

Table of Contents

<i>Introduction</i>	1
About This Book	2
How to Use This Book	3
How This Book Is Organized	3
Part I: Planning and Acquiring Your Network	3
Part II: Implementing Your Wireless Network	4
Part III: Using Your Network Securely	4
Part IV: Keeping Your Network on the Air — Administration and Troubleshooting	4
Part V: The Part of Tens	5
Part VI: Appendixes	5
Icons Used in This Book	5
Where to Go from Here	6
<i>Part I: Planning and Acquiring Your Network</i>	7
Chapter 1: Removing the Tethers: Entering the Wireless World	9
Understanding the Risks and Rewards of Going Wireless	10
What you risk	10
The benefits you gain	11
Applications of Wireless Networks	11
Sorting Out the Nets: Do I Need a WPAN, WLAN, or WMAN?	12
Let's get personal: WPAN	13
The holy grail of wireless networking: WLAN	14
Where the rubber hits the road: WMAN	15
Using Wireless Networks	16
Accessing networks	16
Extending the network	17
Connecting buildings	17
Going mobile	18
Getting mail on the road	19
Turning a Notion into a Network	20
Planning your wireless network	20
Installing your wireless network	20

Configuring a wireless network	21
Staying secure in the wireless world	22
Administering and maintaining a wireless network	22
Convergence of Wireless Technologies —	
What Will the Future Hold?	23
Chapter 2: If You Fail to Plan, You Plan to Fail	25
Evaluating Your Wireless Needs	25
What is my environment?	26
What is my budget?	26
How many clients do I expect?	27
Where will they want to access the network?	28
What does the data look like?	28
What technology do I want to use?	29
Do I need to protect the data?	31
What coverage do I need?	31
Preparing for a Site Survey	32
Analyzing your facility	33
Working with existing networks	33
Area coverage	34
Purpose and business requirements	36
Bandwidth and roaming requirements	37
Available resources	37
Security needs analysis	38
Developing a site survey checklist	38
Using Site Survey Equipment to Get It Right	39
Doing That Site Survey	41
Analyzing your indoor network	42
Analyzing your outdoor network	42
Calculating a link budget	42
Describing Your Final Plan in a Site Survey Report	45
Defining the business requirements and methodology	45
Documenting the requirements	46
Chapter 3: Matching Wireless Technologies to Your Plan	47
Choosing the Right Networking Hardware	47
Are You Being Served? IBSS, BSS, and ESS	50
Selecting the Wireless Mode	51
Considering ad hoc mode	51
Using infrastructure mode	52

Gearing Up to Send and Receive Signals52
 Frequencies and spectrums53
 Get the right antennae54
 Introducing the zone — a wireless diet56
 Understanding and Using Layer 2 and 3 Concepts57

Part II: Implementing Your Wireless Network59

Chapter 4: Getting a Quick Start with Wireless Personal Area Networks 61

Understanding IrDA61
 Installing infrared devices63
 Using IrDA to transfer data64
 Securing IrDA66
 Understanding Bluetooth67
 Adding Bluetooth capabilities71
 Securing Bluetooth74
 Protecting Bluetooth networks75
 IrDA and Bluetooth Comparison82

Chapter 5: Moving On to a Wireless LAN: Your Wireless Access Point 83

Parts Is Parts — Do You Have Them All?83
 Connecting and Configuring Your Access Point84
 Connecting the access point85
 Configure your browser86
 Changing the default network settings87
 Initial Setup and Testing88
 Deciding on initial setup options88
 Performing the advanced setup functions92
 Back up your work94
 Turning Off the Defaults94
 Changing the password95
 Changing the access point name95
 Changing security options96
 Understanding the other options98
 Configuration and setup of a Cisco Aironet 120099
 Testing the Signal102

Chapter 6: Connecting Your Clients	103
Adding Hardware to the PC	104
Peripheral Component Interconnect (PCI)	105
Universal Serial Bus (USB)	106
Ethernet client adapter	106
The final decision	107
Wireless print server	108
Installing the Wireless Hardware	109
Upgrading the firmware or software	109
Important guidelines for upgrading	111
Configuring the Client's Operating System	112
Configuring Windows XP Professional clients	112
Configuring Windows 2000 clients	114
Configuring Mac OS clients	117
Configuring your Centrino systems	118
Configuring Linux and FreeBSD Clients	119
Making Sure the Connection Works	120
Chapter 7: Building the Multi-Zone Network	121
Roaming Around with a Wireless Machine	121
Wireless roaming standards	122
Connectivity issues as you move around	126
Reassociation — Getting back together as you move from AP to AP	129
Load Balancing — Are All Zones Used Equally?	131
Chapter 8: Using Wireless on the Road to Connect to the Office	133
Spontaneous Communities: Ad Hoc Networks	133
Wi-Fi Warriors on the Road	134
Wireless at the airport	135
Wireless in hotels	136
E-Mailing Wirelessly with Microsoft Exchange	137
Setting up POP access	138
Connecting directly to Exchange	140
Wireless Hot Spots: What's New Around the World?	144
In the air	145
New ideas for wireless network attacks	146

Part III: Using Your Network Securely 147**Chapter 9: Considering a Deadbolt: Understanding
the Risks of Wireless Networks 149**

Risks to the Network	149
Going to war: War nibbling, war driving, war flying, and war chalking	150
A roguish WLAN	156
Open broadcast of SSIDs	156
Jamming	157
Signal loss	158
Risks to Your Users	160
Target profiling	160
Identity theft	160
Lack of authentication	161
Default passwords are de fault	162
Risks to Your Data	163
You call that encryption?!	164
Accidental associations	165
Eavesdropping	165
Man-in-the-middle attacks	166
Hijacking	166

Chapter 10: Designing a Secure Network 169

Security as a Cost of Doing Business	170
Developing a Security Architecture	171
Developing a Wireless Security Policy	173
Developing Wireless Security Standards	175
Developing Wireless Security Best Practices	176
General best practices	176
Access point best practices	177
Password best practices	178
SSID best practices	178
Authentication best practices	178
Encryption best practices	179
Client best practices	179
Network best practices	180
Managing Your Wireless Security Policy	181

Designing a Secure Network	182
Performing a Risk Analysis	182

Chapter 11: Maintaining Network Security185

Understanding Security Mechanisms	186
Three States of Authentication	187
Authentication	187
Protecting Privacy	189
Protecting Message Integrity	190
Filtering the Chaff	191
SSID filtering	191
MAC filtering	191
Protocol filtering	193
Using Encryption	193
Hip to WEP	194
WEP weaknesses	196
Attacking WEP	198
Key management problems	199
Protecting WEP Keys	200
Default WEP keys	200
Using WPA	202
AES-CCMP	204
Using Port Authentication	204
Using LEAP, PEAP, and other forms of EAP	206
EAP Questions	207

Chapter 12: Secure Wireless Access with Virtual Private Networking209

Secure Access with a VPN	209
Defining the VPN	211
VPN considerations	213
Understanding tunneling	214
Deploying VPNs in WLANs	216
Wireless VLANs	217
Various Other Methods for Secure Access	218
Using Microsoft's Point-to-Point Tunneling Protocol	218
Considering Layer 2 Tunneling Protocol	225
Using Windows IPSec	225
Oldies but goodies — SSH2	226
Who Is Doing the Talking?	228

***Part IV: Keeping Your Network on the Air —
Administration and Troubleshooting229***

Chapter 13: Problems with Keeping on the Air 231

Troubleshooting Redux	231
Am I in Your Fresnel Zone?	234
Multipath Interference	236
You Can't Go That Far: Free Space Loss	238
Contention-Free Frames	239
Hidden Node — So Where Is It?	241
Managing Power	243
Power over Ethernet (PoE)	244
Calculating your Power Budget	245

Chapter 14: Bridging Networks to Manage Coverage 249

Using That Site Survey	250
Bridges and Switches and Routers, Oh My!	250
Understanding Wireless Bridges	251
Using root mode	254
Using non-root mode	254
Using access point mode	255
Using repeater mode	255
Wireless Workgroup Bridge	255
Going to the Movies: A Bridge Too Far?	257
Building Hardware Bridges	258
Bridging the Gap: Getting Started	259
Troubleshooting Your Bridged Network	260
Building Network Bridges in Windows XP	260
Creating a network bridge	261
Troubleshooting a wireless bridge	262
Using Wireless Switches	262

Chapter 15: Dealing with Network Throughput Issues 265

Watching Traffic	265
Estimating network performance	266
Sniffing your traffic	272
Traffic management and analysis	277
Outsourcing your network management	278
Monitoring the Network for Trouble Spots	279

Chapter 16: It's Ten O'Clock: Do You Know Where Your Access Points Are?283

Discovering the Extent of Your Wireless Network	283
Using programs that came with your operating system	284
Using utilities that came with your network adapter	284
Using war driving or network discovery tools	285
Using traffic management and analysis tools	286
Using network management tools	287
Using vulnerability testing software	289
Detecting Wireless Intrusion	291
Incident Response and Handling	299
Auditing Activities	300

Part V: The Part of Tens303**Chapter 17: Ten Administrator Tools and What They Do 305**

Using Ethereal to Look at Traffic	306
Stumbling on Networks with NetStumbler	306
With Luck, You Can Find Networks with Kismet	308
Surfing for Networks with Wellenreiter	308
Using AirSnort to Obtain WEP Keys	309
Rooting Around with THC-RUT	309
Cracking Encryption with WEPCrack	310
Getting a MAC Address	310
Creating Sham Access Points with FakeAP	311
Let's Sneak a Peek with AiroPeek, Shall We?	312

Chapter 18: Top Ten Ways to Secure Your Network 313

Using the Highest Level of Encryption	314
Changing the Default SSID	315
Looking for Rogue WAPs	315
Disabling Ad Hoc Mode	317
Disabling SNMP or Select Strong String	317
Turning Down the Power	319
Securing WAPs with a Subnet and a Firewall	321
Using a WIDS	325
Disabling Wired Access from Public Areas	325
Hardening the Access Point and Clients	326

Chapter 19: Ten Ways Wireless Is Used in Business 327

Attending Meetings with Tablet PCs327
 Getting Your E-mail As You Wander the Building329
 Getting Corporate Access in the Lunchroom329
 Setting Up Wireless Conference Rooms329
 Querying Your Corporate Database331
 Keeping in Touch at the Airport331
 Maintaining a Presence While Having Coffee332
 Using Bluetooth Phones in Your Car334
 Accessing a Wireless Network in Your Hotel335
 Using the Phone to Check Your Stocks338

Part VI: Appendixes339

Appendix A: Industry Trade Associations 341

Government Organizations341
 International Standards Organizations342
 Wireless-Related Organizations and Associations343
 Local Wireless Groups345
 Other Industry Associations346

Appendix B: Wireless Standards 347

802.1x347
 802.11348
 802.11a348
 802.11b348
 802.11c349
 802.11d349
 802.11e349
 802.11f349
 802.11g350
 802.11h350
 802.11i350
 802.11j350
 802.11k351
 802.11n351
 802.15351
 802.16352

Appendix C: The Fundamentals of Radio Frequency353

Radio Frequency	353
Behavior of Radio Waves	360
Gain	360
Loss	360
Reflection	361
Refraction	361
Diffraction	361
Scattering	361
Absorption	362
Free space loss	362
Fresnel zone	362
RF Units of Measure	362
Watt's that, you say?	363
I hear 'bels	363
RF Mathematics	365
Calculating decibels	365
Calculating path loss	367
Calculating antenna length	367
Calculating coaxial cable losses	368
Calculating the Fresnel zone	368
Calculating the measurements for a home-grown antenna	370

<i>Index</i>	371
---------------------------	------------