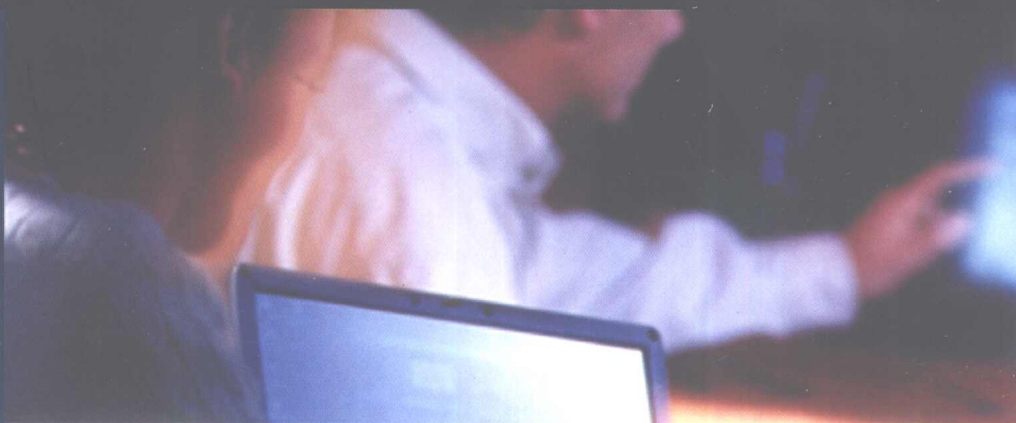


CISCO SYSTEMS



Cisco Press



Cisco ISP 必备手册

Cisco ISP Essentials

A comprehensive guide to the best common practices for Internet service providers

Barry Raveendran Greene

Philip Smith

胡捷 赵晓京

著

译

3.4-62

人民邮电出版社

TP3/24-62 267
G37

Cisco ISP 配置手册

Barry Raveendran Greene 著
Philip Smith

胡捷 赵晓京 译

人民邮电出版社

图书在版编目(CIP)数据

Cisco ISP 必备手册/(美)格林(Greene,B.R.), (美)史密斯(Smith,P.)著; 胡捷, 赵晓京译.—北京: 人民邮电出版社, 2002.11

ISBN 7-115-10634-7

I. C... II. ①... ②史... ③胡... ④赵... III. 因特网—技术手册 IV. TP393.4-62

中国版本图书馆 CIP 数据核字(2002)第 074323 号

版权声明

Barry Raveendran Greene, Philip Smith: Cisco ISP Essentials (ISBN:1587050412)

Copyright © 2002 by Cisco Systems, Inc.

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

All rights reserved.

本书中文简体字版由美国 Cisco Press 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。

Cisco ISP 必备手册

◆ 著 Barry Raveendran Greene Philip Smith
译 胡捷 赵晓京
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 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132705
北京汉魂图文设计有限公司制作
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: 23
字数: 544 千字 2002 年 11 月第 1 版
印数: 1-4 000 册 2002 年 11 月北京第 1 次印刷

著作权合同登记 图字: 01 - 2001 - 4099 号

ISBN 7-115-10634-7/TP · 3091

定价: 48.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

前言

自 20 世纪 90 年代中期以来, Internet 经济在世界经济中起着非常重要的作用。在最初的几年, Internet 曾经一度是专为美国国防和科研机构而设的网络, 而且在当时, 世界上只有为数不多的几个企业家相信基于 TCP/IP 协议的广域网络会发展成为另一个可以提供商业应用的网络, 它们很有可能会代替正在用于商务联系的专用有线网络。许多在那个时期学习了相关技术的 ISP 工程师们在 20 世纪 80 年代末和 90 年代初之间好像已经预感到这样的日子会到来。工作还是一成不变, 不断重复, 与相对轻松和容易的网络配置及使用相比, 其技术上的挑战总是永无止境。但是这种竞争和合作的环境在更友好的商业竞争意识下相互促进, 使得刚刚诞生的 Internet 越来越充满乐趣。

正是由于这种先锋般的开拓精神, 以及 Internet 团体要推动 Internet 成功的强烈意愿, 才最终使得 Internet 在 21 世纪之初成为人们生活中不可或缺的一部分。当前 Internet 已经成为一个巨大的商业网络, 非常具有竞争性, 世界各地的许多机关和团体, 将它们的规模或大或小的网络基础设施加入到 Internet, 成为大家庭中的一员。每一天都有更多的人们成为 Internet 的参与者, 既有使用他所拥有的第一台电脑首次连接到万维网的终端用户, 也有急切地想加入到这个快速增长的产业中来的新 ISP。此外, 世界上为数不多的几个至今尚未与 Internet 连通的国家正在调查其连通的可行性, 同时在认真考虑是否在与 Internet 连通后会对当地经济发展产生推动作用。

由于 Internet 每天都在高速增长, 因此出现了许多有关 Internet 的书籍, 它们希望能帮助 Internet 用户实现淘金的梦想: 图书内容包括从初学者指南到如何设计 Web 页面, 到解释什么是 Internet, 到描述如何进行商业运作以及如何成为一个成功的 ISP。当然, 在所有这些内容中总有一些很宝贵的信息来

告诉 ISP，网络工程师们有关设备配置的概念和配置技巧，这些有价值的内容与他们的日常工作密切相关，正如一句话所说的：“由于我们太忙，以至于我们在 Internet 信息高速公路上虽然修补了路面的凹坑，但是没有时间将我们所做的事情记录下来。”

动机

写这本书的灵感来自于 3 个方面。首先是由于思科的 IOS 软件。思科公司在 Internet 诞生之初就已经成为其一部分，制造出第一台在广域网中传递数据包的设备。在其后的几年中，IOS 从最初的初级软件程序逐步发展到更复杂，具有更多特性，并且功能非常强大的路由器控制套件。IOS 拥有广泛的特性和功能，这些增强的特性和功能在 ISP 看来是非常优秀的，给了网络工程师们在设计不同需求网络时极大的选择余地和能力。人们一直希望 IOS 功能强大和特性繁多，但是 IOS 随之也产生了一个新的问题，网络工程师们成天忙于他们的工作以维护一个网络的正常运转，反而很难有时间来及时跟踪和了解新版 IOS 都增加了哪些特性。许多网络工程师，即使是很有经验的工程师，也不知道在他们的网络中如何、何时以及在何处来部署各种不同版本和特性的 IOS。

这本书重点介绍了世界上一些主要 ISP 在他们的骨干网络中安装的 IOS 每日都需要用到的关键特性。明智地学习和实践本书所提到的内容将有助于减少网络问题的产生，增加安全性，提高网络性能，并且确保 Internet 的运行稳定。

写本书的第二个灵感是，至今还没有一本完整的参考书来指导刚刚进入这个领域的入门者来配置设备和搭建一个 ISP 网络。有许多技术文档谈论关于网络设计和实践、谈论 ISP 商业运作实践、谈论如何配置各种路由选择协议以及谈论所有基于 Internet 之上的高层应用等等。这类书就像《Internet 路由选择体系结构》第二版，以及《ISP 生存指南》一样，虽然已经帮助了许多 ISP 来应付他们骨干网的扩展并且提高了网络商业应用，但是当个新手打开设备的包装箱，面对蓝色/绿色的金属盒子，以及一个介绍这个设备如何使用的所有相关技术文档的光盘时，他一定会感到沮丧：“到底该怎么办？”本书的目的就是同时指导新手和富有经验的工程师如何优化配置这些蓝色/绿色的金属盒子，以及如何优化由这些盒子搭建的网络，将这些设备高效安全地集成到一个 ISP 网络中去，并且使之成为 Internet 骨干网络的一部分。

最后的灵感来自于我们已经提及到的问题：我们都太忙碌以至于没有时间记录下我们所做的事情。我们每天的工作日程包括会晤新的 ISP、帮助优化 ISP 们现有的网络，等等。我们经常碰到一些非常明显的概念重复，但是又没有被收录到技术文档中。《IOS 精华白皮书》针对这些问题，收录了几乎是 ISP 商业网络才会碰到的许多 IOS 特性和功能的介绍。许多这个领域的朋友和同事一直在鼓励我们在白皮书的基础上写一本这方面的书，把我们这个行业里从 20 世纪 90 年代开始就积累下来的经验和知识记录下来，以使他人受益。

本书的读者

本书的内容主要针对 ISP。无论那些专用网络或企业网络是否最终也连接到 Internet 上，我们并不向其他类型的网络从业者推荐本书，虽然我们相信本书的一些想法和建议同样适用于这类网络。

ISP 网络工程师将从本书获益匪浅（所有类型的网络工程师，包括网络管理中心、客户

技术支持中心和专注于维护骨干网络核心设备的工程师)。本书的内容包括 ISP 网络工程相关所有领域将会面临的各种不同的概念及问题,我们希望本书对每个人都有参考价值。本书最后一章还提供了 ISP 基于商业方面的应用和需求的相关内容。就我们的经验来看,规划一个网络并不像我们想象的那样困难。网络规划只是在网络工程师和商业经理之间起到一个连接作用,以确保在网络结构的理想化和建设资金不足的现实之间找到一个最好的平衡点。

章节划分

本书分为 5 章。另外还有一些附录,给读者提供一些与本书内容相关的补充信息的配置技巧和模板。这些章节包括以下主题:

第一章 软件和路由器管理:向读者介绍思科的 IOS 软件、专门针对 ISP 网络而开发的特殊版本和子序列,以及在路由器上如何配置和管理这些软件。本章还介绍了如何管理路由器,包括配置管理、命令行接口 (CLI),以及如何处理路由器生成的对系统管理员有帮助的状态信息。

第二章 常规特性:介绍了 ISP 在组织和管理路由器时需要了解的各种 IOS 软件特性,在 ISP 运行维护一个网络时,了解这些软件特性的优先程度要高于了解如何配置路由选择协议和网络安全。IOS 的特性包括路由器的环回接口、接口配置技巧实践、思科快速转发 (CEF) 和网络流量流向监控软件 Netflow。

第三章 路由选择协议:讲述了 ISP 配置主要的路由选择协议时需要了解的各种软件特性。包括 HSRP、IGP 设计,以及思科 IOS 软件关于 BGP 配置方面已经可实现的软件功能和特性。

第四章 安全:内容涵盖 IOS 软件针对路由器上主要安全问题的特性和所支持的功能,并且就软件支持的特性针对当今很盛行的拒绝服务攻击 (dos) 展开了广泛的讨论。我们的话题还包括路由器的登录、路由选择协议的安全以及网络安全。我们讨论的软件特性包括单播 RPF 以及承诺接入速率 (CAR) 的应用。

第五章 操作实践:最后一章讲述如何对前 4 章进行汇总以帮助建立一个 ISP 骨干网络。内容主要涉及搭建一个 ISP 骨干网络时的典型的处理方式和过程,包括所有设计和部署网络的方式,以及提供和实施高层服务的过程。

附录:附录部分提供了额外的参考信息对前面各章介绍的内容进行补充。包括如何配置路由器以抑制路由摆动,并列出了当前广泛采用的网络管理和监控软件工具,以及如何利用本书中提到的 IOS 软件配置原则来配置一个小型 ISP 网络的工作模板。

最好按照本书的章节顺序来阅读,因为每一章节所讲述的内容都以假设读者对前一章节的内容已经掌握为基础。当然,经验丰富的网络工程师可以跳过某些章节直接进入想了解的部分。本书的编写风格就是想同时满足富有经验的专家和刚刚入门的初学者对本书的学习。

更多信息

这本书并没有完全包括思科为一般公众和它的客户已经提供的所有相关的技术文档和优秀的资料。这本书是基于《IOS 精华白皮书》而编写的,在白皮书中我们已经收集了一些与已经发行的 IOS 版本相关的特性方面的技术文档,当思科的技术文档中还没有相关的论述文件时,我们则编写了一些解释。一般情况下,思科的技术文档总是要推迟很久才将《IOS 精

华》中提到的技术问题以文档形式补充进去。

在编写和出版这本书的同时，作者在 Internet 上建立了一个与本书内容相关的能够提供及时更新信息的网站 <http://www.ispbook.com>。另一个 Web 站点 <http://www.cisco.com/public/cons/isp> 同样也提供对 ISP 可能有帮助的参考材料。

显然，本书的主题并没有深入到足够的技术细节，读者可以在以下站点得到参考资料：

- 思科系统公司的技术文档（Documentation）（一般公众可以在思科网站上获取：<http://www.cisco.com/univercd>）或者从购买路由器时与路由器同时提供给客户的 CD-ROM 光盘；
- Cisco.com；
- 当地的思科公司技术支持渠道；
- Internet 上的公共论坛地址列表。这些地址列表是专门针对采用了思科公司设备的 ISP 网络而设立的，叫作 cisco-nsp 论坛，由 Jared Mauch 主持。cisco-nsp 是一个邮件列表论坛，专门为 ISP 们设立，以讨论思科系统产品和它们的用途。如果希望订阅，请向如下地址发一封电子邮件：majordomo@puck.nether.net 并注明“订阅 cisco-nsp”。

目 录

第 1 章 软件和路由器管理	3
1.1 究竟应该采用哪个版本的 IOS 软件	4
1.1.1 哪里可以获得关于 12.0S 版本的信息	5
1.1.2 关于 IOS 版本情况的进一步参考信息	5
1.2 IOS 软件的管理	7
1.2.1 闪存	7
1.2.2 系统内存	8
1.2.3 何时以及如何升级	9
1.2.4 向闪存中拷贝新的软件	10
1.3 配置管理	13
1.3.1 NVRAM、TFTP 服务器和 FTP 服务器	14
1.3.2 大配置文件	15
1.4 命令行接口	16
1.4.1 编辑键	16
1.4.2 CLI 字符串搜寻	16
1.5 详细的日志信息	18
1.5.1 日志信息采集系统的逻辑拓扑	20
1.5.2 分析系统日志数据	21
1.6 网络时间协议 (NTP)	21
1.6.1 网络时间协议体系结构	22
1.6.2 客户机/服务器模式和联合 (Association) 模式	23
1.6.3 在 ISP 网络中的路由器上实施网络时间协议	24
1.6.4 NTP 部署范例	25
1.6.5 在一个网络节点 (POP) 中实施 NTP(范例)	25
1.6.6 进一步的 NTP 参考信息	27
1.7 简单网络管理协议(SNMP)	28
1.7.1 SNMP 的只读模式	28

1.7.2	SNMP 的读写模式	29
1.7.3	SNMP 和商业化的网络管理软件	30
1.8	HTTP 服务器	30
1.9	内核导出/备份 (Core Dumps)	31
1.10	总结	32
1.11	尾注	32
第 2 章	常规特性	35
2.1	IOS 软件和环回接口	35
2.1.1	使用环回接口的动机	36
2.1.2	BGP 更新的源地址	36
2.1.3	路由器身份标识 (ID)	36
2.1.4	通过 FTP 协议进行内核导出的例外	37
2.1.5	TFTP 服务器的访问	37
2.1.6	SNMP 服务器的访问	37
2.1.7	TACACS/RADIUS 服务器的源接口	38
2.1.8	NetFlow 流量输出	38
2.1.9	NTP 源接口	39
2.1.10	Syslog 源接口	39
2.1.11	远程登录到路由器	40
2.1.12	对路由器实施 RCMD	41
2.2	接口配置	41
2.2.1	描述	41
2.2.2	带宽	41
2.2.3	无编号 IP 地址	42
2.3	接口状态检测	44
2.3.1	显示接口交换状态	44
2.3.2	显示接口状态	45
2.3.3	显示 IDB	46
2.4	思科快速转发	46
2.5	NetFlow	47
2.5.1	NetFlow 特性加速	47
2.5.2	NetFlow 统计——基础	48
2.5.3	NetFlow 数据输出	50
2.6	启用 Nagle	51
2.7	域名服务器 (DNS) 和路由器	51
2.7.1	将 IP 地址映射为名字	52
2.7.2	IOS 软件中的 DNS 解析	53
2.8	总结	54
2.9	尾注	54

第3章 路由选择协议	57
3.1 CIDR 特性	57
3.1.1 IP 无类别	58
3.1.2 全零 IP 子网	59
3.2 选择性数据包丢弃	59
3.3 热备份路由选择协议	60
3.4 IP 源路由	63
3.5 配置路由选择协议	64
3.5.1 路由器身份标识	64
3.5.2 选择一个 IGP	65
3.5.3 将地址前缀注入 IGP	65
3.5.4 IGP 汇聚 (IGP Summarization)	66
3.5.5 由于 IGP 邻接体变化而产生的系统日志	66
3.5.6 将地址前缀注入 BGP	67
3.6 IGP 配置提示	69
3.6.1 网络设计	69
3.6.2 地址前缀类型	69
3.6.3 配置 OSPF	70
3.6.4 配置 IS-IS	72
3.6.5 配置 EIGRP	74
3.6.6 设计总结	75
3.7 BGP 路径选择过程	76
3.8 BGP 特性和命令	78
3.8.1 稳定的 iBGP 配置	78
3.8.2 BGP 自动汇聚	79
3.8.3 BGP 同步	79
3.8.4 BGP 团体属性格式	80
3.8.5 BGP 邻接体关闭	80
3.8.6 BGP 动态重配置	80
3.8.7 BGP 路由反射器和 BGP 族标识	82
3.8.8 下一跳自身	84
3.8.9 BGP 路由摆动抑制	86
3.8.10 BGP 邻接体认证	90
3.8.11 BGP MED 未设置	90
3.8.12 BGP 确定的 MED	91
3.8.13 比较路由器标识	91
3.8.14 BGP 网络声明	91
3.8.15 移去私有自治系统	92
3.8.16 BGP 本地 AS	92

3.8.17 BGP 邻接体改变	93
3.8.18 限制从邻接体来的地址前缀数量	94
3.8.19 限制从邻接体来的 AS 路径长度	94
3.8.20 BGP 快速-外部-故障恢复	95
3.8.21 BGP 对等体组	95
3.8.22 BGP 多路径	97
3.9 实施 BGP 策略	99
3.9.1 采用地址前缀列表进行 BGP 路由过滤	100
3.9.2 BGP 过滤处理顺序	104
3.9.3 BGP 有条件通告	105
3.9.4 BGP 流出路由过滤性能	107
3.10 BGP 策略记账	109
3.10.1 配置	109
3.10.2 显示 BGP 策略记账状态	110
3.10.3 显示 BGP 策略记账统计信息	111
3.11 多协议 BGP	111
3.11.1 开发新类型 CLI 界面的动机	111
3.11.2 命令组机构	112
3.11.3 新旧类型的比较	113
3.11.4 升级到新的 CLI	118
3.11.5 采用新类型 CLI 的例子	118
3.12 总结	120
3.13 尾注	120
第 4 章 安全	123
4.1 路由器安全	124
4.2 不需要的或冒险的接口配置模式下服务	125
4.3 Cisco 设备发现协议	126
4.4 登录标语	127
4.5 使用 enable secret	128
4.6 ident 特性	129
4.7 SNMP 安全	129
4.8 路由器访问：控制谁能够进入路由器	130
4.8.1 原则	130
4.8.2 VTY 和控制台端口超时	131
4.8.3 VTY 端口访问控制列表	131
4.8.4 VTY 访问和 SSH	133
4.8.5 用户认证	134
4.8.6 采用 AAA 保证路由器安全	135
4.8.7 路由器命令审核	136

4.8.8 一次性口令	138
4.8.9 路由器 ICMP 不可到达消息管理	139
4.8.10 部署新的路由器或交换机	140
4.9 路由选择协议安全	142
4.10 网络安全	146
4.10.1 入口和出口过滤	146
4.10.2 路由过滤	147
4.10.3 包过滤	153
4.11 访问控制列表: 通常顺序化 ACL	153
4.11.1 访问控制列表: Turbo ACL	155
4.11.2 基于 ASIC 的 ACL	157
4.11.3 用 ACL 来进行出口包过滤: 防止无效 IP 地址传送	158
4.11.4 用 ACL 进行入口包过滤: 防止无效 IP 地址接收	159
4.11.5 用黑洞路由选择进行包过滤 (转发至 Null0)	161
4.12 BCP 38 使用单播 RPF	162
4.12.1 背景	163
4.12.2 路由选择表的要求	169
4.12.3 uRPF 严格模式下 BCP 38 的实现	169
4.13 速率极限或丢弃包的指定访问速率	178
4.13.1 Smurf 攻击	178
4.13.2 用 CAR 的速率限制	179
4.13.3 Smurf 防御概要	182
4.14 对安全事件做出反应	182
4.14.1 方法	183
4.14.2 例子	183
4.15 总结	184
4.16 尾注	184
第 5 章 操作实践	187
5.1 PoP 的拓扑结构	187
5.1.1 核心层	188
5.1.2 分布层	188
5.1.3 接入层	191
5.1.4 虚拟主机服务	192
5.1.5 小结	193
5.2 接入服务提供点的设计	193
5.3 骨干网络设计	193
5.4 ISP 服务	195
5.4.1 域名服务	195
5.4.2 邮件服务	198

5.4.3	新闻服务	199
5.4.4	保持软件是最新的	200
5.5	在 ISP 骨干网中的 IPv4 地址	201
5.5.1	商业模式和 IP 地址空间	202
5.5.2	地址计划	203
5.5.3	整理地址分配计划	208
5.5.4	用户的地址空间	210
5.5.5	向 RIR 或上层 ISP 申请地址	211
5.5.6	结论	211
5.6	内部路由选择	212
5.6.1	ISP 的 IGP 和 BGP 模式比较	212
5.6.2	扩展内部路由选择协议	213
5.7	外部路由选择	215
5.7.1	自治域号码	215
5.7.2	可扩展的外部对等	215
5.8	多宿主	217
5.8.1	基础	218
5.8.2	多宿主选择	219
5.8.3	到相同 ISP 的多宿主	223
5.8.4	到不同 ISP 的多宿主	230
5.8.5	出口流量负载均衡	234
5.8.6	使用团体	244
5.9	安全	249
5.9.1	ISP 边界包过滤	249
5.9.2	聚合路由器过滤	250
5.9.3	用户路由器过滤	251
5.9.4	ISP 服务器需要考虑的事项	252
5.9.5	防火墙	253
5.9.6	远程访问	253
5.10	带外管理	254
5.10.1	调制解调器	254
5.10.2	控制台服务器	254
5.10.3	带外 ISDN	256
5.10.4	带外链路	256
5.10.5	带外测试	256
5.10.6	小结	257
5.11	测试实验室	257
5.11.1	测试新的硬件和软件	257
5.11.2	设计一个测试实验室	258
5.11.3	小结	259

5.12 运作需要考虑的事项	259
5.12.1 维护	259
5.12.2 网络实施和用户支持	260
5.12.3 工程	260
5.12.4 改变管理	261
5.13 总结	261
5.14 尾注	262
附录 A 访问列表及规则表示	265
A.1 访问列表类型	265
A.2 IOS 软件规则表示	266
A.3 尾注	267
附录 B 剪切和粘贴模板	269
B.1 普通的系统模板	269
B.2 普通接口模板	270
B.3 普通安全模板	271
B.4 普通 iBGP 模板	272
B.5 普通 eBGP 模板	273
B.6 Martian 和 RFC1918 网络模板	274
B.6.1	274
B.6.2	275
附录 C 配置实例	277
C.1 简单网络规划	277
C.2 配置	278
C.2.1 ISP 地址规划	278
C.2.2 边界路由器	279
C.2.3 核心路由器	285
C.2.4 汇聚路由器	289
C.2.5 服务路由器	293
C.2.6 NOC 路由器	297
C.2.7 接入服务器	301
C.2.8 带外控制服务器	305
C.3 总结	310
附录 D 路由摆动抑制	313
D.1 BGP 摆动抑制配置	313
D.1.1 IP 访问列表例子	313
D.1.2 IP 前缀列表例子	315

附录 E 流量工程工具	319
E.1 Internet 流量及网络工程工具	319
E.1.1 CAIDA	320
E.1.2 Scion/NetScarf	320
E.1.3 NeTraMet/NetFlowMet	320
E.1.4 Cflowd	320
E.1.5 MRTG	320
E.1.6 RRDTool	320
E.1.7 Linux 网管工具	321
E.1.8 Vulture	321
E.1.9 Net SNMP	321
E.1.10 SysMon	321
E.1.11 Treno	321
E.1.12 Scotty——网络管理应用的 Tcl 扩展	321
E.1.13 NetSaint	322
E.2 管理网络的其他有用的工具	322
E.2.1 traceroute	322
E.2.2 Looking Glasses	322
E.2.3 whois	323
E.2.4 Gnuplot	323
E.2.5 RTRMon——路由器监视和操作的工具	323
E.2.6 RAToolSet/IRRTToolSet	323
E.2.7 Cisco 的管理信息库	324
E.2.8 替代系统日志后台程序	324
E.3 全面的 Internet 状况及性能工具	324
E.3.1 NetStat	324
E.4 其他 ISP 在做什么	325
E.5 总结	327
附录 F ISP 访问安全的移动计划示例	329
F.1 阶段 1——将接入到在 CIDR 块外的每一个人的功能关掉	329
F.2 阶段 2——在对等连接中增加反欺骗过滤器	331
F.2.1 在哪里设置反欺骗包过滤器	331
F.3 阶段 3——关闭未被授权访问的网络设备	333
F.4 总结	334
F.5 尾注	334
词汇表	337
技术参考及推荐读物	341

