第16卷 第6期
2006年6月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.6
Jun. 2006

NAT 代理服务器穿透方法的研究

刘冠蓉，陈 爽
（武汉理工大学 计算机学院，湖北 武汉 430070）

摘 要：随着网络技术的日益发展，网络地址的大量消耗使得其成为一种非常宝贵的资源，尤其是在以 IPv4 为主的当今网络现状中。虽然 IPv6 技术可以根本解决这个难题，但是它的完全应用还需要一段很长的时间，因此在这种情况下 NAT 技术就应运而生。NAT 技术带来的不光是日益缺乏的网络地址的解决办法，而且还带来了更为安全的网络环境，因此使其在企业内部网中得到了广泛的应用。文中主要介绍了 NAT 技术，以及初步探讨了如何穿透 NAT 代理服务器的方法。

关键词：NAT；IP 地址端口对；NAPT
中图分类号：TP393 **文献标识码**：A **文章编号**：1673－629X(2006)06－0074－03

Research on Method of Going Through NAT

LIU Guan-rong, CHEN Shuang
(Computer School, Wuhan University of Technology, Wuhan 430070, China)

abstract: With the developing of network technology, the address of network is becoming a precious resource, especially in IPv4 network. Despite the advent of IPv6 will completely solve this problem, but its total implementation needs a long time, so NAT technology appears in this situation. It not only brings the solution to the insufficiency of network address, but also a much higher rank security of network environment, so NAT has already been widely used in intranet for years. This paper mainly states what is NAT and its terms, and tries to find ways to get through NAT proxy for host behind different NAT proxy.

Key words: NAT; pair of IP address and port; NAPT

1 NAT 技术

NAT 的全称是网络地址转换(network address translate)[1]。从其字面上的意思来理解，可以猜测到这种技术肯定和网络地址是相关的，其实按照笔者的理解来看，NAT 的中心思想就是将非法的或者是没有经过注册的网络地址翻译成合法的经过注册的网络地址。所谓的非法的网络地址一般是指私有局域网内部的网络地址，这些地址是没有经过网络管理机构注册的，直接用它们来访问外部网络(Internet)是不行的；合法的网络地址也就是经过注册过的，它们通常是公共网络上的地址，这些地址都可以直接地访问 Internet[2]。前面提到过，NAT 技术的目的就是为了解决网络地址缺乏的困扰，它的原理，其实就是把内部局域网的网络地址转换成公网的网络地址，从而实现了内部局域网内的主机也可以接入 Internet 的目的，前提是不再需要为内部局域网的每一台主机都申请一个合法的网络地址，因此用这种方法便可以节省大量的网络地址空间。NAT 工作的原理如图 1 所示。

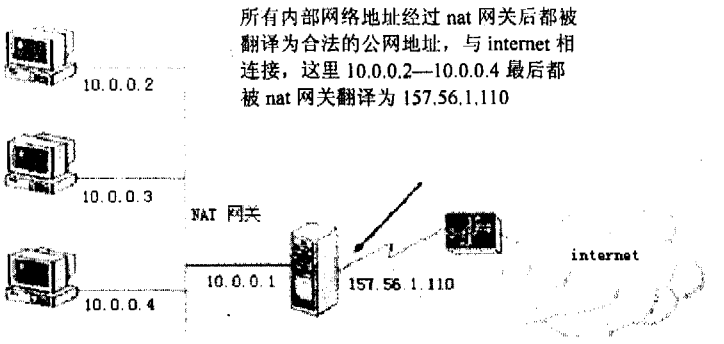

图 1 NAT 工作原理图

NAT 可以大致分为 3 种：静态 NAT、动态 NAT、动态端口 NAT。

1.1 静态 NAT

静态 NAT[1]就是 NAT 网关内每台主机都有一个与之相对应的公网 IP，每当内网主机向公网发送 IP 数据报的时候，当数据报经过 NAT 网关，NAT 网关会把 IP 数据报中的源 IP 地址修改为一个惟一的和该主机内网地址对应的公网 IP 地址，这种映射关系是固定的，而且是一一对应的，就是说内网里面有多少台主机，那么在 NAT 网关处就应该有相同数目的公网 IP 地址，而且每个公网 IP 地址都惟一对应内网中一台主机的 IP 地址。其实这种方法并没有体现出对 IP 地址的节省来，因为它为内网中的每台主机都申请了一个合法的公网 IP，但其优点是可以对

收稿日期：2005－10－03
作者简介：刘冠蓉(1946－)，男，重庆人，副教授，研究方向为计算机网络、分布式计算。

内部网络提供很好的安全保护作用,而且采用这种方法实现的 NAT 网关所需的技术难度也比较低,比较容易实现。

1.2 动态 NAT

动态 NAT[1]技术是相对静态 NAT 技术来说的,它们的实现思想大体上差不多。它也是为 NAT 网关内的每一台主机都映射一个公网上的合法 IP 地址,但是这里它们的对应关系并不像静态 NAT 那样一一对应,而且 NAT 网关处的公网 IP 地址的数目也不一定与内网的主机数相同,一般情况下它的数目会小于等于内网主机的数目。其实动态 NAT 最关键的地方是它引入了 IP 池这个概念,在 IP 池中存放着一定数量的合法 IP 地址。当内网主机向公网中的节点发送 IP 数据报时,在数据报抵达 NAT 网关后,NAT 网关会从 IP 池中取出一个公网 IP 地址,然后将此 IP 地址与这个数据报的源地址形成一个映射关系,修改数据报中的源 IP 地址,最后发送至公网上,当此主机完成其通信后,NAT 网关会根据相关的更新映射的算法将不再需要的 IP 映射关系解除,然后将公网 IP 重新放入 IP 池中,以供其他的内网主机使用。当 IP 池中的 IP 地址都被使用时,NAT 网关对于到来的内网数据报可能采取使其等待的方式或者是丢弃。

1.3 动态端口 NAT

前面提到的两种方法其实在实际应用中用的很少,它们只是用在一些比较特殊的场合,在此笔者认为它们多多少少有些违背 NAT 技术的宗旨:节省 IP 地址空间。而动态端口 NAT(NAPT)[1]就很好地体现了这个宗旨,现在 NAT 设备普遍都是采用这种方法。它与前面两种方法的最大的区别在于,在 NAT 网关处只有一个对外的公网 IP 地址,也就是说内网中的所有的 IP 数据报都是通过把源 IP 地址修改为这个公网 IP 地址而出去的,那么怎么区分来自不同主机的数据报呢? 因为笔者始终都是使用一个公网 IP 地址,在此主要运用 IP 协议的上层 UDP 和 TCP 协议中端口的特性[3],就是用端口来区分来自不同主机的 TCP 或者 UDP 数据报。在 NAT 设备中会有一张 IP 地址和端口对的映射表,它的具体形式可表现如下:

内网	公网
192.168.0.1:3000	→202.234.34.1:4000
192.168.0.2:5000	→202.234.34.1:6000
……	

当某个 TCP(或者 UDP)数据报经过 NAT 网关时,那么网关会检测这张表,检索表中内网部分的信息是否和数据报中包含的源地址信息有相匹配的,如果有则重新刷新表中该行公网部分的信息,否则插入一条新的记录到表中,NAT 会为每个 UDP 或者 TCP 的会话产生一个端口与之相对应。

2 UDP 数据包穿透 NAT 代理或防火墙的方法初探

现在网络环境中大量使用的还是传统的 NAT 设备,所谓传统的 NAT 就是指:对于允许数据包的通过具有单向性,这里的单向性并不是指数据包的流向只是一个方向,而是指只能由内网主机主动向公网发送数据包,而公网上的主机则不行。下面以图 2 为例来说明这个特性。

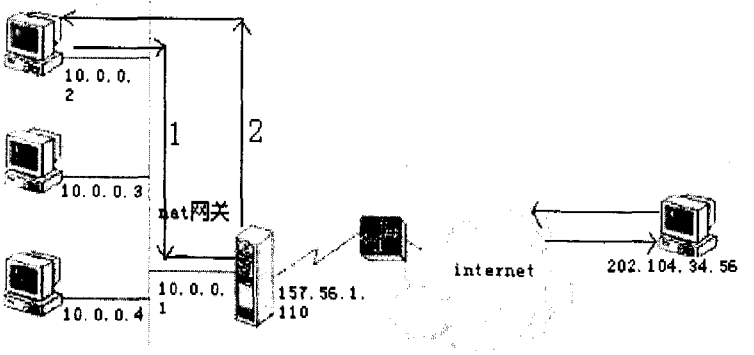

图 2　NAT 原理实例图

如图 2 所示,内网主机 10.0.0.2 主动访问公网主机 202.104.34.56,它使用 UDP 端口 2000 访问 202.104.34.56 的 1000 端口号,当第一个 UDP 数据报到达 NAT 网关的时候,NAT 网关就分配一个端口号给 10.0.0.2:2000,并形成一个映射关系,即 10.0.0.2:2000→157.56.1.10:3000 并将这条记录记入表格中,这样以备 202.104.34.56 发送的回应数据包能够顺利地通过 NAT 网关,这条映射记录一直会保持到这两台主机通信完毕为止。如果反过来由公网主机主动访问内网主机,那么传统的 NAT 网关根本就不会接受首先来自公网的数据报,并且也不会在表格中建立一个合法的映射关系,它所能做的就是丢掉该数据报,因此处于公网上的主机是不可能主动访问到 NAT 内网的主机,除非它是作为对内网主机请求的回应才可以。由于传统 NAT 设备的这种单向性特点,它对 NAT 内网起到了一个天然屏障的作用,但同时它却又给一些网络应用带来了不小的麻烦[4]。

这里主要探讨一下位于 2 个不同 NAT 网关后面的主机如何取得通信,由于传统 NAT 的特性,想让这 2 个分别位于不同 NAT 网关后面的主机直接通信几乎是不可能的(以图 3 来说明这一点)。

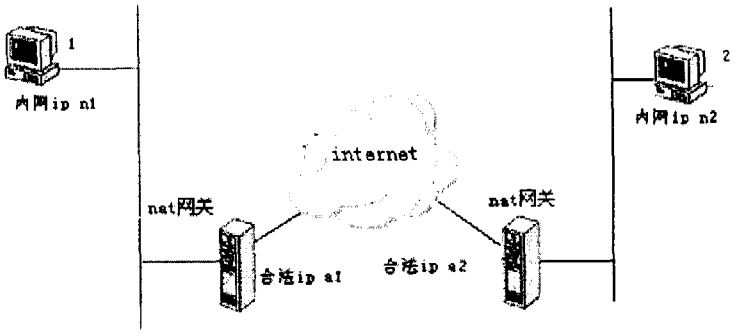

图 3　NAT 下主机通信图

如图 3 所示,现在 1 号主机要与 2 号主机进行通信,2

号主机所使用的 IP 地址是不合法的内网地址,因此不可能用 2 号主机的 IP 地址来进行数据报的传送,现在假设 1 号主机已经知道 2 所在 NAT 网关的公网 IP,此时 1 以 a2 为目标地址向外发送数据报,当 NAT 网关 a2 收到这份数据报时,发现该数据报是从地址 a1 发送过来(经过 NAT 网关 a1 转换),但此时 NAT 网关 a2 的表中并没有任何关于地址 a1 的记录,所以它会选择丢弃该数据报,同理,如果 2 直接给 1 发送数据也会是同样的结果。所以这里就存在一个对 NAT 网关穿透的技术问题。

方法 1:可以使用应用层网关技术来解决(ALG)。ALG 实际上就是放在 NAT 设备上基于应用层的一些程序的集合,通过这些程序可以根据需要来改变 NAT 设备的行为规则,比如图 3 中的主机 1,那么可以在 NAT 网关 a2 上面加上 ALG 程序,使得其判断如果收到数据报的源地址是地址 a1 并且端口是某个值的话,不管表里面是否有符合的记录,都把它的目的地址转换为主机 2 的地址,以及端口的转换,然后再将数据报发送给主机 2。这种方法是最直接的,但是却存在很多问题,首先是现在网络环境中的大多数 NAT 设备都是以前生产制造的,很多都不支持应用层网关(ALG);其次是需要针对每一种情况都制定一些特定的转换规则,这样实现起来工作量是相当繁重的,所以这个方法并不是最理想的。

方法 2:UDP 包轰炸技术[5]。这种技术需要在公网上配置一台服务器,它的作用主要在于握手,就是在通信之前,事先让通信双发知道彼此对方在 NAT 设备上的映射地址和端口,通过图 4 来进行说明。

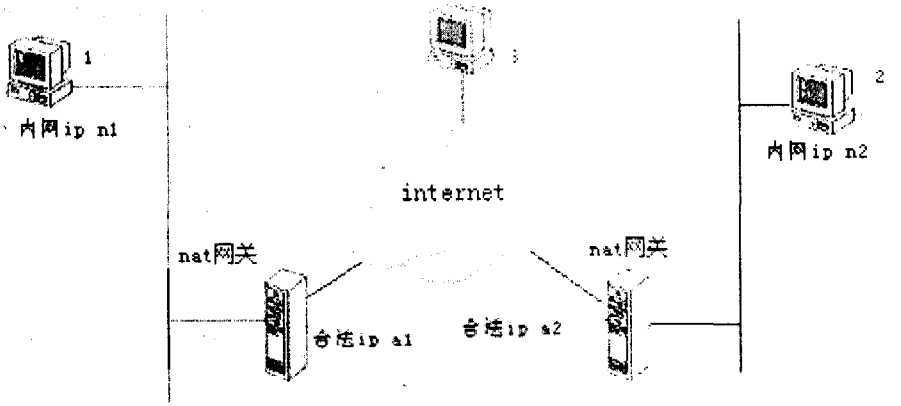

图 4 UDP 穿透方法图

由于传统 NAT 设备的特性,1 和 2 都是可以直接与 3 进行通信的,那么在 1 和 2 建立通信之前,1 先向 3 发送数据报,经过 NAT 网关地址转换后其数据报的源地址为 a1,端口为 p1,此时 3 便将这两个数据记录到自己的数据库中,同理 2 也向 3 发送相同格式的数据报,3 将 2 经过 NAT 网关转换后的地址 a2 和端口 p2 记录到数据库,然后 3 会将记录到的关于 2 的地址和端口返回给 1,同时也将 1 的地址和端口返回给 2(注意:此时由 3 返回给 1 和 2 的数据报是可以穿过 NAT 网关的,因为 NAT 网关的表中已经有了相应的映射记录)。因此经过这 2 个过程以后,1 和 2 就分别知道了对方在其 NAT 网关上的映射地址和端口,但由于双方的 NAT 网关上目前都还没有对方相对应的映射记录,所以现在还是不能够建立通信。那么后面 1 和 2 要做的就是同时向对方发送 UDP 数据报,这里 1 和 2 所使用的端口必须是和先前与 3 通信时使用的端口号一致,这点是非常重要的。以 1 为例来说明这个过程:1 以事先知道的 a2:p2 地址和端口为目的地发送一份 UDP 数据报,经过 NAT 转换后它到达了 NAT 网关 a2,此时由于 a2 中并没有对应的映射记录,a2 选择丢弃该数据报,虽然 a2 把数据报丢掉了,但是在 NAT 网关 a1 里面却记录下了一个映射关系:n1:pn1→a1:p1→a2:p2,这意味着,只要源地址来自于 a2:p2 目标地址指向 a1:p1 的 UDP 数据报就可以穿透 NAT 网关 a1 并且最终到达 1,同理 2 也采用了相同的方法使得 NAT 网关 a2 上面也有了类似的映射的记录,因此 1 和 2 就可以很顺利地与对方进行通信。这种方法最关键的地方在于首先获得对方在公网上的 IP 地址和端口,然后采取尝试发送数据的方式欺骗 NAT 网关使其在映射表中生成一条合法的映射记录。

3 结束语

NAT 技术确实给人们带来了更为安全的网络环境以及最大限度地节省了网络地址空间,特别是大大提高了与外部网络连接的企业内部网的安全性。但由于 NAT 的特性,也给局域网络的一些应用带来了不便,比如就会出现文中所提及的穿透问题,虽然最终可以得到解决,但是还是需要在公网中配置一台“握手”服务器,考虑到成本毕竟并不是所有的企业都愿意这样去做,因此此法在实际运用中的效果还有待考证。

参考文献:

[1] Srisuresh P, Holdrege M. RFC 2663, IP Network Address Translator (NAT) Terminology and Considerations[S]. 1999.

[2] Braden R. STD 3, RFC 1122, Requirements for Internet Hosts - Communication Layers[S]. 1989.

[3] Ford B. Check Your Network Address Translator for Compatibility with UDP - based Peer - to - Peer Protocols[EB/OL]. www.gridforum.org, 2003.

[4] Kegel D. NAT and Peer - to - peer networking[EB/OL]. www.alumnus.caltech.edu, 1999.

[5] Stevens W R. TCP/IP Illustracted Volume 1: The Protocols [M]. [s.l.]: Addison Wesley/Pearson, 2000.