FROM ASTERISK TO ZEBRA WITH EASY-TO-USE RECIPES

LINUX Networking Cookbook™

O'REILLY®

CARLA SCHRODER

FROM ASTERISK TO ZEBRA WITH EASY-TO-USE RECIPES

LINUX NETWORKING COOKBOOK

This wide-ranging recipe collection covers everything you need to know to excel as a Linux network administrator, whether you're new to the job or have years of experience. With complete steps to carry out an array of tasks, *Linux Networking Cookbook* helps you dive straight into the gnarly hands-on work of building and maintaining a computer network. Each recipe includes a clear solution with tested code, plus a discussion on why and how it works.

Running a network doesn't mean you have all the answers. *Linux Networking Cookbook* has solutions that focus on connectivity: firewalls, wireless access points, secure remote administration, remote helpdesk, remote access for users, Virtual Private Networks (VPNs), authentication, system and network monitoring, and the rapidly growing world of Voice over IP (VoIP) services. You'll find recipes for:

- Building a gateway, firewall, and wireless access point on a Linux network
- Building a VoIP server with Asterisk
- Securing remote administration with SSH
- Building secure VPNs with OpenVPN, and a Linux PPTP VPN server
- Single sign-on with Samba for mixed Linux/Windows LANs
- Centralizing the network directory with OpenLDAP
- Network monitoring with Nagios or MRTG
- Getting acquainted with IPv6
- Setting up hands-free network installations of new systems
- Linux system administration via serial console

Linux Networking Cookbook also covers tasks such as networking Linux and Unix boxes, integrating Windows hosts, routing, user identification and authentication, sharing an Internet connection, connecting branch offices, name services, wired and wireless connectivity, security, monitoring, and troubleshooting. When you need to solve a network problem without delay, and you don't have the time or patience to comb through reference books or the Web for answers, this book has what you need.

O'REILLY®

www.oreilly.com

US $44.99 CAN $44.99

ISBN-10: 0-596-10248-8

ISBN-13: 978-0-596-10248-7

9 780596 102487 54499

Linux Networking Cookbook™

Carla Schroder

O'REILLY®
Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

Linux Networking Cookbook™
by Carla Schroder

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

Editor: Mike Loukides
Production Editor: Sumita Mukherji
Copyeditor: Derek Di Matteo
Proofreader: Sumita Mukherji
Indexer: John Bickelhaupt
Cover Designer: Karen Montgomery
Interior Designer: David Futato
Illustrator: Jessamyn Read

Printing History:

November 2007: First Edition.

This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN-10: 0-596-10248-8
ISBN-13: 978-0-596-10248-7
[M]

To Terry Hanson—thank you!
You make it all worthwhile.

Table of Contents

Preface

So there you are, staring at your computer and wondering why your Internet connection is running slower than slow, and wishing you knew enough to penetrate the endless runaround you get from your service provider. Or, you're the Lone IT Staffer in a small business who got the job because you know the difference between a switch and hub, and now you're supposed to have all the answers. Or, you're really interested in networking, and want to learn more and make it your profession. Or, you are already knowledgeable, and you simply have a few gaps you need to fill. But you're finding out that computer networking is a subject with reams and reams of reference material that is not always organized in a coherent, useful order, and it takes an awful lot of reading just to figure out which button to push.

To make things even more interesting, you need to integrate Linux and Windows hosts. If you want to pick up a book that lays out the steps for specific tasks, that explains clearly the necessary commands and configurations, and does not tax your patience with endless ramblings and meanderings into theory and obscure RFCs, this is the book for you.

Audience

Ideally, you will have some Linux experience. You should know how to install and remove programs, navigate the filesystem, manage file permissions, and user and group creation. You should have some exposure to TCP/IP and Ethernet basics, IPv4 and IPv6, LAN, WAN, subnet, router, firewall, gateway, switch, hub, and cabling. If you are starting from scratch, there are any number of introductory books to get you up to speed on the basics.

If you don't already have basic Linux experience, I recommend getting the *Linux Cookbook* (O'Reilly). The *Linux Cookbook* (which I authored) was designed as a companion book to this one. It covers installing and removing software, user account management, cross-platform file and printer sharing, cross-platform user authentication, running servers (e.g., mail, web, DNS), backup and recovery, system rescue and repair, hardware discovery, configuring X Windows, remote administration, and lots more good stuff.

The home/SOHO user also will find some useful chapters in this book, and anyone who wants to learn Linux networking will be able to do everything in this book with a couple of ordinary PCs and inexpensive networking hardware.

Contents of This Book

This book is broken into 19 chapters and 3 appendixes:

Chapter 1, *Introduction to Linux Networking*
: This is your high-level view of computer networking, covering cabling, routing and switching, interfaces, the different types of Internet services, and the fundamentals of network architecture and performance.

Chapter 2, *Building a Linux Gateway on a Single-Board Computer*
: In which we are introduced to the fascinating and adaptable world of Linux on routerboards, such as those made by Soekris and PC Engines, and how Linux on one of these little boards gives you more power and flexibility than commercial gear costing many times as much.

Chapter 3, *Building a Linux Firewall*
: Learn to use Linux's powerful *iptables* packet filter to protect your network, with complete recipes for border firewalls, single-host firewalls, getting services through NAT (Network Address Translation), blocking external access to internal services, secure remote access through your firewall, and how to safely test new firewalls before deploying them on production systems.

Chapter 4, *Building a Linux Wireless Access Point*
: You can use Linux and a routerboard (or any ordinary PC hardware) to build a secure, powerful, fully featured wireless access point customized to meet your needs, including state-of-the-art authentication and encryption, name services, and routing and bridging.

Chapter 5, *Building a VoIP Server with Asterisk*
: This chapter digs into the very guts of the revolutionary and popular Asterisk VoIP server. Sure, these days, everyone has pretty point-and-click GUIs for managing their iPBX systems, but you still need to understand what's under the hood. This chapter shows you how to install Asterisk and configure Asterisk

from scratch: how to create user's extensions and voicemail, manage custom greetings and messages, do broadcast voicemails, provision phones, set up a digital receptionist, do PSTN (Public Switched Telephone Network) integration, do pure VoIP, manage road warriors, and more.

Chapter 6, *Routing with Linux*
: Linux's networking stack is a powerhouse, and it includes advanced routing capabilities. Here be recipes for building Linux-based routers, calculating subnets (accurately and without pain), blackholing unwelcome visitors, using static and dynamic routing, and for monitoring your hard-working little routers.

Chapter 7, *Secure Remote Administration with SSH*
: OpenSSH is an amazing and endlessly useful implementation of the very secure SSH protocol. It supports traditional password-based logins, password-less public-key-based logins, and securely carries traffic over untrusted networks. You'll learn how to do all of this, plus how to safely log in to your systems remotely, and how to harden and protect OpenSSH itself.

Chapter 8, *Using Cross-Platform Remote Graphical Desktops*
: OpenSSH is slick and quick, and offers both text console and a secure X Windows tunnel for running graphical applications. There are several excellent programs (FreeNX, rdesktop, and VNC) that offer a complementary set of capabilities, such as remote helpdesk, your choice of remote desktops, and Linux as a Windows terminal server client. You can control multiple computers from a single keyboard and monitor, and even conduct a class where multiple users view or participate in the same remote session.

Chapter 9, *Building Secure Cross-Platform Virtual Private Networks with OpenVPN*
: Everyone seems to want a secure, user-friendly VPN (Virtual Private Network). But there is a lot of confusion over what a VPN really is, and a lot of commercial products that are not true VPNs at all, but merely SSL portals to a limited number of services. OpenVPN is a true SSL-based VPN that requires all endpoints to be trusted, and that uses advanced methods for securing the connection and keeping it securely encrypted. OpenVPN includes clients for Linux, Solaris, Mac OS X, OpenBSD, FreeBSD, and NetBSD, so it's your one-stop VPN shop. You'll learn how to create and manage your own PKI (Public Key Infrastructure), which is crucial for painless OpenVPN administration. And, you'll learn how to safely test OpenVPN, how to set up the server, and how to connect clients.

Chapter 10, *Building a Linux PPTP VPN Server*
: This chapter covers building and configuring a Linux PPTP VPN server for Windows and Linux clients; how to patch Windows clients so they have the necessary encryption support, how to integrate with Active Directory, and how to get PPTP through an *iptables* firewall.

Chapter 11, *Single Sign-on with Samba for Mixed Linux/Windows LANs*
: Using Samba as a Windows NT4-style domain controller gives you a flexible, reliable, inexpensive mechanism for authenticating your network clients. You'll learn how to migrate from a Windows domain controller to Samba on Linux, how to migrate Windows user accounts to Samba, integrate Linux clients with Active Directory, and how to connect clients.

Chapter 12, *Centralized Network Directory with OpenLDAP*
: An LDAP directory is an excellent mechanism on which to base your network directory services. This chapter shows how to build an OpenLDAP directory from scratch, how to test it, how to make changes, how to find things, how to speed up lookups with smart indexing, and how to tune it for maximum performance.

Chapter 13, *Network Monitoring with Nagios*
: Nagios is a great network monitoring system that makes clever use of standard Linux commands to monitor services and hosts, and to alert you when there are problems. Status reports are displayed in nice colorful graphs on HTML pages that can be viewed on any Web browser. Learn to monitor basic system health, and common servers like DNS, Web, and mail servers, and how to perform secure remote Nagios administration.

Chapter 14, *Network Monitoring with MRTG*
: MRTG is an SNMP-aware network monitor, so theoretically it can be adapted to monitor any SNMP-enabled device or service. Learn how to monitor hardware and services, and how to find the necessary SNMP information to create custom monitors.

Chapter 15, *Getting Acquainted with IPv6*
: Ready or not, IPv6 is coming, and it will eventually supplant IPv4. Get ahead of the curve by running IPv6 on your own network and over the Internet; learn why those very long IPv6 addresses are actually simpler to manage than IPv4 addresses; learn how to use SSH over IPv6, and how to auto-configure clients without DHCP.

Chapter 16, *Setting Up Hands-Free Network Installations of New Systems*
: Fedora Linux and all of its relatives (Red Hat, CentOS, Mandriva, PC Linux OS, and so forth), and Debian Linux and all of its descendants (Ubuntu, Mepis, Knoppix, etc.) include utilities for creating and cloning customized installations, and for provisioning new systems over the network. So, you can plug-in a PC, and within a few minutes have a complete new installation all ready to go. This chapter describes how to use ordinary installation ISO images for network installations of Fedora, and how to create and maintain complete local Debian mirrors efficiently.

Chapter 17, *Linux Server Administration via Serial Console*
: When Ethernet goes haywire, the serial console will save the day, both locally and remotely; plus, routers and managed switches are often administered via the serial console. Learn how to set up any Linux computer to accept serial connections, and how to use any Linux, Mac OS X, or Windows PC as a serial terminal. You'll also learn how to do dial-up server administration, and how to upload files over your serial link.

Chapter 18, *Running a Linux Dial-Up Server*
: Even in these modern times, dial-up networking is still important; we're a long way from universal broadband. Set up Internet-connection sharing over dial-up, dial-on-demand, use *cron* to schedule dialup sessions, and set up multiple dial-up accounts.

Chapter 19, *Troubleshooting Networks*
: Linux contains a wealth of power tools for diagnosing and fixing network problems. You'll learn the deep dark secrets of *ping*, how to use *tcpdump* and Wireshark to eavesdrop on your own wires, how to troubleshoot the name and mail server, how to discover all the hosts on your network, how to track problems down to their sources, and how to set up a secure central logging server. You'll learn a number of lesser-known but powerful utilities such as *fping*, *httping*, *arping*, and *mtr*, and how to transform an ordinary old laptop into your indispensible portable network diagnostic-and-fixit tool.

Appendix A, *Essential References*
: Computer networking is a large and complex subject, so here is a list of books and other references that tell you what you need to know.

Appendix B, *Glossary of Networking Terms*
: Don't know what it means? Look it up here.

Appendix C, *Linux Kernel Building Reference*
: As the Linux kernel continues to expand in size and functionality, it often makes sense to build your own kernel with all the unnecessary bits stripped out. Learn the Fedora way, the Debian way, and the vanilla way of building a custom kernel.

What Is Included

This book covers both old standbys and newfangled technologies. The old-time stuff includes system administration via serial console, dial-up networking, building an Internet gateway, VLANs, various methods of secure remote access, routing, and traffic control. Newfangled technologies include building your own iPBX with Asterisk, wireless connectivity, cross-platform remote graphical desktops, hands-free network installation of new systems, single sign-on for mixed Linux and Windows LANs, and IPv6 basics. And, there are chapters on monitoring, alerting, and troubleshooting.

Which Linux Distributions Are Used in the Book

There are literally hundreds, if not thousands of Linux distributions: live distributions on all kinds of bootable media, from business-card CDs to USB keys to CDs to DVDs; large general-purpose distributions; tiny specialized distributions for firewalls, routers, and old PCs; multimedia distributions; scientific distributions; cluster distributions; distributions that run Windows applications; and super-secure distributions. There is no way to even begin to cover all of these; fortunately for frazzled authors, the Linux world can be roughly divided into two camps: Red Hat Linux and Debian Linux. Both are fundamental, influential distributions that have spawned the majority of derivatives and clones.

In this book, the Red Hat world is represented by Fedora Linux, the free community-driven distribution sponsored by Red Hat. Fedora is free of cost, the core distribution contains only Free Software, and it has a more rapid release cycle than Red Hat Enterprise Linux (RHEL). RHEL is on an 18-month release cycle, is designed to be stable and predictable, and has no packaged free-of-cost version, though plenty of free clones abound. The clones are built from the RHEL SRPMs, with the Red Hat trademarks removed. Some RHEL-based distributions include CentOS, White Box Linux, Lineox, White Box Enterprise Linux, Tao Linux, and Pie Box Linux.

Additionally, there are a number of Red Hat derivatives to choose from, like Mandriva and PCLinuxOS. The recipes for Fedora should work for all of these, though you might find some small differences in filenames, file locations, and package names.

Debian-based distributions are multiplying even as we speak: Ubuntu, Kubuntu, Edubuntu, Xandros, Mepis, Knoppix, Kanotix, and Linspire, to name but a few. While all of these have their own enhancements and modifications, package management with *aptitude* or Synaptic works the same on all of them.

Novell/SUSE is RPM-based like Red Hat, but has always gone its own way. Gentoo and Slackware occupy their own unique niches. I'm not even going to try to include all of these, so users of these distributions are on their own. Fortunately, each of these is very well-documented and have active, helpful user communities, and they're not that different from their many cousins.

Downloads and Feedback

Doubtless this book, despite the heroic efforts of me and the fabulous O'Reilly team, contains flaws, errors, and omissions. Please email your feedback and suggestions to *netcookbook@bratgrrl.com*, so we can make the second edition even better. Be sure to visit *http://www.oreilly.com/catalog/9780596102487* for errata, updates, and to download the scripts used in the book.

Conventions

Italic
: Used for pathnames, filenames, program names, Internet addresses, such as domain names and URLs, and new terms where they are defined.

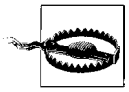
`Constant Width`
: Used for output from programs, and names and keywords in examples.

`Constant Width Italic`
: Used for replaceable parameters or optional elements when showing a command's syntax.

`Constant Width Bold`
: Used for commands that should be typed verbatim, and for emphasis within program code and configuration files.

Unix/Linux commands that can be typed by a regular user are preceded with a regular prompt, ending with `$`. Commands that must be typed as *root* are preceded with a "root" prompt, ending with a `#`. In real life, it is better to use the *sudo* command wherever possible to avoid logging in as *root*. Both kinds of prompts indicate the username, the current host, and the current working directory (for example: `root@xena:/var/llibtftpboot #`).

This icon signifies a tip, suggestion, or general note.



This icon indicates a warning or caution.

Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You do not need to contact us for permission unless you're reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O'Reilly books *does* require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product's documentation *does* require permission.

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, and ISBN. For example: "*Linux Networking Cookbook*, by Carla Schroder. Copyright 2008 O'Reilly Media, Inc., 978-0-596-10248-7."

If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at *permissions@oreilly.com*.

Comments and Questions

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (in the United States or Canada)
707-829-0515 (international or local)
707-829-0104 (fax)

We have a web page for this book, where we list errata, examples, and any additional information. You can access this page at:

http://www.oreilly.com/catalog/9780596102487

To comment or ask technical questions about this book, send email to:

bookquestions@oreilly.com

For more information about our books, conferences, Resource Centers, and the O'Reilly Network, see the web site:

http://www.oreilly.com

Safari® Books Online

When you see a Safari® Books Online icon on the cover of your favorite technology book, that means the book is available online through the O'Reilly Network Safari Bookshelf.

Safari offers a solution that's better than e-books. It's a virtual library that lets you easily search thousands of top tech books, cut and paste code samples, download chapters, and find quick answers when you need the most accurate, current information. Try it for free at *http://safari.oreilly.com*.