

## <<网络拓展配置与管理>>

### 图书基本信息

书名：<<网络拓展配置与管理>>

13位ISBN编号：9787115109378

10位ISBN编号：7115109370

出版时间：2002-12

出版单位：人民邮电出版社

作者：钟小平

页数：486

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网络拓展配置与管理>>

### 内容概要

本书旨在帮助读者快速掌握高级组网技术，提高网络管理水平。

本书主要围绕计算机网络的管理性、扩展性、共享性和安全性，联系组网用网的实际需求，系统地介绍了路由器、远程访问、代理服务器、网络地址转换、防火墙、IPSec和虚拟专用网络等网络技术，并详细讲解了如何使用微软的企业级产品ISA Server实现网络安全和共享服务。

另外，还介绍了网络检测与故障诊断、活动目录、证书服务等内容。

本书兼顾系统性和实用性，在介绍相关背景知识、评介有关产品的基础上，重点介绍具体的软件解决方案，以实例操作一步一步地引导读者来完成网络的配置和管理。

本书同时讲解服务器端和客户端的组网技术，穿插了作者的经验和体会，针对重要问题提供了问题解答，部分章节还安排了练习题。

所提供的软件解决方案，既能满足中小型企业或机构的组网需要，又便于读者学习和试验新的网络技术。

由于Windows 2000 Server本身集成了强大的组网功能，本书介绍的软件解决方案均以微软公司产品

和Windows平台本身内置功能为主，兼顾第三方软件产品。其中服务器端以Windows 2000 Server为主，客户端以Windows 98和Windows 2000为主，兼顾最新的Windows XP。

书中还详解了Windows 2000路由和远程访问服务。

本书面向网络管理人员、网络维护人员和电脑爱好者，要求读者具备初步的局域网知识，特别适合于需要学习高级组网技术的IT技术人员和高校学生，也可作为网络管理参考书和培训教程。

# <<网络拓展配置与管理>>

## 书籍目录

第1章 网络检测和故障诊断	1
1.1 分析和排查网络故障的基本方法	1
1.1.1 OSI模型及其层次结构	1
1.1.2 理解Windows 2000的网络层次	3
1.1.3 分层分析和排查网络故障	4
1.2 网络检测和诊断工具	5
1.2.1 命令行检测工具	6
1.2.2 事件查看器	11
1.2.3 网络监视器	13
第2章 活动目录和证书服务	21
2.1 Active Directory及其配置	21
2.1.1 了解Active Directory目录服务	21
2.1.2 Active Directory结构	22
2.1.3 Active Directory 管理工具	24
2.1.4 安装Active Directory	25
2.1.5 设置Active Directory客户	28
2.1.6 Active Directory的基本管理	30
2.1.7 Active Directory站点简介	35
2.2 通过组策略集中配置Windows 2000网络	35
2.2.1 理解组策略	35
2.2.2 配置组策略对象	37
2.2.3 刷新组策略	39
2.2.4 本地组策略	40
2.3 Windows 2000证书服务	41
2.3.1 公钥基础结构和证书	41
2.3.2 规划证书颁发机构	42
2.3.3 安装证书服务	43
2.3.4 证书颁发机构的配置和管理	44
2.3.5 客户端的证书管理	48
2.3.6 证书注册	49
2.4 理解Windows 2000的身份验证	54
2.4.1 Windows 2000身份验证过程	54
2.4.2 Windows 2000身份验证类型	55
2.4.3 Windows 2000智能卡简介	56
2.4.4 基于证书的身份验证	56
第3章 通过路由器实现网络互联	59
3.1 理解路由技术	59
3.1.1 路由和路由器	59
3.1.2 路由表	60
3.1.3 路由选择过程	62
3.1.4 静态路由和动态路由	63
3.1.5 路由协议	64
3.2 微软的软件路由器解决方案	67
3.3 软件路由器的基本配置	68
3.3.1 了解路由接口	68

## <<网络拓展配置与管理>>

3.3.2 软件路由器配置基本步骤	69
3.4 简单网络的路由器方案--设置静态路由	72
3.4.1 最简单的路由方案	72
3.4.2 多路由器互联网络的静态路由方案	76
3.4.3 设计静态路由应注意的问题	80
3.5 设置RIP路由	80
3.5.1 快速设置Windows 2000 RIP路由	80
3.5.2 进一步配置Windows 2000 RIP路由	82
3.5.3 设计RIP路由网络应注意的问题	86
3.5.4 设计层次结构网络的RIP路由	86
3.5.5 在Windows NT环境下配置RIP路由	87
3.6 设置OSPF路由	88
3.6.1 OSPF路由网络的规划	88
3.6.2 快速配置OSPF路由网络	89
3.6.3 进一步配置OSPF路由	92
3.6.4 设计OSPF路由网络应注意的问题	96
3.7 设置多播路由	96
3.7.1 理解多播和多播路由	96
3.7.2 Windows 2000的多播路由应用场合	98
3.7.3 快速配置IP多播支持	99
3.7.4 进一步配置IP多播支持	100
3.8 使用WinRoute构建软件路由器	102
3.9 使用Windows XP的桥接功能实现网络互联	103
3.9.1 网桥概述	103
3.9.2 用Windows XP桥连多个网段	103
3.10 跨越路由器的DHCP中继	105
3.10.1 DHCP中继代理概述	105
3.10.2 在Windows 2000 Server计算机上实现DHCP代理	106
3.10.3 在Windows NT Server计算机上实现DHCP代理	107
3.11 问题解答	108
3.11.1 如何排查Windows 2000路由器故障	108
3.11.2 Windows 95/98能否作为软件路由器	109
3.11.3 如何确定路由的优先级	109
3.11.4 如何为主机实时配置默认网关	110
3.11.5 如何让路由协议通过防火墙	110
第4章 远程访问	111
4.1 远程访问概述	111
4.1.1 了解远程访问	111
4.1.2 Windows 2000的远程访问	112
4.2 理解Windows 2000拨号网络	112
4.2.1 拨号网络服务器	113
4.2.2 拨号网络客户机	113
4.2.3 拨号连接	113
4.2.4 LAN和远程访问协议	114
4.2.5 远程访问服务器的路由和网关功能	115
4.3 设置拨号网络服务器	116
4.3.1 安装并配置拨号设备	116

## <<网络拓展配置与管理>>

- 4.3.2 配置远程访问服务器 116
- 4.3.3 设置远程用户账户拨入属性 119
- 4.4 设置拨号网络客户机 122
  - 4.4.1 设置Windows 98拨号网络客户机 122
  - 4.4.2 设置Windows 2000拨号网络客户机 124
- 4.5 管理远程访问客户 125
  - 4.5.1 在路由和远程访问控制台中管理远程访问客户 125
  - 4.5.2 通过"网络和拨号连接"文件夹管理远程访问客户 126
- 4.6 远程访问服务器的高级设置 127
  - 4.6.1 配置远程访问端口 127
  - 4.6.2 启用远程访问服务器 128
  - 4.6.3 设置身份验证和记账功能 128
  - 4.6.4 设置TCP/IP协议 131
  - 4.6.5 设置其他网络协议 133
  - 4.6.6 设置PPP选项 133
  - 4.6.7 设置事件日志 133
- 4.7 设置远程访问策略 134
  - 4.7.1 远程访问策略简介 134
  - 4.7.2 远程访问策略应用流程 135
  - 4.7.3 建立自己的远程访问策略 136
  - 4.7.4 管理多个远程访问策略 140
  - 4.7.5 远程访问策略管理模式 140
- 4.8 拨号网络应用范例 142
  - 4.8.1 企业远程访问服务范例 142
  - 4.8.2 Internet接入服务范例 145
- 4.9 对多个远程访问服务器使用RADIUS集中验证 146
  - 4.9.1 RADIUS简介 147
  - 4.9.2 了解Internet验证服务器 147
  - 4.9.3 安装IAS 149
  - 4.9.4 配置RADIUS 149
  - 4.9.5 设置RADIUS远程访问策略 152
  - 4.9.6 IAS应用范例 154
- 4.10 远程访问安全性综述 154
  - 4.10.1 远程访问客户机连接远程访问服务器的过程 154
  - 4.10.2 远程访问的安全措施 155
- 4.11 问题解答 156
  - 4.11.1 Windows 2000远程访问有哪些新特性 156
  - 4.11.2 如何避免策略配置文件设置与服务器属性设置的冲突 157
  - 4.11.3 为什么远程用户连接成功后无法访问网络资源 157
  - 4.11.4 为什么要慎用账户锁定 157
  - 4.11.5 能否对远程访问实现端对端加密 157
  - 4.11.6 如何实现远程访问的名称解析 157
  - 4.11.7 Windows 2000远程访问服务器有哪些日志记录 158
  - 4.11.8 如何通过防火墙进行RADIUS验证 158
- 第5章 远程网络互联 159
  - 5.1 远程网络互联基础 159
    - 5.1.1 远程连接技术简介 159

## <<网络拓展配置与管理>>

- 5.1.2 远程网络互联类型 162
- 5.2 通过专用WAN连接实现远程网络互联 164
- 5.3 通过请求拨号连接实现远程网络互联 165
  - 5.3.1 进一步了解请求拨号路由 165
  - 5.3.2 规划请求拨号路由网络 166
  - 5.3.3 配置请求拨号路由器 167
  - 5.3.4 测试和管理请求拨号路由连接 173
  - 5.3.5 理解请求拨号路由的连接过程 175
  - 5.3.6 进一步配置请求拨号路由器 176
  - 5.3.7 配置单向初始化的请求拨号连接 178
- 5.4 实现复杂网络的请求拨号路由 179
  - 5.4.1 一个网络与多个网络通过请求拨号连接互联 179
  - 5.4.2 互联网络之间的请求拨号连接 181
- 5.5 问题解答 182
  - 5.5.1 专用WAN连接的路由设置应注意哪些问题 182
  - 5.5.2 请求拨号路由与远程访问有什么关系 182
  - 5.5.3 如何选择请求型或持续型请求拨号连接 183
  - 5.5.4 请求拨号连接的路由设置应注意哪些问题 183
  - 5.5.5 如何应用自动静态路由 183
  - 5.5.6 如何根据IP数据包筛选器阻止请求拨号连接 184
- 第6章 代理服务器与网络地址转换 185
  - 6.1 Intranet连入Internet的方式 185
    - 6.1.1 Intranet连入Internet的几种方式 185
    - 6.1.2 Internet连接类型 186
  - 6.2 代理服务器基础 187
    - 6.2.1 代理服务器的功能 187
    - 6.2.2 代理方式 187
    - 6.2.3 反向代理 191
    - 6.2.4 理解缓存 191
    - 6.2.5 代理服务器产品 193
    - 6.2.6 代理服务器的一般配置过程 193
  - 6.3 理解网络地址转换 194
    - 6.3.1 网络地址转换的作用 194
    - 6.3.2 网络地址转换的工作原理 195
    - 6.3.3 网络地址转换的类型 196
    - 6.3.4 网络地址转换产品 196
    - 6.3.5 网络地址转换的一般配置 197
  - 6.4 使用WinGate代理服务器 197
    - 6.4.1 WinGate代理服务器概述 197
    - 6.4.2 WinGate的安装和配置 199
    - 6.4.3 WinGate服务的管理 204
  - 6.5 通过Windows 2000 Server实现网络地址转换 212
    - 6.5.1 深入了解Windows 2000 Server的NAT 212
    - 6.5.2 通过NAT服务器实现网络共享 213
    - 6.5.3 让Internet用户通过NAT服务器访问内部服务 217
    - 6.5.4 查看NAT映射表 219
  - 6.6 微软的Internet连接共享 220

## <<网络拓展配置与管理>>

6.6.1 Windows 98 Se和Windows Me的Internet连接共享	220
6.6.2 Windows 2000的Internet连接共享	221
6.6.3 使用Windows XP的连接共享功能	222
第7章 构筑防火墙实现网络安全	227
7.1 防火墙的作用	227
7.2 防火墙的类型	228
7.2.1 网络级防火墙--包过滤路由器	228
7.2.2 电路级防火墙--电路网关	229
7.2.3 应用级防火墙--应用网关	229
7.2.4 状态检测防火墙	230
7.3 常见的防火墙配置	231
7.3.1 双宿主机关	231
7.3.2 屏蔽主机网关	231
7.3.3 屏蔽子网 ( Screened Subnet )	232
7.4 防火墙产品及其选择	233
7.4.1 硬件防火墙和软件防火墙	233
7.4.2 防火墙产品的功能	234
7.4.3 防火墙产品简介	234
7.5 包过滤的基本配置	235
7.5.1 包过滤原理	235
7.5.2 了解包过滤规则	239
7.5.3 设置包过滤规则应注意的问题	240
7.5.4 常用网络服务的包过滤规则	241
7.6 通过Windows 2000 RRAS实现包过滤	244
7.7 使用WinRoute保护中小型网络安全	246
7.7.1 WinRoute的特性	246
7.7.2 WinRoute的体系结构	248
7.7.3 WinRoute的安装	249
7.7.4 WinRoute网络的基本设置	249
7.7.5 通过NAT方式共享Internet访问	251
7.7.6 通过端口映射开放内部服务器	253
7.7.7 WinRoute的高级NAT设置	257
7.7.8 使用WinRoute构筑包过滤防火墙	260
7.7.9 使用WinRoute代理服务共享Internet访问	267
7.7.10 使用WinRoute的日志和包分析功能	270
7.7.11 使用WinRoute布置非军事区	271
7.7.12 WinRoute与虚拟专用网络	273
7.7.13 将WinRoute用于其他复杂网络	275
7.7.14 WinRoute对特殊服务和应用程序的支持	277
7.8 个人防火墙	277
7.8.1 个人防火墙简介	277
7.8.2 使用Sygate Persional Firewall建立个人防火墙	278
7.8.3 Windows XP的Internet连接防火墙	286
7.9 问题解答	287
7.9.1 WinRoute与哪些软件有冲突	287
7.9.2 WinRoute内置的DNS服务是如何工作的	288
7.9.3 如何使内部用户使用公共域名来访问内部服务器	288



## <<网络拓展配置与管理>>

7.9.4 如何通过WinRoute访问非标准端口FTP服务器 289

第8章 用ISA Server构建企业防火墙 291

8.1 ISA Server的特性 291

8.2 ISA Server服务器安装和基本配置 293

8.2.1 ISA Server的组件 293

8.2.2 ISA Server版本 294

8.2.3 独立服务器和阵列成员 294

8.2.4 ISA Server安装模式 294

8.2.5 ISA Server计算机配置 295

8.2.6 安装ISA Server 296

8.2.7 ISA管理控制台 297

8.2.8 管理ISA服务 298

8.3 ISA Server客户安装和配置 299

8.3.1 选择ISA Server客户端 299

8.3.2 配置SecureNAT客户 300

8.3.3 配置防火墙客户 300

8.3.4 配置Web代理客户 304

8.4 ISA Server策略和策略元素 305

8.4.1 ISA Server策略 305

8.4.2 ISA Server规则 305

8.4.3 配置策略元素 306

8.5 ISA Server分层过滤 311

8.5.1 包过滤 311

8.5.2 电路层过滤 316

8.5.3 应用程序过滤 317

8.6 控制内部用户的外出访问 318

8.6.1 ISA Server如何控制外出请求 318

8.6.2 配置协议规则 318

8.6.3 配置站点和内容规则 321

8.6.4 为外出访问配置IP包过滤器 323

8.6.5 路由规则和防火墙链式配置 324

8.6.6 设置外出Web请求属性 327

8.6.7 使用ISA Server的验证功能 328

8.6.8 通过应用程序过滤器控制外出访问 330

8.7 防止外部用户的非法访问 333

8.7.1 ISA Server对外防御概述 333

8.7.2 配置ISA Server系统安全级别 333

8.7.3 为外来访问配置IP包过滤 334

8.7.4 配置入侵检测 335

8.8 对外发布服务 338

8.8.1 发布服务概述 338

8.8.2 在内部网络中发布Web服务器 338

8.8.3 Web发布规则和路由规则 343

8.8.4 在ISA Server计算机上发布Web服务器 344

8.8.5 在内部网络中发布服务器 345

8.8.6 使用向导创建邮件服务器发布规则 346

8.8.7 自定义服务的发布 348



## <<网络拓展配置与管理>>

- 8.8.8 通过应用程序过滤器来辅助发布服务 348
- 8.9 通过周边网络来强化网络安全 349
  - 8.9.1 构建ISA Server三宿主防火墙 349
  - 8.9.2 背对背周边网络配置 351
- 8.10 通过缓存配置提高网络性能 353
  - 8.10.1 了解ISA Server缓存 353
  - 8.10.2 设置缓存 353
  - 8.10.3 设置缓存空间大小和位置 355
  - 8.10.4 定时内容下载 355
- 8.11 带宽规则 357
  - 8.11.1 创建带宽优先级策略元素 357
  - 8.11.2 创建带宽规则 358
- 8.12 日志记录和实时监控 359
  - 8.12.1 配置警报 359
  - 8.12.2 配置日志 361
  - 8.12.3 通过报表来进行日志记录统计分析 363
  - 8.12.4 实时监控 365
- 8.13 实现虚拟专用网络 366
  - 8.13.1 配置VPN远程访问 366
  - 8.13.2 配置VPN远程网络互联 368
  - 8.13.3 在ISA Server后面使用PPTP客户机 370
- 8.14 企业级扩展 371
  - 8.14.1 分布式缓存阵列 371
  - 8.14.2 链式缓存阵列 372
- 8.15 问题解答 372
  - 8.15.1 安装ISA Server应注意哪些问题 372
  - 8.15.2 ISA Server验证应注意哪些问题 373
  - 8.15.3 用户通过ISA Server进行访问通常会遇到哪些问题 373
  - 8.15.4 如何通过ISA Server发布SSL安全站点 373
  - 8.15.5 周边网络如何与内部网络通信 374
  - 8.15.6 ISA Server与Active Directory如何集成 374
  - 8.15.7 ISA Server如何影响路由和远程访问服务 374
  - 8.15.8 ISA Server能否与IPSec组合使用 374
- 第9章 通过IPSec实现网络安全 377
  - 9.1 IPSec基础 377
    - 9.1.1 IPSec的特性 378
    - 9.1.2 IPSec安全协议 380
    - 9.1.3 IPSec的主要组件 382
    - 9.1.4 IPSec工作原理 384
    - 9.1.5 IPSec的应用 385
  - 9.2 IPSec策略及其配置 385
    - 9.2.1 理解IPSec的组策略 386
    - 9.2.2 启用IPSec策略代理服务 386
    - 9.2.3 IPSec策略管理工具 387
    - 9.2.4 配置IPSec策略 388
    - 9.2.5 指派IPSec策略 394
    - 9.2.6 通过组策略对象来集中管理IPSec策略 395

## <<网络拓展配置与管理>>

- 9.3 使用IPSec保护两个主机之间的网络通信 396
  - 9.3.1 IPSec测试准备 397
  - 9.3.2 使用默认IPSec策略保护两个域成员计算机之间的通信 398
  - 9.3.3 通过自定义IPSec策略保护两个主机之间的通信 403
  - 9.3.4 非域成员计算机间的IPSec通信 408
- 9.4 使用证书进行IPSec验证身份 409
  - 9.4.1 理解用于IPSec的证书验证 409
  - 9.4.2 获得用于IPSec身份验证的证书 409
  - 9.4.3 为IPSec规则配置证书身份验证 413
- 9.5 建立IPSec隧道保护网络之间的通信 414
  - 9.5.1 进一步理解IPSec隧道 415
  - 9.5.2 建立IPSec隧道 415
  - 9.5.3 测试IPSec隧道 422
- 9.6 在Windows XP中使用IPSec 424
- 9.7 问题解答 426
  - 9.7.1 为什么数据通信没有被IPSec保护 426
  - 9.7.2 为什么IPSec SA协商失败 426
  - 9.7.3 使用证书进行验证时IPSec SA协商失败 426
  - 9.7.4 本地计算机IPSec策略未被使用 426
  - 9.7.5 IPSec不能保护哪些类型的IP通信 426
  - 9.7.6 如何使IPSec通信能够通过防火墙 427
  - 9.7.7 为什么NAT与IPSec不兼容 427
  - 9.7.8 IPSec可防御哪些网络攻击 427
  - 9.7.9 是否允许对通信进行单向IPSec保护 428
  - 9.7.10 在一对主机之间只有一个身份验证方法 428
  - 9.7.11 如何在域控制器与DHCP、DNS服务器上应用IPSec 428
- 第10章 构建虚拟专用网络 431
  - 10.1 虚拟专用网络基础 431
    - 10.1.1 虚拟专用网络的工作机制 431
    - 10.1.2 虚拟专用网络的应用 432
    - 10.1.3 VPN标准和协议 434
    - 10.1.4 VPN产品及解决方案 434
  - 10.2 微软的VPN解决方案 435
    - 10.2.1 微软的VPN解决方案概述 435
    - 10.2.2 了解Windows 2000的VPN远程访问 436
    - 10.2.3 Windows 2000的VPN远程网络互联 437
  - 10.3 进一步理解VPN隧道协议 437
    - 10.3.1 理解PPTP协议 438
    - 10.3.2 理解L2TP/IPSec 438
    - 10.3.3 L2TP/IPSec与PPTP的比较 440
  - 10.4 基于PPTP的VPN远程访问 441
    - 10.4.1 设置PPTP VPN的一般步骤 441
    - 10.4.2 配置PPTP服务器 441
    - 10.4.3 设置PPTP客户机 449
  - 10.5 基于L2TP的VPN远程访问 456
    - 10.5.1 设置L2TP VPN的一般步骤 456
    - 10.5.2 配置L2TP服务器 456

## <<网络拓展配置与管理>>

- 10.5.3 配置L2TP客户端 459
- 10.5.4 确认已安装计算机证书 459
- 10.5.5 测试L2TP 460
- 10.6 基于PPTP的VPN远程网络互联 462
- 10.6.1 实现VPN远程网络互联应注意的问题 462
- 10.6.2 规划VPN请求拨号路由网络 463
- 10.6.3 配置PPTP请求拨号路由器 463
- 10.6.4 测试和管理VPN请求拨号路由 468
- 10.6.5 请求型PPTP请求拨号路由 469
- 10.7 基于L2TP的VPN远程网络互联 472
- 10.8 利用自定义的IPSec策略实现L2TP 473
- 10.8.1 修改注册表以更改系统默认设置 473
- 10.8.2 为L2TP/IPSec连接创建使用预共享密钥验证的IPSec策略 474
- 10.9 VPN与其他网络技术的组合使用 475
- 10.9.1 VPN与防火墙组合使用 475
- 10.9.2 VPN与NAT组合使用 476
- 10.9.3 在VPN隧道中建立VPN隧道 477
- 10.10 问题解答 477
- 10.10.1 如何排查Windows 2000的VPN连接故障 477
- 10.10.2 为何要避免远程访问策略配置文件与VPN服务器属性冲突 477
- 10.10.3 为什么不能成功建立L2TP/IPSec 478
- 10.10.4 如何选择虚拟专用网络技术 478
- 10.10.5 VPN服务器的Internet连接方式有哪些 479
- 附录A 练习题参考答案 481
- A.1 第3章练习题参考答案 481
- A.1.1 练习3.1参考答案 481
- A.1.2 练习3.2参考答案 481
- A.1.3 练习3.3参考答案 481
- A.2 第5章练习题参考答案 482
- A.2.1 练习5.1参考答案 482
- A.2.2 练习5.2参考答案 482
- A.3 第7章练习题参考答案 483
- A.3.1 练习7.1参考答案 483
- A.3.2 练习7.2参考答案 483
- A.3.3 练习7.3参考答案 483
- A.3.4 练习7.4参考答案 484
- A.3.5 练习7.5参考答案 484
- 附录B 多宿主(地址)计算机 485
- B.1 多重逻辑地址--单个网络接口支持多个IP地址 485
- B.2 多重物理地址--一台计算机安装多个网卡 485

## <<网络拓展配置与管理>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>