理服务器工作流程如图 3 所示。

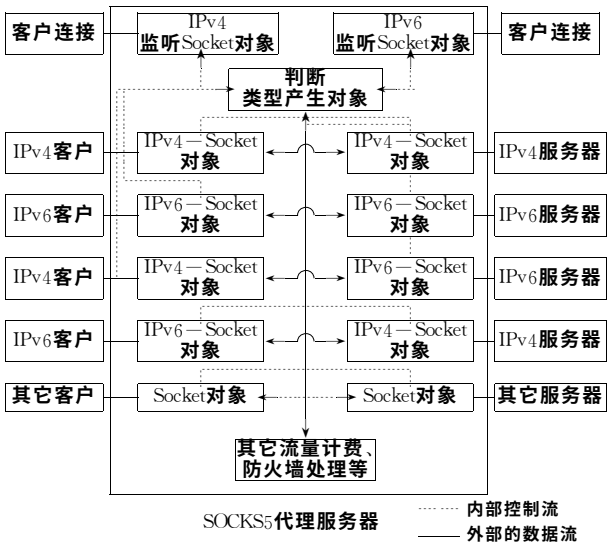

图3 SOCKS5代理器工作流程示意图

Fig. 3 Schematic of SOCKS5 work flow

采用 Microsoft Visual C＋＋6.0 作为开发平台，采用面向对象的方法和 MFC 类库框架，开发了一个 SOCKS5 双协议代理服务器软件。此代理服务器接受 IPv4/IPv6 双协议上的 TCP 连接请求，它用同一端口在 2 种协议栈上开设了 TCP 服务。同时也支持 IPv4/IPv62 种目的地址。因此，利用此代理软件可以实现 IPv6 主机访问 IPv6 主机、IPv6 主机访问 IPv4 主机、IPv4 主机访问 IPv4 主机，IPv4 主机访问 IPv6 主机 4 种访问形式。

2.3 SOCKS5 代理实现 IPv6“孤岛”通信连接

向 IPv6 升级的初期，在广大的 IPv4 的“海洋”中存在一系列的已经实现 IPv6 的网络“孤岛”。我们可以利用所建立的服务器实现这些“孤岛”和广大互联网节点之间的通信，如图 4 所示。其中代理服务器

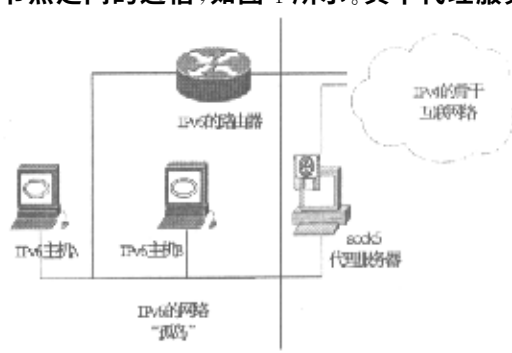

图 4 利用 SOCKS5 代理的解决“孤岛”方案示意图

Fig. 4 Schematic of "isolated island" solving scheme via SOCKS5 proxy

实现 IPv6 主机访问 IPv4 的网络访问形式。

3 结束语

上面讨论的 SOCKS5 代理方案，和其它的 IPv4 和 IPv6 互联方案相比，有很大的优势。体现在具有隔离作用，可以结合防火墙的使用，可以加入加密等安全功能；实现比较方便，可在上层实现；可作双向代理，方便地提供 IPv4-IPv6 网络的互访。但是，这个互联方案也有一定的不足之处，比如代理软件工作方式不是完全非透明的；应用软件必须支持 SOCKS5 协议；服务器上要有完全的 TCP/IPv4 和 TCP/IPv6 双协议实现；不支持 ICMP 报文等。但是从目前代理服务器及防火墙的广泛使用看来，这种 SOCKS5 代理方案作为以后向 IPv4-IPv6 过渡阶段的一种方案可行性是很大的。它不仅可以用在过渡阶段，即使过渡基本完成，IPv6 成为主流，SOCKS5 服务器仍然可以作为防火墙配套方案而继续使用。

参 考 文 献

[1] RFC 1752：The Recommendation for the IP Next Generation Protocol[S].

[2] DEERING S，HINDEN R. RFC 2460：Internet Protocol，Version 6 (IPv6) Specification [R]. 1998.

[3] LEECH M，DAVID Koblas，Ying-Da Lee，Lamont Jones，Ron Kuris，Matt Ganis，RFC 1928：SOCKS Protocol Version 5[S]. 1996.

[4] KITAMURA H. RFC 3098：A SOCKS-based IPv6/IPv4 Gateway Mechanism[R]. 2001.

[5] 凌小峰. IPv6 的过渡方案及初步应用研究[D]. 南京：南京邮电学院. 2001.

（编辑：郭继笃）

（上接 28 页）

射为 SDL 的功能块，将 OSI 的 SAP 映射为 SDL 的信道，将 OSI 的服务原语映射为 SDL 的信号。而且，该方法已经在开发第三代移动通信 TD-SCDMA 终端高层协议软件的项目中得到应用。实践证明，该方法是简洁易行和切实可靠的。当然这种方法只是仿真实现 OSI 参考模型众多方法中的一种。随着 SDL 的不断发展，SDL 的功能日趋完善，加之支持面向对象技术，可以灵活嵌入 C 代码，可以直接转换为可执行的 C 代码，以及强大的调试功能等优点，这种方法必将得到越来越广泛的应用。

参 考 文 献

[1] ITU-T Recommendation Z. 100 - Appendices I and II. SDL METHODOLOGY GUIDELINES，SDL BIBLIOGRAPHY[S]. 1993.

[2] ITU-T Recommendation Z. 100. SPECIFICATION AND DESCRIPTION LANGUAGE (SDL)[S]. 1993.

[3] GSM 04. 01. Digital cellular telecommunications system (Phase 2+)；Mobile Station - Base Station System (MS - BSS) interface General aspects and principles. version 7. 0. 0 [S]. 1998.

[4] GSM 04. 07. Digital cellular telecommunications system (Phase 2)；Mobile radio interface signalling layer 3 General aspects. version 7. 0. 0[S]. 1998.

[5] 程时端. 综合业务数字网[M]. 北京：人民邮电出版社出版，1996.

[6] 陈文云，巩丹宏. 网络通信软件设计原理及应用[M]. 西安：西安交通大学出版，2001.

[7] 朱旭红. 宽带 CDMA：第三代移动通信技术[M]. 卢学军译. 北京：人民邮电出版社，2001.

（编辑：郭继笃）