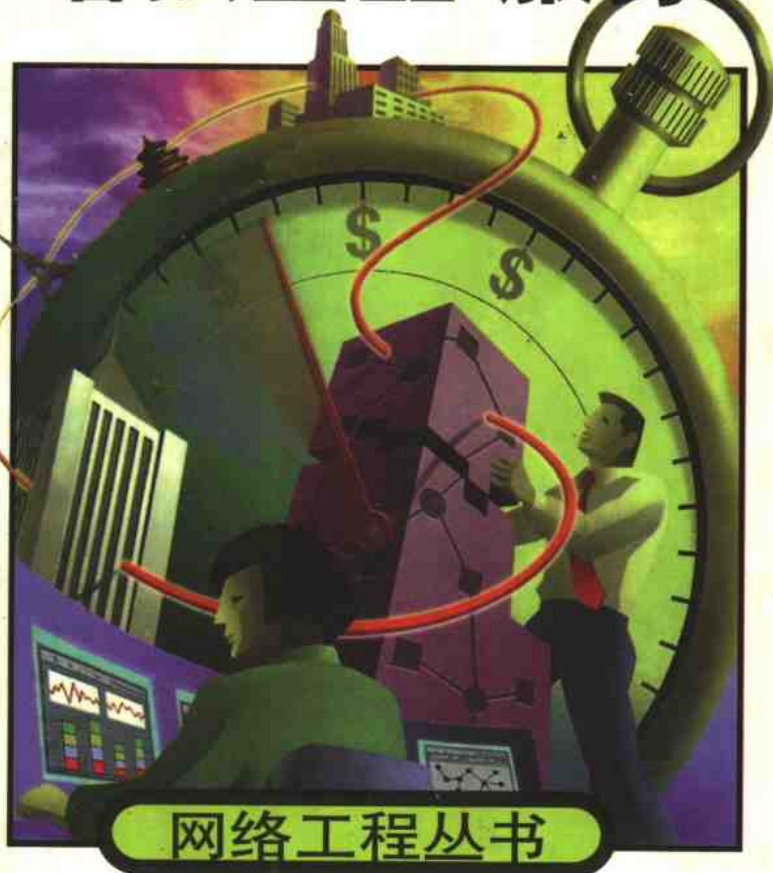


Cisco 网络 增强型IP服务



Enhanced IP Services for Cisco Networks

〔美〕 Donald C. Lee 著

谈利群 张文海 谢能付 等译

CISCO SYSTEMS
CISCO PRESS



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

URL: <http://www.phei.com.cn>

网络工程丛书

Cisco 网络增强型 IP 服务

Enhanced IP Services for Cisco Networks

[美] Donald C. Lee 著

谈利群 张文海 谢能付 等译

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

图书在版编目(CIP)数据

Cisco 网络增强型 IP 服务/(美)李(Lee, D. C.)著;谈利群等译. —北京:电子工业出版社, 2000. 6

(网络工程丛书)

书名原文: Enhanced IP Services for Cisco Networks

ISBN 7-5053-5922-3

I. C… II. ①李…②谈… III. 计算机网络-基本知识 IV. TP393

中国版本图书馆 CIP 数据核字(2000)第 07106 号

丛 书 名: 网络工程丛书

书 名: Cisco 网络增强型 IP 服务

原 书 名: Enhanced IP Services for Cisco Networks

著 者: [美] Donald C. Lee

译 者: 谈利群 张文海 谢能付 等

责任编辑: 窦 昊

特约编辑: 胡万三

排版制作: 电子工业出版社计算机排版室监制

印 刷 者: 北京京安达明印刷厂

出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>

北京市海淀区万寿路 173 信箱 邮编 100036

经 销: 各地新华书店

开 本: 850 × 1168 1/32 印张: 15.375 字数: 443 千字

版 次: 2000 年 6 月第 1 版 2000 年 6 月第 1 次印刷

书 号: ISBN 7-5053-5922-3
TP·3088

印 数: 6000 册 定价: 32.00 元

版权贸易合同登记号 图字: 01-2000-1551

凡购买电子工业出版社的图书, 如有缺页、倒页、脱页者, 请向购买书店调换;
若书店售缺, 请与本社发行部联系调换。电话 68279077

网络工程丛书出版说明

随着网络技术的飞速发展和广泛应用,各种先进而实用的网络技术日益成为人们关注的焦点。为了帮助读者更好地学习和掌握这些网络技术,提高网络理论水平和实际解决问题的能力,我们组织翻译了“网络工程丛书”。这套丛书由世界上最著名的图书出版集团——培生教育集团(Pearson Educational)出版。熟悉出版界状况的人士可能知道,培生教育集团下辖多个著名的出版集团,例如 Prentice Hall、Addison Wisely、Longman 以及 Macmillan 等等,其中 Macmillan 是世界上最大的计算机图书出版集团(1999 年中期并入培生教育集团)。原版的“网络工程丛书”出自于 Macmillan 所属的 Cisco Press、New Riders Publishing、Macmillan Technical Publishing 等几家著名的计算机图书出版公司。

网络工程丛书自 1998 年开始推向市场,现在已经出版了近 20 种图书(见后面的表格)。本套丛书的种类今后将不断扩张,以期包容所有最新、最高层的网络技术,跟踪并掌握各种技术发展动态及其原理,促进我国的计算机网络应用和开发。

网络工程丛书的读者对象

本丛书的读者对象主要是从事网络技术工作的工程技术人员,大专院校计算机专业、通信专业的师生,准备参加各种网络认证考试(包括国内的计算机水平考试、美国微软公司 MCSE 认证考试或 Cisco 公司的认证考试)的学生和职员。还可包括从事其他专业工作,但与网络工作密切相关的技术人员。

网络工程丛书的特点

网络工程丛书有别于普通的网络技术参考书,它以自身独特的优势,已经获得了并且今后会继续获得广大读者的欢迎。

权威著者 无一例外地,网络工程丛书的原文作者均是欧美国家的高层次网络专家。例如,各种国际网络标准组织的技术总监、各种网络标准的

制订者或评审人、获得国际最高级网络认证证书(如 CCIE)的权威网络专家、大型/超大型洲际网络的设计人员和高层网络管理人员。鉴于原出版集团所持的“非最高层作者不用”的原则,本套丛书著者的权威性“毋庸置疑”。

精心翻译 网络工程丛书是电子工业出版社的重点系列丛书,我们对译者、审校和编辑人员的选择采用了十分认真、严格的态度。所有参与本套丛书翻译、加工的人员必须是技术水平高、外语水平好且具有翻译图书经验的专业人员。同时,在其他出版环节,例如印刷、装订等环节,我们均制定了较高的要求。目的只有一个:要出高质量的精品丛书。

先进实用 网络工程丛书注重技术的先进性,关注网络技术的最新发展动态,同时十分注意书籍的实用价值。使读者不但能够了解到最新的技术进展、今后的发展动态,而且能够将其应用到实际的工作之中。特别是,从书中列举了大量的工作实例、故障排除方法及具体实施的经验和技巧,它们可帮助读者用最快的速度、最有效的方法完成任务。同时避免重复他人已经犯过的错误。

易于掌握 尽管本丛书是高水平的技术书籍,但它们并不晦涩难懂。本丛书的语言朴实、简练、易于理解,按照循序渐进、由简单到复杂、由原理到实践的原则,本丛书的内容很容易理解、掌握。只要具备基本的网络知识,便可掌握相关的技术内容,包括那些很深入、很先进的技术专题。

实例丰富 在重视基本原理介绍的同时,实际应用方法和实例是本丛书重要的组成部分,其中的经典实例不但可以帮助读者学习新知识,还可以举一反三,推广到具体实践之中。

资源共享 为方便学习、阅读本书,本丛书通过附加光盘或相关网站提供与书籍相关的材料或辅助软件,以提供更多的可供读者共享的资源(具体的共享资源见每本书的介绍)。

寿命期长 众所周知,网络原理及其标准的变化速度绝不像普通应用软件或操作系统,而且,本丛书合理的结构,使得本书具有较长的生命力。本系列书的原版书和翻译作品均制成精装本形式,也从一个方面说明了出版者对本丛书的信心——它们是可长期应用并颇具收藏价值的优秀系列书。

近期出版的网络工程丛书书目

编号	书 名	译者	定价	出版时间
1	网络互联技术手册(第二版)	包晓路	48.00	1999/04
2	因特网的路由选择技术 ——因特网的路由选择方案与实例	彭业飞等	28.00	1998/04
3	Cisco IOS 广域网解决方案	赵慧玲	40.00	1999/01
4	Cisco IOS 交换服务	彭业飞等	18.00	1999/01
5	Cisco IOS 网络协议解决方案第一卷:IP	夏凌 等	68.00	1999/01
6	Cisco IOS 网络协议解决方案第二卷: IPX, AppleTalk 及其他	张旆 等	98.00	1999/01
7	社区宽带网络	牛中允	24.00	1999/02
8	Cisco IOS 网桥及 IBM 网络解决方案	张惠民	88.00	1999/07
9	Cisco IOS 拨号上网解决方案(上下卷)	陈先中等	128.00	1999/07
10	IP 路由原理与应用	邓迎春等	26.00	1999/08
11	自顶向下网络设计	郑宏 等	38.00	1999/10
12	IP 网络路由基础	金甄平等	24.00	2000/01
13	EIGRP 网络设计 ——改进型内部网关路由协议网	伟峰 等	26.00	2000/02
14	网络互联故障排除手册	杜毅 等	48.00	2000/03
15	千兆位以太网	韩松 等	36.00	2000/03
16	Cisco 网络增强型 IP 服务	谈利群等	估 32.00	2000/05
17	Cisco 互连网络故障查找与排除	屈健 等	42.00	2000/03
18	IP 组播网络设计开发 第 1 卷	顾金星等	估 38.00	2000/05

译者的话

网络使地球变小,使人类开放;路由器是编织网络的千千结。电子工业出版社在这个时候选择这本书献给读者,真有“好雨知时节”的美好情谊。

本书分为管理路由、管理服务质量、管理网络安全性及附录 4 个部分。正文 8 章,讨论了 3 类问题:IP 寻址和路由空间管理,介绍了过滤、重新分配、总汇等基本路由策略;网络服务质量(QoS),介绍了服务质量概念、讨论了提高服务质量的机理和技术;网络安全和用户数据保密,分析了构成威胁的内外因素、探讨了这一领域至今还有效的措施和新技术。5 个附录介绍了路由、路由器、路由选择相关的背景资料和实用技能,给出了 Cisco IOS 的实用入门资料。

本书的特点是内容深、新,讲解易懂,作者思路清晰,按是什么、如何工作、如何配置、如何检验的顺序娓娓道来;精心地穿插一些极为有用的补充内容,指点迷津。本书的宗旨是提高 IOS 服务及 IP 网络的效能,帮助你认识网络安全的脆弱性、复杂性、保护的有效性,指导你配置好、管理好、运行好网络。

本书既适合网络技术专业人员,也适合网络用户。专业人员能获得对 IOS 服务的理解,有助于使网络支持更多的用户、更多的访问和更多的应用;网络用户可学习关于服务质量和 VPN 知识,提高安全性能和高级路由选择性能的必要技术,使自己的网络更安全有效。

参加本书翻译工作的同志还有李权、张曦、李璟、李艳芳;刘栓阳、纪丽珍同志承担了部分译稿的录入工作。我们衷心感谢你阅读本书,欢迎你批评指正。

反 馈 信 息

Cisco 出版社的目标是出版深层次的技术著作。制作出版的每一本书,凝集着相关专业技术领域里一流的最高水准的专家们的心血、智慧和严谨的工作精神。

读者的反馈,是我们出版工作的自然延续。如果你有什么意见,如你认为我们应该怎样改进这本书的质量、内容作某些改动更适合你的需求,可通过 E-mail 地址 ciscopress@mcp.com 与我们联系。来函切记注明本书书名及 ISBN 编号。

我们衷心感激你的帮助。

关于作者

Donald C. Lee(CCIE # 3262)是 Cisco System 公司的高级系统工程师,他具有 8 年多的网络工作实践经验,是毕业于 UCLA 电子工程专业的理学学士。他肩负着 Cisco 最大交易 500 家客户中数家公司的网络解决方案的设计、实现和技术支持工作。从 Prior 到 Cisco,Donn 一直是指导数据存储处理商的顾问系统工程师、消费产品超市管理者的信息系统网络经理/工程师。

关于技术审校者

Erick Mar 是 Cisco Sysem 公司的高级系统工程师,具有路由技术和交换技术领域的 CCIE 证书(CCIE # 3882)。作为一个最近 7 年为各种网络商服务的系统工程师,他已给 500 家大公司提供过网络设计和实现方面的支持。Erick 已获得 Santa Clara 大学的 MBA 学位,还拥有 San Francisco 州立大学商业管理理学学士学位。

Deepak Munjal(CCIE # 4376)已有 10 多年网络工作实践经验,拥有 California Berkeley 大学计算机科学专业的理学学士学位。他目前是 Cisco System 公司的高级系统工程师,他积极地参与了 Cisco 最大买卖 500 家客户的端到端网络解决方案的设计和实现。从 Prior 到 Cisco,Deepak 一直是指导计算机制造业的网络工程师。

致 谢

Kathy Trace, 作为此书的开发编辑, 她对本书作了很多的贡献, 应受到极大的赞扬。另外, 她博学多才, 富有条理, 善于灵活, 乐意助人, 是个非常好的人。

Erick Mar 和 Deepak Munjal 二位, 是这本书的技术审阅者, 他们的审改, 使本书比我原来的书稿大为增色。二位还是我所知道的同行中最好的 Cisco 工程师, 他们也是要好的朋友, 十分感谢二位给予的专业知识、忠告和他们的编辑工作。

Lynette Quinn 所做的本书项目管理工作, 自始至终十分出色, 她的积极态度和负责精神, 为我的工作创造了便利条件。

Alicia Buckley 提供了卓越的行政领导、支持和智慧, 她还听取了我对本书所有的不成熟的观点。像 Cisco 出版小组的所有成员一样, 她工作出色, 十分投入。

Julie Fairweather 和 Kim Lew 二位, 使我迅速开始了这本书的写作, 他们给予过有价值的支持, 和他们一起工作非常愉快。

Amy Lewis 是一位非常好的组织协调者, 他亲自过问具体细节和时间进度, 是成功出书的关键。

工作在幕后的那些 Cisco 出版小组, 是一支第一流的队伍, 衷心感谢他们在插图、编辑、排版等整个出版过程中所作出的贡献。

最后, 那些在 Cisco 工作的朋友对这项周末工程总是给予积极的鼓励和帮助, 我要特别地感谢我的上司 Srinivas Ketavarapu, Pasha Quadri 和 Rico Sacks 各位先生。Cisco 是一个天高任鸟飞的地方, 也正因为这些高人造就了 Cisco。

目 录

第 0 章 引言	(1)
0.1 Cisco 的互联网络操作系统(IOS).....	(2)
0.2 本书目的.....	(3)
0.3 读者对象.....	(3)
0.4 内容结构.....	(4)
0.5 约定和特点.....	(5)
0.6 技术支持.....	(6)

第一部分 管理路由选择

第 1 章 管理 IP 地址空间.....	(8)
1.1 传统 IP 寻址回顾	(9)
1.2 子网化有类别地址空间.....	(11)
1.2.1 主网和子网掩码	(12)
1.2.2 有类别子网化:个例分析	(15)
1.2.3 计算子网中的主机地址数.....	(17)
1.2.4 用提供的主机地址和掩码找出子网信息	(17)
1.2.5 子网化的不利因素	(19)
1.2.6 有关顶端子网和末端子网的规则	(19)
1.2.7 用全零子网(subnet-zero)回避规则.....	(20)
1.3 用可变长度子网掩码子网化.....	(21)
1.3.1 使用 VLSM 提高地址空间的效率:个例分析	(22)
1.3.2 对 Widget 有限公司子网化的最终 VLSM 结果	(30)
1.4 无类别寻址概述.....	(30)
1.4.1 将 VLSM 技术用于无类别寻址.....	(33)

1.4.2 路由选择协议和无类别寻址	(35)
1.5 规划地址总汇	(35)
1.6 用未编号 IP 地址保存子网	(37)
1.7 用网络地址转换法扩展地址空间	(38)
1.7.1 将专用地址转换成公共地址	(40)
1.7.2 配置 NAT	(42)
1.7.3 创建一个非连续地址池	(44)
1.7.4 配置静态 NAT	(44)
1.7.5 特殊应用和 NAT	(45)
1.7.6 有关 NAT 的要点	(45)
1.8 小结	(46)
第 2 章 部署内部路由选择协议	(48)
2.1 网络互联技术简要回顾	(49)
2.2 部署 RIP	(52)
2.2.1 直接连接的网络	(53)
2.2.2 配置 RIP	(56)
2.2.3 校验 RIP 配置	(57)
2.3 部署 IGRP	(60)
2.3.1 配置 IGRP	(61)
2.3.2 校验 IGRP 配置	(62)
2.4 部署增强的 IGRP	(64)
2.4.1 配置 EIGRP	(66)
2.4.2 校验 EIGRP 配置	(67)
2.5 部署 OSPF	(69)
2.5.1 配置 OSPF	(72)
2.5.2 校验 OSPF 配置	(76)
2.6 小结	(78)
第 3 章 理路由选择协议	(80)
3.1 配置被动接口	(80)

3.2	过滤路由选择更新	(83)
3.3	管理重分配	(86)
3.3.1	配置重分配——RIP 和 OSPF	(88)
3.3.2	重分配到 IGRP 和 EIGRP	(92)
3.3.3	理解管理距离	(93)
3.3.4	用路由过滤器控制重分配循环	(97)
3.4	解决 VLSM 和有类别路由选择协议问题	(100)
3.5	调整默认路由选择	(105)
3.5.1	默认路由的传播	(107)
3.5.2	用 RIP 发起默认路由	(108)
3.5.3	用 IGRP 发起默认路由	(110)
3.5.4	用 EIGRP 发起默认路由	(112)
3.5.5	用 OSPF 发起默认路由	(113)
3.5.6	默认路由选择和有类别行为	(115)
3.6	配置路由总汇	(118)
3.6.1	理解 EIGRP 自动总汇	(119)
3.6.2	配置 EIGRP 总汇	(121)
3.6.3	配置区域间 OSPF 总汇	(125)
3.6.4	配置重分配的 OSPF 总汇	(126)
3.7	用路由映射部署策略路由选择	(127)
3.7.1	用路由映射传递通信流	(128)
3.7.2	用路由映射给数据包分类	(138)
3.7.3	联合设置下一跳和优先级	(140)
3.7.4	其他的策略路由选择命令	(141)
3.8	小结	(142)

第二部分 管理服务质量

第 4 章	部署基本的服务质量部分	(146)
4.1	QoS 实例	(146)

4.2 路由器中的排队	(148)
4.2.1 先进先出排队	(149)
4.2.2 一个先进先出例子	(151)
4.3 优先级排队	(152)
4.3.1 按优先级排队来排队和分类包	(153)
4.3.2 优先级排队策略	(155)
4.3.3 配置优先级排队	(156)
4.3.4 验证优先级排队配置	(157)
4.3.5 调整优先级排队的队列大小	(158)
4.4 用户排队	(159)
4.4.1 配置用户排队	(162)
4.4.2 验证用户排队配置	(165)
4.4.3 调整用户排队队列大小	(166)
4.5 理解 IP 优先权	(167)
4.5.1 设置 IP 优先权	(168)
4.5.2 IP 优先权的 QoS 好处	(169)
4.5.3 异种服务重定义 IP 优先权	(169)
4.6 加权公平排队	(171)
4.6.1 配置加权公平排队	(171)
4.6.2 处于活动的公平排队	(173)
4.6.3 公平排队与 FIFO 区别	(174)
4.6.4 加权和 IP 优先权	(177)
4.6.5 网络上的加权公平排队	(178)
4.7 小结	(180)
第 5 章 部署高级的服务质量部分	(181)
5.1 资源预定协议	(181)
5.1.1 RSVP 接纳控制	(182)
5.1.2 RSVP 发信号与成批数据	(184)
5.1.3 RSVP 发送信号过程	(185)

5.1.4	RSVP 和加权公平排队	(190)
5.1.5	配置 RSVP	(192)
5.1.6	验证 RSVP 配置	(194)
5.1.7	配置 IOS 为 path 和 Resv 消息代理	(195)
5.1.8	RSVP 扩展问题(scaling considerations)	(199)
5.2	随机预检测	(199)
5.2.1	网络拥挤的动态性和尾丢包	(200)
5.2.2	全局同步化	(201)
5.2.3	TCP 慢启动(slow start)	(202)
5.2.4	全局同步化和 TCP 慢启动的不良影响	(202)
5.2.5	RED 如何工作	(203)
5.2.6	RED 和 IP 优先权(加权 RED)	(204)
5.2.7	配置 WRED	(205)
5.2.8	验证 WRED 配置	(206)
5.3	委托访问率	(208)
5.3.1	速率策略	(208)
5.3.2	配置 Cisco 快速传送	(210)
5.3.3	配置 CAR	(211)
5.3.4	验证 CAR 配置	(214)
5.4	基于类的 WFQ	(215)
5.4.1	配置 CBWFQ	(216)
5.4.2	验证 CBWFQ	(220)
5.5	小结	(222)

第三部分 管理网络安全性

第 6 章	部署基本安全服务	(226)
6.1	用访问控制表控制通信量	(226)
6.1.1	用访问控制表过滤通信量	(227)
6.1.2	标准 IP 协议访问表	(230)

6.1.3	设计访问表的重点	(237)
6.1.4	每个访问表中的隐藏规则	(240)
6.1.5	扩展 IP 地址访问表	(241)
6.1.6	防止电子欺骗攻击的访问表	(248)
6.2	安全访问路由器	(251)
6.2.1	安全处理路由器启用模式	(252)
6.2.2	安全处理 Telnet 访问	(253)
6.2.3	安全处理控制台端口访问	(256)
6.3	部署认证、授权和记账	(256)
6.3.1	认证、授权和记账	(257)
6.3.2	为基于 PPP 的网络访问配置认证	(261)
6.3.3	使用默认认证表	(265)
6.3.4	配置路由器登录认证	(265)
6.3.5	本地用户名数据库	(267)
6.3.6	配置授权	(268)
6.3.7	配置记账	(269)
6.3.8	把路由器指向 RADIUS 和 TACACS+ AAA 服务器	(270)
6.4	其他 IOS 基本安全命令	(271)
6.4.1	禁止 TCP 和 UDP 小服务	(271)
6.4.2	禁止 IP 地址源路由选择	(272)
6.4.3	禁止公共链路上的 CDP	(273)
6.4.4	禁止接口上直接广播	(273)
6.5	小结	(274)
第 7 章	高级安全服务第一部分:IPsec	(276)
7.1	IPsec 保障虚拟专用网(VPN)	(277)
7.2	IPsec 第 3 层服务带来的好处	(278)
7.3	IPsec 安全概念和密码学基础	(280)
7.3.1	秘密性(加密)	(280)
7.3.2	完整性	(289)

7.3.3	散列算法举例:消息摘要 5 号(Message Digest 5)	(290)
7.3.4	信源认证	(291)
7.3.5	防止模仿操作	(295)
7.4	IPsec 概念	(295)
7.4.1	对等方	(296)
7.4.2	变换集	(296)
7.4.3	安全联接	(297)
7.4.4	传输和隧道模式	(299)
7.4.5	认证头和封装安全有效载荷	(300)
7.5	因特网密钥交换	(302)
7.6	将各部分组合在一起:利用 IPsec 和 IKE 的完整例子	(303)
7.7	配置 IKE	(305)
7.7.1	利用预约共享密钥配置 IKE	(306)
7.7.2	配置带 RSA 加密的 IKE	(309)
7.7.3	配置带 RSA 签名和数字证书的 IKE	(316)
7.7.4	IKE 的附加命令	(325)
7.7.5	确认 IKE 配置	(327)
7.7.6	何时建成 IKE SA	(328)
7.8	配置 IPsec	(328)
7.8.1	密码映射表	(329)
7.8.2	密码映射表配置简介	(331)
7.8.3	配置密码访问表	(331)
7.8.4	一个密码访问表实例	(332)
7.8.5	配置 IPsec 变换集	(336)
7.8.6	配置和应用密码映射表	(338)
7.8.7	何时需要建立 SA	(341)
7.8.8	配置 IPsec SA 的生存期	(342)
7.8.9	配置完全正向保密机制	(343)