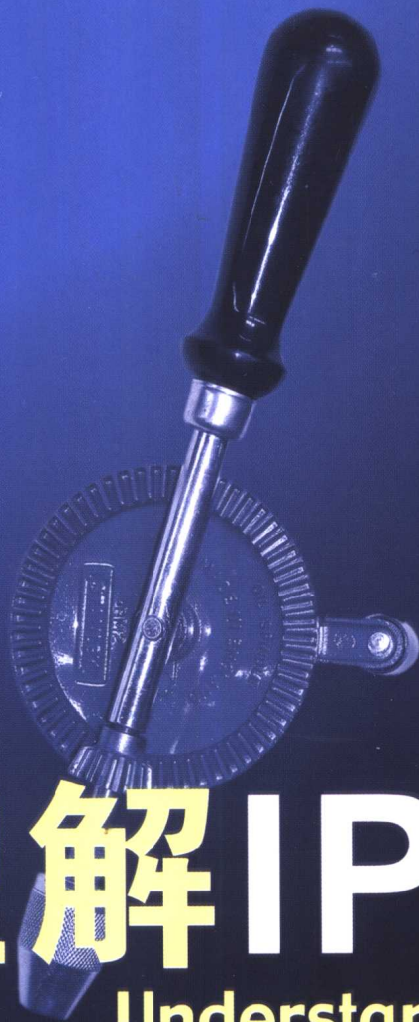


(美) *Joseph Davies* 著



理解 IPv6

Understanding IPv6

张晓彤 晏国晟 曾庆峰 译



清华大学出版社

理解 IPv6

(美) Joseph Davies 著
张晓彤 晏国晟 曾庆峰 译

清华大学出版社
北 京

内 容 简 介

Internet 协议版本 6(IPv6)是 IP 协议的最新版本,可以改善和弥补 IPv4 的固有缺陷。

本书讨论了 IPv6 的概念、原理和作用过程,以及 Windows .NET Server 2003 系列的操作系统如何支持 IPv6。主要内容按逻辑排列,包括 IPv6 的特性和优势、网际控制报文协议版本 6(ICMPv6)、邻节点发现和多播侦听发现、地址自动配置、IPv6 域名解析和路由、共存和移植以及移动 IPv6 等。本书还以附录的形式提供了一些帮助读者更好地理解 IPv6 的内容。

本书适合对 IPv6 的重要性及其工作原理感兴趣,并准备使用 IPv6 联网技术的网络管理员、工程师、技术人员和学生阅读。

理解 IPv6

Understanding IPv6(ISBN 0-7356-1245-5)

Joseph Davies

Copyright © 2003 by Microsoft Corporation

Original English Language Edition Copyright © 2003 by Microsoft Corporation.

Published by arrangement with the original publisher, Microsoft Press,
a division of Microsoft Corporation, Redmond, Washington, U.S.A.

本书中文版由 Microsoft Press 授权清华大学出版社出版。

北京市版权局著作权合同登记号 图字:01-2001-3500

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

理解 IPv6/(美)戴维斯(Davies,J.)著;张晓彤,晏国晟,曾庆峰译.—北京:清华大学出版社,2004

书名原文:Understanding IPv6

ISBN 7-302-08045-3

I.理… II.①戴…②张…③晏…④曾… III.计算机网络—传输控制协议 IV.TN915.04

中国版本图书馆 CIP 数据核字(2004)第 006838 号

出 版 者:清华大学出版社

<http://www.tup.com.cn>

社总机:010-62770175

地 址:北京清华大学学研大厦

邮 编:100084

客户服务:010-62776969

文稿编辑:马云艳

封面设计:陈刘源

印 刷 者:北京世界知识印刷厂

装 订 者:北京市密云县京文制本装订厂

发 行 者:新华书店总店北京发行所

开 本:185×230 印张:25.5 字数:617 千字

版 次:2004 年 3 月第 1 版 2004 年 3 月第 1 次印刷

书 号:ISBN 7-302-08045-3/TP·5823

印 数:1~4000

定 价:43.00 元

前 言

本书讨论了 IPv6 的概念、原理和过程，以及 Windows .NET Server 2003 系列的操作系统如何支持 IPv6。这些讨论的主要对象是协议和过程，而不是规划、配置、部署和管理。同样，这些讨论大部分是针对 IPv6，而不是 Windows .NET Server 2003 的特定实现。因此，本书没有包含 Windows .NET Server 2003 系列中的 IPv6 协议的详细实现细节，如结构、表、缓冲区或编码逻辑。这些细节都是微软公司严加防守的知识产权，只有为数不多的软件开发者才会对此感兴趣。

本书的主旨在于提供一种教学手段，使读者对 IPv6 的技术方面有更多的了解——包括术语、地址、协议和过程。因此，本书并不打算谈论 IPv6 的市场前景及其如何“通过集成的、可交互的技术来引领个人和企业计算进入新纪元”。我会将这种类型的工作留给比我更精于此道的人——毕竟，我只是一个比较了解协议和过程的人。我的主要兴趣在于协议的工作方式，以及传输中的数据包是什么样子的——这些主题将构成本书的主要部分。



注意

本书内容将遵循 IPv6 的 Internet 标准，以及 Windows .NET Server 2003 系列的 IPv6 协议在 Windows .NET Server 2003 系列的 RC1 中的特性集。要了解对本书中有关 Internet 标准改变的信息的更新，以及 Windows .NET Server 2003 系列的 RC1 之后的 Windows .NET Server 2003 系列的 IPv6 的更新，请访问微软公司的 IPv6 站点 <http://www.microsoft.com/ipv6>。

本书读者对象

本书读者对象包括：

- **Microsoft Windows XP 和 Windows .NET Server 2003 的联网咨询师和规划师：**包括那些将要用 Windows XP 和 Windows .NET Server 2003 系列操作系统最终实现 IPv6 迁移的人。
- **Microsoft Windows 网络管理员：**包括那些管理 IPv4 网络，并希望了解 IPv6 及其在 Windows .NET Server 2003 中的实现的技术知识的人。
- **微软认证系统工程师(MCSE)和微软认证培训师(MCT)：**无论微软官方课程(MOC)课件中关于 Windows .NET Server 2003 系列 IPv6 的最终内容是什么，本书都可以作为 MCSE 和 MCT 用以学习 IPv6 技术的标准参考。
- **普通技术人员：**因为本书主要介绍 IPv6 协议和过程，而与其在 Windows .NET Server 2003 系列中的实现无关，因此，普通技术人员可以把此书作为了解 IPv6 技术的较为深入的启蒙读物。

- **IT 学员：**本书最初是微软内部软件开发人员、测试人员和程序经理的课件，因此仍然可以作
为公司或教育机构用以教授 IPv6 课程的课本。

阅读本书的先决条件

本书假设读者具有基本的联网知识，包括基本的联网概念、常用的联网技术，并且十分了解 TCP/IP 协议族。在介绍 IPv6 时，本书将尽可能将其与 IPv4 中的相应特性、行为或组件进行比较，以帮助读者理解。要了解基本的联网概念和技术，可学习其他相关书籍，如 *MCSE Training Kit: Networking Essentials Plus, Third Edition* (Microsoft Press, ISBN 1-57231-902-X)。要了解 TCP/IP 协议族，最好学习 *Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference* (Microsoft Press, ISBN 0-7356-0556-4) 或 *Microsoft Windows .NET Server 2003 TCP/IP Protocols and Services Technical Reference* (Microsoft Press, ISBN 0-7356-1291-9)。与本书一样，这两本书主要也是探讨与具体实现无关的协议和过程。

作为这两本书的合著者，或许我的看法是带有偏见的。但在写作《理解 IPv6》这本书时，它们的确一直萦绕于脑际。事实上，我把此书视为 *Microsoft Windows .NET Server 2003 TCP/IP Protocols and Services Technical Reference* 一书的“姐妹书”。无论您是否使用微软公司的软件，我都建议您拥有一本《理解 IPv6》。

本书组织结构

本书章节按逻辑顺序排列。例如，如果不了解 IPv6 寻址、IPv6 报头和 ICMPv6，就很难理解邻节点发现过程；如果不了解 IPv6 寻址、邻节点发现过程和路由，就几乎无法理解 IPv6/IPv4 共存技术。

本书附录

本书包括如下附录：

- **附录 A：链路层对 IPv6 的支持**

讨论了常用的局域网(LAN)和广域网(WAN)技术的链路层对 IPv6 数据包的封装。这个主题对于我来说很有趣，但是对于大多数人来说可能过于枯燥。因此，这些内容只是作为一个附录出现，而不是作为一章出现。

- **附录 B：支持 IPv6 的 Windows 套接字的变化**

讲述 Windows 套接字为同时支持 IPv6 和 IPv4 而进行的增强。

- **附录 C：IPv6 RFC 索引**

本附录列出了直到本书出版时，与 Windows .NET Server 2003 系列的 IPv6 实现最为相关的

IPv6 RFC 和 Internet 草案。这些列表不可能毫无遗漏，并且，在本书出版时，有些内容当然会有些过时。

- **附录 D：测试的答案**

每一章最后都有一个“本章测试”小节，其中的问题用来复习该章的知识。本附录提供这些复习问题的答案。

- **附录 E：建立一个 IPv6 测试实验室**

本附录提供了如何使用 5 台计算机来建立一个 IPv6 测试实验室的方案，可以利用这一测试实验室来测试自动配置、路由和名称解析。最后，将会得到一个可正常工作的 IPv4/IPv6 网络，可利用此网络进行实验。

- **附录 F：IPv6 参照表**

列出了大多数与 IPv6 相关的表，包括 IPv6 协议字段值和其他参数。

本书配书文件

本书配书文件中包含如下内容：

- **网络监视器捕获文件：**在本书中，数据包结构和协议过程都是用 Microsoft 网络监视器 (Network Monitor——在 Microsoft Systems Management Server 2.0 和 Windows .NET Server 2003 系列中提供的帧捕获和查看程序，也称为网络嗅探器)所显示的实际 IPv6 数据包来演示。练习文件中提供了本书中提到的每次捕获的捕获文件，同时，为了在不能使用网络监视器的情况下也可以查看捕获结果，还提供相应的文本文件(*.txt)。只有 Microsoft Systems Management Server 2.0 和 Windows .NET Server 2003 系列中提供的网络监视器版本才可以解析 IPv6 通讯。本书中显示的网络监视器捕获结果是通过不同版本的网络监视器获得的，在写作本书时，这些版本在微软公司内都可获得。练习文件中的捕获文件的.txt 版本是通过 Windows .NET Server 2003 系列 Release Candidate 1 版本中的网络监视器获得的。练习文件中的捕获文件内的帧的显示情况取决于您所使用的网络监视器版本。因此，在使用网络监视器来显示捕获文件以及捕获文件的.txt 版本时，与书中所引述的帧结构显示可能会有一些差异。
- **IPv6 RFC 和 Internet 草案：**\RFCs_and_drafts 文件夹中提供了与本书内容以及在本书出版时的 Windows .NET Server 2003 系列中的 IPv6 实现最相关的 IETF RFC 和 Internet 草案。由于本书出版需要一定的时间，所以该文件夹中也包含了其他一些在本书中未出现的 RFC 和 Internet 草案。
- **Microsoft IPv6 白皮书：**当本书出版时，这套白皮书已经发布在微软的 Windows IPv6 站点上 (<http://www.microsoft.com/ipv6>)，并同时以 Microsoft Word 格式和 Adobe Acrobat 格式提供。在读完本书后，您会发现书中的一些内容与某些白皮书的内容十分相似。这是因为这些白皮书是我写的，它们成为本书各章的基础。但这并不意味着本书的内容只局限于这些可通过公开

途径获得的白皮书，而是这些白皮书中信息的一个“超集”，并且，我个人认为其内容要比白皮书更好。

- **Checkv4.exe 实用工具：** Checkv4.exe 工具在软件代码中查找 IPv4 特有的 Windows 套接字函数调用，标识出潜在问题或突出显示那些可以从支持 IPv6 的函数或结构中获益的代码，并提供建议。通过使用 Checkv4.exe 实用工具，就可以很容易地将 IPv4 应用程序进行移植，以使其可以同时支持 IPv4 和 IPv6。要了解如何修改应用程序以使其同时支持 IPv4 和 IPv6 的更多信息，请参考“IPv6 Guide for Windows Sockets Applications”(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/ipv6_guide_for_windows_sockets_applications_2.asp)。要了解 Checkv4.exe 的更多信息，请参考“Using the Checkv4.exe Utility”(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/using_the_checkv4_exe_utility_2.asp)。
- **教学幻灯片：** 一组 Microsoft PowerPoint 文件，利用本书来讲授 IPv6。更多信息，请参考“指导教师特别提示”小节。

系统要求

要查看本书中的捕获文件(*.cap)，必须安装 Microsoft Systems Management Server 2.0 或 Windows .NET Server 2003 系列所提供的网络监视器。

IPv6 协议和 Windows 产品的版本

用于 Windows 的 IPv6 协议有不同的版本。本书所讨论的 IPv6 指的是作为产品版本使用的 IPv6——在 Windows .NET Server 2003 系列和 Windows XP Service Pack 1 (及以后版本)中提供的 IPv6。这两个版本中的 IPv6 协议不是完全相同的。

下面几个特性在 Windows .NET Server 2003 系列的 IPv6 协议中包括，但在 Windows XP Service Pack 1 的 IPv6 协议中不包括：

- 对通过 IPv6 发送 DNS 通讯的支持
- 对通过 IPv6 进行文件和打印共享的支持
- 对 Web 服务器的支持
- 对 Windows 媒体服务的支持

在 Windows XP Service Pack 1 的 IPv6 协议中包含 Ipv6.exe 配置工具，以及 Ping6.exe 和 Tracert6.exe 诊断工具。这些工具在 Windows .NET Server 2003 系列的 IPv6 协议中不包含，并且在 Windows XP 未来的版本中也将不再提供。**netsh interface ipv6** 上下文中的命令代替了 Ipv6.exe，支持 IPv6 的

Ping.exe 代替了 Ping6.exe，而支持 IPv6 的 Tracert.exe 代替了 Tracert6.exe。

指导教师特别提示

本书最初是一本教材，现在仍保留一些这样的属性，如：

- 每章开始有内容简介
- 每章最后有复习题
- 练习文件中为每章提供了教学幻灯片

如果您是一位教师，要向其他人讲解 IPv6 协议和过程，强烈建议您使用本书及本书中的幻灯片作为教学的基础。

这些幻灯片是您进行自己的幻灯片演示的基础，其中的内容包括与所属章节内容一致的提要文本或者图形。因为幻灯片是在全书已经完成之后才制作的，因此与每章内容会略有不同。这些更改是为了使您能够更好地利用本书讲解 IPv6。

我尽可能地选择比较简单的幻灯片模板，这样，在您切换到其他模板时，就只需要最少限度的文本和绘图颜色的转换。您可以根据自己的需要，对这些幻灯片进行修改。

如果您要讲授与具体实现无关的 IPv6 技术，建议您跳过第 2 章，并且在讲解了第 4 章后，讲解附录 A。

作为您的同行，我希望您可以成功地讲解这一有趣而重要的新技术。

不承诺声明和支持信息

在 Internet 的技术开发过程中，惟一不变的就是变化。本书只提供了在 Windows .NET Server 2003 系列的 Release Candidate 1 刚刚发布时，关于 IPv6 的 Internet 标准的最准确的信息。有许多计算机技术专业人士正在努力工作，可能使本书的内容被新的技术取代(也许并不是有意的)。Internet 草案的编写者正在努力编写新的 Internet 草案来更新或增强现有的 IPv6 概念和功能。微软公司的软件开发者们正在更新软件代码，以修订 IPv6 协议的功能或使他们的应用程序既支持 IPv4，又支持 IPv6。

要获得关于 IPv6 IETF 标准的最新信息，请参见 IP Version 6 Working Group 的 Web 站点：
<http://www.ietf.org/html.charters/ipv6-charter.html>。

要获得 IPv6 过渡技术的最新信息，请参见 Next Generation Transition Working Group 的 Web 站点：
<http://www.ietf.org/html.charters/ngtrans-charter.html>。

要获得 Windows 操作系统的 IPv6 的最新信息以及对本书中的内容的更新，请参见微软公司的

Windows IPv6 Web 站点: <http://www.microsoft.com/ipv6>。

出版社支持信息

为了降低书的成本,减轻读者负担,对于因内容很少而不值得单独配盘的图书,我们将其范例代码或练习文件放在我们的网站上,供读者下载。请访问以下网址: <http://www.wenyuan.com.cn>, 查找本书的有关链接。

如果您对本书或配书文件有任何建议、意见或想法,请通过以下电子邮件与清华大学出版社计算机应用编辑二室客户服务部取得联系:

service@wenyuan.com.cn

或致函:

北京 100084-157 信箱

读者服务部

邮编: 100084

亦可致电: 010-62792098-220。

请注意,上述地址并不提供软件产品的支持。

致谢

历经紧张的翻译和编辑工作,本书终于得以与广大读者见面。本书在出版过程中,得到了北京科技大学计算机系王沁和李占才教授的大力支持。此外,参与本书翻译工作的还有黄世荣和李红等。在此,对他们的辛勤工作一并表示衷心的感谢!

目 录

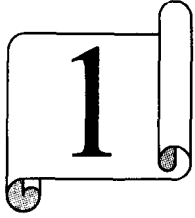
第 1 章 IPv6 概述	1	1.5.6 IPv6 具有内置的 安全性和移动性	13
1.1 IPv4 的局限	1	1.6 本章测试	14
1.1.1 有限的 IPv4 地址空间 所造成的后果	2	第 2 章 Windows .NET Server 2003 系列中的 IPv6 协议	15
1.2 IPv6 的特性	6	2.1 Windows .NET Server 2003 系列的 IPv6 协议的结构	15
1.2.1 新的协议头格式	6	2.2 Windows .NET Server 2003 系列的 IPv6 协议的特性	16
1.2.2 巨大的地址空间	6	2.2.1 基本的协议栈支持	17
1.2.3 有效的、分级的寻址和 路由结构	7	2.2.2 6to4	17
1.2.4 有状态和无状态的 地址配置	7	2.2.3 ISATAP 协议	17
1.2.5 内置的安全性	7	2.2.4 6over4	18
1.2.6 更好地支持 QoS	7	2.2.5 端口代理	18
1.2.7 用新协议处理邻节点 的交互	8	2.2.6 临时地址	18
1.2.8 可扩展性	8	2.2.7 DNS 支持	18
1.3 IPv4 与 IPv6 的比较	8	2.2.8 IPSec 支持	19
1.4 IPv6 术语	9	2.2.9 静态路由器支持	19
1.5 IPv6 的使用情况	11	2.2.10 地址选择	20
1.5.1 IPv6 解决了地址 耗尽问题	12	2.2.11 路由器公告中的 站点前缀	20
1.5.2 IPv6 解决了国际地址 分配问题	12	2.3 应用程序的支持	20
1.5.3 IPv6 重建了端到端 的通信	12	2.3.1 IE 浏览器	21
1.5.4 IPv6 使用限制范围的 地址和地址选择	13	2.3.2 Telnet 客户程序	21
1.5.5 IPv6 保证了更 有效的转发	13	2.3.3 FTP 客户程序	21
		2.3.4 Web 服务器	22
		2.3.5 文件和打印共享	22
		2.3.6 Windows 多媒体服务	22
		2.3.7 Network Monitor	22

2.3.8	SNMP MIB 支持	22	3.5	多播 IPv6 地址.....	51
2.4	应用程序编程接口	23	3.5.1	推荐的多播 IPv6 地址	53
2.4.1	Windows 套接字	23	3.5.2	请求节点地址	53
2.4.2	远程过程调用.....	24	3.6	泛播 IPv6 地址.....	54
2.4.3	IP 助手	24	3.6.1	子网-路由器泛播地址	54
2.4.4	Win32 Internet 扩展.....	24	3.7	主机的 IPv6 地址	55
2.4.5	.NET 框架.....	24	3.8	路由器的 IPv6 地址	55
2.5	安装和配置 IPv6 协议.....	25	3.9	子网化 IPv6 地址空间	56
2.6	支持 IPv6 的工具	25	3.9.1	NLA ID 的子网化.....	56
2.6.1	Ipconfig	25	3.9.2	SLA ID/子网 ID 的子网化.....	60
2.6.2	Route	26	3.10	IPv6 接口标识符.....	64
2.6.3	Ping	28	3.10.1	基于 EUI-64 地址的 接口标识符	65
2.6.4	Tracert	29	3.10.2	临时地址接口标识符	68
2.6.5	Pathping.....	30	3.11	将 IPv6 多播地址映射为 以太网地址	69
2.6.6	Netstat.....	32	3.12	IPv4 地址和 IPv6 地址的对应	70
2.7	IPv6 命令行工具	34	3.13	参考资料.....	71
2.7.1	Netsh.exe	35	3.14	本章测试.....	71
2.7.2	Ipsec6.exe	38	第 4 章	IPv6 报头.....	73
2.8	本章测试	38	4.1	IPv6 数据包的结构.....	73
第 3 章	IPv6 寻址	40	4.2	IPv4 报头	74
3.1	IPv6 的地址空间	40	4.3	IPv6 报头	77
3.1.1	当前的地址分配.....	41	4.3.1	下一个报头字段的值	79
3.2	IPv6 的地址语法	42	4.3.2	比较 IPv4 和 IPv6 的报头	80
3.2.1	零压缩法	44	4.4	IPv6 扩展报头.....	82
3.2.2	IPv6 前缀.....	45	4.4.1	扩展报头的顺序	83
3.3	IPv6 的地址类型	45	4.4.2	逐跳选项报头	84
3.4	单播 IPv6 地址	46	4.4.3	目标选项报头.....	88
3.4.1	可集聚全球单播地址	46	4.4.4	路由报头	95
3.4.2	全球地址中的 拓扑结构	48	4.4.5	片段报头	97
3.4.3	本地使用的单播地址	48	4.4.6	身份验证报头.....	101
3.4.4	特殊的 IPv6 地址	50			
3.4.5	兼容地址	50			
3.4.6	NSAP 地址	51			

4.4.7 封装安全有效载荷 报头和尾部.....	101	6.2.5 公告间隔选项.....	131
4.5 IPv6 MTU.....	102	6.2.6 本地代理信息选项.....	131
4.6 上层校验和.....	103	6.2.7 路由信息选项.....	132
4.7 参考资料.....	104	6.3 邻节点发现报文.....	134
4.8 本章测试.....	104	6.3.1 路由器请求报文.....	135
第 5 章 ICMPv6	105	6.3.2 路由器公告报文.....	136
5.1 ICMPv6 概述.....	105	6.3.3 邻节点请求报文.....	140
5.1.1 ICMPv6 报文的类型.....	106	6.3.4 邻节点公告报文.....	142
5.1.2 ICMPv6 报头.....	106	6.3.5 重定向报文.....	145
5.2 ICMPv6 差错报文.....	107	6.3.6 小结.....	147
5.2.1 目标不可到达.....	107	6.4 邻节点发现过程.....	148
5.2.2 数据包过长.....	109	6.4.1 概念主机数据结构.....	149
5.2.3 超时.....	110	6.4.2 地址解析.....	150
5.2.4 参数问题.....	111	6.4.3 邻节点不可到达检测.....	153
5.3 ICMPv6 信息报文.....	112	6.4.4 重复地址检测.....	156
5.3.1 回送请求报文.....	112	6.4.5 路由器发现.....	160
5.3.2 回送应答报文.....	113	6.4.6 重定向功能.....	165
5.4 ICMPv4 和 ICMPv6 报文的比较.....	114	6.5 主机发送算法.....	168
5.5 路径 MTU 发现.....	115	6.6 IPv4 邻节点报文和功能以及相应的 IPv6 邻节点报文和功能.....	170
5.5.1 PMTU 的改变.....	116	6.7 参考资料.....	170
5.6 参考资料.....	117	6.8 本章测试.....	170
5.7 本章测试.....	117	第 7 章 多播侦听发现	172
第 6 章 邻节点发现	119	7.1 多播侦听发现概述.....	172
6.1 邻节点发现概述.....	119	7.2 IPv6 多播概述.....	172
6.1.1 邻节点发现报文的格式.....	121	7.2.1 主机对多播的支持.....	173
6.2 邻节点发现选项.....	121	7.2.2 路由器对多播的支持.....	174
6.2.1 源链路层地址和目标 链路层地址选项.....	122	7.3 MLD 数据包的结构.....	177
6.2.2 前缀信息选项.....	124	7.4 MLD 协议的报文.....	177
6.2.3 重定向报头选项.....	127	7.4.1 多播侦听查询报文.....	178
6.2.4 MTU 选项.....	128	7.4.2 多播侦听报告报文.....	179
		7.4.3 多播侦听已完成报文.....	181
		7.5 MLD 协议小结.....	183
		7.6 参考资料.....	183

7.7 本章测试	183	10.2.1 源主机上的 IPv6	202
第 8 章 地址的自动配置	184	10.2.2 路由器上的 IPv6	203
8.1 地址自动配置概述	184	10.2.3 目标主机上的 IPv6	205
8.1.1 自动配置地址的状态	184	10.3 IPv6 的路由协议	209
8.1.2 自动配置的类型	185	10.3.1 动态路由概述	209
8.2 自动配置的过程	186	10.3.2 路由协议技术	210
8.2.1 Windows .NET Server 2003 系列和 Windows XP 中的 IPv6 协议的自动 配置的特点	187	10.3.3 IPv6 路由协议	211
8.2.2 Windows .NET Server 2003 系列和 Windows XP 中的 IPv6 协议自动配置 的地址	190	10.4 Windows .NET Server 2003 系列 和 Windows XP 中的 IPv6 协议 的静态路由	213
8.3 参考资料	192	10.5 参考资料	217
8.4 本章测试	193	10.6 本章测试	218
第 9 章 IPv6 和名称解析	194	第 11 章 共存和移植	219
9.1 IPv6 的名称解析	194	11.1 共存和移植概述	219
9.2 IPv6 DNS 功能的增强	194	11.1.1 节点的类型	220
9.3 Windows .NET Server 2003 系列 中对名称解析的支持	195	11.1.2 兼容的地址	221
9.3.1 Hosts 文件	196	11.2 共存的机制	222
9.3.2 DNS Server 服务	196	11.2.1 双 IP 层	222
9.3.3 DNS 解析器	197	11.2.2 IPv6 穿越 IPv4 的隧道	223
9.3.4 DNS 动态更新	197	11.2.3 DNS 结构	225
9.3.5 地址选择规则	197	11.2.4 隧道的配置	226
9.4 参考资料	198	11.2.5 路由器到路由器	226
9.5 本章测试	198	11.2.6 主机到路由器和路由 器到主机	227
第 10 章 IPv6 路由	199	11.2.7 主机到主机	228
10.1 IPv6 中的路由	199	11.2.8 隧道的类型	228
10.1.1 IPv6 路由由表	199	11.3 6over4	230
10.2 IPv6 的端到端传送过程	202	11.4 6to4	233
		11.4.1 Windows XP 和 Windows .NET Server 2003 系列对 6to4 协议的支持	236
		11.5 ISATAP	238
		11.5.1 使用 ISATAP 路由器	240

11.5.2 将运行 Windows XP 和 Windows .NET Server 2003 系列的 IPv6 协议 的主机配置为 ISATAP 路由器	245	12.4.2 移动节点和本地代理 之间的通信	271
11.5.3 ISATAP 和 6to4 的例子	245	12.5 移动 IPv6 的处理过程	277
11.6 端口代理	249	12.5.1 连接到本地链路	277
11.7 移植到 IPv6	251	12.5.2 从本地链路移动到 外地链路	278
11.8 参考资料	252	12.5.3 从一个外地链路移动到 另一个外地链路	285
11.9 本章测试	252	12.5.4 返回本地	287
第 12 章 移动 IPv6	254	12.5.5 移动 IPv6 主机的 发送算法	289
12.1 移动 IPv6 概述	254	12.5.6 移动 IPv6 主机的 接收算法	292
12.1.1 移动 IPv6 的组成部分	255	12.6 参考资料	293
12.2 移动 IPv6 的报文和选项	257	12.7 本章测试	293
12.2.1 目标选项报头 中的选项	257	附录 A 链路层对 IPv6 的支持	296
12.2.2 ICMPv6 报文	259	附录 B 支持 IPv6 的 Windows 套接字的变化	314
12.2.3 对邻节点发现报文和 选项的修改	261	附录 C IPv6 RFC 索引	324
12.3 移动 IPv6 的数据结构	262	附录 D 测试的答案	330
12.3.1 绑定高速缓存	262	附录 E 建立一个 IPv6 测试实验室	348
12.3.2 绑定更新列表	263	附录 F IPv6 参照表	363
12.3.3 本地代理列表	264	词汇表	368
12.4 移动 IPv6 的通信	265		
12.4.1 移动节点和通信节点 之间的通信	265		



IPv6 概述

通过本章的学习，您将掌握如下内容：

- IPv4 和当前 Internet 的缺陷，以及 IPv6 如何弥补这些缺陷
- IP 地址耗尽问题是怎样导致对网络地址转换协议(NAT)的使用，以及由于 NAT 的使用而产生的一些端到端的通信问题
- IPv6 的特性
- IPv4 和 IPv6 之间的主要区别
- 部署 IPv6 的原因

1.1 IPv4 的局限

自从 RFC 791 于 1981 年发布以后，当前版本的 IP 协议(即版本 4 或 IPv4)就没有发生什么实质性的变化。实践证明，IPv4 是健壮的，易于实现的，并且具有很好的互操作性。它本身也经受住了互联网从小型发展到今天这种全球规模的考验。这些都是对 IPv4 协议初始设计的肯定。

然而，IPv4 在设计之初，也有一些预想不到的方面：

- 近年来，随着 Internet 成指数倍增长，出现了迫在眉睫的 IP 地址空间耗尽问题
尽管 IPv4 的 32 位地址空间可以容纳多达 4 294 967 296 个地址，但早前和现在的 IP 地址分配准则把公共 IP 地址的数目限制到了只有几百万个。结果，IPv4 的可分配地址数就变得相对较少，从而迫使一些机构不得不通过网络地址转换器(NAT)把一个公共的 IP 地址映射为多个内部的 IP 地址。尽管 NAT 转换支持对内部 IP 地址的重用，但它同时也造成了性能和应用的瓶颈。
此外，随着连入 Internet 的设备和应用程序的数目日益增加，必然导致 IPv4 地址空间的最终耗尽。

- **Internet 的发展和 Internet 上的骨干路由器维护大路由表的能力**

根据已有的和正在进行的 IPv4 网络 ID 的分配方式，现今 Internet 上的骨干路由器的路由表中通常都有超过 85 000 条的路由。当前 IPv4 的路由结构由扁平和层级两种结构组成。

- **对更简便配置的需求**

在当前 IPv4 协议的实现方案中，多数情况下都要进行手工配置，或者使用一个有状态的地址配置协议——例如：动态主机配置协议(DHCP)。随着越来越多的计算机和相关设备使用 IP 协议，需要一种更加简便和自动的地址配置方式，或者是一种不需要依赖 DHCP 协议管理的配置方式。

- **对 IP 级安全性的需求**

途经公共网络(如 Internet)的专用通信需要使用加密服务，以保证所传输的数据不会在传输过程中被查看或者修改。尽管当前已经存在一个标准(即 IPSec)，可以为 IPv4 数据包的传输提供安全保证，但因为这个标准对 IPv4 来说是可选的，因而还广泛存在着很多并非通用的安全解决方案。

- **需要对实时数据传送有更好的支持，也称作服务质量(QoS)**

尽管 IPv4 中已有 QoS 标准，但对实时通信流传送的支持还是依赖于传统的 IPv4 协议中的服务类型(TOS)字段，以及报文标识，这些报文标识通常使用用户数据报协议(UDP)或者传输控制协议(TCP)端口。遗憾的是，IPv4 的 TOS 字段功能有限，而且经过一段时间以后，它已被重新定义，并在本地解析。此外，当 IP 数据包的有效载荷以加密的形式传送时，报文标识也不能使用 TCP 或 UDP 端口了。

为解决以上这些问题以及其他相关问题，互联网工程任务组织(IETF)开发了一套新的协议和标准，即 IP 版本 6(IPv6)。这个新版本，以前称为 IP-下一代(Ipng)，吸纳了很多用于更新 IPv4 协议的新思想。IPv6 在设计时，力图对上、下层协议造成最小的影响，并避免随意引入新的特性。

1.1.1 有限的 IPv4 地址空间所造成的后果

在 IPv4 协议中，由于公共 IP 地址相对较少，我们便采用 NAT 转换来重复使用 IPv4 的内部地址空间。在公共 IP 地址相对较少的地方，客户端和 Internet 之间会有多级的 NAT 转换。尽管 NAT 转换器的确使得更多的客户端能够连接到 Internet，但与此同时，它们也成为一些通信方式的瓶颈，甚至是障碍。下面我们要分析一下 NAT 的运行机制，进而说明为什么网络地址转换是一种不可升级的、权宜的解决方案，并且这种解决方案削弱了端到端的通信能力。

假设一家小公司的内部网络使用从 192.168.0.0~192.168.0.24 的专用 IP 地址，并且这家公司从 ISP 那里得到了公共 IP 地址 131.107.47.119 的使用授权。在公司内部网络和外部 Internet 的接口处，这家公司使用 NAT 转换器，将从 192.168.0.0 到 192.168.0.24 范围之间的公司内部 IP 地址，映射到公共 IP 地址 131.107.47.119。NAT 转换器使用动态选择的 TCP 和 UDP 端口来区分公司内部的不同主机。本

例的配置如图 1.1 所示。

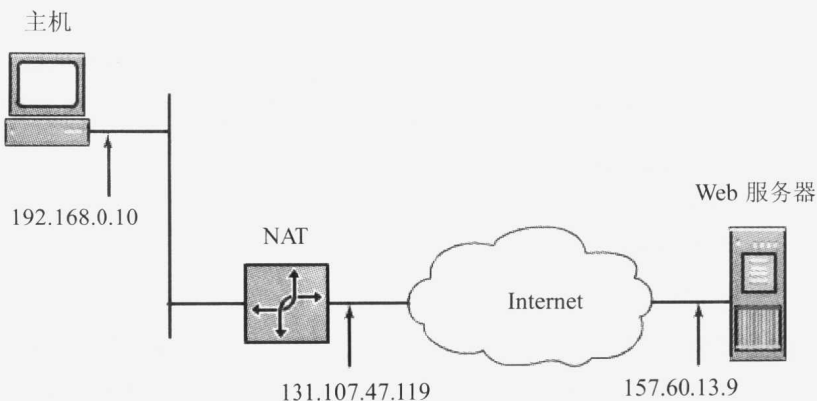


图 1.1 一个 NAT 的例子

假设一台内部 IP 地址为 192.168.0.10 的内部主机,用浏览器访问 IP 地址为 157.60.13.9 的 Web 服务器。则内部主机会产生一个如下所示的数据包:

- 目标地址: 157.60.13.9
- 源地址: 192.168.0.10
- 目标 TCP 端口: 80
- 源 TCP 端口: 1025

接着,这个数据包被转发到 NAT, NAT 转换器将数据包中的源地址和源 TCP 端口转化成如下形式:

- 目标地址: 157.60.13.9
- 源地址: **131.107.47.119**
- 目标 TCP 端口: 80
- 源 TCP 端口: **5000**

同时, NAT 转换器在自己的转化表中保存一个从 {192.168.0.10, TCP 1025} 到 {131.107.47.119, TCP 5000} 的映射, 以备以后使用。

经过转换的数据包通过 Internet 发送出去, Web 服务器在收到数据包后, 会发回应答, 并被 NAT 接收。在 NAT 转换器收到的应答中会包含如下信息:

- 目标地址: 131.107.47.119
- 源地址: 157.60.13.9