

Contents at a Glance

Introduction	xvii
Part I	Managing Routing 2
Chapter 1	Managing Your IP Address Space 4
Chapter 2	Deploying Interior Routing Protocols 38
Chapter 3	Managing Routing Protocols 62
Part II	Managing Quality of Service 112
Chapter 4	Deploying Basic Quality of Service Features 114
Chapter 5	Deploying Advanced Quality of Service Features 144
Part III	Managing Security 180
Chapter 6	Deploying Basic Security Services 182
Chapter 7	Advanced Security Services, Part I: IPsec 222
Chapter 8	Advanced Security Services, Part II: IOS Firewall Feature Set 284
Part IV	Appendixes 310
Appendix A	Obtaining IETF RFCs 312
Appendix B	Retrieving Internet Drafts 316
Appendix C	Common TCP and UDP Ports 320
Appendix D	Password Recovery 324
Appendix E	A Crash Course in Cisco IOS 330
Bibliography	376
Index	380

Table of Contents

Introduction xvii

Part I Managing Routing 2

Chapter 1	Managing Your IP Address Space	4
	Review of Traditional IP Addressing	6
	Subnetting a Classful Address Space	7
	Major Nets and Subnet Masks	8
	Classful Subnetting: An Example	11
	Calculating the Number of Host Addresses in a Subnet	12
	Finding Subnet Information, Given a Host Address and the Mask	13
	Disadvantages of Subnetting	14
	The Rules on Top and Bottom Subnets	14
	Using Subnet-Zero to Get Around the Rules	15
	Subnetting with Variable Length Subnet Masks	16
	Using VLSM for Address Space Efficiency: An Example	16
	Final VLSM Results for Widget, Inc.	23
	Overview of Classless Addressing	24
	Using VLSM Techniques with Classless Addressing	26
	Routing Protocols and Classless Addressing	27
	Planning for Address Summarization	28
	Conserving Subnets with IP Unnumbered	29
	Scaling the Address Space with Network Address Translation	30
	Translating Private Addresses into Public Addresses	31
	Configuring NAT	33
	Creating a Pool of Discontiguous Addresses	34
	Configuring Static NAT	35
	Special Applications and NAT	35
	More Important Points on NAT	35
	Summary	36
Chapter 2	Deploying Interior Routing Protocols	38
	A Brief Review of Internetworking	39

Deploying RIP	42
Directly Connected Networks	43
Configuring RIP	44
Verifying RIP Configuration	45
Deploying IGRP	47
Configuring IGRP	48
Verifying IGRP Configuration	49
Deploying Enhanced IGRP	50
Configuring EIGRP	51
Verifying EIGRP Configuration	52
Deploying OSPF	54
Configuring OSPF	55
Verifying OSPF Configuration	59
Summary	60

Chapter 3 Managing Routing Protocols 62

Configuring Passive Interfaces	63
Filtering Routing Updates	65
Managing Redistribution	68
Configuring Redistribution—RIP and OSPF	70
Redistributing into IGRP and EIGRP	72
Understanding Administrative Distance	73
Controlling Redistribution Loops with Route Filters	76
Resolving Issues with VLSM and Classful Routing Protocols	78
Leveraging Default Routing	82
Propagation of Default Routes	84
Originating a Default Route with RIP	85
Originating a Default Route with IGRP	86
Originating a Default Route with EIGRP	88
Originating a Default Route with OSPF	88
Default Routing and Classful Behavior	89
Configuring Route Summarization	92
Understanding EIGRP Auto-Summarization	92
Configuring EIGRP Summarization	94
Configuring OSPF Summarization Between Areas	97
Configuring OSPF Summarization During Redistribution	98

Deploying Policy Routing with Route Maps	99
Forwarding Traffic with Route Maps	100
Classifying Packets with Route Maps	107
Setting Next-Hop and Precedence in Tandem	109
Other Policy-Routing Commands	109
Summary	110

Part II Managing Quality of Service 112

Chapter 4 Deploying Basic Quality of Service Features 114

The Case for QoS	115
Queuing in a Router	117
First-In, First-Out Queuing	117
FIFO: An Example	119
Priority Queuing	120
Queuing and Classifying Packets with Priority Queuing	121
Priority Queuing Strategy	123
Configuring Priority Queuing	124
Verifying the Priority Queuing Configuration	125
Adjusting the Queue Sizes in Priority Queuing	125
Custom Queuing	126
Configuring Custom Queuing	129
Verifying the Custom Queuing Configuration	131
Adjusting the Queue Sizes in Custom Queuing	132
Understanding IP Precedence	133
Setting IP Precedence	133
QoS Benefits of IP Precedence	134
Diffserv Redefines IP Precedence	134
Weighted Fair Queuing	135
Configuring Weighted Fair Queuing	136
Fair Queuing in Action	137
Fair Queuing Versus FIFO	138
Weighting and IP Precedence	140
Weighted Fair Queuing on a Network	141
Summary	143

Chapter 5 Deploying Advanced Quality of Service Features 144

Resource Reservation Protocol	145
RSVP Admission Control	146

RSVP Signaling Versus Bulk Data	148
The RSVP Signaling Process	149
RSVP and Weighted Fair Queuing	154
Configuring RSVP	155
Verifying RSVP Configuration	157
Configuring IOS as a Proxy for Path and Resv Messages	158
RSVP Scaling Considerations	161
Random Early Detection	161
Dynamics of Network Congestion and Tail Drops	162
Global Synchronization	163
TCP Slow Start	163
Ill Effects of Global Synchronization and TCP Slow Start	164
How RED Works	165
RED and IP Precedence (Weighted RED)	165
Configuring WRED	166
Verifying WRED Configuration	167
Committed Access Rate	168
Rate Policies	168
Configuring Cisco Express Forwarding	169
Configuring CAR	170
Validating CAR Configuration	173
Class-Based WFQ	173
Configuring CBWFQ	174
Verifying CBWFQ	177
Summary	178

Part III Managing Security 180

Chapter 6 Deploying Basic Security Services 182

Controlling Traffic with Access Control Lists	183
Filtering Traffic with Access Lists	184
Standard IP Access Lists	187
Important Points for Designing Access Lists	192
The Invisible Rule in Every Access List	193
Extended IP Access Lists	194
Access Lists for Combating Spoofing Attacks	200
Securing Access to the Router	202
Securing the Enable Mode of a Router	203
Securing Telnet Access	204
Securing Access to the Console Port	205

Deploying Authentication, Authorization, and Accounting	206
Authentication, Authorization, and Accounting	207
Configuring Authentication for Network Access over PPP	210
Using the Default Authentication List	213
Configuring Authentication for Router Logins	214
The Local Username Database	215
Configuring Authorization	216
Configuring Accounting	216
Pointing the Router to the RADIUS or TACACS+ AAA Server	217
Other IOS Commands for Basic Security	218
Disable TCP and UDP Small Servers	218
Disable IP Source Routing	219
Disable CDP on Public Links	219
Disable Directed Broadcasts on Interfaces	220
Summary	220

Chapter 7	Advanced Security Services, Part I: IPsec	222
	IPsec Enables Virtual Private Networks	224
	Benefits of IPsec's Layer 3 Service	225
	Basic IPsec Security Concepts and Cryptography	226
	Confidentiality (Encryption)	227
	Integrity	233
	Hashing Algorithms: Examples with Message Digest 5	234
	Origin Authentication	236
	Anti-Replay	238
	IPsec Concepts	239
	Peers	239
	Transform Sets	239
	Security Associations	240
	Transport and Tunnel Modes	241
	Authentication Header and Encapsulating Security Payload	242
	Internet Key Exchange	244
	Tying All of the Pieces Together: A Comprehensive Example with IPsec and IKE	245
	Configuring IKE	246
	Configuring IKE with Pre-Shared Keys	246
	Configuring IKE with RSA Encryption	249
	Configuring IKE with RSA Signatures and Digital Certificates	253
	Additional Commands for IKE	260

Validating IKE Configuration	262
When Are IKE SAs Established?	262
Configuring IPsec	263
Crypto Maps	263
Crypto Map Configuration Overview	264
Configuring Crypto Access Lists	265
Crypto Access Lists: An Example	266
Configuring IPsec Transform Sets	269
Configuring and Applying Crypto Maps	270
When Are SAs Established?	272
Configuring IPsec SA Lifetimes	273
Configuring Perfect Forward Secrecy	274
Configuring Dynamic Crypto Maps	274
Tunnel Endpoint Discovery	276
Validating IPsec Configuration	277
Troubleshooting IPsec and IKE	278
Check Configurations and Show Commands	278
Enable Debugging and Clearing Existing SAs	279
Summary	281
Chapter 8 Advanced Security Services, Part II: IOS Firewall Feature Set	284
IOS Firewall Fundamentals	285
Defending the Perimeter Against Attacks	286
How Context-Based Access Control Works	287
Configuring CBAC	288
CBAC Example: A Basic Two-Port Firewall	288
Validating CBAC Configuration	292
Configuring CBAC Inspection of Other Applications	294
Adjusting CBAC Timers and Thresholds	296
Adjusting CBAC Session Timers	296
Overriding Global Timers with Inspection Rules	298
Adjusting CBAC Denial of Service Thresholds	298
Enabling Auditing of Sessions	300
CBAC with a Demilitarized Zone	300
Basic Security Commands for the Firewall Router	301
Configuring the Inspection Rule	302
Configuring the Private Network Interface	302
Configuring the DMZ Network Interface	303
Configuring the Internet Interface	304

Notes on CBAC Performance	305
Configuring Java Applet Blocking for Security	305
The IOS Intrusion Detection System	306
Configuring IDS	307
Additional Commands for IDS	308
Summary	309

Part IV Appendixes 310

Appendix A Obtaining IETF RFCs 312

Via the World Wide Web	313
Via FTP	314
Via E-Mail	314
Finding Current RFCs	314
Authoring RFCs	315

Appendix B Retrieving Internet Drafts 316

Via the World Wide Web	317
Via FTP	317
Via E-Mail	318
Authoring Internet Drafts	318

Appendix C Common TCP and UDP Ports 320

Appendix D Password Recovery 324

Recovering a Lost Password on Most Router Models	327
Recovering a Lost Password on Other Router Models	329

Appendix E A Crash Course in Cisco IOS 330

Connecting to the Router	331
Connect via Direct Serial Cable to the Console Port	331
Connect via Telnet over the IP Network	332
Connect via the AUX Port or Other Asynchronous Serial Port	332
Modes	332
User EXEC Mode	332
Privileged EXEC Mode (Enable Mode)	333

Global Configuration Mode	334
Interface Configuration Mode	334
Subinterface Configuration Mode	335
Line Configuration Mode	335
Other Configuration Modes	336
Context-Based Help, Navigation, and Line Editing	336
Context-Based Help	336
Navigation	337
Line Editing	339
Common IOS Commands	339
Extended Ping	342
Extended Traceroute	343
Common Configuration Tasks	345
The Setup Utility (Initial Configuration Dialog)	345
Set the Enable Password	347
Set the Router's Hostname	347
Make a Banner	347
Set the System Clock and Date	348
Set the Domain Name	348
Set the Name Server(s)	348
Populate the Router's Local Host Table	348
Set SNMP Community Strings	348
Set SNMP Trap Hosts	349
Enable the Router to Send SNMP Traps	349
Point the Router to a Syslog Server	349
Configure Timestamping of System and Debug Messages	349
Point the Router to a Network Time Protocol (NTP) Server	350
Set the Time Zone	350
Set Daylight Saving Time Information	350
Configure a Static Route	351
Configure a Default Route	351
Configure an IP Address on an Interface	352
Other Interface Configuration Tasks	352
Configure the Location of the Boot Image	353
Retract (undo) Configuration Commands	354
Common Show Commands	354
General Show Commands	354
Resource Show Commands	357
Interface Show Commands	360
Network Show Commands	364
Routing Show Commands	366

Using the Router as a Terminal Server (Communications Server) 368

Enabling IOS Web-Based Management 373

Bibliography 376

Index 380