[3] 张志涌，徐彦琴等．Matlab 教程——基于 6.x 版本．北京航空航天大学出版社，2001.
[4] 范影乐，杨胜天，李铁．Matlab 仿真应用详解．人民邮电出版社，2001.

作者简介：黄东杰（1981-），男，汉族，北京工业大学在读硕士，电路与系统专业。
作者声明：自愿将本文稿酬捐为“仪器仪表用户杂志爱心助学基金”

文章编号：1671-1041(2006)05-0130-02

现代 NAT 检测技术的原理与应用

谭 超
（吉林大学 软件学院，长春 130012）

摘 要：NAT(网络地址转换)技术是近年来随着网络及网络共享的发展而发展起来的一门新技术。它在方便网络代理者进行客户端配置的同时，也为用户私自共享上网提供了方便。通过 NAT 检测技术查找私自共享，维护网络经营者的利益势在必行。本文通过对各种 NAT 检测技术的分析、试验，提供了一种有效的 NAT 检测手段。

关键词：网络地址转换；检测技术；原理与应用
中图分类号：TP393.0 文献标识码：B

The principle and application of modern NAT detect technology

TAN Chao
(Software College of Jilin University, Changchun 130012)

Abstract: The NAT (Network Address Translation) is a newly developed technology in recent years with the advancement of network and network sharing technology. It provides convenience to both network agents in configuring clients' application and private customers in sharing network access. When searching for NAT-protected private networks, the protection of network providers is imperative. This article will introduce an effective NAT detecting method which is based on the analysis and test of various NAT technologies.

Key words: NAT; Detect technology;principle and application

1 引言

代理服务器的最主要功能就是提供共享上网服务，但由于其无法直接支持新出现的网络应用，而且对每一种网络应用都需要进行服务器端与客户端配置，客户的网络应用软件也需要支持代理服务，使用上非常不便。针对这些问题，NAT(网络地址转换)技术应运而生，NAT 技术的出现极大地缓解了 IPv4 地址空间耗尽的问题，同时也给防火墙技术带来了新的发展方向，为共享上网提供了更为方便的解决办法。

然而任何一种新技术都是一把双刃剑，NAT 为网络运营商带来方便的同时也带来了一些不可避免的问题。如多用户私自共享上网，甚至私自建立网吧经营逃避监管等。随着 NAT 技术的平民化、大众化，上述现象迅速蔓延，已经变得非常普遍，导致网络接入服务商巨额的基础建设费用难以正常回收。黑网吧的大量出现，也严重地影响了社会的稳定。因此对 NAT 检测技术的需求也越来越迫切。

2 NAT 检测技术的现状

NAT(后文均泛指 NAT 与 NAPT)的工作原理：NAT 设备工作在 OSI 网络参考模型的第三、四层，通过替换数据包的源 IP、端口及 MAC 地址，隐藏内部主机真实地址，同时 NAT 设备在其内部增加一个会话记录表，将此会话 IP、端口及原会话 IP、端口对应记录到此表中，并发送该数据包。等待目标返回数据包时做反向操作将数据包对应到内部端口，通过多台主机 IP 与端口到一台或几台主机 IP 与端口的对应，从而实现多主机共享上网。

NAT 技术的特点就是对外隐藏了内部主机的特性，从外部看如同是一台主机在访问网络。由于 NAT 技术的固有特征使得对其内部检测非常困难，只能依靠并发连接数，持续流量等相关指标从侧面分析，难以准确、可靠地判断单一 IP 接入的用户数量，使不法用户有了可乘之机。

近年来，BT、eMule 等 P2P 协议迅速发展，使得单用户上网的并发连接数与持续流量也很高，传统 NAT 检测技术的误判、漏判率极高，导致仅有的检测技术近乎失效。基于数据包 TTL 值的检测技术也随着 NAT 设备的反 TTL 检测（对通过设备的数据包 TTL 值加 1）而变得无法检测出 NAT 设备的存在。由于同种操作系统默认的 TTL 值是相同的，理论上也只能区分 NAT 设备后是否隐藏着不同操作系统的主机，而无法检测出同种操作系统的主机数量。只能作为一种辅助的检测方式而不能独立应用。

NAT 设备支持 SNMP(简单网络管理协议)，而 SNMP 存在默认的只读共同体（密码），可以用 SNMP 管理软件直接读取 NAT 设备的管理信息，从中准确地获得 NAT 设备后面隐藏的主机数，但是这种检测方法需要 NAT 设备的支持，用户可以通过对 NAT 设备 SNMP 模块密码修改、端口重定向甚至关闭 SNMP 模块等方法逃避 NAT 检测。

3 基于 TCP/IP 协议栈的 NAT 检测技术原理

通过对 TCP 数据包包头的研究发现，TCP 协议为了可靠地传输数据，使用了一个序列码字段以确定数据包发出的顺序，TCP 协议 3 次握手时发起方发出 TCP SYN 标志数据包以建立连接，此数据包的序列码称之为 ISN(初始序列码)，而后的数据包序列码逐个加 1，以便接收方能够按发送顺序恢复 TCP 包中的信息。由于 TCP 连接建立时的三次握手是必不可少的，因此每个 TCP 连接建立时都会向外发出 TCP SYN 数据包，从 TCP SYN 数据包中即可以提取出源主机的 ISN。

目前广泛使用的 WINDOWS 操作系统对 ISN 的选取采用的是一个与“时间相关”的算法，即每过一段时间 ISN 就被自动加上一个小的固定数值。这使得基于 TCP SYN 数据包 ISN 值的 NAT 检测成为可能。在 NAT 设备外部进行抓包、分析并记录 NAT 设备流出的数据包的 ISN 值可发现同一主机的 ISN 数值随时间的推移缓慢增加并成为一条连线，而不同主机之间由于起始值和流逝的时间不同，ISN 数值一般相互离散而成为数条连线。对一小段时间的数据进行统计分析即可判断出被检测流量是由一台计算机产生的还是由多台不同计算机产生的，甚至还可以根据离散连线的条数确定出 NAT 设备后隐藏的主机数目。由于序列码字段是 TCP 传输中不可缺少的，因而不存在逃避检测的可能。

进一步研究还可以发现，TCP ISN 的取值是与应用程序无关的。无论客户端使用 IE 浏览器还是 NC 浏览器，无论上层协议使用 HTTP 还是 FTP，其 TCP 的 ISN 数值都符合时间模型。由于上层应用软件发送和接收数据包都必须使用操作系统提供的 API 接

收稿日期：2006-05-29

口，而 ISN 的取值完全由操作系统根据系统的内部状态产生，因此基于 TCP ISN 的 NAT 检测不受上层应用程序的种类和应用程序并发连接数的影响。而不同操作系统生成 ISN 的算法一般不同，因此在实际应用中要先采用目前较为成熟的远端操作系统辨别技术区分出不同的操作系统排除干扰或在统计分析时去掉那些离散的、不符合时间相关模型的采样点。

4 NAT 设备的预检测方法

TCP 连接数方法：普通用户上网时单个操作系统打开的 TCP 连接数通常不会超过某一数值（例如 20），某个 IP 地址经过 NAT 设备共享后由于多用户同时上网，从 NAT 设备外部跟踪该 IP 地址的打开连接数会大于这个数值，通过设置门限值，对超门限值的网络用户进行进一步检测。

最小持续带宽方法：单一用户上网对数据传输的操作是随机的，大部分时间是没有网络流量的。多人同时共享上网时根据统计原理，网络的流量不再具有突发性，会表现出一个持续稳定的流量。据此通过设置最小持续流量也可筛选出一些可能共享网络的用户。同时需要注意用户持续传输大文件时该方法会产生误判。

TTL 数值法：根据 TCP/IP 协议，数据包每通过一个三层网络设备 IP 包头中的 TTL 字段值会自动减 1。因此通过 NAT 设备的数据包 TTL 值会比同等条件下没有通过 NAT 设备的数据包 TTL 值小 1。在同类用户中检测 TTL 值小 1 的用户即可初步判定出 NAT 设备的存在。

5 TCP ISN 值的 NAT 检测技术实际测试结果

5.1 软件情况测试

测试环境：一条 LAN 用户线后挂接一组计算机，均通过一台安装了代理软件（SYGATE）的服务器上网，或使用 Windows 连

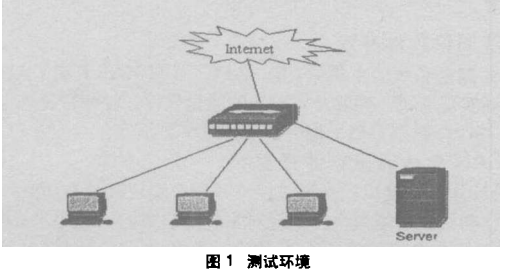

图 1 测试环境

接共享上网。测试环境如图 1。

(1)SYGATE 软件共享上网

测试结果如图 2。将 20s 内抓到的数据包 TCP ISN 数值作 X-Y 散点图后可明显看出图像趋于 4 条直线，由此可推断出 NAT 设

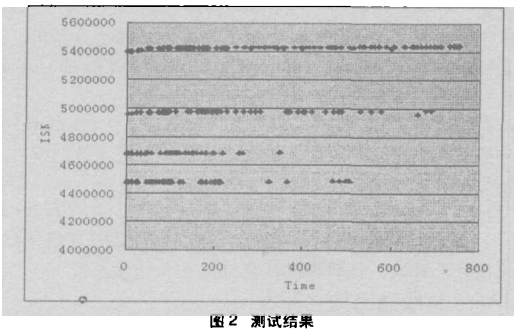

图 2 测试结果

备后隐藏的实际主机数为 4，如表 1。

(2)WINDOWS 网络共享

测试结果如图 3。将 25s 内抓到的数据包 TCP ISN 数值作 X-Y 散点图后可明显看出图像趋于 2 条直线，由此可推断出 NAT 设备后隐藏的实际主机数为 2，如表 2。

5.2 硬件情况测试

表 1

测试环境	实际机器数	检测到的机器数
SyGate 共享	4	4

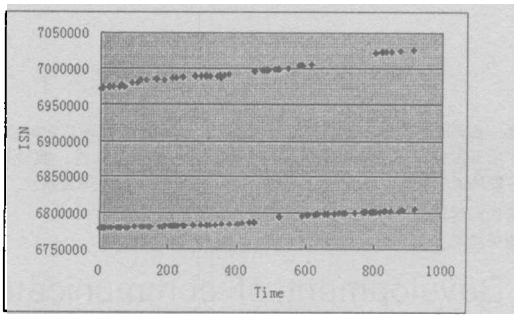

图 3 测试结果

测试环境：一组计算机通过一个路由设备开启 NAT 共享同一 IP 上网。测试环境如图 4，测试结果如图 5。

将 35s 内抓到的数据包 TCP ISN 数值作 X-Y 散点图后可明显看出图像趋于 5 条直线，由此可推断出 NAT 设备后隐藏的实际主机数为 5，如表 3。

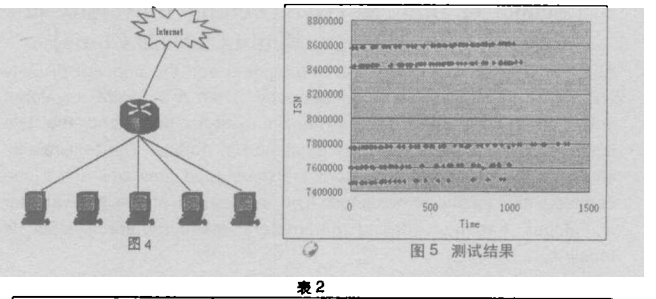

图 4　　图 5 测试结果

表 2

测试环境	实际机器数	检测到的机器数
ICS 共享	2	2

表 3

测试环境	实际机器数	检测到的机器数
硬件 NAT 共享	5	5

5.3 多台计算机分时上网测试

测试环境：一组计算机通过一台安装代理软件（Sygate）的服务器不同时上网，或该组计算机通过硬件 NAT 共享设备不同时上网。

测试结果：机器分时上网时，检测结果为当时同时上网机器数，对于采用硬件 NAT 共享上网用户，检测方法不会把 NAT 设备当成一台计算机，但安装了虚拟操作系统的设备会被当成一台计算机。

6 结束语

本文通过对传统 NAT 检测技术的分析，研究并提出了基于 TCP ISN 值的 NAT 检测原理，并在实际应用环境中予以论证。互联网络是一个庞大而复杂的系统，连接的终端数目与品种繁多，使用的操作系统多种多样，单一的检测手段很难做到一劳永逸。因此，需采用多种方法组合检测，才能达到预期效果。

参考文献

[1] 麦格雷戈．CCNP 思科网络技术学院教程．人民邮电出版社，2001.

[2] 兰少华．TCP/IP 网络与协议．清华大学出版社，2006.

[3] 史蒂文斯 W.R.TCP/IP 详解 卷 1 协议．机械工业出版社，2000.

作者简介：谭超（1985-），男，大学本科，所学专业：电子信息科学与技术。

作者声明：自愿将本文稿酬捐为“仪器仪表用户杂志爱心助学基金”