Windows 技术丛书

Windows 2000 路由和远程访问服务

（美） Kackie Charles 著

袁勤勇 邓 静 丁之岩 等译

机械工业出版社
China Machine Press

需要全本请访问 www.ertongbook.com

本书是为经验丰富的管理员编写的。全书共分为三个部分：第一部分包括路由器、远程访问和拨号网络的安装。第二部分涉及高级管理工具和其他一些实现 RRAS 的特性，包括虚拟专用网络（VPN）和 Internet 认证服务（IAS），以及带宽、远程访问通信技术和设计等问题。第三部分研究 RRAS 规划问题，包括带宽和远程通信技术以及 Internet 连接共享等。附录包括安全、故障诊断和词汇表。本书由浅入深，内容全面，各种规模的网络的管理员都可以从本书中找到有用的信息。

Kackie Charles: Windows 2000 Routing and Remote Access Service.

Authorized translation from the English language edition published by New Riders Publishing, an imprint of Macmillan Computer Publishing U.S.A.

Copyright © 2000 by New Riders Publishing. All rights reserved.

Chinese simplified language edition published by China Machine Press.

Copyright © 2001 by China Machine Press.

本书中文简体字版由美国 New Riders 公司授权机械工业出版社独家出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

版权所有，侵权必究。

本书版权登记号：图字：01 - 2000 - 1569

图书在版编目（CIP）数据

Windows 2000 路由和远程访问服务/（美）查尔斯（Charles, K.）著；袁勤勇等译. - 北京：机械工业出版社，2002.1

（Windows 技术丛书）

书名原文：Windows 2000 Routing and Remote Access Service

ISBN 7 - 111 - 09487 - 5

Ⅰ. W… Ⅱ. ①查…②袁… Ⅲ. ①服务器 - 操作系统（软件），Windows 2000 - 路由选择②远程网络 Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字（2001）第 078848 号

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：贾 梅

北京第二外国语学院印刷厂印刷·新华书店北京发行所发行

2002 年 1 月第 1 版第 1 次印刷

787mm × 1092mm 1/16· 15.25 印张

印数：0 001 - 4 000 册

定价：28.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

前　言

欢迎阅读《Windows 2000 路由和远程访问服务》。撰写本书的目的是帮助你使用Windows 2000系统，以不同的方法连接自己的网络和用户。路由和远程访问服务（RRAS）中有许多令人兴奋的新特性，可以很容易地集成到新的或已有的网络中。在你发现了这些新特性，并且知道它们能够做些什么之后，本书将指导你来实现这些新特性。

本书的读者

《Windows 2000 路由和远程访问服务》这本书是为经验丰富的管理员编写的。本书的读者应熟悉 TCP/IP 协议、Windows NT 域和活动目录方面的知识。各种规模的网络的管理员都可从本书中找到有用的信息，用来计划和实现 RRAS。具有大型路由网络经验的读者或 Internet 服务供应商的管理员会发现本书尤其有参考价值。

本书的内容

本书的内容分为三部分。第一部分包括路由器、远程访问和拨号网络的安装。第二部分涉及高级管理工具和其他一些实现 RRAS 的特性，包括虚拟专用网络（VPN）和 Internet 认证服务（IAS），以及带宽、远程访问通信技术和设计等问题。第三部分研究 RRAS 规划问题，包括带宽和远程通信技术以及 Internet 连接共享等。附录包括安全、故障诊断和词汇表的内容。

第一部分：安装与配置

这部分包括安装和配置远程访问服务、拨号网络和路由器所需要的内容。第 1 章，“概述、特性和优点”，提供了对新特性的概述和使用 Windows 2000 路由和远程访问服务后的益处。远程访问组件和路由组件在该章中分别进行讨论。第 2 章，“远程访问服务器”，深入讨论 Windows 2000 中的远程访问服务、它的设置、以及认证方法。第 3 章，“拨号网络”，概括了拨号网络，即远程访问服务的客户端。调制解调器的安装和连接配置在这里讨论。第 4 章，“路由协议”，讨论 Windows 2000 中包含的路由协议。第 5 章，“配置 Windows 2000 路由器”，将用实例详细介绍如何配置 Windows 2000 路由器。

第二部分：高级管理

第二部分讨论其他的管理工具和 Windows 2000 RRAS 的特性，并且着眼于介绍 RRAS 设计方案。第 6 章，“路由工具”，提供了有关 RRAS 的命令行管理的内容以及 Windows 2000 中其他各种各样的管理工具。虚拟专用网络的内容将在第 7 章，“虚拟专用网络”讨论，该章是关于虚拟专用网络（VPN）的一般知识以及 Windows 2000 VPN 特有的内容。第 8 章，

“Windows 2000 连接服务”，将示例如何生成、管理和发布电话本给远程用户。第 9 章，“Internet 认证服务”，讨论 Internet 认证服务；IAS 是 Microsoft 的适应请求注解（RFC）的远程认证拨号用户服务（RADIUS）服务器。

第三部分：RRAS 规划

第三部分讨论 RRAS 的设计环节。带宽和远程通信技术将在第 10 章“带宽和远程通信技术”中讲述。该章将演示 Windows 2000 如何帮助用户尽量利用可用带宽。各种各样的远程通信技术服务也在该章讨论。第 11 章，“共享的 Internet 连接性”，把目标集中在使用 Windows 2000 如何把自己的网络连接到 Internet 上。这部分还包括第 12 章，“网络设计”，将着眼于介绍各种规模网络的 RRAS 设计选项。

附录

由三个附录组成。附录 A，“RAS 通信技术概述”，提供了 Windows 2000 中的一些安全特性和配置 Internet 协议安全（IPSec）的说明。附录 B，“故障诊断”，是排除故障的指导，将帮助用户解决通常的 RRAS 问题。最后，附录 C，“词汇表”，是与 RRAS 有关的术语。

如何使用本书

对路由和远程访问经验不多的管理员将会发现从头到尾阅读第一部分是很有帮助的。经验较丰富的管理员可能愿望使用目录来直接找到他们感兴趣的特定问题。第二部分对所有的管理员都具有吸引力，这部分可以很好地指导用 RRAS 完成一些其他的事情。阅读该部分的一个好方法是先浏览各章，大概了解各个特性所涉及的内容，然后返回去，对感兴趣的章节再仔细阅读。最后一部分是一个参考工具。你可以前后翻动来查找术语或缩写的定义，或者浏览故障诊断和安全性附录来发现感兴趣的主题。

作者欢迎读者对本书提出批评和意见。她的邮件账号是 author@kcse．net。

参与本书翻译的有袁勤勇、邓静、丁之岩、刘霞飞、王富华、李栋梁、何铮、郑屹立、王海艳、康巍巍。

目　录

前言

第一部分　安装与配置

第 1 章　概述、特性和优点 …… 1
1.1　远程访问组件 …… 1
1.1.1　按需拨入路由 …… 2
1.1.2　认证协议 …… 2
1.1.3　数据加密 …… 2
1.1.4　点对点隧道 …… 2
1.1.5　高效带宽利用 …… 3
1.1.6　向导 …… 3
1.1.7　安全性和策略 …… 3
1.1.8　认证、授权和账号管理 …… 3
1.1.9　Internet 连接共享 …… 3
1.2　路由组件 …… 3
1.2.1　用于 IP 网络的路由信息协议第 1 版和第 2 版 …… 4
1.2.2　开放最短路径优先 …… 4
1.2.3　DHCP 中继代理 …… 4
1.2.4　IP 多播 …… 4
1.2.5　用于 IPX 网络的路由信息协议和服务通告协议 …… 5
1.2.6　AppleTalk 路由 …… 5
1.3　其他特性 …… 5
1.3.1　Internet 认证服务 …… 5
1.3.2　虚拟专用网络 …… 5
1.3.3　连接管理器服务 …… 5
1.4　总结 …… 6
第 2 章　远程访问服务器 …… 7
2.1　RAS 概述 …… 7
2.1.1　远程访问不是远程控制 …… 7
2.1.2　远程访问服务器结构 …… 8
2.1.3　启动路由和远程访问服务 …… 9
2.1.4　RAS 支持的局域网协议 …… 10
2.1.5　远程访问协议 …… 13
2.2　认证和授权 …… 14
2.2.1　EAP …… 14
2.2.2　CHAP、MS-CHAP 和 MS-CHAP v2 …… 17
2.2.3　非认证访问 …… 22
2.2.4　认证提供者 …… 24
2.3　用户访问配置 …… 26
2.3.1　用户账号配置 …… 26
2.3.2　远程访问策略 …… 27
2.4　总结 …… 31
2.5　参考资料 …… 31
第 3 章　拨号网络 …… 32
3.1　拨号网络概述 …… 32
3.1.1　连接性组件 …… 33
3.1.2　LAN 协议 …… 35
3.2　硬件安装 …… 36
3.2.1　调制解调器安装 …… 36
3.2.2　ISDN 适配器安装 …… 37
3.2.3　X.25 卡安装 …… 38
3.3　配置拨号参数 …… 38
3.3.1　一般信息 …… 38
3.3.2　区域码规则 …… 38
3.3.3　拨号卡 …… 39
3.3.4　智能卡安装 …… 39
3.4　配置拨号连接 …… 39
3.4.1　连接属性 …… 39
3.4.2　高级配置 …… 41
3.4.3　复制拨号连接 …… 42
3.5　传入连接 …… 43
3.6　总结 …… 44
3.7　参考资料 …… 44
第 4 章　路由协议 …… 45
4.1　路由概念 …… 46
4.1.1　路由表 …… 46
4.1.2　静态和动态路由器 …… 47
4.2　单播路由 …… 49

需要全本请访问 www.ertongbook.com

4.3 多播 …… 49
4.3.1 多播的使用 …… 50
4.3.2 多播组和 IGMP …… 50
4.3.3 路由协议 …… 51
4.3.4 多播寻址 …… 51
4.3.5 Windows 2000 多播 …… 51
4.4 IP 路由 …… 52
4.4.1 用于 IP 的 RIP …… 52
4.4.2 OSPF …… 62
4.4.3 网络地址转换 …… 72
4.4.4 ICMP 路由器发现 …… 74
4.4.5 DHCP 中继代理 …… 75
4.5 其他路由协议 …… 75
4.5.1 IPX 路由协议 …… 75
4.5.2 AppleTalk …… 76
4.6 按需拨号路由 …… 78
4.6.1 按需拨号网络样本 …… 78
4.6.2 连接过程 …… 79
4.6.3 更新 …… 80
4.6.4 按需拨号路由器连接 …… 81
4.7 总结 …… 81
4.8 参考资料 …… 82
第 5 章 配置 Windows 2000 路由器 …… 83
5.1 基本配置 …… 83
5.1.1 安装 Windows 2000 路由器 …… 83
5.1.2 路由组件 …… 84
5.2 IP 路由 …… 85
5.2.1 常规 …… 85
5.2.2 静态路由 …… 87
5.2.3 DHCP 中继代理 …… 87
5.2.4 RIP …… 88
5.2.5 OSPF …… 90
5.2.6 IGMP …… 93
5.2.7 多播边界和心跳 …… 93
5.2.8 IP-in-IP 隧道 …… 94
5.3 IPX 路由 …… 94
5.3.1 常规属性 …… 95
5.3.2 NetBIOS 广播 …… 95
5.3.3 静态路由 …… 95
5.3.4 静态服务和静态 NetBIOS 名称 …… 96
5.3.5 用于 IPX 的 RIP …… 96
5.3.6 用于 IPX 的 SAP …… 97
5.4 按需拨号路由 …… 97
5.4.1 第一部分：配置路由器 A …… 98
5.4.2 第二部分：配置路由器 B …… 101
5.4.3 第三部分：初始化按需拨号连接 …… 104
5.5 AppleTalk 路由 …… 104
5.6 过滤 …… 105
5.7 总结 …… 106

第二部分 高级管理

第 6 章 路由工具 …… 107
6.1 Netsh …… 107
6.1.1 命令 …… 107
6.1.2 上下文 …… 109
6.1.3 Netsh 和自动静态更新 …… 111
6.2 mrinfo …… 112
6.3 pathping …… 112
6.4 调度工具 …… 114
6.4.1 调度任务 …… 114
6.4.2 at 命令 …… 114
第 7 章 虚拟专用网络 …… 116
7.1 VPN 定义 …… 116
7.2 Windows 2000 VPN 的新特性 …… 117
7.3 VPN 连接剖析 …… 118
7.4 VPN 的类型 …… 119
7.4.1 基于 Internet 的 VPN 连接 …… 119
7.4.2 基于内部网的 VPN 连接 …… 119
7.4.3 Internet-Intranet VPN 连接 …… 120
7.5 VPN 隧道协议 …… 120
7.5.1 IPSec …… 120
7.5.2 PPTP …… 120
7.5.3 L2TP …… 122
7.6 VPN 路由 …… 123
7.6.1 拨号客户 …… 124
7.6.2 LAN 上的拨号客户 …… 125
7.6.3 拨号 VPN 客户 …… 125
7.7 VPN 和防火墙 …… 126
7.7.1 位于防火墙前的 VPN 服务器 …… 126
7.7.2 位于防火墙后的 VPN 服务器 …… 127

7.8 VPN 配置 …… 127
7.8.1 设计思考和建议 …… 128
7.8.2 远程访问 VPN …… 129
7.8.3 路由器对路由器 VPN …… 136
7.9 参考资料 …… 143
第 8 章 Windows 2000 连接服务 …… 144
8.1 连接点服务 …… 145
8.1.1 安装和配置连接点服务 …… 145
8.1.2 管理连接点服务 …… 146
8.2 连接管理器 …… 148
8.2.1 要求 …… 148
8.2.2 服务配置文件 …… 148
8.2.3 连接管理器配置 …… 148
8.2.4 高级服务配置文件配置 …… 152
8.3 参考资料 …… 153
第 9 章 Internet 认证服务 …… 154
9.1 IAS 概述 …… 154
9.1.1 功能性 …… 154
9.1.2 为什么使用 IAS …… 156
9.2 规划 IAS 部署 …… 157
9.2.1 性能 …… 157
9.2.2 安全性 …… 157
9.2.3 日志 …… 158
9.3 安装和配置 …… 159
9.4 IAS 方案 …… 161
9.4.1 小型 IAS 的部署 …… 161
9.4.2 大型 IAS 的部署 …… 162
9.5 参考资料 …… 163

第三部分 RRAS 规 划

第 10 章 带宽和远程通信技术 …… 165
10.1 带宽和利用统计 …… 165
10.1.1 Windows 2000 带宽控制特性 …… 165
10.1.2 WAN 分析 …… 167
10.2 远程通信技术服务 …… 169
10.2.1 POTS …… 170
10.2.2 ISDN …… 170
10.2.3 T-载波 …… 171
10.2.4 包交换服务 …… 171
10.3 参考资料 …… 173
第 11 章 共享的 Internet 连接性 …… 175
11.1 网络地址转换协议 …… 175
11.1.1 转换组件 …… 176
11.1.2 编址组件 …… 176
11.1.3 命名解析组件 …… 177
11.1.4 问题和思考 …… 177
11.1.5 配置 NAT …… 178
11.2 Internet 连接共享 …… 181
11.2.1 CIS 配置 …… 181
11.2.2 ICS 思考 …… 182
11.3 参考资料 …… 182
第 12 章 网络设计 …… 183
12.1 小型办公室/家庭办公室网络 …… 183
12.2 中等规模的网络 …… 186
12.2.1 通用基础结构概述 …… 186
12.2.2 RRAS 部署选项 …… 186
12.3 大型网络 …… 188
12.4 参考资料 …… 189

附 录

附录 A RAS 通信技术概述 …… 191
附录 B 故障诊断 …… 207
附录 C 词汇表 …… 216

第一部分　安装与配置

第 1 章　概述、特性和优点

随着 Windows 2000 的推出，微软公司引入了当今特性最丰富的路由和远程访问服务（RRAS）版本。这个版本把以前的各个版本的多协议路由器和 Windows NT 拥有的远程访问服务（RAS）的功能结合起来，并且进行了很多加强，包括配置过程的辅助向导和新的安全特性。把具有远程访问服务的多协议路由器结合进单个服务的理论基础是点对点协议（PPP）。PPP 用于协商和建立用于 RAS 的点对点的拨号连接和 Windows 2000 的按需拨号路由功能。微软公司认定在此基础上把这两种服务结合起来会很完美，而实际上也的确如此。路由和远程访问服务给管理员提供了一个统一的工具，它可以应用于从由两台计算机组成的小型的办公室/家庭（SOHO）网络，到由在不同地点的数千台计算机组成的网络的各种规模的网络。

越来越多的公司都有职员在家里通过使用与工作单位连接的计算机终端，进行远距离工作。另外，还有出现外部网的巨大趋势，在这种网络中公司允许他们的职员和用户在总公司资源的配合下访问或加入他们的资源。这种类型的业务方式正在变得越来越普遍。已经实现了多个允许远程访问或加入不同网络的解决方案，它们使用了几个不同厂家的工具。

有了 Windows 2000 路由和远程访问服务，管理员只需一个工具就可以满足所有路由、远程访问和虚拟专用网络（VPN）的需求。

本章是对路由和远程访问服务的一般概述。下面的章节将详细讲述这些服务的各种组件及对它们的配置。本章括号中的注解会指导读者在其他章节中找到有关具体主题的详细内容。由于远程访问服务部分是大多数管理员较熟悉的一部分，我们就从这部分开始介绍。然后讲述有关路由的部分，最后以 Windows 2000 中进一步加强了的路由和远程访问服务性能的其他特性的概览来结束本章。

1.1　远程访问组件

Windows 2000 的远程访问是一个将要实现的梦想。它可以用于从标准拨号、ISDN 线路到高速连接（如帧中继）等多种连接方法。第 2 章“远程访问服务器”将讲述远程访问服务器端的细节。第 3 章“拨号网络”讲述客户端。这部分引导读者进入 Windows 2000 的远程访问特性，具体包括：

- 按需拨入路由

- 认证协议的综合集
- 数据加密方法
- 包括 VPN 功能的点对点隧道
- 高效带宽利用
- 基于向导的配置
- 安全性和策略
- 认证、授权和账号管理
- Internet 连接共享

1.1.1　按需拨入路由

使用按需拨入路由可以减少基于广域网（WAN）的网络通信费用。如果用户网络的特定 WAN 线路经常使用但不是一直使用，那么用户就可能想在这种连接之上实现按需拨入路由。在线路一端的路由器收到一个要发往线路另一端的远程网络的数据包时，这个路由器就会拨号另一端的路由器，并把数据传送过去。因为广域网连接只是按需使用，并且可以配置成在预先定义的休止状态周期之后断开连接，与一个专用线路有关的使用费用就可以减少。

1.1.2　认证协议

Windows 2000 支持很多种认证协议，这样就可以让用户把远程访问服务扩展到各种各样的客户端类型。包含的认证协议是：

- 口令认证协议（PAP）
- Shiva-PAP（SPAP）
- 询问握手认证协议（CHAP）
- 微软询问握手认证协议（MS-CHAP），第 1 版和第 2 版
- 可扩展认证协议（EAP），包括 EAP-TLS 和 EAP-MD5
- 远程认证拨号用户服务（RADIUS）

1.1.3　数据加密

路由和远程访问服务提供了强大的连接加密方法，这种方法适用于北美和不在美国禁运名单上的国家。路由和远程访问服务还同时提供了可满足加密输出限制需求的方法。

1.1.4　点对点隧道

Windows 2000 支持使用点对点隧道协议（PPTP）和第 2 层隧道协议（L2TP）的隧道。这两种隧道方法都可以用于以客户/服务器或服务器/服务器为基础的虚拟专用网络（VPN）解决方案（详细内容见第 7 章“虚拟专用网络”）。与其他只支持客户/服务器隧道的商用 VPN 的解决方案相比，这种方法具有明显的优点。

1.1.5　高效带宽利用

除了按需拨入路由外，路由和远程访问服务还支持像节省带宽这样的特性：使用带宽分配协议（BAP）的多连接和远程访问服务（RAS）空闲断开。多连接是适应请求注解（RFC）的方法，这种方法捆绑多个 WAN 连接来生成一个大带宽虚拟隧道。BAP 建立在多连接功能基础上，来根据需要动态增加或断开线路。远程访问服务（RAS）空闲断开用来释放 WAN 连接，它是根据空闲时间或使用的带宽量，在使用率下降到低于管理设置级别时就释放连接（详细内容参阅第 10 章）。

1.1.6　向导

路由和远程访问服务使用了一系列的向导，可以很容易地配置各种各样的服务和远程访问组件。尽管可以直接配置服务组件，但当进行初始配置时，向导就有很大的帮助，它会给出与使用和配置参数有关的技巧和提示。

1.1.7　安全性和策略

路由和远程访问服务的安全部分包括使用远程客户访问智能卡的功能。访问也可以通过策略控制，策略根据 Windows 2000 的组成员资格或时间这些参数禁止或允许访问（有关智能卡的支持和生成远程访问策略的详细内容参见第 2 章）。

1.1.8　认证、授权和账号管理

认证指的是验证用户身份的过程；授权指的是决定是否允许用户访问的过程；而账目管理指的是跟踪使用一个具体服务（如远程访问服务器）的过程。对远程访问用户来说，有两种认证和授权方法可供使用：Windows 2000 的账号数据库和 RADIUS 服务器，如Windows 2000 中的 Internet 认证服务（IAS）（第 2 章有关于认证和授权的讨论，而更多有关 RADIUS 和 IAS 的内容参见第 9 章）。IAS 还可以用来提供账目管理服务。

1.1.9　Internet 连接共享

通过拨号网络，用户可以与一个网络中的其他计算机共享一个单独的 Internet 连接。在 SOHO 网络上，这是允许几个计算机访问 Internet 的理想方法（详见第 11 章“共享 Internet 连接”）。

1.2　路由组件

Windows 2000 路由器是一个全功能的多协议路由器。它是现在市场上可用的其他路由产品的划算的替代者。Windows 2000 与很大范围的局域网和广域网适配器兼容，这就意味着有极大的可能也支持你现在的 Windows 基础结构。它是一个开放的、可扩展的平台，即第三方软件或硬件供应商可以编写他们自己定做的解决方案来集成到路由和远程访问服务中。除了这些特性外，还支持广泛的路由协议集，包括：

- 用于 IP 网络的路由信息协议（RIP），第 1 版和第 2 版
- 开放最短路径优先（OSPF）
- 动态主机配置协议（DHCP）中继代理
- IP 多播路由
- 用于 IPX 网络的路由信息协议和服务通告协议（SAP）
- AppleTalk 路由
- 网络地址传输

这一部分主要提供这些协议的概要。你可以在第 4 章“路由协议”和第 5 章“配置 Windows 2000 路由器”中获得更详细的内容。

1.2.1　用于 IP 网络的路由信息协议第 1 版和第 2 版

路由信息协议（RIP）是适用于小型到中型网络的理想的路由协议，它是一个距离矢量路由协议。距离矢量路由使用 Bellman-Ford 算法。每个路由器保存一张路由表，该表为系统中的每个可能的目的地都留有条目。RIP 路由器通过公告共享 RIP 路由环境中的路由信息。Windows 2000 的 RIP 很容易配置，并且能与其他公司运行 RIP 的路由器共同使用。然而，因为在 RIP 环境中路由信息发布的方式，它不适合用于大型路由网络。

1.2.2　开放最短路径优先

Windows 2000 的开放最短路径优先（OSPF）是一个适应请求注解（RFC）的连接状态 IP 路由协议。它是由 Microsoft 和 Bay Networks 共同开发的。因为 OSPF 使用 Dijkstra 算法来计算到达目的地的最佳路由，因此在大型路由网络中它比 RIP 的效率更高。这个算法分析记录在路由器上连接状态数据库中的网络拓扑来确定最小代价的路由。OSPF 还排除发生在 RIP 路由网络中的环路问题。

1.2.3　DHCP 中继代理

DHCP（动态主机配置协议）中继代理使一个单独的 DHCP 服务器能为其并没有直接连接的网络服务。DHCP 通信量通常不能通过路由器传递，也就是意味着 DHCP 客户端必须和 DHCP 服务器位于同一个网络以利用 DHCP 的动态寻址功能。代理监听 DHCP 客户端的通信量并把通信传递给 DHCP 服务器。

1.2.4　IP 多播

Windows 2000 路由器支持多播传送和一种有限的多播路由。在 IP 多播中，主机使用 Internet 组管理协议（IGMP）给 IP 路由器提示主机正在监听有关一个特定的 IP 多播地址的 IP 多播通信量。多播路由器传送多播通信到那些主机已指示其正在监听这个通信的网络上。所有的 Windows 2000 计算机都具有 IP 多播功能，可以发送和接受 IP 多播通信。

需要全本请访问 www.ertongbook.com

1.2.5　用于 IPX 网络的路由信息协议和服务通告协议

Novell NetWare 网络通常使用互联网络包交换（IPX）作为它们主要的 LAN 协议。路由和远程访问服务可以在这样的环境下成功地实现 Windows 2000 路由器。IPX 网络的路由信息协议用于把 IPX 网络路由播放到其他的路由器。服务通告协议（SAP）则使得给其他服务器（如文件和打印服务器）提供服务的服务器能够通告它们的地址和它们提供的服务。

1.2.6　AppleTalk 路由

把 Windows 2000 路由器集成到 AppleTalk 网络中是可能的。路由和远程网络服务支持 AppleTalk 籽晶路由，并且可以使 Macintosh 网络在不需要另外的客户端软件的情况下实现互连。

1.3　其他特性

Windows 2000 还有其他的几个特性加强了路由和远程访问服务，这些特性包括：

- 互联网认证服务，一个适应 RFC 的 RADIUS 服务器
- 虚拟专用网络
- 连接管理器管理工具包

1.3.1　Internet 认证服务

互联网认证服务（IAS）提供认证、授权和用户账号的中心管理。它可以有效地从一个中心数据库（而不是从几个不同的服务器）管理远程用户访问。用户可以实现的一个 IAS 策略是协同使用 IAS 和拨号访问其他提供者（如 ISP）的外协远程用户。第 9 章解释了这个策略是如何把用户从维护成排的调制解调器和昂贵的拨号线路中解脱出来的。

1.3.2　虚拟专用网络

VPN 可以使远程用户或一个整个远程网络访问共同的局域网。VPN 连接是一种安全地通过公共网（如互联网）发送私人数据的隧道和加密方法。VPN 还用来在专用网上为共同局域网的数据传输提供额外的安全等级。Windows 2000 支持使用 Microsoft 点对点加密方法（MPPE）的点对点隧道协议（PPTP）和使用互联网协议安全（IPSec）的第二层隧道协议（L2TP）。有关 VPN 的功能和配置的详细内容参见第 7 章。

1.3.3　连接管理器服务

连接管理器是一个执行客户拨号和连接服务的应用程序。Windows 2000 中包括的两个组件可以让用户高效地为远程用户配置连接管理器。第一个组件，“连接管理器管理工具包”（CMAK），可以在连接管理器中给远程用户一本定制的拨号网络电话本。定制的连接管理器拨号器可以包括各种各样的存在点（POP）访问号码。拨号器可以在拨号一个远程访问连接之前或之后自动运行特定的应用程序。连接管理器服务的第二个组件是连接点服务。这个服务运行在 Windows 2000 服务器上，它为已经配置这个服务的远程客户更新电话本信息。有关

这些特性的详细内容参见第 8 章“Windows 2000 连接服务”。

1.4 总结

就像你看到的一样，Windows 2000 路由和远程访问服务是一个功能强大的产品。可把服务集成进现有网络的方法种类和建立新网络时把它用做一个组成部分的方法都是不可限量的。RRAS 利用当前的连接方法并且也可以扩展——也就是说对应新技术的新的解决方案可以很容易地开发和实现。另外，它可以替代许多第三方产品，而这些产品也许正是你已经考虑好要在你的网络中实现的，这样就节省了这笔潜在的花费。在你完成阅读本书的其他部分的过程中，你就会看到 Windows 2000 路由和远程访问服务是很容易配置的，并且很容易地在任何大小的网络中或配置中实现。

第 2 章　远程访问服务器

Windows 2000 提供了一个特性丰富的远程访问服务器（RAS），它可以使得远程客户端具有连接专用网络、局域网和互联网的功能。Windows 2000 RAS 是一个基于 PPP、TCP/IP、IPX 等工业标准的开放的和可扩展的远程访问平台。应用程序编程接口（API）可以供开发人员开发管理工具或插件（snap-in）来支持 RAS 不支持的协议。

由于 RAS 客户端和服务器软件已经彻底集成进 Windows 2000 操作系统中，因此你可以很容易地为你的用户设置远程访问系统。你可以让连接到远程访问服务器的用户只访问该服务器上的资源，也可以访问网络上的其他资源。RAS 的服务器访问叫做点对点远程访问连接，而整个网络访问叫做点对局域网远程访问连接。如果用户是所连接的局域网上的一个节点，他就可以访问网络上的资源。

2.1　RAS 概述

Windows 2000 RAS 为客户端提供了三种不同的远程访问连接类型，它们是：

- 拨号网络（DUN）
- 虚拟专用网络（VPN）
- 直接串口或红外连接

第 3 章“拨号网络”将详细介绍 DUN 的客户端；第 7 章“虚拟专用网络”讲述 VPN 的客户端和服务器端。本章的重点是 RAS 的服务器实现，包括远程访问组件、它们的功能以及如何安装和配置。

运行 Windows 2000 Professional 的计算机可以接收 3 个进入的呼叫，但对上面列出的类型而言，每种类型的呼叫最多不能超过一个。在 Windows 2000 服务器上，拨入呼叫的个数只能受到计算机的硬件配置的限制。这是在以前版本的 Windows NT 上的提高，Windows NT 在服务器上的同时拨入连接最多是 256 个，在工作站上只能有一个。

2.1.1　远程访问不是远程控制

在我们讨论 RAS 是什么、做什么之前，先说说 RAS 不是什么。远程访问服务和远程控制软件（如 pcANYWHERE）不是一回事，二者不应该混为一谈。RAS 是软件连接的解决方案，它连接用户以访问远程网络上的资源。多协议路由器把从服务器来的拨入通信信息向前传输到远程网络的资源，而服务器则接收拨入呼叫。

相反，远程控制软件是设计用来让远程用户通过远程连接运行应用程序并使用服务器的 CPU、键盘、鼠标等。远程控制软件是远程检查计算机故障的卓越方法，因为它给人一种就像正坐在远程计算机面前的感觉。如果你想提供一种工具让远程用户访问公司的网络资源，而他们却正在出差，RAS 就是一种较好的选择，主要有以下原因：

• 第一，它集成在 Windows 2000 中，所以你不需要购买其他的软件。

• 第二，它就是用来处理多用户的通信问题的，要比远程控制解决方案要好。

• 最后，它可以使你的用户远程访问所需要的资源，而同时有 Windows 2000 的安全机制保护网络。

2.1.2　远程访问服务器结构

我们以研究服务的技术结构来开始对 Windows 2000 RAS 的研究。图 2-1 是 RAS 的组件图。下面是对每个组件的解释。

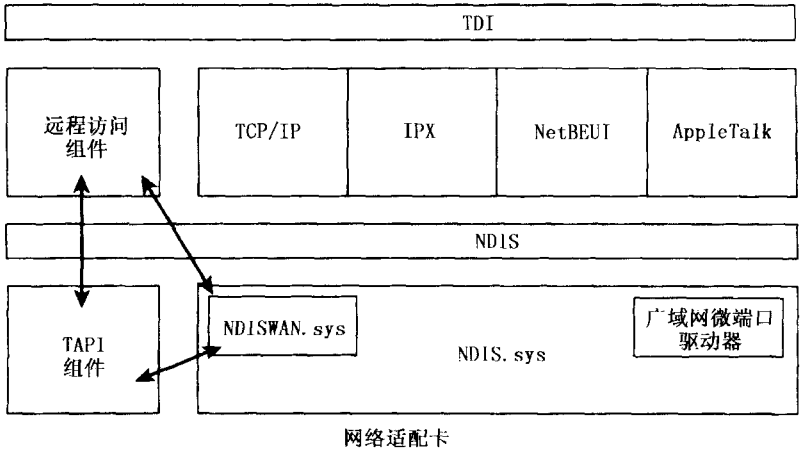


图 2-1　远程访问服务器结构

• 局域网协议　WindowsRAS 支持 TCP/IP、IPX、NetBEUI 和 AppleTalk。

• 远程访问组件　这些 RAS 应用程序编程接口提供了 RAS 应用程序与连接控制协议、认证协议、网络控制协议和远程访问协议之间的接口。就像图中所示，远程访问组件或者通过与 NDISWAN.sys 通信，或者通过与 TAPI（电话 API）通信来提供这些服务。

• 电话 API（TAPI）组件　这些应用程序编程接口为所有的电话 API 应用提供呼叫控制。TAPI 组件与 NDISWAN 驱动器通信进行连接管理。

• NDIS.sys　这个接口为所有支持的网络协议提供一个网络驱动器接口规范（NDIS）包装器接口。

• NDISWAN.sys　这个接口在给局域网协议驱动器提供 IEEE802.3 微端口接口的同时，也为广域网微端口驱动器提供局域网协议接口。远程访问连接从该驱动器获得数据包帧组，然后压缩、加密。

• 广域网微端口驱动器　每个物理拨号设备都有一个广域网微端口驱动器。

称为 RAS 服务器接口的单个适配器代表所有的 RAS 拨入连接。由远程访问服务器发起的每个呼出连接都要生成一个单独的接口。

某些事件被触发，就会在远程客户端和 RAS 服务器端之间建立一个任务：

1）客户端从服务器请求一个连接。这个请求由 RAS 组件收取，RAS 组件把呼叫连接信息传递给 TAPI 组件。

2）TAPI 组件把连接信息发送到电话设备，比如调制解调器或 ISDN 适配器。

3）RAS 组件直接与 NDISWAN.sys 协商 PPP 连接。RAS 组件确定该连接使用哪个连接、哪种认证、哪个网络控制协议。

在连接建立以后，NDISWAN.sys 可以从局域网协议驱动器接收请求。NDISWAN.sys 的工作是决定这个连接使用的合适的设备和端口。然后压缩并加密数据，把整个 PPP 帧发送到广域网微端口驱动器。广域网微端口驱动器把这个帧向前传送到拨号适配器。

既然远程访问连接已经建立并且是可使用的，远程客户端就能访问 RAS 上或远程网络上 RAS 之外的主机上的资源。如果正好是后一种情况，RAS 起到一个多协议路由器的作用，把信息量向前传送到合适的目的地。Windows 2000 RAS 可以路由 IP、IPX 和 AppleTalk 协议。点对局域网（Point-to-LAN）路由是管理员可以配置的一个选项。出于安全原因，你可能想把这个特性关闭掉，以避免远程访问客户访问你的网络的其他部分。

为支持使用 NetBEUI 的远程客户，Windows 2000 包括一个 NetBIOS 网关。这个 NetBIOS 网关允许远程用户使用 NetBEUI、TCP/IP 和 IPX 访问从远程访问服务器上可到达的任何基于 NetBIOS 的网络资源。但必须牢记，基于套接字（sockets-based）的资源对 NetBEUI 拨号客户而言是不可访问的。

在 NetBEUI 远程访问客户建立连接时，客户把它的 NetBIOS 名传递给 NetBIOS 网关。网关负责保证把客户的 NetBIOS 名称加到服务器上的 NetBIOS 名称表中。然后，从远程客户来的 NetBIOS 信息流被传送到 NetBIOS 网关，并使用合适的协议再传送到网络上的 NetBIOS 资源。反过程也是正确的：当远程访问服务器从网络主机接收到包时，就要检查包中的客户 NetBIOS 名。如果远程客户确实是目的地，就使用 NetBEUI 把数据发送到客户端，同时网关处理需要的协议转换。

2.1.3　启动路由和远程访问服务

要启动路由和远程访问服务（RRAS），只需执行下列步骤：

1）安装和配置适当的硬件。

2）打开“Routing and Remote Access”控制台，点击“Start”→“Programs”→“Administrative”，从菜单中选择“Routing and Remote Access”。

3）缺省状态下，本地计算机被显示出来。如果没有列出来，或者你想增加另外一台服务器，右键点击“Server Status”，然后点击“Add Server”。

4）在“Add Server”对话框中，选择你想增加的服务器应用选项，然后点击“OK”。

5）右键点击你想启用为远程访问服务器的服务器，并点击“Configure and Enable Routing and Remote Access”。

6）路由和远程访问向导就会出现，按照屏幕上的提示步骤做。在向导完成时，就会提示你启动路由和远程访问服务。

在该项服务启动后，你可以直接编辑远程访问服务器的属性，如图 2-2 所示。

右键点击你要修改的服务器并从菜单中选择“Properties”。属性对话框包含下述配置信息：

- 该服务器是否作为路由器和/或远程访问服务器。
- 使用的认证方法和提供者。配置选项在本章2.2节的“认证和授权”中讨论。
- 是只允许远程用户访问该服务器，还是访问整个网络。属性对话框中的每个协议标签都将以稍微不同的方法问这个问题。
- IP和/或IPX地址是如何分配给所连接的客户的。
- 多连接的PPP配置选项，LCP扩展和软件压缩。这些主题将要在第10章“带宽和远程通信技术”中叙述。
- 事件日志设置。

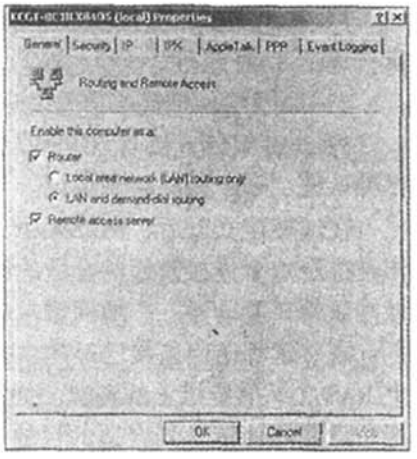


图2-2　路由和远程访问服务器的属性对话框

当RRAS在服务器上初始启动时，路由和远程访问向导需要请求这些信息。向导还请求有关服务器上安装的特定设备是如何配置的信息。你可以逐个配置设备，也可以把设备配置为一个组。在向导完成后，可以通过打开端口属性对话框为适当的服务器改变配置。

2.1.4　RAS支持的局域网协议

Windows 2000远程访问服务器通过PPP连接支持TCP/IP、IPX、NetBEUI和AppleTalk协议。这样就给系统管理员一个能力，他能容易地在使用这些协议的网络中加入一台运行Windows 2000 Server的计算机。因为Windows 2000 Server自动地使用所支持的且已经安装并运行在服务器上的协议，因此把一个服务器配置为一个远程访问服务器就相当简单。这部分讨论局域网协议和针对这些协议的配置选项。

1．TCP/IP协议

TCP/IP协议是世界上使用最广泛的协议。因其可伸缩性和高适应性，因此被用于各种规模的网络上，从只含有两个工作站的网络到含有异地数千台计算机由各种类型的局域网、城域网和广域网连接组成的大型网络。

配置一个TCP/IP的RAS服务器要求你确定如何给远程客户分配一个IP地址。命名解析也是一个重要的配置选项。这些参数在服务器到服务器（server-by-server）的情况下需要配置。让我们从检查IP地址分配开始本部分的学习。

分配IP地址

当远程客户连接到远程访问服务器时，它会被以下述三种方式之一分配一个地址：

- 从DHCP服务器
- 从一个静态IP地址池中
- 从用户账号的拨入属性页上所分配的静态IP地址中

需要全本请访问 www.ertongbook.com