Cisco Routers for the Small Business

A Practical Guide for IT Professionals

Jason C. Neumann

Apress®

Cisco Routers for the Small Business: A Practical Guide for IT Professionals

Copyright © 2009 by Jason C. Neumann

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13 (pbk): 978-1-4302-1851-7

ISBN-13 (electronic): 978-1-4302-1852-4

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jonathan Gennick
Technical Reviewers: Dean Olsen, Sebastien Michelet
Editorial Board: Clay Andres, Steve Anglin, Mark Beckner, Ewan Buckingham, Tony Campbell, Gary Cornell, Jonathan Gennick, Michelle Lowman, Matthew Moodie, Jeffrey Pepper, Frank Pohlmann, Ben Renow-Clarke, Dominic Shakeshaft, Matt Wade, Tom Welsh
Project Manager: Sofia Marchant
Copy Editor: Octal Publishing, Inc.
Associate Production Director: Kari Brooks-Copony
Production Editor: Kari Brooks-Copony
Compositor: Pat Christenson
Proofreader: Katie Stence
Indexer: Broccoli Information Management
Artist: April Milne
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress directly at 2855 Telegraph Avenue, Suite 600, Berkeley, CA 94705. Phone 510-549-5930, fax 510-549-5939, e-mail `info@apress.com`, or visit `http://www.apress.com`.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at `http://www.apress.com/info/bulksales`.

The information in this book is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

Contents at a Glance

About the Author xvii

About the Technical Reviewers xix

Acknowledgments. xxi

Introduction xxiii

CHAPTER 1 Getting to Know Your Router. 1

CHAPTER 2 Configuring Your Router 17

CHAPTER 3 Configuring DSL Using PPPoE. 57

CHAPTER 4 Configuring a VPN Using IPSec. 81

CHAPTER 5 Beyond the Basics 105

CHAPTER 6 Understanding Binary and Subnetting 143

CHAPTER 7 Routing—What Routers Do Best 157

CHAPTER 8 Understanding Variable Length Subnet Mask Networking. 173

APPENDIX A Sample Configuration for a Cable Modem. 183

APPENDIX B Sample Configuration for DSL and PPPoE. 189

APPENDIX C Sample Configuration IPSec VPN Over DSL 197

APPENDIX D CCNA CLI Command Reference 207

APPENDIX E ACL and Firewall Names Used in This Book. 231

INDEX 233

Contents

About the Author xvii
About the Technical Reviewers. xix
Acknowledgments. xxi
Introduction xxiii

CHAPTER 1 **Getting to Know Your Router**. 1

Understanding Your Ports 1
The Console Port. 1
LAN Ethernet Ports (E0 or VLAN1) 2
WAN Ethernet Port (E1 or FA4) 2
Connecting to Your Router 2
Attach the Console Cable. 3
Configure Hyper Terminal 3
Power Up the Router. 5
Welcome to the Command Line. 6
Your First CLI Commands 7
Turn On Privileged EXEC Mode. 9
Set the Date and Time 9
Get Help 10
Using Global Configuration Mode. 10
Set Your Router's Hostname 11
Set the Privileged EXEC Mode Password 11
Display and Save Your Configuration. 12
Summary 13
Ports 14
User EXEC Mode Commands 15
Privileged EXEC Mode Commands. 15
Global Configuration Mode Commands. 16
Display and Save Your Configuration. 16

CHAPTER 2 Configuring Your Router 17

Erasing the Startup Configuration 17
Learning Some CLI Tips and Tricks. 19
Use Keyboard Shortcuts. 19
Suppress Console Messages 19
Undo the Effects of a Command. 20
Configuring Your LAN Interface 20
Step 1: Assign a Hostname to Your Router. 21
Step 2: Start Interface Configuration Mode 21
Step 3: Add a Description to Your Interface 21
Step 4: Assign an IP Address to Your Interface 21
Step 5: Bring Up the Interface. 21
Step 6: Exit from Interface Configuration Mode. 22
Step 7: Check Your Work. 22
Configuring a DHCP Server. 23
Step 1: Define the DHCP Pool Name 23
Step 2: Define the Network Address for DHCP. 23
Step 3: Define Your Domain Name. 24
Step 4: Define the Default Gateway. 24
Step 5: Define Your DNS Servers 24
Step 6: Define a WINS Server (Optional) 24
Step 7: Define a DHCP Lease Time 24
Step 8: Define a DHCP-Excluded Address Range 25
Step 9: Test DHCP Using a Workstation 25
Step 10: Check Your DHCP Status with the IOS. 26
Configuring Telnet on Your Router. 26
Step 1: Set Your Privileged EXEC Mode Password 27
Step 2: Set Your VTY Login Password 27
Securing VTY. 28
Step 1: Create and Name Your ACL. 29
Step 2: Apply Your ACL to VTY 29
Configuring Your WAN Interface—Dynamic IP 30
Step 1: Start Interface Configuration Mode 30
Step 2: Add a Description to Your Interface 30
Step 3: Configure Your WAN Interface to Use DHCP. 31
Step 4: Set the Duplex and Speed on Your Interface 31
Step 5: Bring Up the Interface. 31
Step 6: Enable Domain Lookup. 31

Configuring Your WAN Interface—Static IP 32
Step 1: Start Interface Configuration Mode 33
Step 2: Add a Description to Your Interface 33
Step 3: Assign an IP Address to Your Interface 33
Step 4: Set the Duplex and Speed on Your Interface 33
Step 5: Bring Up the Interface. 33
Step 6: Assign the Default Gateway. 33
Step 7: Enable Domain Lookup. 34
Configuring NAT on Your Router 34
Step 1: Create and Name an Extended ACL for NAT. 35
Step 2: Create an ACL Rule 35
Step 3: Configure Inside Address Translation 35
Step 4: Apply NAT to Your Interfaces. 36
Securing Your Interfaces 36
Step 1: Disable IP Unreachable Messages 36
Step 2: Disable IP Redirects 37
Step 3: Disable Proxy ARP 37
Creating a Basic Firewall. 37
Creating an Advanced Firewall. 38
Step 1: Create Application Rules 38
Step 2: Apply the Rules Outbound 38
Creating an ACL for Your WAN Interface. 39
Step 1: Allow Ping and Traceroute. 40
Step 2: Apply the ACL Inbound 40
Configuring a Basic DMZ. 40
Step 1: Remove the Existing IPFW-ACL. 41
Step 2: Create a New IPFW-ACL. 41
Step 3: Configure NAT to Forward Traffic to a LAN Host 41
Step 4: Apply the Inside Source Rule. 42
Saving Your Configuration. 43
Restoring the Default Configuration 44
Verifying Your Setup. 44
Check Your Interfaces 44
Check NAT 46
Check Your ACLs. 47
Check Your Firewall 48

Summary 48
Erase the Startup Configuration 49
Configure an IP Address on Your LAN Interface 49
Configure a DHCP Server 49
Configure Telnet on Your Router 50
Secure VTY with an ACL 50
Configure Your WAN Interface—Dynamic IP 51
Configure Your WAN Interface—Static IP 51
Secure Your Interfaces 52
Configure NAT on Your Router 52
Create an Advanced Firewall 53
Set Up a Basic DMZ 54
Save Your Configuration 54
Restore the Default Configuration 54
Verify Your Setup 55

CHAPTER 3 **Configuring DSL Using PPPoE** 57

Introducing PPPoE 57
Overview of the Steps 58
Collecting Information from Your ISP 59
Enabling Virtual Private Dialup Networking 59
Preparing the Physical WAN Interface 60
Configuring the Virtual WAN Interface 61
Configuring NAT on the Virtual WAN Interface 64
Setting the Default Gateway 65
Adjusting the MSS on the LAN Interface 65
General Troubleshooting 66
Check That the DSL Circuit Has Been Activated 66
Check Your Username and Password and MTU 66
Verify That the Circuit Is Functional 67
Print a Copy of Your Router's Configuration 67
Use the IOS to Troubleshoot PPPoE 67
Using the Cisco Debugger 68
Enable Buffered Logging 68
Check for PPPoE Response 69
Debug the PPP 71
Stop Debugging and Logging 74
A Word About ISPs 75

Summary 76
What You Need from Your ISP. 76
Enable VPDN and Create a Dial Group (If Necessary) 76
Prepare the Physical WAN Interface 77
Configure the Virtual WAN Interface 77
Configure NAT on the Virtual WAN Interface (Dialer 1) 77
Assign the Default Gateway to Use the Virtual WAN Interface 78
Adjust the MSS on the LAN Interface. 78
Troubleshooting. 78

CHAPTER 4 Configuring a VPN Using IPSec 81

Preparing Your Sites. 81
Setting Up the VPN 82
Step 1: Create a VPN-Friendly ACL for NAT 83
Step 2: Define a VPN Routing Policy for Your WAN Interface 83
Step 3: Apply Your VPN Routing Policy to NAT. 84
Step 4: Define a VPN Routing Policy for Your LAN Interface 84
Configuring IKE Phase 1 85
Step 1: Create a Key Exchange Policy. 85
Step 2: Define the Encryption Type 86
Step 3: Define a Cryptographic Hash Function 86
Step 4: Define Your IKE Key Type. 86
Step 5: Define Your IKE Key Size 86
Step 6: Create a Preshared Key 87
Configuring IPSec Phase 2 88
Step 1: Create a VPN-ACL 89
Step 2: Create a Transform Set 89
Step 3: Create a Crypto Map 89
Step 4: Set the VPN Peer 90
Step 5: Set the Transform Set. 90
Step 6: Set the PFS Group 90
Step 7: Apply Your VPN ACL 90
Step 8: Apply the Crypto Map 90
Modifying Your IPFW-ACL 90
Verifying Your VPN Connection. 92
Troubleshooting 94
General Network Settings 94
IKE Phase 1 Settings. 94
IPSec Phase 2 Settings 95
When in Doubt, Print It Out 95

Summary 95
Set Up the VPN. 95
Branch Office VPN Configuration 98
Corporate Office VPN Configuration 100
Troubleshoot Your VPN. 102

CHAPTER 5 Beyond the Basics 105

Creating a Local User on the Router 105
Step 1: Create a User and Password 106
Step 2: Set the Login to Local 107
Configuring Secure Shell (SSH) 107
Step 1: Generate the RSA Keys. 107
Step 2: Set the VTY Transport Input Type 108
Step 3: Use SSH to Log in to the Router 108
Recovering a Lost Password. 109
Overview of the Process 109
Step 1: Bypass the IOS. 110
Step 2: Modify the Configuration Register 110
Step 3: Copy the Configuration and Reset Passwords 111
Step 4: Reset the Configuration Register 112
Upgrading the IOS. 113
Step 1: Display the Contents of Flash Memory 113
Step 2: Back Up the Existing IOS Image File 115
Step 3: Delete the Old IOS Image. 117
Step 4: Install the New IOS Image 118
Step 5: Boot the New Image 120
Backing Up Your Configuration. 121
Method 1: Back Up to Flash Memory. 121
Method 2: Back Up to a TFTP Server. 122
Method 3: Back Up to an FTP Server. 123
Tuning Your ACLs for Performance 124
Step 1: Display ACL Rule Matches. 124
Step 2: Reorder the ACL Rules 125
Step 3: Apply the Established Rule 126
Protecting Your Passwords. 126
Disabling Show and Tell 127

Safeguarding Your E-mail Server. 127
Step 1: Name the EIE Firewall. 128
Step 2: Define the Protocols 128
Step 3: Apply the Firewall 129
Configuring a Logging Host for Intrusion Detection 129
Step 1: Perform Basic KIWI Set Up. 130
Step 2: Configure E-mail Alarms 130
Step 3: Set the Message Threshold 131
Configuring Logging on Your Router 133
Step 1: View Your Trap Levels 133
Step 2: Change the Log Level. 134
Step 3: Timestamp Your Logs. 134
Step 4: Define Your Logging Host 135
Defining a Login Banner 135
Summary 136
Create a Local User on the Router 136
Configure Secure Shell (SSH) 136
Recover a Lost Password. 137
Back Up the IOS. 137
Upgrade the IOS 138
Back Up Your Configuration. 138
Tune Your ACLs for Performance 139
Protect Your Passwords 139
Disable Show and Tell 140
Safeguard Your E-mail Server. 140
Set Up an Intrusion Detection System 140
Define a Login Banner 141

CHAPTER 6 Understanding Binary and Subnetting 143

Decimal—Base 10. 144
Binary—Base 2. 145
Subnet Masks 146
Dividing Your Network 147
Method 1: Keeping the Same Subnet Mask. 147
Method 2: Subnetting a Network. 147
Determining How the Bits Are Used. 148
Determining the Number of Subnets Available 148
Determining the Network Numbers and Number of Hosts. 149
More Examples 151

Summary 154
Decimal—Base 10 155
Binary—Base 2 155
Subnet Mask 155
Dividing Your Network 155
Determining the Number of Subnets 155
Determining the Network Number and Number of Hosts. 156
Quiz Answers. 156
Binary Quiz Answers. 156
Subnetting Quiz Answers. 156

CHAPTER 7 **Routing—What Routers Do Best** 157

Routing Defined 157
Routing vs. Routed Protocols 158
Routing Information Protocol (RIP) 158
RIP Basics. 158
Configuring RIP on a Router 158
Step 1: Enable RIP. 160
Step 2: Advertise Your Networks 160
Configuring RIP on a Neighbor Router. 160
Step 1: Enable RIP. 161
Step 2: Advertise Your Networks 161
Step 3: Configure a Passive Interface 161
Verifying RIP Routing 161
Use Show IP Protocols 161
Use Show IP Route 162
Setting Up a True DMZ. 163
The Bastion Host 164
Configuring Your Gateway Router 165
Configuring Your Interior Router. 166
A Note on VPNs and DMZs 167
Summary 168
Configure RIP. 169
Configure RIP on a Neighbor Router 169
Verify RIP Routing 170
Set Up a True DMZ 171
VPN Configuration. 171

CHAPTER 8 **Understanding Variable Length Subnet Mask Networking** 173

Getting Started 173
Planning a VLSM Network 175
Route Summarization (Supernetting) 178
Summary 180
Planning a VLSM Network 180
Route Summarization 181

APPENDIX A **Sample Configuration for a Cable Modem** 183

Standard Setup 184
LAN Interface 184
WAN Interface 184
Router Passwords 185
NAT Setup 185
CBAC Firewall 186
DHCP Server 186
IPFW Access List 187
VTY Access List 187
Configure SSH (Version 2) 188
Encrypt All Router Passwords 188
Save the Configuration 188

APPENDIX B **Sample Configuration for DSL and PPPoE** 189

Standard Setup 190
LAN Interface 190
ENABLE PPPoE 191
WAN Interface (Physical) 191
WAN Interface (Virtual Dialer) 191
Router Passwords 192
NAT Setup 192
CBAC Firewall 193
DHCP Server 193
IPFW Access List 194
VTY Access List 194
Configure SSH (Version 2) 195
Encrypt All Router Passwords 195
Save the Configuration 195

APPENDIX C Sample Configuration IPSec VPN Over DSL 197

Standard Setup 198
LAN Interface. 198
Enable PPPoE 199
WAN Interface (Physical) 199
WAN Interface (Virtual Dialer) 199
Router Passwords. 200
NAT Setup 200
CBAC Firewall 201
VPN Cryptographic Settings 202
DHCP Server 203
IPFW Access List. 203
VTY Access List. 204
Configure SSH (Version 2). 204
Encrypt All Router Passwords. 205
Save the Configuration. 205

APPENDIX D CCNA CLI Command Reference 207

Cisco Router Commands. 207
- Access Control List (ACL). 208
- Backup and Restore the IOS 210
- Cisco Discovery Protocol (CDP). 210
- Command History 211
- Configuration Register Commands 211
- Password Recovery. 212
- Console Messages 213
- Date and Time 213
- DHCP Configuration 213
- DNS Lookup 213
- Frame-Relay. 214
- Hostname and Message of the Day (MOTD). 214
- Interface—Configuration 214
- Interface—Verifying TCP/IP Configurations 215
- Network Address Translation (NAT) 216
- Password—Encryption 219
- Password—Setting. 219
- PPP Configuration 219
- Routing—Default Routes. 220
- Routing—EIGRP 221

Routing—IGRP. 221
Routing—OSPF 221
Routing—RIP 222
Routing—Static Routes 223
Secure Shell (SSH) 223
Startup-Config and Running-Config Files 223
Telnet 224
VTY ACL for Telnet and SSH 224
Cisco Catalyst Switch Commands 225
Hostnames 225
Interface Configuration. 225
Passwords 226
Port Security. 226
Saving and Deleting Configurations. 226
VLAN—Configuration 227
VLAN—Inter-VLAN Routing Example. 228
VLAN—VTP Domain Configuration. 230

APPENDIX E ACL and Firewall Names Used in This Book 231

ACL Names 231
CBAC Firewall Names 232
DHCP Pool Name 232
Routing Policy Names 232

INDEX 233

About the Author

Having been professionally involved in computer networking for over 20 years, **JASON NEUMANN** has worked with Cisco routers for more than 10 of those years. Jason is the owner of LAN Technologies LLC, a small networking company located in Anchorage, Alaska, that provides local and wide-area network solutions and support to small businesses using high-end operating systems including the Cisco IOS, Microsoft, Linux, and BSD UNIX. He holds many credentials from industry leaders including Cisco, Microsoft, and Novell.

About the Technical Reviewers

A telecommunications engineer and consultant, **DEAN OLSEN** has over 20 years of experience in IP networking and services. He specializes in IP-based carrier technologies such as MPLS, SONET, Carrier Ethernet, and GSM wireless data networks. Throughout his career Dean has been responsible for designing, implementing, and troubleshooting a variety of networks from simple point-to-point transport to complex multipoint converged service delivery architectures. Currently Dean is working with a regional carrier on the design and implementation of a large-scale multivendor GSM-based converged network supporting SS7 Sigtran, VoIP, and MMS technologies.

SEBASTIEN MICHELET (CCIE #16877) is a senior network engineer in the R&D department at ADP (Automatic Data Processing). He designs and installs Cisco IP telephony solutions for the car dealership market. Before diving into the VoIP world, he was a networking engineer responsible for maintaining, securing, and monitoring large networks of firewalls and routers. His career in Cisco networking spans 12 years. He has an MS in mechanical engineering from the University of Poitiers, France.

Acknowledgments

I wish to extend my sincere gratitude to Lois Weber for her proofreading skills and keen eye for detail; to my daughter, Terra Vleeshouwer-Neumann, for her impeccable knowledge of grammar; to my son, Gabe, for allowing me to cut into our “guy time”; and to my wife, Sharon, for helping me with pretty much every aspect of this book!

Introduction

"The creation of this book, like many things in life, was a complete accident."

This book is intended for the average network administrators or IT professionals who manage small networks and are currently using, or want to use Cisco IOS-based routers in their networks. After all, why should Cisco routers be reserved for elite Cisco gurus when all you need to know are a few simple concepts and commands? This book is about a Cisco CLI for the regular guy or gal. After reading this book, you'll no longer have to use cheap consumer-grade routers on your small business network. You, too, can have all the reliability and advanced functionality that the Cisco IOS offers.

In my experience, the best way to learn this material is through hands-on experience. The more the better! Therefore, you may want to have a spare Cisco router to work with. You can use the book without one, but it really helps to have an actual router on hand to work through the material. The Cisco 831 and 851 routers will be used throughout my examples. If you don't have a router, you can easily find an older 800 series router on eBay or some other used computer site. In secondary markets like eBay, a Cisco 831 or SOHO91 series router is inexpensive, easy to come by, and will work well with the material. Keep in mind that you will need a router with at least *64 MB of memory* to configure DSL using PPPoE. Also, I assume that the router has an IOS version of 12.4 or greater.

Each chapter of this book has specific configuration examples, in the form of command listings, showing how to configure the features of your Cisco router. Chapters 1 through 4 provide tutorial-based examples of how to configure your router for different broadband technologies, including cable modems, DSL, and setting up VPNs using IPSec. Chapter 5 explains some of the more advanced—but not too advanced—features of the IOS.

Chapter 6 provides IP networking fundamentals that can be very useful to network administrators, IT professionals, or anyone who is preparing to become Cisco CCNA certified. Chapter 7 provides information about setting up an advanced IP network using multiple Cisco routers and the Routing Information Protocol (RIP) to configure a true DMZ on a separate private network. Chapter 8 is about VLSM networking, which is a necessary concept to understand for CCNA certification.

At the end of each chapter is a summary that can be used for quick reference once you're familiar with Cisco concepts and commands, or it can be used right away to help configure your router if you already have some Cisco networking experience.

Finally, there are appendixes at the end of the book that provide keystroke-for-keystroke commands used to configure a router for various scenarios. Although you can use this information exclusively to configure your router, I recommend you first read Chapters 1 through 6 to get a feel for the Cisco IOS and some networking concepts. Appendix D has an extensive IOS command reference guide geared toward CCNA exam preparation.