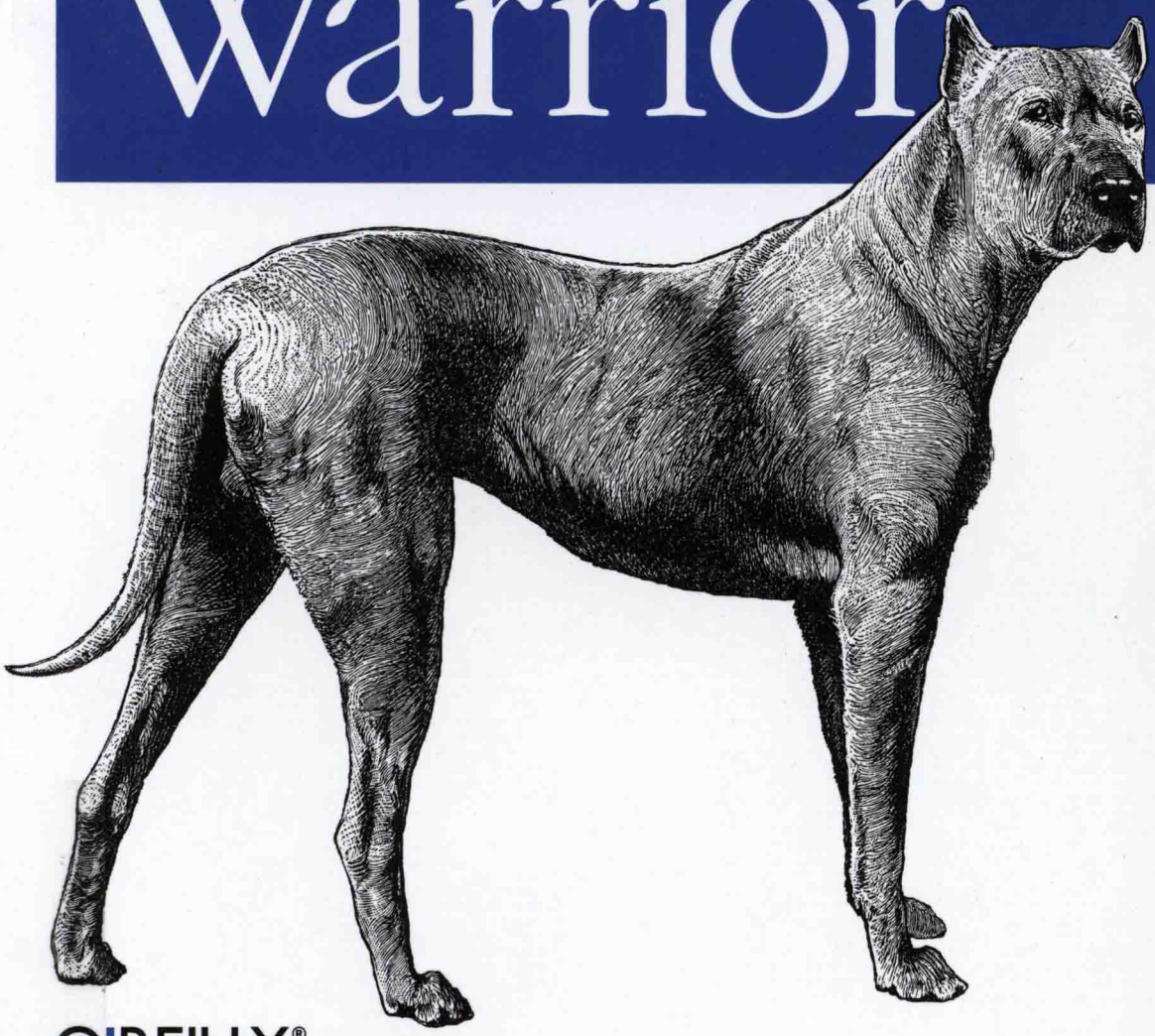
Network Warrior

—思科网络工程师必备手册（影印版）

第二版

涵盖Nexus

Network Warrior



O'REILLY®

東南大學出版社

Gary A. Donahue 著

（第2版）

Network Warrior（影印版）

——思科网络工程师必备手册

Network Warrior

Gary A. Donahue

O'REILLY®

Beijing · Cambridge · Farnham · Köln · Sebastopol · 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

Network Warrior：思科网络工程师必备手册：第2版：英文/（美）唐纳修（Donahue, G. A.）著. —影印本. —南京：东南大学出版社，2011.10

书名原文：Network Warrior, Seconde Edition

ISBN 978-7-5641-2939-2

I. ① N… II. ①唐… III. ①计算机网络－手册－英文 IV. ① TP393-62

中国版本图书馆CIP数据核字（2011）第175018号

江苏省版权局著作权合同登记

图字：10-2010-416号

Network Warrior

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：江建中
网　　址：http://www.seupress.com
电子邮件：press@seupress.com
印　　刷：扬中市印刷有限公司
开　　本：787毫米×960毫米　16开本
印　　张：49.25
字　　数：965千字
版　　次：2011年10月第1版
印　　次：2011年10月第1次印刷
书　　号：ISBN 978-7-5641-2939-2
定　　价：98.00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

Network Warrior（影印版）

——思科网络工程师必备手册

Network Warrior

Preface

The examples used in this book are taken from my own experiences, as well as from the experiences of those with or for whom I have had the pleasure of working. Of course, for obvious legal and honorable reasons, the exact details and any information that might reveal the identities of the other parties involved have been changed.

Cisco equipment is used for the examples within this book and, with very few exceptions, the examples are TCP/IP-based. You may argue that a book of this type should include examples using different protocols and equipment from a variety of vendors, and, to a degree, that argument is valid. However, a book that aims to cover the breadth of technologies contained herein, while also attempting to show examples of these technologies from the point of view of different vendors, would be quite an impractical size. The fact is that Cisco Systems (much to the chagrin of its competitors, I'm sure) is the premier player in the networking arena. Likewise, TCP/IP is the protocol of the Internet, and the protocol used by most networked devices. Is it the best protocol for the job? Perhaps not, but it is the protocol in use today, so it's what I've used in all my examples. Not long ago, the Cisco CCIE exam still included Token Ring Source Route Bridging, AppleTalk, and IPX. Those days are gone, however, indicating that even Cisco understands that TCP/IP is where everyone is heading. I have included a chapter on IPv6 in this edition, since it looks like we're heading that way eventually.

WAN technology can include everything from dial-up modems (which, thankfully, are becoming quite rare) to T1, DS3, SONET, MPLS, and so on. We will look at many of these topics, but we will not delve too deeply into them, for they are the subject of entire books unto themselves—some of which may already sit next to this one on your O'Reilly bookshelf.

Again, all the examples used in this book are drawn from real experiences, most of which I faced myself during my career as a networking engineer, consultant, manager, and director. I have run my own company and have had the pleasure of working with some of the best people in the industry. The solutions presented in these chapters are the ones my teams and I discovered or learned about in the process of resolving the issues we encountered.

I faced a very tough decision when writing the second edition of this book. Should I keep the CatOS commands or discard them in favor of newer Nexus NX-OS examples? This decision was tough not only because my inclusion of CatOS resulted in some praise from my readers, but also because as of this writing in early 2011, I'm still seeing CatOS switches running in large enterprise and ecommerce networks. As such, I decided to keep the CatOS examples and simply add NX-OS commands.

I have added many topics in this book based mostly on feedback from readers. New topics include Cisco Nexus, wireless, MPLS, IPv6, and Voice over IP (VoIP). Some of these topics are covered in depth, and others, such as MPLS, are purposely light for reasons outlined in the chapters. Topics such as Nexus and VoIP are vast and added significantly to the page count of an already large and expensive book. I have also removed the chapters on server load balancing, both because I was never really happy with those chapters and because I could not get my hands on an ACE module or appliance in order to update the examples.

On the subject of examples, I have updated them to reflect newer hardware in every applicable chapter. Where I used 3550 switches in the first edition, I now use 3750s. Where I used PIX firewalls, I now use ASA appliances. I have also included examples from Cisco Nexus switches in every chapter that I felt warranted them. Many chapters therefore have examples from Cat-OS, IOS, and NX-OS. Enjoy them, because I guarantee that CatOS will not survive into the third edition.

Who Should Read This Book

This book is intended for anyone with first-level certification knowledge of data networking. Anyone with a CCNA or equivalent (or greater) knowledge should benefit from this book. My goal in writing *Network Warrior* is to explain complex ideas in an easy-to-understand manner. While the book contains introductions to many topics, you can also consider it a reference for executing common tasks related to those topics. I am a teacher at heart, and this book allows me to teach more people than I'd ever thought possible. I hope you will find the discussions both informative and enjoyable.

I have noticed over the years that people in the computer, networking, and telecom industries are often misinformed about the basics of these disciplines. I believe that in many cases, this is the result of poor teaching or the use of reference material that does not convey complex concepts well. With this book, I hope to show people how easy some of these concepts are. Of course, as I like to say, "It's easy when you know how," so I have tried very hard to help anyone who picks up my book understand the ideas contained herein.

If you are reading this, my guess is that you would like to know more about networking. So would I! Learning should be a never-ending adventure, and I am honored that you have let me be a part of your journey. I have been studying and learning about computers, networking, and telecom for the last 29 years, and my journey will never end.

This book does not explain the OSI stack, but it does briefly explain the differences between hubs, switches, and routers. You will need to have a basic understanding of what Layer 2 means as it relates to the OSI stack. Beyond that, this book tries to cover it all, but not like most other books.

This book attempts to teach you what you need to know in the real world. When should you choose a Layer-3 switch over a Layer-2 switch? How can you tell if your network is performing as it should? How do you fix a broadcast storm? How do you know you're having one? How do you know you have a spanning tree loop, and how do you fix it? What is a T1, or a DS3 for that matter? How do they work? In this book, you'll find the answers to all of these questions and many, many more. I tried to fill this book with information that many network engineers seem to get wrong through no fault of their own. *Network Warrior* includes configuration examples from real-world events and designs, and is littered with anecdotes from my time in the field—I hope you enjoy them.

Conventions Used in This Book

The following typographical conventions are used in this book:

Italic
: Used for new terms where they are defined, for emphasis, and for URLs

`Constant width`
: Used for commands, output from devices as it is seen on the screen, and samples of Request for Comments (RFC) documents reproduced in the text

`Constant width italic`
: Used to indicate arguments within commands for which you should supply values

`Constant width bold`
: Used for commands to be entered by the user and to highlight sections of output from a device that have been referenced in the text or are significant in some way

Indicates a tip, suggestion, or general note

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: "*Network Warrior, Second Edition,* by Gary A. Donahue (O'Reilly). Copyright 2011 Gary Donahue, 978-1-449-38786-0."

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*.

We'd Like to Hear from You

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/9781449387860

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

bookquestions@oreilly.com

For more information about our books, courses, conferences, and news, see our website at *http://www.oreilly.com*.

Find us on Facebook: *http://facebook.com/oreilly*

Follow us on Twitter: *http://twitter.com/oreillymedia*

Watch us on YouTube: *http://www.youtube.com/oreillymedia*

Safari® Books Online

Safari Books Online is an on-demand digital library that lets you easily search over 7,500 technology and creative reference books and videos to find the answers you need quickly.

With a subscription, you can read any page and watch any video from our library online. Read books on your cell phone and mobile devices. Access new titles before they are available for print, and get exclusive access to manuscripts in development and post feedback for the authors. Copy and paste code samples, organize your favorites, download chapters, bookmark key sections, create notes, print out pages, and benefit from tons of other time-saving features.

O'Reilly Media has uploaded this book to the Safari Books Online service. To have full digital access to this book and others on similar topics from O'Reilly and other publishers, sign up for free at *http://my.safaribooksonline.com*.

Acknowledgments

Writing a book is hard work—far harder than I ever imagined. Though I spent countless hours alone in front of a keyboard, I could not have accomplished the task without the help of many others.

I would like to thank my lovely wife, Lauren, for being patient, loving, and supportive. Lauren, being my in-house proofreader, was also the first line of defense against grammatical snafus. Many of the chapters no doubt bored her to tears, but I know she enjoyed at least a few. Thank you for helping me achieve this goal in my life.

I would like to thank Meghan and Colleen for trying to understand that when I was writing, I couldn't play. I hope I've helped instill in you a sense of perseverance by completing this book. If not, you can be sure that I'll use it as an example for the rest of your lives. I love you both "bigger than the universe" bunches.

I would like to thank my mother—because she's my mom, and because she never gave up on me, always believed in me, and always helped me even when she shouldn't have (Hi, Mom!).

I would like to thank my father for being tough on me when he needed to be, for teaching me how to think logically, and for making me appreciate the beauty in the details. I have fond memories of the two of us sitting in front of my RadioShack Model III computer while we entered basic programs from a magazine. I am where I am today largely because of your influence, direction, and teachings. You made me the man I am today. Thank you, Papa. I miss you.

I would like to thank my Cozy, my faithful Newfoundland dog who was tragically put to sleep in my arms so she would no longer have to suffer the pains of cancer. Her body failed while I was writing the first edition of this book, and if not for her, I probably

would not be published today. Her death caused me great grief, which I assuaged by writing. I miss you my Cozy—may you run pain free at the rainbow bridge until we meet again.

I would like to thank Matt Maslowski for letting me use the equipment in his lab that was lacking in mine, and for helping me with Cisco questions when I wasn't sure of myself. I can't think of anyone I would trust more to help me with networking topics. Thanks, buddy.

I would like to thank Jeff Fry, CCIE# 22061, for providing me temporary access to a pair of unconfigured Cisco Nexus 7000 switches. This was a very big deal, and the second edition is much more complete as a result.

I would like to thank Jeff Cartwright for giving me my first exciting job at an ISP and for teaching me damn-near everything I know about telecom. I still remember being taught about one's density while Jeff drove us down Interstate 80, scribbling waveforms on a pad on his knee while I tried not to be visibly frightened. Thanks also for proofreading some of my telecom chapters. There is no one I would trust more to do so.

I would like to thank Mike Stevens for help with readability and for some of the more colorful memories that have been included in this book. His help with PIX firewalls was instrumental to the completion of the first edition. You should also be thankful that I haven't included any pictures. I have this one from the Secaucus data center...

I would like to thank Peter Martin for helping me with some subjects in the lab for which I had no previous experience. And I'd like to extend an extra thank you for your aid as one of the tech reviewers for *Network Warrior*—your comments were always spot-on and your efforts made this a better book.

I would like to thank another tech reviewer, Yves Eynard: you caught some mistakes that floored me, and I appreciate the time you spent reviewing. This is a better book for your efforts.

I would like to thank Sal Conde and Ed Hom for access to 6509E switches and modules.

I would like to thank Michael Heuberger, Helge Brummer, Andy Vassaturo, Kelly Huffman, Glenn Bradley, Bill Turner, and the rest of the team in North Carolina for allowing me the chance to work extensively on the Nexus 5000 platform and for listening to me constantly reference this book in daily conversation. I imagine there's nothing worse than living or working with a know-it-all writer.

I would like to thank Christopher Leong for his technical reviews on the telecom and VoIP chapters.

I would like to thank Robert Schaffer for helping me remember stuff we'd worked on that I'd long since forgotten.

I would like to thank Jennifer Frankie for her help getting me in touch with people and information that I otherwise could not find.

I would like to thank Mike Loukides, my editor, for not cutting me any slack, for not giving up on me, and for giving me my chance in the first place. You have helped me become a better writer, and I cannot thank you enough.

I would like to thank Rachel Head, the copyeditor who made the first edition a much more readable book.

I would like to thank all the wonderful people at O'Reilly. Writing this book was a great experience, due in large part to the people I worked with at O'Reilly.

I would like to thank my good friend, John Tocado, who once told me, "If you want to write, then write!" This book is proof that you can change someone's life with a single sentence. You'll argue that I changed my own life, and that's fine, but you'd be wrong. When I was overwhelmed with the amount of remaining work to be done, I seriously considered giving up. Your words are the reason I did not. Thank you.

I cannot begin to thank everyone else who has given me encouragement. Living and working with a writer must, at times, be maddening. Under the burden of deadlines, I've no doubt been cranky, annoying, and frustrating, for which I apologize.

My purpose for the last year has been the completion of this book. All other responsibilities, with the exception of health and family, took a back seat to my goal. Realizing this book's publication is a dream come true for me. You may have dreams yourself, for which I can offer only this one bit of advice: work toward your goals, and you will realize them. It really is that simple.

Table of Contents

Preface xvii

1. What Is a Network? 1

2. Hubs and Switches 5
Hubs 5
Switches 10
Switch Types 14
Planning a Chassis-Based Switch Installation 16

3. Autonegotiation 19
What Is Autonegotiation? 19
How Autonegotiation Works 20
When Autonegotiation Fails 21
Autonegotiation Best Practices 23
Configuring Autonegotiation 23

4. VLANs 25
Connecting VLANs 25
Configuring VLANs 29
CatOS 29
IOS Using VLAN Database 31
IOS Using Global Commands 33
Nexus and NX-OS 35

5. Trunking 37
How Trunks Work 38
ISL 39
802.1Q 39
Which Protocol to Use 40
Trunk Negotiation 40

Configuring Trunks 42
IOS 42
CatOS 44
Nexus and NX-OS 46

6. VLAN Trunking Protocol 49
VTP Pruning 52
Dangers of VTP 54
Configuring VTP 55
VTP Domains 55
VTP Mode 56
VTP Password 57
VTP Pruning 58

7. Link Aggregation 63
EtherChannel 63
EtherChannel Load Balancing 64
Configuring and Managing EtherChannel 68
Cross-Stack EtherChannel 75
Multichassis EtherChannel (MEC) 75
Virtual Port Channel 75
Initial vPC Configuration 76
Adding a vPC 77

8. Spanning Tree 81
Broadcast Storms 82
MAC Address Table Instability 86
Preventing Loops with Spanning Tree 88
How Spanning Tree Works 88
Managing Spanning Tree 91
Additional Spanning Tree Features 95
PortFast 95
BPDU Guard 96
UplinkFast 97
BackboneFast 99
Common Spanning Tree Problems 100
Duplex Mismatch 100
Unidirectional Links 101
Bridge Assurance 103
Designing to Prevent Spanning Tree Problems 104
Use Routing Instead of Switching for Redundancy 104
Always Configure the Root Bridge 104

9. Routing and Routers 105
Routing Tables 106
Route Types 109
The IP Routing Table 109
Host Route 111
Subnet 112
Summary (Group of Subnets) 112
Major Network 113
Supernet (Group of Major Networks) 114
Default Route 114
Virtual Routing and Forwarding 115

10. Routing Protocols 119
Communication Between Routers 120
Metrics and Protocol Types 123
Administrative Distance 125
Specific Routing Protocols 127
RIP 129
RIPv2 132
EIGRP 133
OSPF 137
BGP 143

11. Redistribution 147
Redistributing into RIP 149
Redistributing into EIGRP 152
Redistributing into OSPF 154
Mutual Redistribution 156
Redistribution Loops 157
Limiting Redistribution 159
Route Tags 159
A Real-World Example 163

12. Tunnels 167
GRE Tunnels 168
GRE Tunnels and Routing Protocols 173
GRE and Access Lists 178

13. First Hop Redundancy 181
HSRP 181
HSRP Interface Tracking 184
When HSRP Isn't Enough 186

Nexus and HSRP 189
GLBP 189
Object Tracking in GLBP 194

14. Route Maps 197
Building a Route Map 198
Policy Routing Example 200
Monitoring Policy Routing 203

15. Switching Algorithms in Cisco Routers 207
Process Switching 209
Interrupt Context Switching 210
Fast Switching 211
Optimum Switching 213
CEF 213
Configuring and Managing Switching Paths 216
Process Switching 216
Fast Switching 218
CEF 219

16. Multilayer Switches 221
Configuring SVIs 223
IOS (4500, 6500, 3550, 3750, etc.) 223
Hybrid Mode (4500, 6500) 225
NX-OS (Nexus 7000, 5000) 227
Multilayer Switch Models 228

17. Cisco 6500 Multilayer Switches 231
Architecture 233
Buses 234
Enhanced Chassis 237
Vertical Enhanced Chassis 238
Supervisors 238
Modules 240
CatOS Versus IOS 249
Installing VSS 253
Other Recommended VSS Commands 259
VSS Failover Commands 261
Miscellaneous VSS Commands 262
VSS Best Practices 263

18. Cisco Nexus 265
Nexus Hardware 265

Nexus 7000 266
Nexus 5000 268
Nexus 2000 270
Nexus 1000 Series 272
NX-OS 273
NX-OS Versus IOS 274
Nexus Iconography 279
Nexus Design Features 280
Virtual Routing and Forwarding 281
Virtual Device Contexts 283
Shared and Dedicated Rate-Mode 287
Configuring Fabric Extenders (FEXs) 290
Virtual Port Channel 294
Config-Sync 300
Configuration Rollback 309
Upgrading NX-OS 312

19. Catalyst 3750 Features 317
Stacking 317
Interface Ranges 319
Macros 320
Flex Links 324
Storm Control 325
Port Security 329
SPAN 332
Voice VLAN 336
QoS 338

20. Telecom Nomenclature 341
Telecom Glossary 342

21. T1 355
Understanding T1 Duplex 355
Types of T1 356
Encoding 357
AMI 357
B8ZS 358
Framing 359
D4/Superframe 360
Extended Super Frame 360
Performance Monitoring 362
Loss of Signal 362
Out of Frame 362

Bipolar Violation 362
CRC6 363
Errored Seconds 363
Extreme Errored Seconds 363
Alarms 363
Red Alarm 364
Yellow Alarm 364
Blue Alarm 366
Troubleshooting T1s 366
Loopback Tests 366
Integrated CSU/DSUs 369
Configuring T1s 370
CSU/DSU Configuration 370
CSU/DSU Troubleshooting 371

22. DS3 375
Framing 375
M13 376
C-Bits 377
Clear-Channel DS3 Framing 378
Line Coding 379
Configuring DS3s 379
Clear-Channel DS3 379
Channelized DS3 381

23. Frame Relay 387
Ordering Frame Relay Service 390
Frame Relay Network Design 391
Oversubscription 393
Local Management Interface 394
Congestion Avoidance in Frame Relay 395
Configuring Frame Relay 396
Basic Frame Relay with Two Nodes 396
Basic Frame Relay with More Than Two Nodes 398
Frame Relay Subinterfaces 401
Troubleshooting Frame Relay 403

24. MPLS 409

25. Access Lists 415
Designing Access Lists 415
Named Versus Numbered 415
Wildcard Masks 416