

契合用户实际需求 · 精选热门网络应用

提供实用解决方案 · 精讲具体实施案例

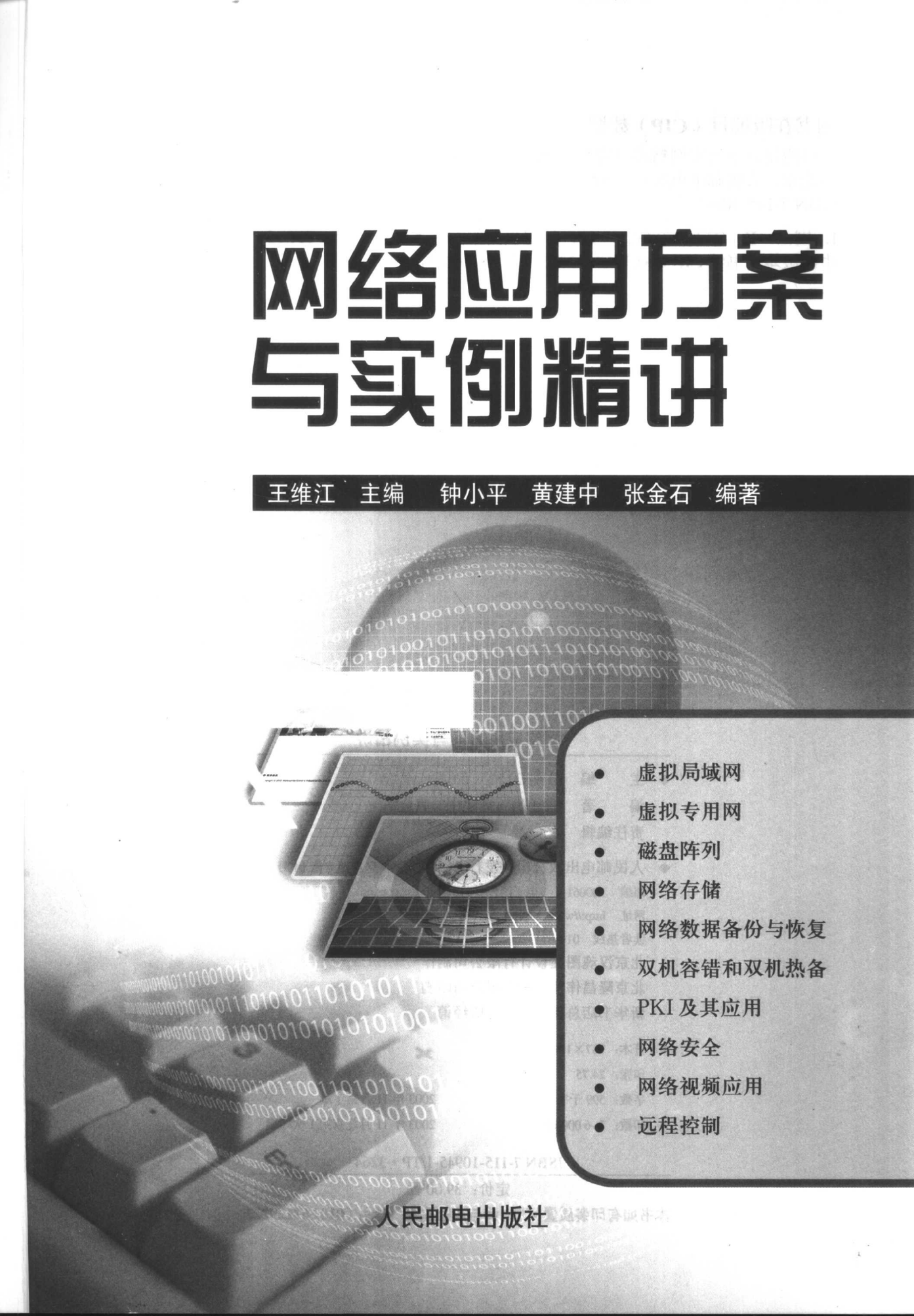
网络应用方案 与实例精讲

王维江 主编 钟小平 黄建中 张金石 编著

- 
- 虚拟局域网
 - 虚拟专用网
 - 磁盘阵列
 - 网络存储
 - 网络数据备份与恢复
 - 双机容错和双机热备
 - PKI 及其应用
 - 网络安全
 - 网络视频应用
 - 远程控制

网络应用方案 与实例精讲

王维江 主编 钟小平 黄建中 张金石 编著

- 
- 虚拟局域网
 - 虚拟专用网
 - 磁盘阵列
 - 网络存储
 - 网络数据备份与恢复
 - 双机容错和双机热备
 - PKI 及其应用
 - 网络安全
 - 网络视频应用
 - 远程控制

人民邮电出版社

图书在版编目 (CIP) 数据

网络应用方案与实例精讲/王维江主编 钟小平编著.

—北京: 人民邮电出版社, 2003.11

ISBN 7-115-10945-1

I. 网... II. ①王...②钟... III. 计算机网络—基本知识 IV. TP393

中国版本图书馆 CIP 数据核字 (2003) 第 086951 号

网络应用方案与实例精讲

- ◆ 主 编 王维江
编 著 钟小平 黄建中 张金石
责任编辑 杨 璐
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132692
北京汉魂图文设计有限公司制作
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销
- ◆ 开本: 787×1092 1/16
印张: 24.75
字数: 599 千字 2003 年 11 月第 1 版
印数: 1-6 000 册 2003 年 11 月北京第 1 次印刷

ISBN 7-115-10945-1/TP · 3264

定价: 39.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

内 容 提 要

本书旨在帮助读者了解和掌握高端网络应用技术,提升网络应用水平。主要针对中小型网络,联系中小企业或机构的实际需求,对虚拟局域网(VLAN)、虚拟专用网(VPN)、磁盘阵列、网络存储、网络数据备份、双机容错与双机热备份、PKI 应用、Web 安全、网络视频应用、远程管理与控制等 10 种网络应用技术进行专题介绍,内容包括技术介绍、解决方案和具体应用实例。

书中内容突出实用性,针对每一种应用,在介绍目前主流的技术解决方案之后,从中选择一个或几个方案,并通过实例来进一步讲解实施步骤。在写作中抛开专深的原理,侧重功能实现与问题解决,重点放在实际方案的比较选择和具体实例的实施示范上。书中还穿插了作者的实践经验和体会,并针对重要问题提供了问题解答。

本书结合中小企业和机构的网络应用实际需要,考虑中小型网络的特点,在介绍方案时,侧重于纯软件和软硬结合的解决方案,并且以 Windows 平台的解决方案和实例为主。对于以硬件方案为主的应用,主要介绍主流的产品以及实现模式。

本书适合于网络管理人员、网络工程师,以及需要学习网络应用技术的高校学生和 IT 技术人员,要求读者具备一定的网络基础知识。本书也可作为网络管理和网络工程参考书。

本书编委会

策 划 钟小平

主 编 王维江

编 委	钟小平	黄建中	张金石
	郝卫东	李贝贝	龙厚斌
	潘晓晟	尚顶洪	肖文光
	崔旭峰	高 红	田华明
	陈景亮	蒋定定	亓海芸

编者的话

随着计算机网络逐步普及和网络应用的不断深入,广大用户不再局限于简单的文件共享、信息管理等应用,而是要根据任务需求不断改造和完善现有网络,开展新的应用业务,解决新的问题,这就需要 IT 主管和网络管理员根据实际需要,选择合适的、具体的解决方案。在国内,除政府、银行、电力、电信和海关等行业用户和大型集团企业涉及大型网络外,绝大多数企业和组织机构只能拥有中小型网络。在这些拥有中小型网络的单位中,网络管理员和技术支持人员不足的情况很普遍,一些单位配备有专职网络管理员,还有许多单位和部门只能配备兼职管理员。这些人员需要尽快地了解 and 掌握一些网络高端应用技术,提升本单位和部门的网络应用水平。本书旨在满足此类读者的需要,结合中小型网络的实际情况,提供实用的、可操作性强的应用方案与实例。

本书特点

本书采用单刀直入,简明扼要的写法,围绕每一种应用技术专题,简单介绍特点、功能、应用领域和技术实现方案,重点放在实际方案的比较选择和具体实例的实施示范上。对于这些应用,大中型机构多采用专门的硬件解决方案,而中小型机构则尽可能采用软件解决方案或软硬结合的方案。考虑到这种情况,本书侧重于纯软件的解决方案和软硬结合的解决方案,以 Windows 平台的解决方案和实例为主。对于以硬件方案为主的应用,只介绍主流的产品以及实现模式。

内容突出实用性,针对每一种应用,在介绍目前的技术解决方案之后,从中选择一个或几个方案,并通过实例来进一步讲解实施步骤。在写作中抛开专深的原理,侧重功能实现与问题解决;突出具体实例,穿插了作者的经验和体会;主要章节都针对重要问题提供了问题解答,帮助读者顺利设计和实施网络方案。

主要内容

本书主要围绕中小型网络的高端应用,联系中小企业或机构的实际需求,重点选取了虚拟局域网(VLAN)、虚拟专用网(VPN)、磁盘阵列、网络存储、网络数据备份、双机容错与双机热备份、PKI 应用、Web 安全、网络视频应用、远程

管理与控制等应用技术进行介绍,对相关知识进行了归纳和总结,对设备的选型、方案的选择有很强的指导作用。全书共 10 章,每一章都是一个相对独立的网络应用技术专题,内容包括技术介绍、解决方案和具体应用实例。

阅读提示

为便于读者阅读,对书中的小栏目进行了分类,并加上了图标,图标的具体含义说明如下。

 **提示** 对需要注意的地方进行特别说明。

 **提高** 对所涉及的内容进行深入阐述,或介绍相关内容的扩展知识。

 **点评** 对提供的案例进行综合评价。

 **注释** 对正文中出现的、未给出解释的概念或名词术语进行详细说明。

 **小结** 对部分内容进行总结。

读者对象

本书适合于网络管理员、网络工程师,以及需要学习网络应用技术的高校学生和 IT 技术人员,要求读者具备一定的网络基础知识。

由于编写时间仓促,书中难免有错漏之处,恳请各位专家和读者朋友指正。在阅读本书过程中如果有疑难问题,欢迎您和我们联系,我们的 E-mail 为: zxp169@163.com。本书责任编辑的 E-mail 为: luyang@ptpress.com.cn。

编 者
2003.10

目 录

第 1 章 虚拟局域网	1
1.1 VLAN 概述	1
1.1.1 VLAN 的概念	1
1.1.2 VLAN 的优点	3
1.1.3 VLAN 的应用	3
1.1.4 VLAN 的技术标准	5
1.1.5 VLAN 的类型	8
1.2 VLAN 的划分方式	9
1.2.1 按端口划分 VLAN	9
1.2.2 按 MAC 地址划分 VLAN	10
1.2.3 基于网络层划分 VLAN	10
1.2.4 基于 IP 广播组划分	11
1.2.5 基于规则的 VLAN	12
1.3 VLAN 之间的通信	12
1.4 VALN 的解决方案	13
1.4.1 如何规划 VLAN	13
1.4.2 如何选择 VLAN 的划分方式	14
1.4.3 如何选择交换机产品	14
1.5 VLAN 配置实例	18
1.5.1 采用 VLAN 技术升级现有网络	18
1.5.2 采用 VLAN 技术组建新的网络	23
1.6 VLAN 的发展趋势	28
1.7 本章小结	29
第 2 章 虚拟专用网	31
2.1 VPN 简介	31
2.1.1 VPN 的概念	31
2.1.2 VPN 的优势	32
2.1.3 VPN 应用范围	32
2.1.4 VPN 的应用模式	32

2.2 VPN 的实现技术	35
2.2.1 基于隧道的 VPN	35
2.2.2 基于虚电路的 VPN	37
2.2.3 MPLS VPN	38
2.2.4 VPN 实现技术的选择	39
2.3 VPN 的类型	40
2.3.1 按应用范围划分	40
2.3.2 按 VPN 网络结构划分	40
2.3.3 按接入方式划分	40
2.3.4 按隧道协议划分	41
2.3.5 按隧道建立方式划分	41
2.3.6 按路由管理方式划分	41
2.4 VPN 的解决方案	42
2.4.1 是自建 VPN 还是外包 VPN	42
2.4.2 是选择硬件 VPN 还是软件 VPN 方案	43
2.4.3 如何选择 VPN 产品	43
2.4.4 VPN 硬件产品	45
2.4.5 微软的 VPN 解决方案	45
2.5 VPN 组网实例	46
2.5.1 在宽带城域网中使用 VPN 实现同城互联	46
2.5.2 组建远程访问 VPN 网络	54
2.5.3 使用 VPN 路由器组建 VPN 网络	61
2.6 动态 VPN 的实现方案与实例	65
2.6.1 动态 VPN 技术简介	65
2.6.2 基于动态域名服务的动态 VPN	65
2.6.3 基于目录服务的动态 VPN	67
2.6.4 基于内网地址的动态 VPN	68
2.6.5 最新的动态 VPN 实现技术	68
2.7 问题解答	70
2.8 本章小结	74
第 3 章 磁盘阵列	75
3.1 RAID 技术基础	75
3.1.1 RAID 概述	75
3.1.2 RAID 级别	76
3.1.3 如何确定 RAID 级别	79
3.2 RAID 技术解决方案	80
3.2.1 是选择硬件 RAID 还是软件 RAID	80
3.2.2 是选择外置式 RAID 还是内置式 RAID	82

3.2.3	是选择 SCSI 阵列还是 IDE 阵列	82
3.2.4	综合考察 RAID 的各项指标	84
3.2.5	基于 SCSI 的 RAID 产品和解决方案	85
3.2.6	基于 IDE 的 RAID 产品和解决方案	86
3.2.7	软件 RAID 产品和解决方案	91
3.3	硬件 RAID 的配置和管理	92
3.3.1	关于硬件 RAID 配置的一般性问题	92
3.3.2	SCSI RAID 配置和管理实例	93
3.3.3	IDE RAID 配置和管理实例	95
3.4	软件 RAID 的配置和管理实例	97
3.4.1	用 Windows 2000 实现软件 RAID 的预备知识	97
3.4.2	在 Windows 2000 Server 上实现 RAID 0	98
3.4.3	在 Windows 2000 Server 上实现 RAID 1	101
3.4.4	在 Windows 2000 Server 上实现 RAID 5	104
3.4.5	在 Windows 2000 Server 上实现 JBOD	106
3.5	问题解答	107
3.6	本章小结	108
第 4 章	网络存储	109
4.1	网络存储概述	109
4.1.1	传统的存储技术 DAS	109
4.1.2	网络附加存储 (NAS)	110
4.1.3	存储区域网络 (SAN)	113
4.1.4	NAS 与 SAN 的比较	115
4.1.5	值得关注的 iSCSI	116
4.1.6	中小型网络数据存储技术的选择	118
4.2	NAS 的解决方案与实例	119
4.2.1	选择 NAS 产品的原则	119
4.2.2	中低端 NAS 解决方案与产品介绍	121
4.2.3	中小型网络 NAS 应用实例	125
4.3	问题解答	127
4.4	本章小结	129
第 5 章	网络数据备份与恢复	131
5.1	数据备份和恢复概述	131
5.1.1	理解备份与恢复的概念	131
5.1.2	数据备份的类型	133
5.1.3	与网络存储相适应的网络备份技术	135

5.2 中小型网络数据备份的解决方案	136
5.2.1 备份设备和介质的选择	137
5.2.2 备份软件的选择	139
5.2.3 数据备份方案选择实例	141
5.3 使用 Windows 2000 备份工具实现单机备份	142
5.3.1 了解 Windows 2000 备份的特性	142
5.3.2 Windows 2000 备份操作	143
5.3.3 Windows 2000 还原操作	145
5.3.4 系统修复	146
5.4 使用第三方备份工具进行备份	147
5.4.1 GRBackPro 简介	147
5.4.2 备份数据	148
5.4.3 恢复数据	150
5.5 使用 VERITAS Backup Exec 实现网络备份	151
5.5.1 进一步了解 VERITAS Backup Exec	151
5.5.2 安装和启动 VERITAS Backup Exec	153
5.5.3 安装和配置 Backup Exec 工作站代理	154
5.5.4 安装和配置 Backup Exec 服务器远程代理	155
5.5.5 使用 Backup Exec 备份数据	157
5.5.6 使用 Backup Exec 恢复数据	160
5.5.7 SQL Server 数据库的备份与恢复	161
5.5.8 使用 Advanced Open File Option	167
5.5.9 灾难修复	168
5.6 问题解答	170
5.7 本章小结	170
第 6 章 双机容错和双机热备	173
6.1 双机集群概述	173
6.1.1 集群技术和双机技术的有关概念	173
6.1.2 双机集群的工作模式	174
6.1.3 双机集群技术的应用领域	175
6.2 共享磁盘阵列方式和纯软件方式	176
6.2.1 共享磁盘阵列方式	176
6.2.2 纯软件方式	177
6.2.3 选择共享磁盘阵列还是纯软件方式	178
6.3 双机集群的解决方案	178
6.3.1 软件厂商提供的双机软件	178
6.3.2 存储设备厂商提供的配套解决方案	182
6.3.3 服务器厂商提供的全套解决方案	183

6.3.4	中小型网络如何选择双机集群方案.....	184
6.3.5	中小型网络双机集群方案选择实例.....	185
6.4	使用 Legato Co-StandbyServer 实现双机容错	186
6.4.1	进一步了解 Co-StandbyServer 2000	187
6.4.2	安装 Co-StandbyServer 2000	189
6.4.3	Co-StandbyServer 2000 管理入门	191
6.4.4	定义双机集群	192
6.4.5	创建和管理组	193
6.4.6	创建和管理镜像分区	194
6.4.7	创建和管理资源	195
6.4.8	配置和管理切换	198
6.4.9	如何恢复失效服务器	200
6.4.10	管理应用程序	201
6.4.11	数据库服务器管理实例	202
6.5	使用 Legato RepliStor 实现双机热备	206
6.5.1	进一步了解 Legato RepliStor	206
6.5.2	安装 Legato RepliStor	207
6.5.3	镜像数据	208
6.5.4	配置切换	214
6.5.5	恢复失效服务器	222
6.5.6	切换应用程序	226
6.5.7	SQL Server 2000 管理实例	226
6.5.8	双网卡 RepliStor 服务器的配置实例	228
6.5.9	在广域网上部署 RepliStor 双机热备	230
6.6	问题解答	230
6.7	本章小结	231
第 7 章	PKI 及其应用	233
7.1	PKI 概述	233
7.1.1	网络安全需求与公钥技术	233
7.1.2	理解 PKI 的概念	234
7.1.3	数字证书	235
7.1.4	PKI 的核心——认证机构	237
7.1.5	PKI 应用技术	238
7.1.6	基于 PKI 的安全应用标准和协议	239
7.1.7	PKI 的应用	245
7.2	部署自己的 PKI——CA 的建立和管理	246
7.2.1	CA 产品的选择	246
7.2.2	规划证书颁发机构	248

7.2.3	安装证书服务	250
7.2.4	证书颁发机构的配置和管理	251
7.2.5	证书申请和注册	254
7.2.6	客户端的证书管理	258
7.3	基于 SSL 的 Web 安全访问	260
7.3.1	SSL Web 安全解决方案	260
7.3.2	申请和安装服务器证书	261
7.3.3	在 Web 服务器上启用 SSL	264
7.3.4	在 Web 浏览器端安装根 CA 证书	265
7.3.5	测试 SSL 连接	267
7.3.6	对 SSL 客户端进行验证	267
7.3.7	在 Web 服务器上使用证书信任列表进一步限制访问	268
7.4	基于 S/MIME 的安全电子邮件	269
7.4.1	设置 Outlook Express 的安全选项	270
7.4.2	申请并安装安全电子邮件证书	271
7.4.3	设置邮件账号的安全功能	272
7.4.4	邮件的数字签名和验证	273
7.4.5	邮件的加密和解密	275
7.4.6	对邮件同时签名和加密	277
7.5	问题解答	278
7.6	本章小结	279
第 8 章	Web 安全	281
8.1	Web 安全概述	281
8.1.1	面临的 Web 安全问题	281
8.1.2	Web 安全问题的基本解决方案	282
8.2	提高操作系统的安全性	283
8.2.1	升级系统和安装补丁	283
8.2.2	限制用户权限	283
8.2.3	增强文件系统的安全性	285
8.2.4	删除或禁用不必要的组件和服务	288
8.2.5	严格控制网络共享	290
8.2.6	保护注册表	291
8.2.7	修改注册表以强化系统安全	291
8.2.8	启用日志和审核功能	292
8.2.9	提高系统的防病毒能力	293
8.2.10	使用 Web 安全模板在操作系统级加固 IIS 服务器	293
8.3	确保 Web 服务器的网络安全	295
8.3.1	部署防火墙保护 Web 服务器	295

8.3.2	在 Web 服务器上部署实时安全保护系统	298
8.3.3	保护 Web 通信安全	298
8.4	Web 服务器自身的安全配置	298
8.4.1	理解 IIS 的安全机制	298
8.4.2	设置 IP 地址限制	299
8.4.3	设置用户身份验证	300
8.4.4	设置 Web 服务器权限	302
8.4.5	控制 IIS 应用程序	302
8.4.6	设置目录或文件的 NTFS 权限	303
8.4.7	审核 IIS 日志记录	304
8.4.8	禁止或删除不必要的 IIS 选项或相关组件	305
8.4.9	禁用 Content-Location 标头的 IP 地址	306
8.4.10	使用微软的 IIS 锁定向导优化安全配置	307
8.5	其他 Web 安全措施	310
8.5.1	使用安全的 Web 应用程序	311
8.5.2	后端数据库服务器的安全	313
8.5.3	注意远程控制的安全	315
8.5.4	做好数据备份	315
8.6	Web 安全测试和评估	315
8.6.1	安全扫描和评估简介	315
8.6.2	使用 MBSA 评估 Windows 系统安全漏洞和弱点	316
8.6.3	使用 X-Scan 进行安全漏洞检测	319
8.7	本章小结	320
第 9 章	网络视频应用	321
9.1	视频点播	321
9.1.1	视频点播简介	321
9.1.2	VOD 方案选择的注意事项	323
9.1.3	VOD 软件的选择	324
9.1.4	VOD 服务器硬件的选择	326
9.1.5	VOD 终端硬件	327
9.1.6	传输网络	327
9.1.7	用 Windows Media 建立视频点播系统	328
9.1.8	快速构建 Web 视频点播系统	333
9.1.9	构建专业的宽带 VOD 系统	335
9.2	视频广播	336
9.2.1	视频广播简介	336
9.2.2	视频广播的解决方案	338
9.2.3	用 Windows Media 建立视频广播系统	339

9.2.4 轻松构建 Web 视频广播系统	349
9.3 视频会议	350
9.3.1 视频会议简介	350
9.3.2 视频会议实现技术	353
9.3.3 中低端视频会议解决方案	356
9.3.4 中小型网络视频会议应用实例	360
9.4 本章小结	361
第 10 章 远程控制	363
10.1 远程控制的工作机制	363
10.2 远程控制的应用	364
10.3 远程控制软件类型	365
10.3.1 根据客户端和服务端实现方式划分	366
10.3.2 根据网络连接方式划分	366
10.4 远程控制软件的选择	367
10.4.1 典型远程控制软件介绍	367
10.4.2 选择远程控制软件需要考虑的因素	371
10.4.3 典型应用场合的远程控制软件选择	371
10.5 远程控制解决方案与实例	372
10.5.1 用 Windows 终端服务来管理服务器	373
10.5.2 用 RemotelyAnywhere 来管理服务器	376
10.5.3 用 Remote-Anything 进行多机监控	379
10.6 问题解答	381
10.7 本章小结	382

第 1 章 虚拟局域网

虚拟局域网（VLAN）是一种发展很快的局域网技术，其核心是通过路由和交换设备，在网络物理结构的基础上建立逻辑网络，使得网络中的任意节点能根据需要组成一个逻辑的局域网。VLAN 组网技术具有高速、灵活、管理简便和扩展容易的特点，被广泛应用于局域网建设。由于 VLAN 技术的普及，设备的性价比不断提高，越来越多的中小企业和单位在组建新的网络，或者升级改造现有网络时，开始采用 VLAN 技术。VLAN 能更好地满足企业发展的需要，可突破物理网段的限制来建立部门网络，对网络通信进行隔离，提供一定的安全性，提高网络带宽的利用率，简化网络管理，便于网络的调整和扩展。本章介绍了 VLAN 的基本概念和实现技术，以及中小型 VLAN 的解决方案，结合典型实例讲解 VLAN 的配置过程。

1.1 VLAN 概述

VLAN 是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。VLAN 涉及到多种网络技术，如虚拟网络技术、分布式路由技术、高速交换技术及网络管理技术等。采用 VLAN 技术，不但可以满足用户对网络灵活性和扩展性方面的要求，而且有助于隔离网络故障和分配网络带宽。

1.1.1 VLAN 的概念

早期的共享 LAN 限制了网络带宽的利用，网络交换机的引入解决了共享冲突问题。交换机在网络的源端口与目的端口之间提供直接、快速、准确的点到点连接，提供高速低延时通信，提高了网络的效率，但是从根本上说，它仍是一个高速网桥，无法过滤局域网的广播信息。当网络中节点数足够多时，广播信息包所占用的带宽就可能影响其他信息流的传输，使网络的性能迅速下降，这就是所谓的“广播风暴”。

抑制广播风暴的基本方法是隔离广播域。显而易见的解决方法是限制以太网上的节点，这就需要对网络进行物理分段。将网络进行物理分段的传统方法是使用路由器，如图 1.1 所示。路由器的基本作用是只发送和接收来往于不同物理网段的信息。路由器处于 OSI 参考模型的第 3 层，能够实现网络互联，具有许多相对复杂的功能。例如，它不转发广播包，支持路由选择、多路重发以及错误检测等，还能将不同类型的网络连接在一起。

路由器所连接的网络是不同的逻辑子网，但这种子网是根据物理网络结构来划分的，配置工作量大。随着网络的不断扩展，接入设备逐渐增多，网络结构日趋复杂，必须使用更多的路由器才能将不同的用户划分到各自的广播域中，在不同的局域网之间提供网络互连。大量使用路由器无疑是一笔不小的投资，同时，路由器所造成的通信“瓶颈”也会使网络的效率大打折扣。

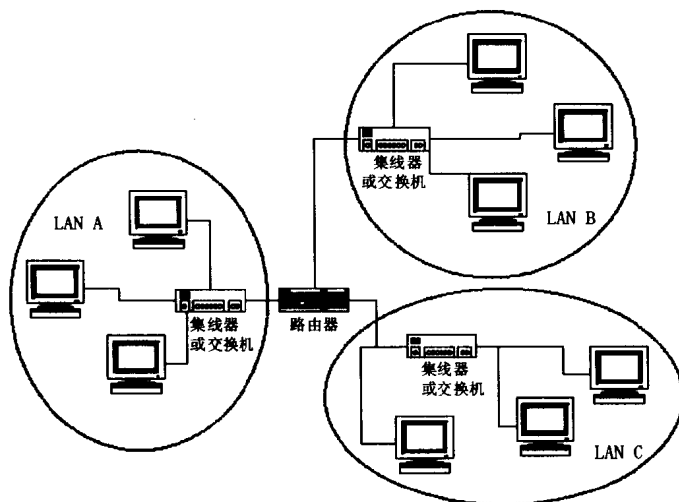


图 1.1 使用路由器对网络分段

VLAN 是一种不用路由器解决隔离广播域的网络技术。VLAN 概念的引入,使交换机代替路由器承担了网络的分段工作,如图 1.2 所示。VLAN 打破了传统网络的许多固有观念,使网络结构变得灵活、方便、随心所欲。VLAN 不必考虑用户的物理位置,根据功能、应用等因素,将用户从逻辑上划分为一个个功能相对独立的工作组,每一个 VLAN 都可以对应于一个逻辑单位,如部门、项目组等。同一个 VLAN 中的成员都共享广播,而不同 VLAN 之间广播信息是相互隔离的。这样,将整个网络分割成多个不同的广播域。例如,网络管理员可以把相关的客户和服务分别构成不同的 VLAN,同一 VLAN 内客户和服务可以方便地频繁通信,在同一个 VLAN 中的用户相互存取网络资源就如同在使用传统的局域网一样。

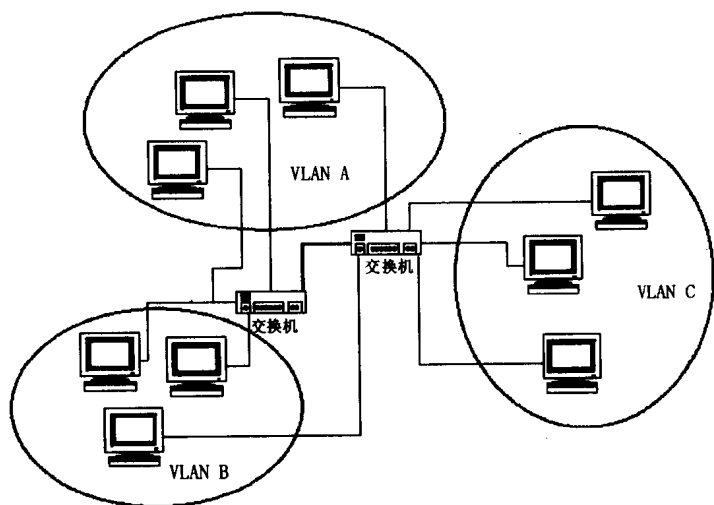


图 1.2 VLAN 的网段划分

由于 VLAN 基于逻辑连接而不是物理连接,因此配置十分灵活。VLAN 在逻辑上等价于广播域,可以将 VLAN 类比成一组最终用户的集合。这些用户可以处在不同的物理局域网上,但他们之间可以像在同一个局域网上那样自行通信,而且不受物理位置的限制。网络的定义和划分与物理位置和物理连接是没有任何必然联系的。网络管理员可以根据不同的需要,通过