

SIP Proxy 系统中穿透 NAT 的实现

钟宝荣¹, 杜红², 涂继辉²

(1. 长江大学 计算机学院, 湖北 荆州 434023;

2. 长江大学 电信学院, 湖北 荆州 434023)

摘要: SIP 协议以其在开放性、扩展性以及 Internet 结合紧密的优势在 VoIP 应用中广泛采用, 而 NAT 是主要用来通过防火墙或者路由器使多个局域网的私有 IP 共享一个共有的 IP 的技术。介绍了 NAT 的穿透原理, 然后介绍了在 SIP Proxy 系统中穿透 NAT 的方法, 并且分析了这种方法如何和 SIP 的信令结合在一起。该方法可以大大地拓宽 VoIP 系统的应用范围, 使得在目前 IP 地址资源非常紧缺的情况下有更多的用户可以享受到 VoIP 的服务, 并已经在开发的 VoIP 系统得到了运用, 系统稳定且有效。

关键词: NAT 穿透; P2P; SIP; VoIP

中图分类号: TN915.04

文献标识码: A

文章编号: 1673-629X(2006)11-0054-02

Implementation of NAT Traversal on SIP Proxy System

ZHONG Bao-rong¹, DU Hong², TU Ji-hui²

(1. Computer College, Yangtze University, Jingzhou 434023, China ;

2. Electrical and Information College, Yangtze University, Jingzhou 434023, China)

Abstract: SIP is widely used in VoIP system newly because of the advantage of degree of open, extension and connection with Internet. NAT is a technology most commonly used by firewalls and routers to allow multiple devices on a LAN with private IP addresses to share a single public IP address. This paper introduces the concept of NAT traversal, then discusses the method of NAT traversal on SIP proxy system, and analyses how to combine this method and SIP signal together. The method discussed in the paper can enlarge the application scope of VoIP system, it makes more users can gain the service of VoIP in the case resource of IP address is lacking and it has used in the VoIP system the author developed, the system is stable and effective.

Key words: NAT traversal; P2P; SIP; VoIP

1 问题的提出

SIP(Session Initiation Protocol)协议^[1]以更加开放、更易扩展、与 Internet 紧密结合等特性, 逐渐战胜 H.323, MGCP 等协议, 成为 NGN 的核心协议。随着语音和视频业务的蓬勃发展, SIP 中的 NAT(Network Address Translators)问题已成为了基于 SIP 的 VoIP 技术在 NAT 设置的城域网和企业网推广应用中的最大障碍。

对基于 SIP 的交换系统, 要进行处理的消息有两类: 一类是信令, 即呼叫的建立和拆除的消息; 另外一类是媒体流, 即利用 RTP 进行传输的媒体消息。在基于 SIP 的 Proxy 系统中, 终端把消息交给 Proxy, Proxy 负责把消息发送到接收消息的源地址, 而如何发送到这个源地址则是需要研究的问题。

2 NAT 的穿透原理

NAT^[2,3]: 网络地址转换是在 IP 地址日益缺乏的情况下产生的, 它的主要目的就是为了解决地址重用。NAT 通信过程是简单的, 就是网络内部的节点要访问网络外部, 基本的 NAT 就负责把节点的子网内 IP 转化为一个全球惟一的 IP 然后发送出去。NAT 分为两大类: 基本的 NAT 和 NATP(Network Address/Port Translator)。

NAPT 不但会改变经过这个 NAT 设备的 IP 数据包的 IP 地址, 还会改变 IP 数据包的 TCP/UDP 端口。下面通过一个例子看看 NATP 如何穿透。比如 A 计算机的内网 IP 是 10.106.1.21, A 所在网络的外网 IP 是 202.134.2.23, A 有个进程(进程的 socket 绑定的端口 1234)想发送数据到 202.103.20.123 的 1235 端口上, 那么数据通过 NAT 的时候, NAT 会把数据包的源地址改为 202.134.2.23, 接着 NAT 会为这个传输创建一个 Session, 并且给这个 Session 分配一个端口, 比如 50000, 然后改变这个数据包的源端口为 50000。所以本来(10.106.1.21:1234 -> 202.103.20.123:1235)的数据包到了互联网上变为了(202.134.2.23:50000 -> 202.103.20.123:1235)。当

收稿日期: 2006-02-15

基金项目: 国家自然科学基金资助项目(40472080)

作者简介: 钟宝荣(1963-), 男, 江苏人, 副教授, 硕士研究生, 研究方向为计算机通信与数据库。

NAT 创建了 Session, NAT 就会记住 50000 端口对应的是 10.106.1.21 的 1234 端口,以后只要发送到 202.134.2.23 的 50000 端口的数据就会被 NAT 转发到 10.106.1.21,这样 A 就与 Server(202.103.20.123)建立一个连接。如图 1 所示。

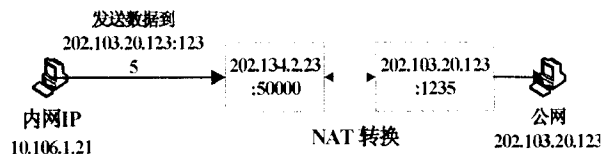


图 1 LAN 内的客户端与 Internet 的客户端的通信

如果要把一个数据从外网传给内网,则要用到一种打洞技术来完成。其原理是从内部某台主机(比如:192.168.20.10)向外部的某个 IP(比如:219.237.60.1)发送一个 UDP 包,那么就在这内网的 NAT 设备上打了一个方向为 219.237.60.1 的“洞”(这就是称为 UDP Hole Punching 的技术),以后 219.237.60.1 就可以通过这个洞与内网的 192.168.20.10 联系了(但是其他的 IP 不能利用这个洞)。

如果想要两个不同的局域网中的客户端之间能够通信,就可以利用图 2 所示的办法。

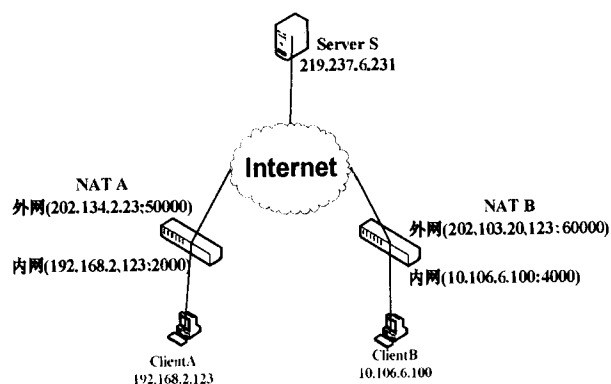


图 2 不同 LAN 内的客户端通信的穿透原理

首先,Client A 登录服务器 Server S, NAT A 为这次的 Session 分配了一个端口 50000,则 Server S 收到的 Client A 的地址是 202.134.2.23:50000,这就是 Client A 的外网地址了。同理,Client B 登录 Server S, NAT B 给此次 Session 分配的端口是 60000,则 Server S 收到的 B 的地址是 202.103.20.123:60000。此时,Client A 与 Client B 都可以与 Server S 通信了。如果 Client A 此时想直接发送信息给 Client B,Client A 可以从 Server S 处获得 Client B 的公网地址 202.103.20.123:60000。这时候 Client A 向这个地址发送信息给 Client B,Client B 也是收不到。因为这样发送信息,NAT B 会将这个信息丢弃(因为这样的信息是不请自来的,为了安全,大多数 NAT 都会执行丢弃动作)。只有在 NAT B 上打一个方向为 202.103.20.123(即 Client A 的外网地址)的洞,Client A 发送到 202.103.20.123:40000 的信息,Client B 才能收到。而这个打洞命令 Server S 来发送完成,此时 Client A 和 Client B 就可以通信了。以上的过程是适合于 NAT Cone 的情况。

3 利用 NATP 解决 SIP Proxy 的穿透

在 SIP 系统中^[4,5],终端之间在通讯之前首先要向 SIP Proxy 进行注册,也就是告诉服务器客户端的位置。注册就是发送一个 Register 的请求信令。那么这个注册过程,正好理解为是 NATP 中的打洞过程。然后,一个 SIP 终端对另外一个 SIP 终端要进行呼叫连接,就可以正好利用前面打好的洞。下面就利用 SIP 的 Register 和 INVITE 请求信令来理解 NAT 穿透过程:首先,对于一个 SIP 终端向一个 SIP Proxy 服务器进行注册,注册成功后,就利用数据库记录这个终端连接 SIP Proxy 的 IP 地址和端口号。这个过程就完成了上面所说的打洞过程。注册过程如图 3 所示。

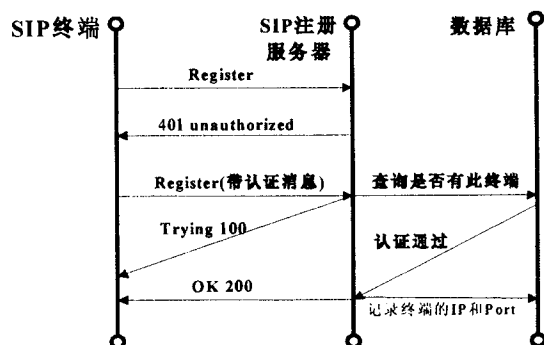


图 3 SIP 终端的注册流程

接下来,看看如何利用前面打好的洞进行 NAT 穿透。一个终端向另外一个终端呼叫(这两个终端都已经成功地注册到 SIP Proxy 上了),首先一个终端发送 INVITE 消息给 SIP Proxy,让它转发到另外一个终端。当 SIP Proxy 收到终端送来的 SIP 消息,它会先去数据库中认证这个终端,如果认证通过,那么就去找数据库查找另外一个终端注册时留下的 IP 地址和端口。这时候,SIP Proxy 就可以把 INVITE 发送到指定的终端了。这时候就成功地完成了 Proxy 的穿透。示意图如图 4 所示。

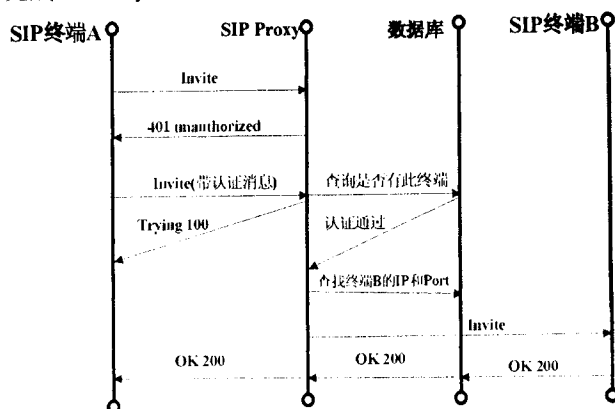


图 4 SIP 终端实现穿透的流程

4 小结

综上所述,利用上面的 NAT 穿透原理,并且结合 SIP 信令的特点,很容易实现 SIP Proxy 的 NAT 穿透。笔者

(下转第 58 页)

根据 Vapnik^[8] 等的分析,判定分类面函数的 VC 维存在如下的定理:假设训练样本完全包含在一个最大直径为 D_{\max} 的球内,不同类别样本之间的最小边际距离是 M_{\min} ,则分类面函数的 VC 维 h 满足

$$h \leq D_{\max}^2 / M_{\min}^2 + 1 \quad (11)$$

可见,SVM通过最大化边际距离 M_{\min} ,实现对 VC 维大小的控制,降低模型复杂度,从而体现 SRM 原理。

2.3 线性不可分的广义最优分类面

考虑到可能存在一些样本不能被超平面正确分类,即对线性不可分情况,可以引入松弛变量 $\xi_i \geq 0, i = 1, 2, \dots, l$,得到新的凸规划问题:

$$\begin{cases} \min & \frac{1}{2} \|w\|^2 + C \sum_{i=1}^l \xi_i \\ \text{s. t.} & y_i((w \cdot x_i) + b) \geq 1 - \xi_i \quad (i = 1, \dots, l) \\ & \xi_i \geq 0 \quad (i = 1, \dots, l) \end{cases} \quad (12)$$

求解问题(12)与求解问题(9)本质上是一样的。得到的最优超平面决策函数仍然为:

$$M(x) = \text{sgn}\left(\sum_{i=1}^l \alpha_i^* y_i (x \cdot x_i) + b^*\right)$$

对于多类线性分类问题的一种解决办法式把它转化为多个二类线性分类问题解决。 K 类分类问题可以转化为 K 个二类划分问题。其中每个二类划分都是判断样本点属于第 i 类或不属于第 i 类。

2.4 高维空间的最优分类面

对于空间 L 内非线性分类问题,可以通过一非线性变换 $\Phi(x)$,将数据 x 从原空间 L 映射到一个高维特征空间 H ,再在空间 H 建立最优分类面。这时的分类函数是:

$$M(x) = \text{sgn}((w^* \cdot \Phi(x)) + b^*) = \text{sgn}\left(\sum_{i=1}^l \alpha_i^* y_i (\Phi(x_i) \cdot \Phi(x)) + b^*\right) \quad (13)$$

这里只是用 $\Phi(x)$ 和 $\Phi(x_i)$ 代替了 x 和 x_i ,因此计算过程相同。根据 Mercer 定理知由点积定义的核必是 Mercer 核: $K(x, y) = (\Phi(x) \cdot \Phi(y))$,则上式可以化简为:

$$M(x) = \text{sgn}\left(\sum_{i=1}^l \alpha_i^* y_i K(x_i, x) + b^*\right) \quad (14)$$

这种核函数的变换处理,为支持向量机提供了极大的灵活性,使其有了更广泛的应用范围。常见的核函数类

型有:多项式核函数、径向基函数 RBF、样条核函数。

3 结 论

支持向量机是基于统计学习理论的新的机器学习方法,具有严格的理论基础,能够较好地解决小样本、非线性、高维数和局部最小点等问题,在许多问题上它有着其他统计学习方法难以比拟的优越性,支持向量机在模式识别(字符识别、文本自动分类、人脸检测、头的姿态识别)、函数逼近、时间序列预测、故障识别和预测、信息安全、电力系统及电力电子等方面都有很好的应用前景,因此成为 20 世纪 90 年代末发展最快的研究方向之一。文中深入推导了用于解决分类问题的 SVM 方法,与其它方法相比,支持向量机具有泛化性强、效率高等特点。但由于支持向量机是一种尚未成熟的新技术,它目前仍有很多局限,其最大的局限就是核函数的选择和参数的确定,虽然目前已有一些研究者对使用先验知识选择核进行了研究,但对于特定问题选择最佳的核仍是一个难以解决的问题;另一方面,支持向量机的训练速度极大地受到训练集规模的影响;此外,支持向量机对多类问题的处理能力仍有待进一步研究和改善。

参考文献:

- [1] Vapnik V. The nature of statistical learning theory[M]. New York: Springer Verlag, 1995.
- [2] Cortes C, Vapnik V. Support Vector Networks[J]. Machine Learning, 1995, 20(3): 273-297.
- [3] Cortes C, Vapnik V. Support vector networks[J]. Machine learning, 1995, 20(1): 273-297.
- [4] Haykin S. 神经网络原理[M]. 叶世伟,史忠植,译. 北京:机械工业出版社,2004.
- [5] 张学工. 关于统计学习理论与支持向量机[J]. 自动化学报, 2000, 26(1): 32-42.
- [6] 边肇祺,张学工. 模式识别(第2版)[M]. 北京:清华大学出版社,2000: 284-303.
- [7] 陈永义. 处理非线性问题分类和回归问题的一种新方法——支持向量机方法简介[J]. 应用气象学报, 2004(2): 345-354.
- [8] Vapnik V. Statistical learning theory[M]. New York: John Wiley & Sons, 1998.

(上接第 55 页)

开发的 VoIP 系统就是利用这种机制成功地完成了 NAT 穿透。经过反复的测试,此平台性能稳定,适用了各种中小营运商的需要。

参考文献:

- [1] RFC3261. SIP: Session Initiation Protocol[S]. 2002.
- [2] RFC1631. NAT: The IP Network Address Translator[S].

2002.

- [3] Collins D. VoIP 技术与应用[M]. 舒华英,李 勇,等译. 北京:人民邮电出版社,2003.
- [4] Camarillo G. SIP 揭密[M]. 白建军,彭 晖,田 敏,等译. 北京:人民邮电出版社,2003.
- [5] RFC3266. Support for IPv6 in Session Description Protocol [S]. 2002.