

FROM ASTERISK TO ZEBRA WITH EASY-TO-USE RECIPES



LINUX Networking Cookbook™

中文版

O'REILLY®
东南大学出版社

CARLA SCHRODER 著
冯亮 译

Linux Networking CookbookTM

Carla Schroder 著

冯亮 译

O'REILLY[®]

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权东南大学出版社出版

东南大学出版社

图书在版编目 (CIP) 数据

Linux Networking Cookbook = Linux 网络 Cookbook/
(美) 施罗德 (Schroder, C.) 著; 冯亮译. —南京: 东南大学出版社, 2009.4

书名原文: Linux Networking Cookbook

ISBN 978-7-5641-1520-3

I. L… II. ①施… ②冯… III. Linux 操作系统
IV. TP316.89

中国版本图书馆 CIP 数据核字 (2009) 第 022504 号

江苏省版权局著作权合同登记

图字: 10-2008-352 号

©2008 by O'Reilly Media, Inc.

Simplified Chinese Edition, jointly published by O'Reilly Media, Inc. and Southeast University Press, 2009. Authorized translation of the English edition, 2008 O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 O'Reilly Media, Inc. 出版 2008。

简体中文版由东南大学出版社出版 2009。英文原版的翻译得到 O'Reilly Media, Inc. 的授权。此简体中文版的出版和销售得到出版权和销售权的所有者——O'Reilly Media, Inc. 的许可。

版权所有, 未得书面许可, 本书的任何部分和全部不得以任何形式复制。

Linux Networking Cookbook

出版发行: 东南大学出版社

地 址: 南京四牌楼 2 号 邮编: 210096

出 版 人: 江 汉

网 址: <http://press.seu.edu.cn>

电子邮件: press@seu.edu.cn

印 刷: 扬中市印刷有限公司

开 本: 787 毫米 × 980 毫米 16 开本

印 张: 41 印张

字 数: 689 千字

版 次: 2009 年 4 月第 1 版

印 次: 2009 年 4 月第 1 次印刷

书 号: ISBN 978-7-5641-1520-3

印 数: 1~5000 册

定 价: 88.00 元 (册)

本社图书若有印装质量问题, 请直接与读者服务部联系。电话 (传真): 025-83792328

O'Reilly Media, Inc. 介绍

为了满足读者对网络 and 软件技术知识的迫切需求，世界著名计算机图书出版机构 O'Reilly Media, Inc. 授权东南大学出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 Unix、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》(被纽约公共图书馆评为 20 世纪最重要的 50 本书之一)到 GNN(最早的 Internet 门户和商业网站)，再到 WebSite(第一个桌面 PC 的 Web 服务器软件)，O'Reilly Media, Inc. 一直处于 Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得 O'Reilly Media, Inc. 形成了一个与其他出版商迥然不同的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为 O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以 O'Reilly Media, Inc. 知道市场上真正需要什么图书。

作者简介

Carla Schroder 是一位自学成才的 Linux 和 Windows 系统管理员，她自 37 岁生日那天开始接触第一台计算机。她的第一台 PC 是 Macintosh LC II。然后是一台运行 MS-DOS 5 和 Windows 3.1 的 386sx IBM 兼容机，连接着一个 14 英寸的彩色显示器，在这台计算机上愉快地玩若干个小时的 DOOM 游戏那是足够了。再后来，大约 1997 年左右，她发现了 Red Hat 5.0，由此便开始探索一个全新的世界。

一路走来，她为小型商业企业和家庭用户提供技术咨询服务，同时支持 Linux 和 Windows 用户，并且在局域网上将 Linux 和 Windows 无缝地整合在一起。她是《Linux Cookbook》(O'Reilly) 一书的作者，还为多家计算机刊物撰写关于 Linux 基础知识的文章。

Carla 以实践证明，尝试新事物永远不嫌年老，计算机充满了太多乐趣，任何人都可以学着去做任何事。想了解更多关于 Carla 的事，可访问 <http://tuxcomputing.com>。

封面设计

《Linux Networking Cookbook》封面图案是一位女铁匠。在历史上，女性通常从事裁缝和教师职业，从事铁匠职业的妇女早在中世纪就逐步退出舞台了。尽管中世纪的妇女大多待在家里做饭、烤面包和缝织衣物，还是有一些妇女成为了铁匠，锻造兵器，以保卫她们的家园和城堡。

虽然她们从事此项职业曾有相当长的历史，但妇女在钢铁工业中的出现还是常常令很多人感到惊讶。1741 年，作家兼书店主人 William Hutton 在英国乡间旅行时路过一家铁匠铺。在那间铺子里，他见证了“一位或多位妇女，脱去她们的上衣，收入低的不能再低，以女性特有的姿势挥舞铁锤”的场景。据猜想，由于发现女人——而非男人——从事铁匠工作这件事令 Hutton 深感震惊，她们的衣着反倒并不那么重要。

关于妇女是否可以从事铁匠职业的论战曾几度发生。1895 年，Hattie Graham 女士向马萨诸塞州的萨德伯里 (Sudbury) 市政厅提交申请，要求批准其在 Mary Heard 小姐所拥有的铺子里从事铁匠工作。当时，一位妇女拥有一家铁匠铺并不会引发社会议

论，而一位妇女从事铁匠工作就会。尽管如此，Graham以精湛的技艺最终击败了那些抗议其早先在铁匠铺工作的反对声浪。

时至今日，还是有不少人对妇女此前曾经做过铁匠的事实表示惊讶。据报道，游客漫步威廉斯堡（Williamsburg）殖民地的时候经常会问，是否妇女曾经真地被准许从事铁匠工作，或者想知道这项工作对于她们来说是否力所能及。

到了21世纪，铸铁锻造逐步向特许行业和艺术表演方向发展。2001年，一份名为“Mama Wahunzi”（斯瓦希利语中的“女铁匠”）的档案，将三位妇女学习并制作她们自用的轮椅并自行控制轮椅活动的故事载入了编年史。在非洲，女铁匠与农妇合作，自行设计和维护她们的劳动工具。在美国，如今估计还有50位左右的全职女铁匠，她们中的很多人正在制作公共艺术品，帮助恢复旧建筑和制造现代家具。

封面图像和每个章节的开篇图案均取自《Dover's Women: A Pictorial Archive from 19th-Century Sources》一书。

关于译者

冯亮，杭州人。沉浸于Linux系统管理十余年，以此为业逾五载。目前供职于阿里巴巴（中国）网络技术有限公司，任运维架构师。业余偶猎文史哲社政法诸学，好读书，不求甚解。游戏文字，自娱娱人。聊为无益之事，以遣有涯之生也。

关于本书中文译本的任何反馈，请发送电子邮件给译者：fengliang@zhidaofenzi.com（译者博客 <http://hutuworm.blogspot.com>）。

目录

前言	1
第 1 章 Linux 网络概述	9
1.0 介绍	9
第 2 章 建立基于单板计算机的 Linux 网关	20
2.0 介绍	20
2.1 熟悉 Soekris 4521	22
2.2 配置多个 Minicom 概要	25
2.3 在 CF (Compact Flash) 卡上安装 Pyramid Linux	26
2.4 在 Debian 上进行 Pyramid 网络安装	27
2.5 在 Fedora 上进行 Pyramid 网络安装	30
2.6 启动 Pyramid Linux	33
2.7 寻找和编辑 Pyramid 文件	35
2.8 安全加固 Pyramid	36
2.9 获取并安装最新版 Pyramid	37
2.10 为 Pyramid Linux 添加额外的软件	38
2.11 添加新硬件驱动程序	41

2.12	定制 Pyramid 内核	42
2.13	更新 Soekris comBIOS	44
第 3 章 搭建 Linux 防火墙		46
3.0	介绍	46
3.1	组装一台 Linux 防火墙服务器	54
3.2	在 Debian 上配置网卡	55
3.3	在 Fedora 上配置网卡	58
3.4	识别相应网卡	60
3.5	基于动态 WAN IP 地址建立 Internet 连接共享防火墙	61
3.6	基于静态 WAN IP 地址建立 Internet 连接共享防火墙	66
3.7	显示防火墙状态	67
3.8	关闭 iptables 防火墙	68
3.9	在系统启动时开启 iptables, 并且手动启动和停止防火墙	70
3.10	测试防火墙	72
3.11	为远程 SSH 管理配置防火墙	75
3.12	允许远程 SSH 穿越 NAT 防火墙	77
3.13	用多个 SSH 主机密钥穿越 NAT	79
3.14	基于私有 IP 地址运行公共服务	80
3.15	架设单机防火墙	82
3.16	架设服务器防火墙	87
3.17	配置 iptables 日志记录	90
3.18	编写出站规则	91
第 4 章 建立 Linux 无线接入点		94
4.0	介绍	94
4.1	架设 Linux 无线接入点	98
4.2	桥接无线网络至有线链路	99
4.3	设立域名服务	102
4.4	从 DHCP 服务器获取并设定静态 IP 地址	105

4.5	配置 Linux 和 Windows 静态 DHCP 客户端	107
4.6	给 dnsmasq 添加邮件服务器	109
4.7	使 WPA2-Personal 和 WPA-Enterprise 一样安全	110
4.8	使用 RADIUS 服务器进行企业级验证	113
4.9	配置无线接入点以使用 FreeRADIUS	118
4.10	通过 FreeRADIUS 验证客户端	119
4.11	连接 Internet 并使用防火墙	120
4.12	使用路由代替桥接	121
4.13	探测无线网卡	127
4.14	改变 Pyramid 路由器的主机名	128
4.15	关闭天线分集	129
4.16	管理 dnsmasq 的 DNS 缓存	131
4.17	管理 Windows 的 DNS 缓存	134
4.18	在系统启动时更新时间	136

第 5 章 建立基于 Asterisk 的 VoIP 服务器 137

5.0	介绍	137
5.1	从源码安装 Asterisk	141
5.2	在 Debian 上安装 Asterisk	145
5.3	启动和停止 Asterisk	147
5.4	测试 Asterisk 服务器	150
5.5	在 Asterisk 中加入电话分机并呼叫	150
5.6	设置软电话	158
5.7	通过 Free World Dialup 获得真正的 VoIP 电话	160
5.8	将你的 Asterisk PBX 连接至模拟电话线路	163
5.9	创建数字接线员	166
5.10	记录定制提示	168
5.11	维护每日提示消息	171
5.12	转移呼叫	173
5.13	转接呼叫至多组电话	174
5.14	停泊呼叫	175

5.15	定制呼叫保持音乐	176
5.16	在 Asterisk 上播放 MP3 声音文件	177
5.17	传递语音邮件广播解决方案	178
5.18	使用 Asterisk 进行电话会议	179
5.19	监控会议	180
5.20	让 SIP 流量穿越 iptables NAT 防火墙	181
5.21	让 IAX 流量穿越 iptables NAT 防火墙	184
5.22	使用 AsteriskNOW, “30 分钟学会 Asterisk”	184
5.23	在 AsteriskNOW 上安装和移除软件包	186
5.24	连接漫游用户和远程用户	187

第 6 章 使用 Linux 路由 189

6.0	介绍	189
6.1	用 ipcalc 计算子网	192
6.2	设置默认网关	194
6.3	设立简单本地路由器	197
6.4	配置最简单的 Internet 连接共享	199
6.5	配置跨子网的静态路由	201
6.6	使静态路由持久化	203
6.7	在 Debian 上使用 RIP 动态路由	204
6.8	在 Fedora 上使用 RIP 动态路由	208
6.9	使用 Quagga 的命令行	209
6.10	远程登录 Quagga 守护进程	211
6.11	从命令行运行 Quagga 守护进程	212
6.12	监控 RIPD	214
6.13	使用 Zebra 进行黑洞路由	215
6.14	使用 OSPF 进行简单动态路由	216
6.15	为 RIP 和 OSPF 增加一些安全性	218
6.16	监控 OSPFD	220

第 7 章 使用 SSH 进行安全远程管理	221
7.0 介绍	221
7.1 启动和停止 OpenSSH	224
7.2 创建强口令	225
7.3 为最简单验证设定主机密钥	226
7.4 生成和拷贝 SSH 密钥	228
7.5 使用公钥验证以保护系统密码	230
7.6 管理多个身份密钥	232
7.7 安全加固 OpenSSH	232
7.8 变更口令	234
7.9 取回密钥指纹	234
7.10 检查配置语法	235
7.11 使用 OpenSSH 客户端配置文件简单登录	236
7.12 基于 SSH 安全地建立 X Windows 隧道	237
7.13 不使用远程 Shell 执行命令	239
7.14 用注释标记密钥	240
7.15 使用 DenyHosts 以抵御 SSH 攻击	240
7.16 创建 DenyHosts 启动文件	243
7.17 使用 sshfs 挂载整个远程文件系统	244
 第 8 章 使用跨平台远程图形桌面	 246
8.0 介绍	246
8.1 通过 rdesktop 从 Linux 访问 Windows	248
8.2 生成和管理 FreeNX SSH 密钥	251
8.3 使用 FreeNX 从 Windows 运行 Linux	252
8.4 使用 FreeNX 从 Solaris、Mac OS X 或 Linux 运行 Linux	256
8.5 管理 FreeNX 用户	257
8.6 从 FreeNX 服务器监视 Nxclient 用户	258
8.7 启动和停止 FreeNX 服务器	260
8.8 配置定制桌面	261

8.9	创建额外的 Nxclient 会话	263
8.10	在 Nxclient 中启用文件和打印机共享以及多媒体	265
8.11	在 Nxclient 中防止保存密码	266
8.12	FreeNX 故障诊断	267
8.13	使用 VNC 从 Linux 控制 Windows	268
8.14	使用 VNC 同时控制 Windows 和 Linux	270
8.15	使用 VNC 进行远程 Linux 对 Linux 的管理	271
8.16	给多个远程用户显示同样的 Windows 桌面	274
8.17	变更 Linux VNC 服务器密码	276
8.18	定制远程 VNC 桌面	277
8.19	设置远程 VNC 桌面大小	278
8.20	连接 VNC 至现有的 X 会话	279
8.21	通过 SSH 安全地建立 x11vnc 隧道	281
8.22	在 Linux 和 Windows 之间建立 TightVNC 隧道	282

第 9 章 使用 OpenVPN 建立安全的

跨平台虚拟专用网 286

9.0	介绍	286
9.1	安装一个安全的 OpenVPN 测试实验环境	288
9.2	启动并测试 OpenVPN	291
9.3	使用静态密钥测试加密	294
9.4	使用静态密钥连接远程 Linux 客户端	296
9.5	创建你自己的 OpenVPN PKI	298
9.6	配置用于多个客户端的 OpenVPN 服务器	301
9.7	配置 OpenVPN 在开机时启动	303
9.8	撤销证书	304
9.9	设置桥接模式的 OpenVPN 服务器	306
9.10	以非特权用户身份运行 OpenVPN	307
9.11	连接 Windows 客户端	308

第 10 章 建立 Linux PPTP VPN 服务器..... 310

10.0 介绍	310
10.1 在 Debian Linux 上安装 Poptop	313
10.2 给 Debian 内核打 MPPE 支持补丁	314
10.3 在 Fedora Linux 上安装 Poptop	316
10.4 给 Fedora 内核打 MPPE 支持补丁	317
10.5 设置独立的 PPTP VPN 服务器	319
10.6 将你的 Poptop 服务器加入活动目录	322
10.7 连接 Linux 客户端至 PPTP 服务器	323
10.8 让 PPTP 穿越 iptables 防火墙	325
10.9 监控你的 PPTP 服务器	326
10.10 PPTP 故障诊断	326

第 11 章 在混合 Linux/Windows 的局域网中

使用 Samba 进行单点登录 330

11.0 介绍	330
11.1 确认一切就绪	332
11.2 从源码编译 Samba	335
11.3 启动和停止 Samba	338
11.4 将 Samba 用作主域控制器	339
11.5 从 NT4 PDC 迁移至 Samba 主域控制器	343
11.6 将 Linux 加入活动目录域	345
11.7 将 Windows 95/98/ME 连接至 Samba 域	349
11.8 将 Windows NT4 连接至 Samba 域	350
11.9 将 Windows NT/2000 连接至 Samba 域	351
11.10 将 Windows XP 连接至 Samba 域	352
11.11 使用命令程序将 Linux 客户端连接至 Samba 域	352
11.12 使用图形化程序将 Linux 客户端连接至 Samba 域	356

第 12 章 使用 OpenLDAP 提供集中式	
网络目录服务	359
12.0 介绍	359
12.1 在 Debian 上安装 OpenLDAP	366
12.2 在 Fedora 上安装 OpenLDAP	368
12.3 配置并测试 OpenLDAP 服务器	369
12.4 在 Fedora 上创建一个新数据库	372
12.5 在你的目录中添加更多用户	375
12.6 修正目录条目	377
12.7 连接至远程 OpenLDAP 服务器	379
12.8 在你的 OpenLDAP 目录中搜索	380
12.9 为你的数据库建立索引	382
12.10 使用图形界面管理你的目录	384
12.11 配置 Berkeley DB	387
12.12 配置 OpenLDAP 日志记录	392
12.13 备份和恢复你的目录	393
12.14 细化访问控制	395
12.15 变更密码	399
第 13 章 使用 Nagios 监控网络	401
13.0 介绍	401
13.1 从源码安装 Nagios	402
13.2 为 Nagios 配置 Apache	406
13.3 有条不紊地组织 Nagios 的配置文件	409
13.4 配置 Nagios 以监控 Localhost	411
13.5 为完全 Nagios Web 访问配置 CGI 权限	420
13.6 在开机时启动 Nagios	421
13.7 加入更多 Nagios	422
13.8 使用 check_icmp 加速 Nagios	424
13.9 监控 SSHD	425

13.10 监控 Web 服务器	428
13.11 监控 Mail 服务器	431
13.12 使用 Servicegroups 将相关服务分组	434
13.13 监控域名服务	435
13.14 使用 OpenSSH 进行安全的远程 Nagios 管理	437
13.15 使用 OpenSSL 进行安全的远程 Nagios 管理	438

第 14 章 使用 MRTG 监控网络 440

14.0 介绍	440
14.1 安装 MRTG	441
14.2 在 Debian 上配置 SNMP	442
14.3 在 Fedora 上配置 SNMP	445
14.4 为 MRTG 配置你的 HTTP 服务	446
14.5 在 Debian 上配置并启动 MRTG	447
14.6 在 Fedora 上配置并启动 MRTG	450
14.7 监控活跃 CPU 负载	452
14.8 监控 CPU 用户和闲置时间	455
14.9 监控物理内存	457
14.10 监控交换空间和内存	458
14.11 监控磁盘利用率	460
14.12 监控 TCP 连接	461
14.13 寻找并测试 MIB 与 OID	462
14.14 测试远程 SNMP 查询	464
14.15 监控远程主机	466
14.16 创建多个 MRTG 索引页面	467
14.17 将 MRTG 作为守护进程运行	468

第 15 章 认识 IPv6..... 471

15.0 介绍	471
15.1 测试 Linux 系统的 IPv6 支持	476

15.2	ping 链路本地 IPv6 主机	477
15.3	在网卡上设置唯一本地单播地址	479
15.4	使用基于 IPv6 的 SSH	480
15.5	基于 IPv6 使用 scp 拷贝文件	481
15.6	使用 IPv6 进行自动配置	482
15.7	计算 IPv6 地址	483
15.8	使用 Internet 上的 IPv6	485
 第 16 章 建立新系统自动网络安装服务		486
16.0	介绍	486
16.1	为 Fedora Linux 创建网络安装启动介质	487
16.2	使用网络启动介质进行 Fedora 网络安装	489
16.3	建立基于 HTTP 的 Fedora 安装服务器	491
16.4	建立基于 FTP 的 Fedora 安装服务器	492
16.5	创建 Fedora Linux 定制安装	495
16.6	使用 kickstart 文件进行 Fedora Linux 自动安装	497
16.7	通过 PXE 网络启动进行 Fedora 网络安装	499
16.8	网络安装 Debian 系统	501
16.9	使用 apt-mirror 建立 Debian 完全镜像	502
16.10	通过 apt-proxy 建立 Debian 部分镜像	505
16.11	配置客户端 PC 以使用本地 Debian 镜像	506
16.12	建立 Debian PXE 网络启动服务器	507
16.13	从你的本地 Debian 镜像安装新系统	509
16.14	使用预置文件自动化 Debian 的安装	510
 第 17 章 通过串行控制台管理 Linux 服务器		513
17.0	介绍	513
17.1	准备用于串行控制台管理的服务器	514
17.2	使用 LILO 配置无外设服务器	518
17.3	使用 GRUB 配置无外设服务器	520

17.4 在 Debian 上启动至文本模式	523
17.5 设置串行控制台	525
17.6 配置用于拨入管理的服务器	527
17.7 拨入服务器	531
17.8 增强安全性	532
17.9 配置日志记录	534
17.10 上传文件至服务器	535
第 18 章 运行 Linux 拨号服务器	537
18.0 介绍	537
18.1 使用 WvDial 配置单一拨号账户	537
18.2 在 WvDial 中配置多个账户	540
18.3 为非 root 用户配置拨号权限	541
18.4 为非 root 用户创建 WvDial 账户	543
18.5 共享拨号 Internet 账户	544
18.6 设置按需拨号	545
18.7 使用 cron 调度拨号可用性	547
18.8 基于语音邮件断续音拨号	548
18.9 撤销呼叫等待	549
18.10 将密码移出配置文件	550
18.11 创建单独的 pppd 日志文件	551
第 19 章 网络故障诊断	552
19.0 介绍	552
19.1 准备一台用于网络诊断和修复的笔记本电脑	553
19.2 使用 ping 测试连通性	557
19.3 使用 Fping 和 Nmap 探测你的网络	559
19.4 使用 arping 寻找重复的 IP 地址	561
19.5 使用 httping 测试 HTTP 吞吐量和延时	562
19.6 使用 traceroute、tcptraceroute 和 mtr 定位网络问题	565