学校编码：10384
学号：X2009221031
分类号__共享级__
UDC___

厦门大学

工 程 硕 士 学 位 论 文

基于 NDIS 的网络地址转换(NAT)的设计与实现

The Design and Implementation of NAT System based on NDIS

吴德进

指导教师姓名：曲延云副教授
专　业　名　称：计算机技术
论文提交日期：
论文答辩时间：
学位授予日期：

答辩委员会主席：__
评阅人：__

2012 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　）1.经厦门大学保密委员会审查核定的保密学位论文，于 年 月 日解密，解密后适用上述授权。

（ ）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年 月 日

摘 要

近年来基于 IPv4 协议的因特网得到了蓬勃发展，无论是网络覆盖的范围与网络容量，还是网民数量与业务类型都在飞速增长。IPv4 下其可用的 IP 地址越来越少，一些解决地址危机的办法开始得以广泛使用，其中中短期解决方案——网络地址转换技术是目前最常用的解决地址短缺的有效的方法。

论文首先分析了计算机网络参考模型 TCP/IP，并对网络地址转换的原理和工作过程进行了研究，提出了在链路层之上基于 NDIS（中间层驱动）模块化插件式的的解决方案；软件由两部分组成：内核部分工作在操作系统内核层(0 层)，完成网络数据的截获、分析、跟踪、过滤、转换等功能，控制部分工作在应用层，负责与内核的通信与控制。内核部分可以对所有的进出数据全部截获，通过增加各层的封包处理模块，可以实现 2-7 层的数据分析与控制,有很大的扩展空间;同时可以在这些基础上，开发 PC 防火墙，网络嗅探器等相关软件，比如杀毒软件卡巴斯基、网络嗅探器 sniffer 等都基于 NDIS 实现。本文实现了一个动态地址转换和端口复用相结合的功能及扩展接口；同时进行了运行测试，给出真实机和 VMWare 虚拟机测试环境，测试结果说明了所提解决方案的有效性。

关键词：网络地址转换；NAT；NDIS；中间层驱动；

ABSTRACT

Recent years, Internet based on IPv4 protocol has been flourishing, whether the scope of the network coverage and network capacity or the number of Internet users and business types is in the rapid growth. So the amount of available IP address is less and less under IPv4.Some of solutions to IP address crisis begin to be widely used. NAT technology is a short term solution, and it is the most common and effective solution to the shortage of address.

The thesis firstly analysises of the computer network reference model of TCP/IP, and studys on the principles and process of Network Address Translation.

Software consists of two parts: The core part of the work in the operating system kernel layer (Layer 0), to complete the interception of network data, analysis, tracking, filtering, conversion. Control part of the work at the application layer is responsible for the kernel of communication and control. Part of the kernel can intercepted all incoming and outgoing data. Layer 2-7 data and control can be achieved by increasing the packet processing module of layers, there are a lot of room for expansion. On the basis of the development of PC firewall, network sniffer software. Such as antivirus software Kaspersky, network sniffer sniffer and so on based on NDIS. and implementates the function of joining dynamic Network Address Translation with Network Address Port Translation. Run the test at the same time, given the real machine and VMWare virtual machine test environment, test results illustrate the effectiveness of the proposed solutions.

Key Words：Network Address Translation; NAT; NDIS; Intermediate Driver;

目 录

第一章引言 1

1.1 背景 1

1.2 国内外发展现状 1

1.3 研究目的 3

1.4 开发环境及语言 3

1.5 论文结构安排 4

1.6 定义 4

第二章 NAT 的原理 5

2.1 计算机软件参考模型和 NAT 在协议栈中的位置 5

2.2 NAT 的概述 7

2.3 NAT 技术原理分析及实现 9

2.4 NAT 的技术分析 13

2.5 以太网环境下 NAPT 网关的工作流程 14

第三章 NAT 系统的功能简介 17

3.1 数据包截获模块 17

3.2 数据包分析模块 17

3.3 连接跟踪模块 17

3.4 网络地址转换模块 17

3.5 转换表管理模块 17

3.6 控制管理模块 17

3.7 扩展插件模块 18

第四章 NAT 的设计与实现 19

4.1 系统结构 19

4.2 网络数据包截获 20

4.3 数据包分析 25
4.4 连接跟踪 25
4.5 转换表管理 26
4.6 网络地址转换 28
4.7 控制管理 36
第五章系统测试 39
5.1 测试环境 39
5.2 功能测试 40
5.3 性能测试 41
第六章 总结和展望 43
6.1 总结 43
6.2 展望 43
附录一 NAT 系统核心源码 45
附录二 软件使用手册 57
1. 简介 57
2.适用对象 57
3. 性能特点 57
4. 关键技术 57
5. 架构设计方面 58
6. 安装说明 58
7. 运行环境 69
参考文献 70
致谢 72

Contents

Chapter One Introducton 1

1.1 Background 1

1.2 Development in the world 1

1.3 Research purposes 3

1.4 Development environment and language 3

1.5 Paper structure arrangements 3

1.6 Defined 4

Chapter Two The principle of NAT 5

2.1 Computer software reference model and the NAT protocol stack 5

2.2 Overview of the NAT 7

2.3 Analysis and Implementation of the principle of NAT technology 9

2.4 Technical Analysis of the NAT 13

2.5 NAPT gateway Ethernet environment 14

Chapter Three Introduction of the NAT system 17

3.1 Packet capture module 17

3.2 Packet analysis module 17

3.3 Connection tracking module 17

3.4 Network Address Translation Module 17

3.5 Conversion table management module 17

3.6 Control and management module 17

3.7 Extension module 18

Chapter Four Design and Implementation of the NAT 19

4.1 System architecture 19

4.2 Network packet capture 20

4.3 Packet analyzer 25

4.4 Connection tracking 25

4.5 Conversion table management 26
4.6 Network Address Translation 28
4.7 Control and management 36
Chapter Five System testing 39
5.1 Test environment 39
5.2 Functional test 40
5.3 Performance test 41
Chapter Sis Summary and Prospect 43
6.1 Summary 43
6.1 Prospect 43
Appendix One NAT kernel source 45
Appendix Two Software Manuals 57
1. Introduction 57
2. Applicable 57
3. Performance characteristics 57
4. Key technologies 57
5. Architecture design 57
6. Installation Instructions 58
7. Operating environment 69
Acknowledgements 70
References 72

第一章 引言

网络地址转换(Network Address Translation 简称 NAT)最初是为了解决 Internet 上 IP 地址资源枯竭的问题而提出的，然而，由于它在客观上使得内部网络的信息对外部网络不可见。所以，它逐渐成为一项重要的网络安全技术。[4] [16]- [22] 目前,很多的操作系统都把这项技术集成到系统中。本文描述如何利用 Windows 2003 系统提供的网络驱动体系来方便地实现 NAT。

1.1 背景

近年来，Internet 技术日趋成熟，已经开始了从以提供和保证网络连通性为主要目标的第一代 Internet 技术向以提供网络数据信息服务为特征的第二代 Internet 技术的过渡。作为全球范围最大的信息网，Internet 自身协议的开放性极大地方便了各种计算机联网，拓宽了共享资源。但是，由于在早期网络协议设计上对安全问题的忽视，以及在使用和管理上的无政府状态，逐渐使 Internet 自身的安全受到严重威胁，与它有关的安全事故屡有发生。网络地址转换 NAT (Network Address Translation)技术可以使内部局域网络通过一个合法 IPv4 地址来响应外部网络的寻址。它提供了一种掩饰网络内部本质的方法，为保护本地局域网安全提供了保障，因此在局域网中得到了广泛的应用。另一方面，由于使用 NAT 使得本地局域网可以通过一个外部合法 IPv4 地址访问 Internet，这可以极大地节省 IPv4 地址资源。[3]-[8]由于 Internet 网络发展迅猛， IPv4 网络 IP 地址已经接近枯竭，目前，短时间内 Internet 网络不可能完成 IPv4 到 IPv6 的过渡，为了缓解 IP 地址资源紧张现状，我们暂时必须采用 NAT 网络地址转换技术来解决这一难题。它可以使 Internet 网得到足够的喘息时间来等待新一代 IP 协议的普及。

1.2 国内外发展现状

NAT 作为一种实用的技术，它的实现方法不是单一的。它的实现方法一般有以下几种：（1）基于硬件实现的独立的 NAT 设备。（2）集成在网络防火墙中，成为其

中的一个功能模块。(3)集成在操作系统中，通过用户配置来实现的 NAT 功能。(4)在边缘路由器上实现。

NAT 有三种类型：静态 NAT(StaticNAT)、动态地址 NAT(PooledNAT)、网络地址端口转换 NAPT（Port－LevelNAT)。[24]-[30]

其中静态 NAT 设置起来最为简单和最容易实现的一种，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。而动态地址 NAT 则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，三种 NAT 方案各有利弊。

动态地址 NAT 只是转换 IP 地址，它为每一个内部的 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号，对于频繁的远程联接也可以采用动态 NAT。当远程用户联接上之后，动态地址 NAT 就会分配给他一个 IP 地址。用户断开时，这个 IP 地址就会被释放而留待以后使用。

网络地址端口转换 NAPT（Network Address Port Translation）是人们比较熟悉的一种转换方式。NAPT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

在 Internet 中使用 NAPT 时，所有不同的信息流看起来好像来源于同一个 IP 地址。这个优点在小型办公室内非常实用，通过从 ISP 处申请的一个 IP 地址，将多个连接通过 NAPT 接入 Internet。实际上，许多 SOHO 远程访问设备支持基于 PPP 的动态 IP 地址。这样，ISP 甚至不需要支持 NAPT，就可以做到多个内部 IP 地址共用一个外部 IP 地址上 Internet，虽然这样会导致信道的一定拥塞，但考虑到节省的 ISP 上网费用和易管理的特点，用 NAPT 还是很值得的。

目前很多厂商推出了带有 NAT 功能的路由器或网关产品，这些硬件 NAT 设备能够提供高效的地址转换和高速的网络连接，但是价格昂贵并不适合中小企业和家庭上网。与硬件 NAT 对应，许多厂商开发了软件 NAT，这种软件 NAT 作为插件运行在 PC 机或服务器的操作系统之上，这种方式的 NAT 虽然性能与硬件 NAT 有一定差距但是价格低廉，更多的得到了中小企业和家庭用户的采用，目前主要的软件 NAT 有

Windows 平台上的 sygate、wingate 和 Linux 平台上的 IPtable 等。在现有的 NAT 的软件基本上都是在网络及以上层来实现的，总体上能满足中小型局域网的要求。但是由于是在网络层及以上层实现的，相对处理速度会慢一些。而本系统将直接在网络层以下来实现，数据包的处理、路由等都由软件自身来解决，不需要经过网络层，大大的加快了速度。

1.3 研究目的

本课题旨在解决目前网络 IP 地址短缺的问题，同时它能增加网络的安全性。对于比较大的局域网环境，如果经济允许，可以使用路由器来实现（路由器通常有 NAT 模块），当然也可以用本软件来实现；而对于小型局域网，如学生宿舍、多电脑的家庭使用本软件是最佳选择，从经济角度上省去买路由器的开支，从技术角度上不是每个人都能配置路由器，但是，只要你会装应用程序就能配置本软件。同时本软件的扩展空间非常好，可以增加防火墙，网络嗅探器等模块以满足不同的应用环境。

1.4 开发环境及语言

1.4.1 Microsoft.Net 开发平台

.Net 开发平台的发布标志着近十年来微软开发平台第一个重大的转变。这个开发平台包括一个用于加载和运行应用程序的新的软件基础（.NetFramework），新的开发环境（Visual Studio.Net），以及支持该结构的编程语言。

1.4.2 Microsoft Drive Development Kit (DDK) 2003

DDK 是 Windows 平台下，驱动程序的开发包，是开发 Windows 平台下驱动程序的必备工具。[1]-[3]

1.4.3 开发语言 C 和 VC++

做底层驱动开发 C 语言是首选语言，它与运行速度有着密不可分的关系。运行在底层的驱动程序，要有很高的运行效率，而 C 语言与生俱来就有这个能力，它能

直接对底层硬件进行操作。所以用 C 语言来开发 NAT 的内核部分。[1]-[3]

而在内核与应用层通信的模块，用 C++写具有更高的可读性和可扩展性，所以用 C++来开发 NAT 的应用层管理模块。

1.5 论文结构安排

本文共分六章，具体结构安排如下：

第一章：绪论。阐述了本课题的研究背景及意义，分析了国内外研究现状及开发平台。

第二章：研究了计算机网络参考模型 TCP/IP 及 NAT 的原理及在协议栈的位置，分别介绍了几种 NAT 技术的原理和对 NAT 的实现形式化模型。

第三章：NAT 系统功能简介，各模块的简要介绍

第四章：提出了 NAT 设计与实现的整个结构框架，并分别对各个模块的具体实现进行了说明，给出关键程序和流程图；然后详细说明 TCP、UDP、ICMP 数据报文的实现

第五章：对软件进行测试，并给出测试结果分析报表

第六章：总结本文研究内容以及存在问题和进一步展望。

1.6 定义

NAT: Network Address Translation(网络地址转换)

NDIS: Network Driver Interface Specification(网络驱动接口标准/规范)

DDK: Driver Development Kit (驱动程序开发包)

第二章 NAT 的原理

首先介绍计算机网络的软件协议模型即应用最多的 TCP/IP 协议模型，明确 NAT 协议在协议栈中的位置，介绍 NAT 的概念、类型和建立连接的原理以及数据通信原理。

2.1 计算机软件参考模型和 NAT 在协议栈中的位置[4]-[9]

计算机网络技术是计算机技术和通信技术的有机结合的产物，也被称为数据通信。计算机网络的硬件设施主要包括了局域网（LAN）、城域网（MAN）、广域网（WAN）、无线网和互联网。这里主要讨论网络的软件参考模型。目前用得最多的是 TCP/IP 参考模型，TCP/IP 参考模型如图 2-1 所示：

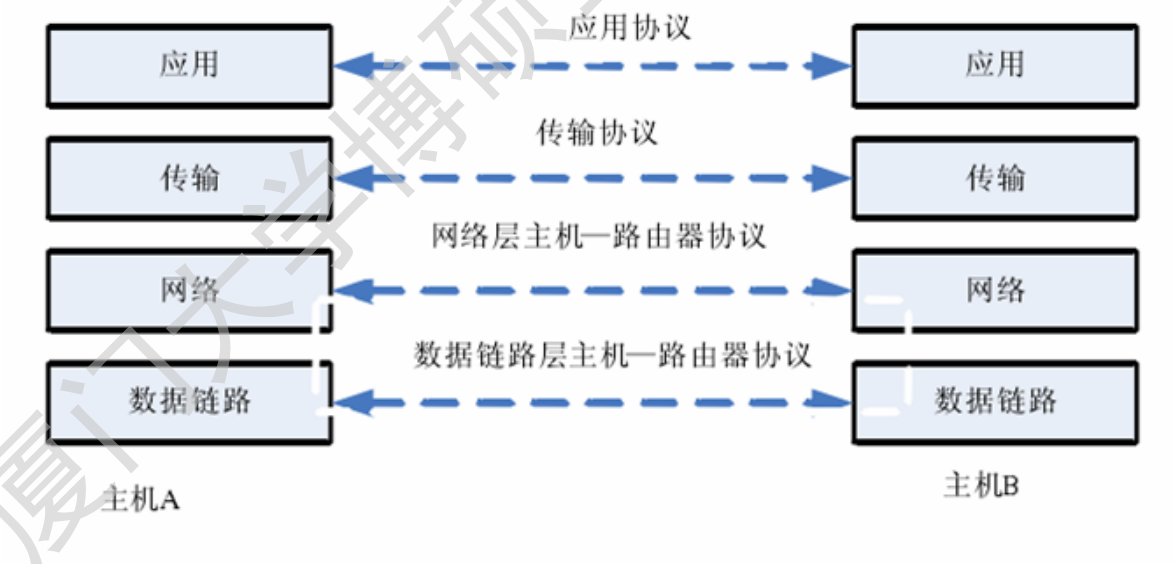

图 2-1 TCP/IP 参考模型

在上图中，每一层负责不同的功能：

（1）数据链路层

链路层，有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

(2) 网络层

网络层，有时也称作互联网层，处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（网际协议），ICMP 协议（Internet 互联网控制报文协议），以及 IGMP 协议(Internet 组管理协议)。

(3) 运输层

运输层，主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于运输层提供了高可靠性的端到端的通信，因此应用层可以忽略所有这些细节。而另一方面，UDP 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端。任何必需的可靠性必须由应用层来提供，这两种运输层协议分别在不同的应用程序中有不同的用途。

(4) 应用层

应用层，负责处理特定的应用程序细节。几乎各种不同的 TCP/IP 实现都会提供下面这些通用的应用程序：

- Telnet 远程登录。
- FTP 文件传输协议。
- SMTP 简单邮件传送协议。
- SNMP 简单网络管理协议。

在 TCP/IP 的协议族中有很多种协议，TCP/IP 协议中的协议层次如图 2-2 所示。NAT 协议是一个嵌套在网络层和运输层之间的协议。NAT 协议不仅仅处理网络层的 ICMP 报文，而且处理 TCP/UDP 报文同时还要处理特殊的用户进程。所以 NAT 协议的研究和实现需要熟悉网络层和传输层的背景知识，通过一些特殊的处理让 NAT 协议能够尽量多的穿透 TCP/IP 协议栈。

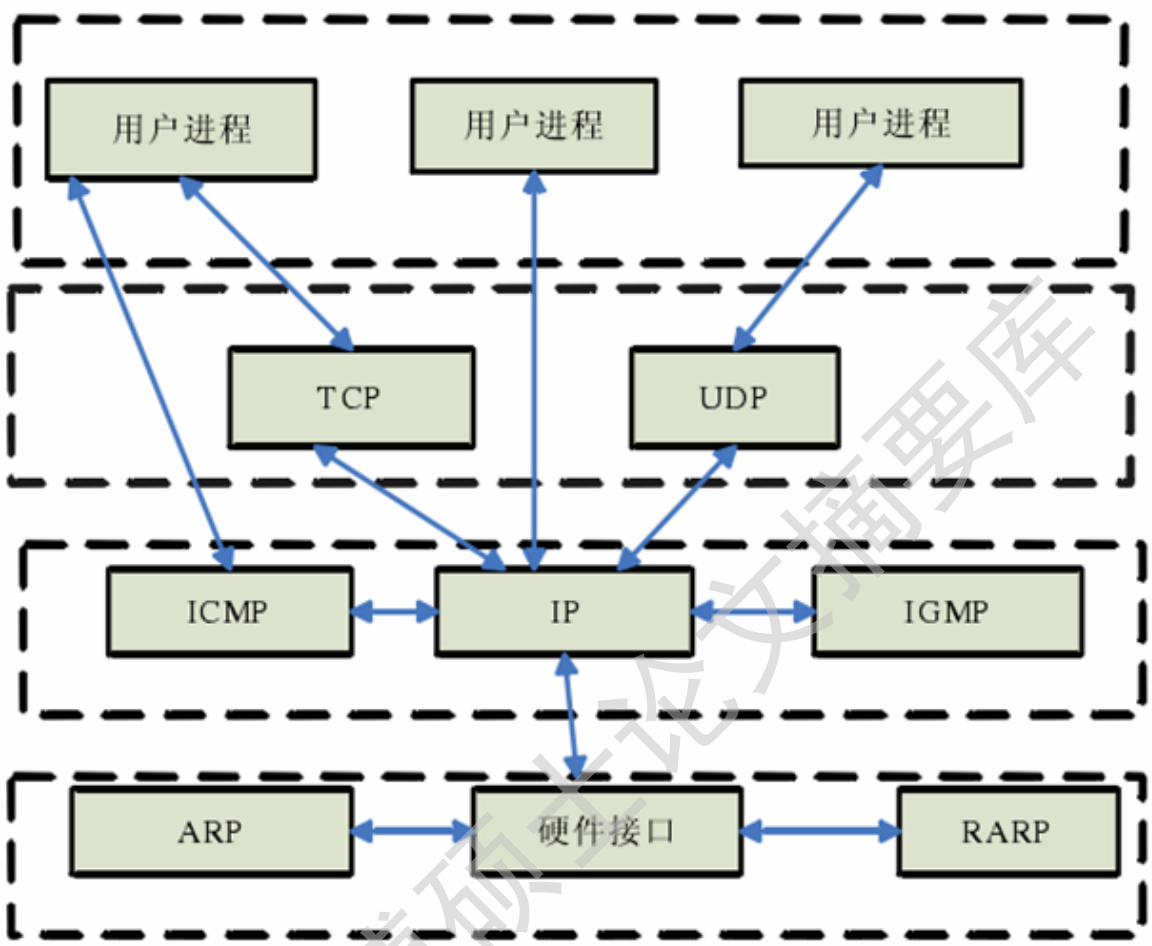

图 2-2 TCP/IP 协议族的四个层次

TCP 和 UDP 是两种最为著名的运输层协议，二者都使用 IP 作为网络层协议。虽然 TCP 使用不可靠的 IP 服务，但它却提供一种可靠的运输层服务。UDP 为应用程序发送和接收数据报。一个数据报是指从发送方传输到接收方的一个信息单元（例如，发送方指定的一定字节数的信息）。但是与 TCP 不同的是，UDP 是不可靠的，它不能保证数据报能安全无误地到达最终目的。域名系统、TFTP（简单文件传送协议）、BOOTP（引导程序协议）、SNMP 等都是使用 UDP 的应用程序。

2.2 NAT 的概述

1981 年 9 月 IETF 公布了 IPv4 协议的规范 RFC791。1983 年 1 月 1 日 TCP/IP 成为 APRANET 上唯一正式的协议后，APRANET 上连接的网络、机器和用户以每 18 个月翻一翻的速度快速增长。到目前为止，网络已经发展为仅路由器就以亿为单位来计算的庞大规模。[4]