

高级技术培训教材系列

实现和维护

Windows Server 2003

网络基础结构：网络服务

北京希望电子出版社 总策划
杨洪振 编 著



中国科学技术出版社
CHINA SCIENCE AND TECHNOLOGY PRESS



北京希望电子出版社
Beijing Hope Electronic Press
www.bhpe.com.cn

高级技术培训教材系列

实现和维护

Windows Server 2003

网络基础结构：网络服务

北京希望电子出版社 总策划
杨洪振 编 著



中国科学技术出版社
CHINA SCIENCE AND TECHNOLOGY PRESS



北京希望电子出版社
Beijing Hope Electronic Press
www.bhpe.com.cn

图书在版编目 (CIP) 数据

实现和维护 Windows Server 2003 网络基础结构: 网络服务/
杨洪振编著. —北京: 中国科学技术出版社; 2005.5
高级技术培训教材系列

ISBN 7-5046-3765-3

I. 实... II. 杨... III. 服务器—操作系统
(软件), Windows Server 2003—技术培训
—教材 IV. TP316.86

中国版本图书馆 CIP 数据核字 (2004) 第 024252 号

书 名: 实现和维护 Windows Server 2003 网络基础结构: 网络服务
总 策 划: 北京希望电子出版社
著 者: 杨洪振
责 任 编 辑: 安源
出版、发行者: 中国科学技术出版社 北京希望电子出版社
地 址: 北京市海淀区中关村南大街 16 号 100081
北京市海淀区上地信息产业基地 3 街 9 号金隅嘉华大厦 C 座 610 100085
网址: www.bhp.com.cn E-mail: lwm@bhp.com.cn
电话: 010-82702660, 010-82702658, 010-62978181 转 103 或者 238
经 销: 各地新华书店、软件连锁店
排 版: 希望图书输出中心 娄艳
印 刷 者: 北京双青印刷厂
开本 / 规格: 787 毫米×1092 毫米 1/16 26.375 印张 645 千字
版次 / 印次: 2005 年 5 月第 1 版 2005 年 5 月第 1 次印刷
印 数: 1~5000 册
书 号: ISBN 7-5046-3765-3
定 价: 45.00 元

内 容 简 介

本书是 Windows Server 2003 高级技术培训教材之一。

全书共分 12 章，内容包括：企业中的路由规划；使用 DHCP 为企业中的主机自动分配 IP 地址；满足企业名称解析需求，使用 DNS 来实现主机名解析，使用 WINS 来实现 NetBIOS 名称解析；使用 IPSec 来设计实现安全的网络通信过程；用证书服务来实现企业的安全身份验证过程；企业对远程访问方案的需求，详细讲解了远程访问方案的设计实现，包括使用拨号访问、无线连接、VPN 等多种方式进行远程访问，并设计实现远程访问的集中身份验证。

本书结构清晰，内容详尽，通过实例分析和课后练习来帮助学习者理解和掌握所学习的知识、概念和操作技巧。本书是网管人员、技术爱好者系统全面学习 Windows Server 2003 的很好的辅助教材，同时也可以作为参加 Windows Server 2003 系统工程师认证（对应 MCSE 课程号 2277，考试号 70-291）的很好的参考资料。

总 序

“Windows 团队有 5000 个成员，加上额外的 5000 个合作伙伴，于是生产了超过 5000 万行的 Windows Server 2003 代码。所有人员遵从统一的领导制造代码，生成他们的工作结果，编译并连接为可执行程序或其他组件，最后组成一个 Windows 的 CD。这个过程持续 12 到 13 小时，每一天都在进行，这是曾经尝试过的最大的软件工程任务，没有其他软件项目可与之相比。”

——Mark Lucovsky（Windows Server 的设计师）

从微软公司推出 Windows Server 2003 beta 版本以来，我们就一直对它密切跟踪着。随着产品的发布，人们对它的兴趣也越来越浓。为了让广大读者、技术爱好者能找到一本专业的教材，我们集中了多名对 Windows Server 2003 感兴趣的工程师，他们都是处在微软教学第一线 MCT（Microsoft Certified Trainer）的教员，以及对微软产品有着深厚经验技术的爱好者，这样大家就开始了 Windows Server 2003 技术的研究学习。针对这套知识体系以及微软公司新推出的面向 Windows Server 2003 的考试，我们策划编写了这一套丛书，希望通过它可以帮助大家 Windows Server 2003 技术进行全面的了解，并对参加 MOC 考试有所帮助。经过我们的不懈努力，现在这套教材终于与大家见面。

在这套丛书中，每一章的开始都简单介绍章节的主要内容和学习目标，以便读者在学习过程中作为参照。每章都包含部分的案例研究分析，从读者的角度去理解案例，可以大大加深读者的学习效果。结尾处均包含相关 MCSE 考试的模拟试题和答案分析。这些模拟试题能有效地帮助读者在学习具体知识的同时备战 MCSE 考试。

本套丛书注重理论联系实际，所有内容采用图文并茂的形式帮助读者理解，每一张截图都是作者从实际网络环境中精心准备得来。每章都设计了实践操作部分，让读者不仅可以学到理论知识，而且能在书中的指导下进行实践操作。丛书是想系统全面学习 Windows Server 2003 的网管人员、技术爱好者很好的辅助教材，其中的典型模拟试题的分析更是希望参加微软 Windows Server 2003 系统工程师认证（MCSE）人员的很好的参考资料。

丛书中我们介绍了一些使用经验和心得，难免有不当之处，或者还有更好的方法欢迎赐教。如果有需要交流的地方可与作者联系，欢迎与您的真诚交流。

一件作品的完成是众人智慧与努力的结晶，在此特别感谢北京希望电子出版社。感谢编辑栾大成先生的努力工作，他的幽默风趣的言谈，踏实的工作态度让我记忆深刻。没有他的专业眼光和地细节的关注，这一系列图书的出版不能如此顺利。同时感谢在本书的编写过程中曾给予我帮助的朋友们：我的挚友刘春田、李明清，以及身边的众多给予帮助的朋友，你们带给了我启发和欢笑，愿你们可以完成心中所愿。给予我心灵上支持的杨蓉：带给你祝福，坚持下去，你的愿望一定会实现。谢谢朋友们的大力支持。

MCT（微软认证讲师）
杨洪振

前言

Windows Server 2003 是继 Windows 2000 之后微软公司推出的新一代操作系统。本书详细讲解了基于 Windows Server 2003 的基础网络架构,其中包含真实的背景资料,图文并茂,实践操作性强。在课程中,对每一步的操作都提供了截图,给读者提供一个真实的场景实践,确保读者可以从本书中得到实践操作的环境。

全书共分 12 章内容,系统介绍了一个完整的企业基础网络架构。内容以企业应用需求为主线,详细地讲解包括:企业中的路由规划;使用 DHCP 为企业中的主机自动分配 IP 地址;满足企业名称解析需求,使用 DNS 来实现主机名解析,使用 WINS 来实现 NetBIOS 名称解析;使用 IPSec 来设计实现安全的网络通信过程;用证书服务来实现企业的安全身份验证过程;企业对远程访问方案的需求,详细讲解了远程访问方案的设计实现,包括使用拨号访问、无线连接、VPN 等多种方式进行远程访问,并设计实现远程访问的集中身份验证。

对于 DHCP、DNS 和 WINS 这三大服务,以及远程访问是本书的重点所在。另外,考虑到安全性规划,则使用 IPSec 来实现安全的网络通信,使用证书实现安全的身份验证,这些也是 MOC 的考点,所以本书的内容在 Windows servers 2003 课程体系中占有十分重要的地位。

本书每一章的开始都简单介绍本章的主要内容,以及本章的学习目标,以便读者在学习过程中作为参照。每一章中都包含详细的实践操作步骤和部分的案例研究分析,从读者的角度去理解操作步骤,可以大大加深读者的学习效果。结尾处均包含 MCSE(对应课程号 2277,考试号 70-291)考试的模拟试题和答案分析,这些模拟试题能有效地帮助读者在学习具体知识的同时备考 Windows Server 2003 MCSE 考试。

由于时间仓促,编写者水平有限,书中介绍的使用经验和心得难免有不当之处,或还会有更好的方法,恳请读者指正。

杨洪振:资深 MCT (Microsoft Certified Trainer), MCSE、MCDBA MLC 讲师,曾长时间从事系统技术支持,系统集成项目以及讲授相关产品课程等工作。对于 Microsoft 系列产品有深入研究,在基于微软平台的网络系统,服务器应用以及网络安全等方面具有丰富经验,包括 Windows 2000、Exchange Server, ISA Server, SharePoint Portal Server, BizTalk Server, Small Business Server 并是国内第一批使用和研究 Windows Servers 2003, Exchange Server 2003 的技术人员。

曾主持设计了多个网络系统方案集成和开发,如中国联通河北分公司网络基础架构,办公系统集成,邮件提醒平台,高可靠性群集方案,北京佳诚无限科技有限公司 Exchange 邮件系统平台,Portal 平台的建设,同时为其他众多知名公司提供信息化咨询。教学经验丰富:曾为多个知名企业进行 IT 培训,如建设银行、河北省委办公厅、中国联通、中国网通、河北电力公司等企业进行了多种 IT 系统方面的培训。其幽默风趣的授课风格,丰富的理论知识和经验,得到了大家的认可。

编者

出版说明

Windows Server 2003 推出已经有两年时间了，但这种有史以来最强大的服务器操作系统却迟迟未能普及，很大的原因是缺乏相应的系统完整的教材和培训。为此，我们特组织优秀的微软认证讲师（MCT）编写了本套 Windows Server 2003 高级技术培训教材，以帮助你快速系统地掌握 Windows Server 2003 的相关技术和技巧，同时本书也可以作为获得微软最新的 MCSE/MCSA 认证的参考资料及自学培训教材。

全套教材共 6 本：

序号	书 名
1	管理 Windows Server 2003 环境
2	维护 Windows Server 2003 环境
3	实现 Windows Server 2003 网络基础结构：网络主机
4	实现和维护网络基础结构：网络服务
5	计划和维护 Windows Server 2003 网络基础结构
6	计划、实现和维护 Windows Server 2003 活动目录结构

本套培训教材都由第一线的微软认证高级技术培训中心讲师（MCT）编写，凝聚了 MCT 们多年实践和教学的经验，教材的每章都有学习重点，在必要章节附有实验供读者练习。另外，本套教材还包括大量的模拟试题，所有模拟试题都加入了试题分析和知识点解析以适应读者在各种环境中的实践能力。力求通过学习本套教材，即可成为一名优秀的 Windows Server 2003 系统管理人员，与此同时你将具备参加 MCSE/MCSA 考试的各种相关知识。

本套教材既可供系统管理员、广大网络技术人员和爱好者学习、参考使用 Windows Server 2003 系统，也可以作为微软认证 MCSE/MCSA 的自学参考教材。

编 者

目 录

第 1 章 配置路由功能.....1	
1.1 路由基础知识.....1	
1.1.1 路由在网络中的作用.....1	
1.1.2 本地路由和远程路由的区别.....2	
1.2.3 微软提供的路由方案.....3	
1.2 路由和远程访问服务.....3	
1.2.1 路由器.....3	
1.2.2 路由接口.....5	
1.2.3 路由表.....6	
1.2.4 路由协议.....9	
1.2.5 Windows Server 2003 路由 和远程访问服务.....11	
1.3 安装和配置路由和远程访问服务.....11	
1.3.1 前期工作.....12	
1.3.2 配置“路由和远程访问”服务.....14	
1.3.3 删除“路由和远程访问”服务.....19	
1.4 包过滤.....20	
1.4.1 包过滤概述.....20	
1.4.2 包过滤工作流程.....22	
1.4.3 配置包过滤.....24	
1.5 模拟试题分析.....28	
第 2 章 使用 DHCP 分配 IP 地址.....33	
2.1 DHCP 简介.....33	
2.1.1 DHCP 简介.....34	
2.1.2 DHCP 地址租约.....35	
2.1.3 DHCP 分配 IP 地址信息过程.....36	
2.1.4 DHCP 地址租约更新.....38	
2.2 安装并授权 DHCP 服务.....40	
2.2.1 安装 DHCP.....41	
2.2.2 多 DHCP 服务器的 20/80 原则.....41	
2.2.3 活动目录授权机制.....42	
2.2.4 授权 DHCP 服务器.....44	
2.2.5 案例：添加并授权 DHCP 服务器.....45	
2.3 配置 DHCP 作用域.....46	
2.3.1 DHCP 作用域.....47	
2.3.2 配置过程.....48	
2.3.3 超级作用域.....49	
2.4 配置 DHCP 保留.....51	
2.4.1 DHCP 保留.....51	
2.4.2 配置 DHCP 保留.....52	
2.5 配置 DHCP 选项.....53	
2.5.1 DHCP 选项.....54	
2.5.2 DHCP 选项级别.....54	
2.5.3 类选项.....55	
2.5.4 配置 DHCP 选项过程.....57	
2.6 DHCP 中继代理.....60	
2.6.1 跨路由网络中的 DHCP 设计.....60	
2.6.2 DHCP 中继代理.....62	
2.6.3 Hop 计数.....63	
2.6.4 DHCP 中继代理启动阈值.....64	
2.6.5 配置 DHCP 中继代理.....64	
2.7 模拟试题分析.....66	
第 3 章 管理和监控 DHCP.....71	
3.1 管理 DHCP 数据库.....71	
3.1.1 管理 DHCP 数据库概述.....71	
3.1.2 DHCP 数据库.....72	
3.1.3 DHCP 数据库的备份和还原.....73	
3.1.4 DHCP 数据库的一致性.....77	
3.2 监控 DHCP.....78	
3.2.1 概述.....78	
3.2.2 DHCP 统计信息.....79	
3.2.3 DHCP 审核日志.....81	
3.2.4 使用性能计数器监控 DHCP 服务器.....86	
3.3 配置 DHCP 安全性.....90	
3.3.1 限制非法客户机获得 IP 地址租约.....91	
3.3.2 限制非授权的服务器提供 IP 地址租约.....92	
3.3.3 限制 DHCP 管理员数目.....93	
3.3.4 实现 DHCP 数据库安全性.....94	
3.4 考题分析.....95	
第 4 章 名称解析.....97	

4.1 名称方案.....	97	5.4.4 区域文件.....	146
4.1.1 主机名称 (Host Name)	97	5.4.5 DNS 区域与活动目录集成.....	147
4.1.2 NetBIOS 名称.....	99	5.4.6 区域查找类型.....	148
4.1.3 配置客户端的名称.....	102	5.4.7 配置过程.....	148
4.1.4 名称解析.....	105	5.5 DNS 区域传输.....	151
4.2 配置主机名称解析.....	106	5.5.1 DNS 区域传输.....	151
4.2.1 主机名称解析概述.....	106	5.5.2 DNS 通知.....	154
4.2.2 客户端解析程序缓存.....	107	5.5.3 区域传输的安全性.....	155
4.2.3 主机文件.....	109	5.5.4 配置过程.....	156
4.2.4 DNS 服务器.....	111	5.6 DNS 动态更新.....	157
4.3 NetBIOS 名称解析.....	111	5.6.1 DNS 动态更新.....	158
4.3.1 NetBIOS 名称解析的过程.....	112	5.6.2 DNS 客户端动态更新.....	159
4.3.2 NetBIOS 名称缓存.....	113	5.6.3 DHCP 服务器代替客户端 进行动态更新.....	160
4.3.3 本地广播.....	115	5.6.4 活动目录集成区域的动态更新.....	161
4.3.4 Lmhosts 文件.....	116	5.6.5 配置过程.....	163
4.4 实验.....	118	5.7 区域委派.....	166
第 5 章 DNS 名称解析.....	121	5.7.1 区域委派.....	166
5.1 DNS 简介.....	121	5.7.2 配置过程.....	167
5.1.1 域名系统.....	122	5.8 配置 DNS 客户端.....	168
5.1.2 名称空间.....	123	5.8.1 客户端 DNS 服务器指向.....	169
5.1.3 DNS 命名标准.....	125	5.8.2 客户端 DNS 后缀.....	170
5.2 DNS 的工作过程.....	126	5.8.3 配置过程.....	171
5.2.1 DNS 系统的组件.....	126	5.9 模拟试题分析.....	174
5.2.2 DNS 查询.....	127	第 6 章 管理优化 DNS 方案.....	181
5.2.3 DNS 根提示.....	130	6.1 监视 DNS 服务器工作状态.....	181
5.2.4 转发器.....	131	6.1.1 监视 DNS 服务器.....	182
5.2.5 DNS 服务器缓存.....	132	6.1.2 配置过程.....	183
5.2.6 配置过程.....	135	6.2 资源记录的 TTL 值.....	184
5.3 安装 DNS 服务器服务.....	138	6.2.1 TTL 值如何工作.....	184
5.3.1 安装 DNS 服务前的准备工作.....	138	6.2.2 设置 TTL 值.....	185
5.3.2 安装 DNS 服务器服务.....	139	6.3 过期资源记录的处理.....	186
5.4 DNS 区域.....	140	6.3.1 老化和清理.....	186
5.4.1 资源记录, 区域和区域文件.....	140	6.3.2 老化和清理工作过程.....	188
5.4.2 资源记录.....	141	6.3.3 老化和清理配置过程.....	189
5.4.3 区域.....	143		

6.4 DNS 方案的可靠性.....192	7.4.1 管理 WINS 数据库记录.....240
6.4.1 多台 DNS 服务器使用区域复制192	7.4.2 筛选并查看 WINS 记录.....241
6.4.2 使用服务器群集技术提高 DNS 可靠性193	7.4.3 爆发处理244
6.5 监视 DNS 服务器性能.....194	7.4.4 配置过程244
6.5.1 监视 DNS 服务器性能195	7.5 WINS 复制246
6.5.2 DNS 事件日志197	7.5.1 WINS 复制简介247
6.5.3 DNS 调试日志198	7.5.2 复制伙伴248
6.5.4 配置过程200	7.5.3 WINS 复制属性249
6.6 优化 DNS 服务器性能.....200	7.5.4 配置 WINS 复制过程251
6.6.1 如何优化 DNS 服务器性能201	7.6 管理 WINS 数据库252
6.6.2 禁用递归查询201	7.6.1 WINS 数据库的备份和还原253
6.6.3 删除和修改根提示202	7.6.2 压缩 WINS 数据库253
6.6.4 优化 DNS 响应时间203	7.6.3 清理 WINS 数据库254
6.6.5 使用 EDNS0 优化服务器功能208	7.6.4 手工删除记录256
6.6.6 配置过程209	7.6.5 WINS 数据库的一致性检查256
6.7 名称解析故障排除.....213	7.6.6 删除 WINS 服务器257
6.7.1 故障排除213	7.6.7 管理 WINS 数据库配置过程258
6.7.2 故障排除常用工具214	7.7 考题分析.....265
6.7.3 常见的 3 类 DNS 问题219	第 8 章 网络通信安全性.....268
6.7.4 典型故障问题举例220	8.1 介绍 IPSec268
6.7.5 配置错误后的恢复功能222	8.1.1 日益严重的网络安全问题268
6.8 监视 DNS 服务器工作状态.....223	8.1.2 什么是 IPSec.....271
第 7 章 WINS 解决方案.....227	8.1.3 IPSec 工作机理.....273
7.1 NetBIOS 简介227	8.1.4 IP 安全策略.....273
7.1.1 NetBIOS 名称227	8.1.5 系统默认的 IP 安全策略.....276
7.1.2 NetBIOS 名称解析231	8.2 实现 IPSec279
7.2 WINS 服务.....232	8.2.1 IP 安全策略的应用规则.....280
7.2.1 WINS 服务结构232	8.2.2 配置 IP 安全策略.....280
7.2.2 NetBIOS 节点类型233	8.2.3 启用 IP 安全策略.....287
7.2.3 NetBIOS 名称注册, 更新和释放 ...234	8.2.4 实践建议: 平衡安全性与性能287
7.3 配置 WINS 服务器和客户机.....236	8.3 监控 IPSec288
7.3.1 安装配置 WINS 服务器236	8.3.1 IP 安全监视器.....288
7.3.2 安装配置 WINS 客户端237	8.3.2 事件查看器监控 IPSec.....289
7.4 管理 WINS.....239	8.3.3 IPSec 策略一般故障解决.....290
	8.4 案例分析: 实现网络通信安全性.....291

8.5 考题分析	294
第9章 证书身份验证机制	296
9.1 PKI (公共密钥基础结构)	296
9.1.1 什么是 PKI	297
9.1.2 公共密钥加密技术 (公钥加密)	300
9.1.3 数字签名	302
9.2 证书服务---CA	303
9.2.1 CA (Certification Authority —证书颁发机构)	303
9.2.2 CA 的层次结构	304
9.2.3 Windows Servers 2003CA 类型	305
9.3 安装和配置证书服务	307
9.4 客户端证书的申请	311
9.4.1 证书请求向导	311
9.4.2 证书服务 Web 页	313
9.4.3 检查证书请求的状态	314
9.4.4 安装已颁发的证书	315
9.5 管理证书	316
9.5.1 处理用户的证书请求	316
9.5.2 证书存储区	317
9.5.3 吊销证书	319
9.5.4 证书导入和导出	322
9.5.5 CA 的备份和恢复	326
9.5.6 证书故障排除	328
9.5.7 卸载证书服务	329
9.6 证书应用例证: IPSec 和证书	330
9.6.1 使用证书与 IPSec 来保护 网络通信	330
9.6.2 配置 IPSec 使用证书	330
9.7 考题分析	332
第10章 远程访问方案	336
10.1 远程访问概述	336
10.1.1 资源访问需求	336
10.1.2 远程访问结构	337
10.1.3 远程访问服务器和客户端	338

10.1.4 远程访问身份验证	339
10.2 拨号远程访问方案	341
10.2.1 拨号远程访问概述	341
10.2.2 拨号连接的组成	343
10.2.3 拨号连接的身份验证方法	344
10.2.4 配置远程访问服务器	344
10.2.5 配置拨号访问客户端	348
10.3 VPN 远程访问方案	350
10.3.1 VPN (虚拟专用网) 概述	351
10.3.2 VPN 的组成	352
10.3.3 VPN 连接的加密协议	353
10.3.4 配置 VPN 服务器	354
10.3.5 配置 VPN 远客户端	358
10.4 无线连接方案	360
10.4.1 无线远程访问概述	360
10.4.2 无线连接的组成	362
10.4.3 无线网络的国际标准	362
10.4.4 无线网络的身份验证方法	364
10.4.5 配置无线连接远程访问客户端	365
10.4.6 为远程访问配置智能卡 身份验证	366
10.5 控制用户对网络的访问	368
10.5.1 远程访问控制方法: 远程 访问策略	368
10.5.2 用户账户拨入权限	369
10.5.3 配置远程访问用户账户	369
10.5.4 远程访问策略	370
10.5.5 远程访问控制的实现	374
10.5.6 配置远程访问策略	374
10.6 考题分析	378
第11章 远程访问的集中身份验证 (IAS)	383
11.1 IAS 概述	383
11.1.1 集中身份验证需求	383
11.1.2 IAS 实现集中身份验证	384
11.1.3 集中验证过程	385

11.2 安装和配置 IAS.....	386	12.2.2 监视监视器使用的对象 和计数器	395
11.2.1 安装 IAS 服务器	386	12.2.3 监视无线网络	396
11.2.2 配置 IAS 服务器	387	12.3 远程访问故障排除	398
11.2.3 配置 IAS 客户端---远程 访问服务器	389	12.3.1 事件日志	398
第 12 章 远程访问管理和故障排除.....	391	12.3.2 本地日志文件	400
12.1 管理远程访问	391	12.3.3 常用故障排除工具	402
12.1.1 管理远程访问服务	391	12.3.4 故障排除流程	404
12.1.2 管理远程访问客户端	393	12.3.5 配置过程总结	405
12.2 监视远程访问性能	394	12.4 考题分析	410
12.2.1 监视性能数据的工具	395		

第 1 章 配置路由功能

- 路由基础知识
- 路由和远程访问服务
- 安装和配置路由和远程访问服务
- 包过滤
- 模拟试题分析

路由指的是在相互连接起来的 IP 网络之间转发数据包的过程。不同的 IP 网络之间必须经过路由（Routing）来进行通信，行使路由功能的设备就是路由器（Router），Windows Servers 2003 支持路由功能，可以作为路由器来配置。

作为网络路由器启用时，Windows Server 2003 既支持本地路由，也支持远程路由。除了物理的拨号连接、帧中继连接、ISDN（Integrated Services Digital Network——综合业务数字网）连接或 X.25 这些连接之外，可能的连接还包括到公司网络的直接连接，或通过因特网的点对点虚拟专用网络（VPN）的连接。

本章中，主要阐述网络中路由器的主要作用，路由基本知识，以及怎样将运行 Windows Server 2003 的计算机配置成网络路由器。

学习目标

- ✎ 理解路由在网络中的作用
- ✎ 安装和配置路由和远程访问服务（RRAS）
- ✎ 配置包过滤

1.1 路由基础知识

- 路由在网络中的作用
- 本地路由和远程路由的区别
- 微软提供的路由方案

路由器是互联网的主要节点设备。路由器通过路由表决定数据的转发。转发策略称为路由选择（routing），作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互连网络 Internet 的主体脉络，也可以说，路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。

1.1.1 路由在网络中的作用

路由指的是在相互连接起来的 IP 网络之间转发数据包的过程。不同的 IP 网络之间是不能直接通信的，必须经过路由（Routing），行使路由功能的设备就是路由器（Router），路由是 Internet Protocol（IP-Internet 协议）的组成部分。联合使用路由与其他的网络协议服务，可以在一个大规模的基于 TCP/IP（Transmission Control Protocol/Internet Protocol）的网

络内，在位于不同网段的主机之间提供数据转发能力。路由器的功能之一就是实现数据包的转发，另外一个功能就是把两个或者两个以上分离的 IP 网络连接成一个大的网络。

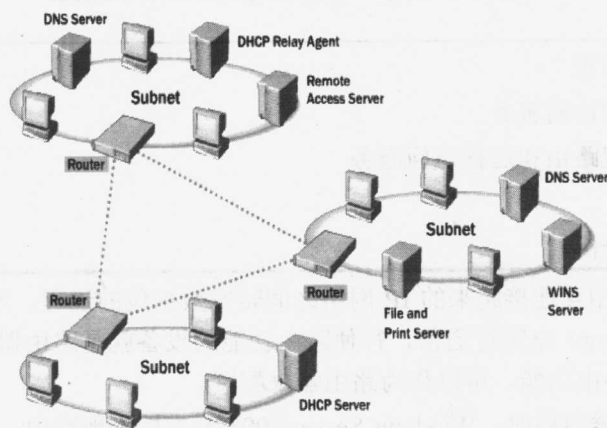


图 1-1 路由在网络中的作用

路由器中存储有一个路由表，而且连接着很多网络的多个路由器之间，通过相互之间交流，共享这个路由表，使各个路由器中的路由表达达到一致，来实现无误的数据包转发，路由表中包含有到达不同网络的路径，路由器依据路由表确定将数据包转发到哪里。利用路由表，路由器能作出适宜的决策，确定将网络数据流转发到正确的目标，从而实现数据包的有效传输。清楚地理解路由器和路由表，将有助于你有效地为自己的网络环境配置路由器。

路由器是互联网的主要节点设备。路由器通过路由表决定数据的转发。转发策略称为路由选择（routing），这也是路由器名称的由来（router，转发者）。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互连网络 Internet 的主体脉络，也可以说，路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。

1.1.2 本地路由和远程路由的区别

下面我们通过一个客户端访问资源的实际例子，来说明本地路由和远程路由。

1. 客户端 A 由于要访问某个资源，而试图向目的主机 B 发送一个数据包，在要发送的数据包的报头中包含两个 IP 地址：发送主机的源地址以及接收主机的目标地址。
2. 客户端自己检查，源地址和目标地址，如果源地址和目标地址是同一个网络，这证明是一个发向本地的数据包，此时数据包不发向路由器，而是直接发送给目的主机，数据包可以直接的到达目标，这就称作本地路由。
3. 如果目标地址和源地址不是同一个网络，这时数据包就会发送到客户端 A 的所在网络的路由器上（默认网关），由路由器来检查目标地址到底在哪个网络，这个数据包该发向哪里。
4. 如果路由器了解到目标地址所在的网络，恰恰是它直接相连的网络，路由器就会直接把数据包转发到目的网络，也就是它直连的网络中。

5. 如果目标地址所在的网络不是路由器的直接相连网络,属于远程网络,这时,路由器就会察看自己的路由表,去路由表中查找该把这个数据包发向哪里,寻找一条最优的路径,把这个数据包发送出去,这个过程就是远程路由。

路由表中存放有到达各个网络的路径,路由器可以根据一定的算法,得到到达各个网络的最优路径,路由表在各个不同的路由器之间共享,而且不同的路由器之间还要交流路由表,学习路由表中的条目,进而使不同的路由器中的路由表信息达到一致。

1.2.3 微软提供的路由方案

Windows Server 2003 通过“路由和远程访问”(Routing and Remote Access)来实现路由功能,“路由和远程访问”是作为一种服务存在的,属于软件路由,Windows Server 2003 将路由作为其多个处理进程中的一个来完成。

1.2 路由和远程访问服务

- 路由器
- 路由接口
- 路由表
- 路由协议
- Windows Server 2003 路由和远程访问服务

路由指的是在相互连接起来的 IP 网络之间转发数据包的过程。不同的 IP 网络之间是不能直接通信的,必须经过路由(Routing),行使路由功能的设备就是路由器(Router),路由是 IP 协议的组成部分,路由器依据路由表确定将数据包转发到哪里。利用路由表,路由器能作出适宜的决策,确定将网络数据流转发到正确的目标,从而实现数据包的有效传输。Windows Server 2003 利用“路由和远程访问服务”来实现路由功能。

本节讲述路由的知识,以及 Windows Server 2003 的路由和远程访问服务。

1.2.1 路由器

网络中包含各种不同的设备,例如集线器、网桥、交换机以及路由器。利用路由器,可以通过将网络信息流分段,来扩展网络并维护带宽。路由器依据路由表确定将数据包转发到哪里。利用路由表,路由器能作出适宜的决策,确定将网络数据流转发到正确的目标,从而实现数据包的有效传输。清楚地理解路由器和路由表,将有助于你有效地为自己的网络环境配置路由器。如图 1-2 所示。

路由指的是在相互连接起来的 IP 网络之间转发数据包的过程。不同的 IP 网络之间是不能直接通信的,必须经过路由(Routing),行使路由功能的设备就是路由器(Router),路由是 Internet Protocol (IP-Internet 协议)的组成部分。联合使用路由与其他的网络协议服务,可以在一个大规模的基于 TCP/IP (Transmission Control Protocol/Internet Protocol)的网络内,在位于不同网络段的主机之间提供数据转发能力。如果想将两个或多个物理上分开的 IP 网络段连接起来,路由器就是达到这种目的的主要手段。所有的 IP 路由器都有两个基本的特征:

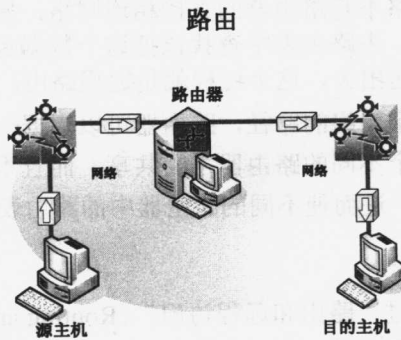


图 1-2 路由

- ✎ 连接不同的网络：IP 路由器相当于具有多个地址主机，它利用两个或多个网络连接接口将分开的网络段相连接。
- ✎ 数据包的转发：IP 路由器为其他 TCP/IP 主机提供数据包转发功能。

IP 路由器必须能够为其他的网络主机在网络之间转发基于 IP 的通信。

路由器中存储有一个路由表，而且连接着很多网络的多个路由器之间，通过相互之间交流，共享这个路由表，使各个路由器中的路由表达到一致，来实现无误的数据包转发，路由表中包含有到达不同网络的路径，路由器依据路由表确定将数据包转发到哪里。利用路由表，路由器能作出适宜的决策，确定将网络数据流转发到正确的目标，从而实现数据包的有效传输。清楚地理解路由器和路由表，将有助于你有效地为自己的网络环境配置路由器。

路由器是互联网的主要节点设备。路由器通过路由表决定数据的转发。转发策略称为路由选择（routing），这也是路由器名称的由来（router，转发者）。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互连网络 Internet 的主体脉络，也可以说，路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。

路由器的分类

- ✎ 硬件路由器（Hardware router） 这种路由器将路由作为它自己的专门功能来完成。它有专门的硬件，这种硬件是专门针对路由功能进行设计和优化的。例如 CISCO 公司出品的系列路由器
- ✎ 软件路由器（Software router） 这种路由器并不是专门用来完成路由功能的。它将路由功能作为在路由器计算机上运行的多个进程中的一个来完成。Windows Server 2003 “路由和远程访问”（Routing and Remote Access）就是一种服务，它将路由作为其多个处理进程中的一个来完成。

路由术语

下面的术语对于理解路由有所帮助，它们经常在一些技术文献中出现：

- ✎ 端系统（End systems） 端系统也被称为主机（hosts）。常规意义上的用户端的计

算机它不具备在网络的各部分之间转发数据包的能力。端系统也被称为主机(hosts)。常规意义上的用户端的计算机。

- ✎ **中间系统(Intermediate systems)** 是一种网络设备,它可以在网络的各部分之间转发数据包。网桥、交换机、路由器是中间系统的实例。
- ✎ **路由接口** 路由接口是一个物理接口或逻辑接口,通过它可以转发 IP 数据包。
- ✎ **路由协议** 路由器利用路由协议来交换路由器之间的信息(路由表),用以传播网络地址和连接信息。
- ✎ **路由表** 路由器利用来自路由表的数据决定如何转发 IP 数据包。路由表维护着到达各个不同网络的路径信息。

其他关键词

- ✎ **集线器(HUB)** 网络设备之一,工作在 OSI 参考模型的第一层——物理层,主要用于早期的 10M, 10M/100M 以太网,最早的中央集线设备,是星型网络的中央汇聚点。
- ✎ **交换机(Switch)** 网络设备之一,工作在 OSI 参考模型的第二层,数据链路层,它可以实现数据包基于 MAC 地址的转发,用在局域网中,可以提供比集线器更快的速度,更少的冲突产生。
- ✎ **路由器(Router)** 相对于集线器和交换机,路由器工作在 OSI 参考模型的第三层:网络层,它可以实现数据包基于网络层的转发,在目前的 TCP/IP 网络中,就是基于 IP 地址的转发(IP 地址定义在网络层),用于连接不同的 IP 网络,数据包的转发。

1.2.2 路由接口

路由接口是一个物理接口或逻辑接口,通过它可以转发 IP 数据包,基于 Windows Server 2003 的路由器就是使用路由接口来进行数据包的转发的:例如对 IP、IPX 或者 AppleTalk 数据包的转发。

路由接口

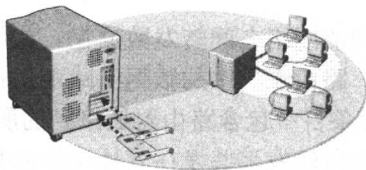


图 1-3 路由接口

Windows Server 2003 提供两种路由接口:

- ✎ **LAN 接口** 代表一个局域网连接,该连接利用 LAN 技术,例如以太网或令牌环网。LAN 接口表示为一个已经安装好的网络适配器(网卡)。也就是说,只要 Windows Server 2003 启动了路由和远程访问服务后,LAN 接口总是活动的,并且,每个网卡(也就是网络适配器)就代表一个 LAN 接口,LAN 接口通常不要求身份鉴定过程就可以成为活动的。