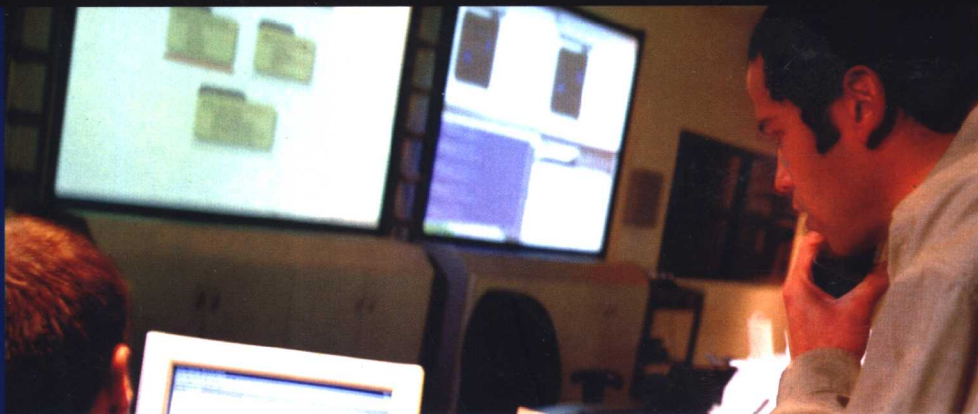




自顶向下网络设计 (第二版)

Top-Down Network Design

Second Edition

A systems analysis approach to
enterprise network design

[美] Priscilla Oppenheimer 著
胡捷 毛拥华 译

图书在版编目 (CIP) 数据

自顶向下网络设计: 第2版 / (美) 奥本海默 (Oppenheimer, P.) 著; 胡捷, 毛拥华译.
—北京: 人民邮电出版社, 2005.2

ISBN 7-115-13007-8

I. 自... II. ①奥...②胡...③毛... III. 计算机网络—设计 IV. TP393.02

中国版本图书馆 CIP 数据核字 (2005) 第 003103 号

版 权 声 明

Priscilla Oppenheimer: Top-Down Network Design, Second Edition (ISBN: 1587051524)

Authorized translation from the English language edition published by Cisco Press.

Copyright © 2004 by Cisco Systems, Inc.

All rights reserved.

本书中文简体字版由美国 Cisco Press 公司授权人民邮电出版社出版。未经出版者书面许可, 对本书任何部分不得以任何方式复制或抄袭。

版权所有, 侵权必究。

自顶向下网络设计 (第二版)

- ◆ 著 [美] Priscilla Oppenheimer
译 胡 捷 毛拥华
责任编辑 李 际
- ◆ 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 ciscobooks@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132705
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787×1092 1/16
印张: 24.5
字数: 608 千字 2005 年 2 月第 1 版
印数: 1-4 000 册 2005 年 2 月北京第 1 次印刷
著作权合同登记 图字: 01-2004-2604 号

ISBN 7-115-13007-8/TP · 4401

定价: 49.00 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

本书是围绕自顶向下网络设计步骤编写的，提供给网络设计者一种系统的结构化网络设计方法。全书分为四个部分，即客户需求和目标、逻辑网络设计、物理网络设计，以及网络测试、优化和文档编写。四个部分分别对应着网络设计的各个重要阶段。每个阶段都提供给读者详细的设计指导原则，内容涵盖网络设计的方方面面。从用户商业和技术目标的分析入手，从而制定出相应的网络流量、负载和 QoS 需求，进而开发网络的逻辑拓扑结构，然后进入地址规划、协议选择、网络安全和网络管理实施策略制定，最后是对网络设备的选型建议以及网络实施、测试和文档编写。本书的最后给出了工作站启动时的网络流量特征描述和主要术语词汇表。从事网络技术的专业人员将从本书中受益匪浅。

关于作者

Priscilla Oppenheimer 自从 1980 年在密歇根大学获得信息科学硕士学位后，一直从事数据通信和网络系统的开发工作。在从事了多年的软件开发工作之后，她成为一名技术讲师和培训设计者，已教授了来自财富 500 强公司的 2000 多名网络工程师。她曾任职于苹果计算机公司、NetWork Ceneral 和 Cisco Systems 等公司，这些经历给了她许多对实际网络中有关设计问题的故障排查经验，并提供机会积累了开发企业网络设计的实际经验。Priscilla 是“Cisco 互连网络设计”课程的开发者之一，并且是“设计 Cisco 网络”课程的创办者。她同时拥有 CCNP 和 CCDP 认证。Priscilla 目前在南俄勒冈州大学教授计算机网络课程。

致 谢

我首先要感谢 Cisco Press 的员工和参与这个项目的人对本书出版付出的辛苦工作。并且对本书的技术审稿人表示感谢,他们是 Matthew Birkner, Blair Buchanan 和 Peter Welcher 博士。他们阅读了全部原稿并提出了许多有益的建议。我对书稿中依然会出现的错误,以及我没有听从审稿人建议而坚持保留的一些原始素材负责。我同样感谢在本书第一版中的技术审稿人,他们是 Alex Cannara 博士, David Jansson 和 Hank Mauldin。他们当初付出的杰出努力在本书的第二版中仍然依稀可见。

在本书第一版由于我的疏忽错过了对 Howard Berkowitz 的感谢,但是我很高兴第二版的出版为我弥补了这个机会。自从 1995 年他为我的“Cisco 网络互连”课程进行审校时起,我从他那里学到了很多。本书中的许多概念都是受到他潜移默化的影响,体现了我本人对他的尊敬和感激。

我还要借此感谢其他团队的负责人,我与他们共同工作了多年,包括 Connect802 小组的 Joseph Bardwell 和 Anita Lenk,以及学习讨论小组的其他同事,他们为我解答了许多技术问题。这些同事包括(但不限于)Paul Borghese(协调人), Marty Adkins, Ken Chipps, Daniel Cotts, Annlee Hines, Chuck Larrieu, Larry Letterman, Tom Lisa, David Madland, Jenny McLeod, John Neiberger, Fred Reimer, Peter van Oene, Scott Vermillion, Alaerte Vidali, 和 Cyrus Wekesa。

我对南俄勒冈大学的同事和学生感到非常满意,他们与我进行了多次有益的技术探讨。这些人包括(但不限于)Dan Wilson 博士, Lynn Ackler 博士, Louis Kowolowski, Jason Moreland(小 Jason), 和 Jason Winters(大 Jason)

最后,我要感谢 Alan Oppenheimer,他在本书出版的全过程中担任我的代理、技术顾问、医师、厨师和最好的朋友。请不要对本书中 AppleTalk 范例一事指责他。正像前面提到的,我对坚持保留一些传统教材以利于读者理解协议行为和发展过程负责。

献 辞

此书献给我的父母, Stephen T. Worland(博士)和 Roberta Worland 太太(硕士)。他们培养我从小对知识、逻辑和分析充满尊重, 并教导我“有志者事竟成”的人生格言。

关于技术审校人

Matthew H. Birkner, CCIE No. 3719, Cisco Systems 公司技术顾问, 专长是 IP、MPLS 和 QoS 网络设计。他在全球范围内参与了多个大型服务提供商和企业网络设计。Matt 在过去几年中经常在美国的 EMEA Cisco 网络用户大会发表关于 MPLS 的演讲。他拥有双 CCIE 认证, 并且撰写了“Cisco 互连网络设计”一书, 已由 Cisco Press 出版(该书中文版已由人民邮电出版社出版, 编辑注)。Matt 毕业于 Tufts 大学, 获得电子工程科学学士学位。

Blair Buchanan, CCIE No. 1427, 加拿大渥太华 Sherwood Cameron Associates 有限公司的资深技术架构师和网络集中策略制定者。他在通信领域拥有 28 年的工作经验, 他在这个领域最初是从从事过程控制应用的数据实时通信方面的软件开发工作。Blair 参加了 ISO 标准组织, 并且在加拿大和美国的许多大型企业和服务提供商的网络互连设计中起到主导作用, 目前主要对集成业务方面的网络互连进行规划和设计。Blair 毕业于西安大略大学(1975), 拥有计算机科学与数学学士学位。他于 1992 年开始讲授 Cisco 培训课程, 并保持着他的 Cisco 路由选择与交换 CCIE 认证。

Dr. Peter J. Welcher, CCIE No. 1773, CCIP, CCSI, 麻省理工学院数学博士。他在美国海军学院开始教授数学课程的同时, 还在购买并维护着 UNIX 系统, 同时还在撰写一部专著, 并且在用 C 语言编写一套主要的计算机程序。他的专著于 1993 年出版, 之后为 Mentor Technologies 公司(前身是 Chesapeake 计算机顾问公司)教授多门 Cisco 培训课程, 与此同时从事着网络顾问工作。Pete 目前在 Chesapeake Netcraftsmen 公司主要从事高层面的网络顾问工作, 包括为几个大型企业客户提供网络设计、安全、QoS 和 IP 电话方面的咨询。他为 Cisco Press 和其他出版社审校了大量书籍, 并且

为 Cisco 及其他设备制造商编写、管理、开发了多门课程。Pete 经常为 “*Enterprise Networking Magazine*” 撰写文章。他还经常在 Cisco 位于东海岸的办公地点主持技术研讨，涉及从园区网设计到 WLAN 安全等各个领域。可以在 <http://www.netcraftsmen.net/welcher> 了解到相关文章和研讨资料。

前言

新的商业实践正在促使企业网络发生变化。从产业经济到信息经济的转变，已经改变了雇员的工作方式。空前的全球经济竞争现象的出现加速了企业必须适应技术、金融等方面变化的步伐。

为减少开发及产品销售的时间，许多公司允许雇员需要获取销售、市场、金融、工程等方面的数据作出具有战略性的决策。工作在企业总部和全球范围各地办公室内的企业雇员们，以及在家办公的雇员们，都需要立即访问数据，不论这些数据是存储在中心服务器上还是在部门服务器上。

为向国内外市场销售或分销产品，商业企业正越来越多地依赖于本地或全球性合作伙伴以形成商业联盟。商业系统正在仔细规划他们的网络设计以满足安全目标的同时满足遍布于世界各地的分销商、设备制造商、客户、潜在客户以及合同制工人对网络接入方面的需求。

为适应对远程访问、安全、带宽、可扩展性以及可靠性等方面不断增长的需求，设备制造商和标准化组织以相当快的速度引入新的协议和新的技术。网络设计者必须面对挑战开发采用最新技术的网络，即使新技术是不断变化和发展的。

不论你是刚刚涉足网络领域的设计者，还是一位富有经验的网络设计师，你可能一直关注如何使设计出来的网络跟上互连网络业日益变化的步伐这一问题。本书的目标就是向你讲授一套系统的设计方法用以满足一个组织的需求，而不管这些应用和技术到底有多新和多复杂。

第二版的变化

《自顶向下网络设计》第一版教授你直到今天仍可从中受益的经典网络设计方法。自顶向下方法专注于需求分析和体系结构设计，这些步骤应该在进入到特定的网络组件选择之前完成。自顶向下的方法可以适用于各种网络，包括采用10Mbit/s以太网或令牌环的老式网络，也包括采用吉比特以

太网、同步光纤网络（SONET）和无线网络的现代网络。

除了自顶向下这一永恒的自然规则之外，为了适应现代商业实践的需求，还必须对某些地方进行调整。商业目标会随政治和经济的演变而变化。商业目标还随人力资源策略的演变而变化。网络设计也必须随这些因素的改变做出调整。

在过去的几年中，下列商业目标和所涉及的问题已经显现甚至多次显现，成为网络设计领域迫切需要关注的需求：

- 支持移动和远程用户的需求；
- 网络安全方面持续增长的需求；
- 网络可恢复性方面持续增长的需求；
- 网络可管理性方面持续增长的需求；
- 对多个网络项目必须基于财政目标区分出优先级这一观点的重新认识；
- 对将语音和数据进行网络融合以获取经济利益这一过程的重新关注。

为了解决这些商业需求，《自顶向下网络设计》第二版已经对下列主题进行了补充和更新：

- 无线网络；
- 虚拟专用网络（VPN）；
- 网络安全；
- 网络冗余；
- 模块化网络设计；
- IPv4 和 IPv6 的动态编址；
- 新网络设计和管理工具；
- 以太网扩展性选项，包括 10Gbit/s 以太网，城域以太网和长距以太网；
- 设计一个可同时承载语音和数据流量的网络。

目标

《自顶向下网络设计》第二版的目标是帮助你设计出能够满足客户商业及技术目标的网络。无论你的客户是你本公司内部的一个部门，还是外面的客户，本书为你提供测试过程和工具，以帮助你理解通信流量、协议行为和网络互连技术。在你读完本书之后，你就能设计出可满足客户对功能、容量、性能、可用性、可扩展性、可购买性、安全性及可管理性等各方面需求的企业网络。

读者

如果你是网络互连专业人员，负责设计和维护大、中型企业网络的话，本书正适合你。如果你是一位具备网络协议和技术工作经验的网络工程师、架构师或者技术员的话，本书将为你提供应用你的知识进行网络互连设计方面的实际建议。

本书还包括其他一些有益信息，这些信息对于为客户设计企业网络的顾问、系统工程师、销售工程师们非常有用。许多系统工程师处在尽快将产品或解决方案销售给用户的大环境中，通常很难将他们的进度放慢并坚持采用自顶向下、结构化系统分析方法。不论怎样，这本书所讲授的捷径和假设都可以加快网络设计的过程。

最后要说明的是，本书对于那些计算机科学和信息科学专业的大学在校学生或毕业生也

很有帮助。已经学习了一到两门网络理论课程的学生会发现《自顶向下网络设计》第二版提供了一种循序渐进的方法和步骤来解决工程和商业问题，这些问题涉及到解决典型商业问题的真实网络的开发。

结构

本书是围绕自顶向下网络设计步骤编写的。全书分为四个部分，分别对应着网络设计的各个重要阶段。

第一部分：辨明客户的需求和目标

第一部分涉及需求分析阶段。这一阶段从辨明商业目标和技术需求开始。刻划现有网络的任务包括体系结构和主要网段及设备的性能。这一阶段的下一个步骤是分析网络流量，包括通信流量和负载、协议行为、以及服务质量（Qos）需求。

第二部分：逻辑网络设计

在逻辑网络设计阶段，网络设计者开发网络的拓扑结构。根据网络规模和流量特性的不同，拓扑结构可以从简单到复杂变化，有不同的层次化和模块化需求。在这个阶段，网络设计者还需要设计网络层编址模型、并且选择交换和路由选择协议。逻辑设计还包括安全规划，网络管理设计，以及对服务提供商能够满足的广域网和远程访问的需求作初步调查。

第三部分：物理网络设计

在物理网络设计阶段，需要选择特定的技术和产品以实现逻辑网络设计。物理网络设计阶段首先从园区网络选择技术和设备开始，包括电缆布线、以太网交换机、无线接入点、无线网桥、以及路由器。然后为远程访问和广域网需求选择技术和设备。另外，与逻辑网络设计同步开始的服务提供商内部调查，必须在本阶段完成。

第四部分：网络测试，优化和文档编写

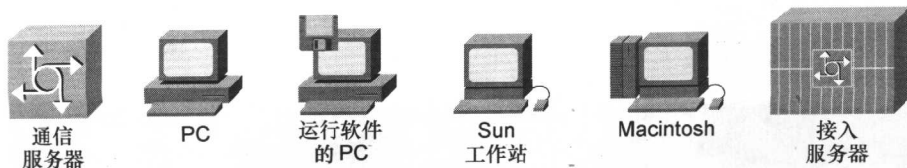
自顶向下网络设计的最后一步是编写并实施测试计划，创建原型或试验系统，优化网络设计，在网络设计建议书基础上形成文档等。如果你的测试结果表明存在性能问题，那么在这个阶段，你应该更新你的设计，将一些功能，如流量整形、先进的路由器排队和交换机制等包括进去。

附录 A 介绍了网络工作站引导时的网络流量特征。提供了 IP、AppleTalk、NetWare、NetBIOS 和系统网络体系结构（SNA）会话信息。附录 B 是参考和推荐阅读材料的列表。附录 B 之后是网络技术术语简表。

配套网站

《自顶向下网络设计》第二版的英文版在 www.topdownbook.com 上提供配套网站。配套网站包括本书英文版的更新、到相关白皮书的链接，以及设计资源的补充信息。

本书所用的图标





命令语法约定

本书采用与 IOS 命令参考一样的命令语法约定格式，即：

- **粗体**表明按照显示的文字输入命令及关键字。在实际配置范例及输出（不是一般的命令语法）中，粗体表明需要用户手工输入的命令（例如 **Show** 命令）；
- *斜体*表示由用户给出的参数实际值；
- 互斥的元素用竖线（|）分隔；
- 方括号（[]）表明可选元素；
- 大括号（{}）表明必选元素；
- 方括号包含大括号（{[]}）表明在可选项中必选其中一个。

目 录

第一部分 客户需求分析阶段

第 1 章 分析商业目标和制约	5
1.1 采用自顶向下的网络设计方法	5
1.1.1 使用结构化网络设计方法	6
1.1.2 系统开发生命周期	7
1.1.3 规划设计实现操作优化 (PDIOO) 的网络生命周期	8
1.2 分析商业目标	9
1.2.1 与你的客户一同工作	9
1.2.2 企业网络中的变化	10
1.2.3 典型网络设计的商业目标	12
1.2.4 识别网络设计项目的范围	13
1.2.5 识别客户的网络应用	14
1.3 分析商业制约	16
1.3.1 政治和政策	16
1.3.2 预算与员工制约	17
1.3.3 项目时间进度表	18
1.4 商业目标检查表	18
1.5 小结	19
第 2 章 分析技术目标与折衷	21
2.1 可扩展性	21
2.1.1 扩展规划	22
2.1.2 访问数据扩展	22
2.1.3 可扩展性制约	23
2.2 可用性	23
2.2.1 灾难恢复	24
2.2.2 指定可用性要求	24
2.3 网络性能	27
2.3.1 网络性能定义	27
2.3.2 最优网络利用率	27
2.3.3 吞吐量	29
2.3.4 精确度	31

2.3.5 效率	32
2.3.6 延迟和延迟变量	33
2.3.7 响应时间	36
2.4 安全性	37
2.4.1 网络资产鉴定	37
2.4.2 安全性威胁分析	38
2.4.3 制定安全性要求	39
2.5 可管理性	40
2.6 可用性	41
2.7 适应性	41
2.8 可购买性	41
2.9 网络设计折衷方案	42
2.10 技术目标检查表	44
2.11 小结	44
第3章 刻划现有互连网络的特征	47
3.1 刻划网络基础设施特征	47
3.1.1 绘制网络结构图	48
3.1.2 刻划网络编址和命名特征	51
3.1.3 刻划布线与介质特征	52
3.1.4 检查建筑结构及环境制约	54
3.2 检查现有互连网络的健壮性	57
3.2.1 制定网络性能基线	57
3.2.2 分析网络可用性	58
3.2.3 分析网络的利用率	58
3.2.4 分析网络精确度	60
3.2.5 分析网络效率	62
3.2.6 分析延迟和响应时间	63
3.2.7 检查主要路由器、交换机和防火墙的状态	64
3.3 刻划现有网络特征的工具	65
3.3.1 协议分析仪	66
3.3.2 网络监测和管理工具	66
3.3.3 远程监测工具	67
3.3.4 刻划现有互连网络特征的 Cisco 工具	67
3.3.5 提供刻划现有网络特征信息的组织	68
3.4 网络健康检查表	68
3.5 小结	69
第4章 刻划网络流量特征	71
4.1 刻划通信流量特征	71
4.1.1 识别主要流量源和存储	72
4.1.2 记录现有网络的通信流量	72
4.1.3 刻划新网络应用的流量类型特征	73
4.1.4 记录新的和现有的网络应用通信流量	78
4.2 刻划流量负载特征	78

4.2.1 计算理论流量负载	79
4.2.2 记录应用程序使用模式	80
4.2.3 精确估计应用程序产生的流量负载	80
4.2.4 估计由路由选择协议引起的流量负载	82
4.3 刻划流量行为特征	83
4.3.1 广播/组播行为	83
4.3.2 网络效率	84
4.4 刻划服务质量需求特征	87
4.4.1 ATM 服务质量规范	88
4.4.2 IETF 综合服务工作组服务质量规范	90
4.4.3 IETF 区分服务工作组服务质量规范	92
4.4.4 语音应用的服务等级要求	92
4.4.5 记录服务质量需求	93
4.5 网络流量检查表	93
4.6 小结	94
4.7 第一部分总结	94

第二部分 逻辑网络设计

第 5 章 设计网络拓扑结构	99
5.1 层次化网络设计	100
5.1.1 为什么使用层次化网络设计模型	100
5.1.2 经典的三层层次化模型	105
5.1.3 层次化网络设计原则	106
5.2 冗余网络设计拓扑结构	108
5.2.1 备用路径	108
5.2.2 负载分担	109
5.3 模块化的网络设计	109
5.4 设计园区网络拓扑结构	111
5.4.1 生成树协议	111
5.4.2 扩展生成树协议	114
5.4.3 虚拟局域网	115
5.4.4 无线局域网	118
5.4.5 布线局域网中的冗余和负载分担	119
5.4.6 服务器冗余	120
5.4.7 工作站 - 路由器冗余	122
5.5 设计企业网络边界拓扑结构	125
5.5.1 冗余广域网网段	125
5.5.2 多宿主 Internet 连接	126
5.5.3 虚拟专用网	128
5.5.4 服务提供商边界	130
5.6 保护网络设计拓扑结构的安全	131
5.6.1 规划物理安全性	131
5.6.2 使用防火墙拓扑结构满足安全性目标	132

5.7 小结	133
第6章 设计编址和命名模型	135
6.1 分配网络层地址的原则	136
6.1.1 使用结构化网络层编址模型	136
6.1.2 通过中心授权机构管理地址	136
6.1.3 编址的分布授权	137
6.1.4 为终端系统使用动态编址	138
6.1.5 在 IP 环境中使用私有地址	142
6.2 使用层次化模型分配地址	144
6.2.1 为什么使用层次化模型进行编址和路由选择	144
6.2.2 层次化路由选择	145
6.2.3 无类域间路由选择	145
6.2.4 无类路由选择与分类路由选择	146
6.2.5 路由汇总(汇聚)	146
6.2.6 不连续子网	148
6.2.7 可变长度子网掩码	150
6.2.8 IPv6 地址的层次	150
6.3 设计命名模型	153
6.3.1 命名的分布授权	154
6.3.2 分配名字的原则	154
6.3.3 在 NetBISO 环境中分配名字	155
6.3.4 在 IP 环境中分配名字	157
6.4 小结	158
第7章 选择交换和路由选择协议	161
7.1 自顶向下网络设计中的决策过程	162
7.2 选择桥接与交换协议	163
7.2.1 透明桥接	163
7.2.2 透明交换	164
7.2.3 使用生成树协议的增强功能	165
7.2.4 传送 VLAN 信息的协议	168
7.3 选择路由选择协议	170
7.3.1 刻划路由选择协议的特征	171
7.3.2 IP 路由选择	177
7.3.3 AppleTalk 路由选择	183
7.3.4 Novell NetWare 路由选择	185
7.3.5 在互连网络中使用多重路由选择协议	187
7.4 IP、AppleTalk 和 IPX 路由选择协议小结	190
7.5 小结	191
第8章 制定网络安全策略	193
8.1 网络安全设计	194
8.1.1 辨明网络资产和风险	194
8.1.2 分析安全折衷	195

8.1.3 制定安全规划	195
8.1.4 制定安全策略	196
8.1.5 制定安全流程	196
8.2 安全机制	197
8.2.1 物理安全	197
8.2.2 认证	197
8.2.3 授权	198
8.2.4 统计(审计)	198
8.2.5 数据加密	198
8.2.6 数据包过滤器	200
8.2.7 防火墙	201
8.2.8 入侵检测系统	201
8.3 模块化安全设计	202
8.3.1 保护 Internet 的连接	202
8.3.2 保护远程访问和虚拟专用网	204
8.3.3 保护网络业务和网络管理	206
8.3.4 保护服务器集群	207
8.3.5 保护用户业务	207
8.3.6 保护无线网络	208
8.4 小结	213
第 9 章 制定网络管理策略	215
9.1 网络管理设计	215
9.2 网络管理流程	216
9.2.1 性能管理	216
9.2.2 故障管理	218
9.2.3 配置管理	218
9.2.4 安全管理	219
9.2.5 记账管理	219
9.3 网络管理体系结构	219
9.3.1 带内监测和带外监测	220
9.3.2 集中式与分布式监测	221
9.4 选择网络管理协议	221
9.4.1 简单网络管理协议	221
9.4.2 Cisco 发现协议	224
9.4.3 估计网络管理引起的流量	224
9.5 选择网络管理工具	225
9.6 小结	227
9.7 第二部分总结	227

第三部分 物理网络设计

第 10 章 选择园区网络技术和设备	231
10.1 局域网布线规划设计	232