

# Contents

|                                                                        |             |
|------------------------------------------------------------------------|-------------|
| <b>Foreword</b>                                                        | <b>xxxi</b> |
| <b>Chapter 1 Implementing DNS<br/>in a Windows Server 2003 Network</b> | <b>1</b>    |
| Introduction                                                           | 2           |
| Reviewing the Domain Name System                                       | 3           |
| A Brief History of DNS                                                 | 3           |
| DNS Namespaces                                                         | 3           |
| The DNS Structure                                                      | 4           |
| DNS in Windows Operating Systems                                       | 5           |
| New Features in Windows Server 2003 DNS                                | 6           |
| Conditional Forwarders                                                 | 6           |
| Stub Zones                                                             | 6           |
| Active Directory Zone Replication                                      | 6           |
| Enhanced Security                                                      | 7           |
| Enhanced Round Robin                                                   | 7           |
| Enhanced Logging                                                       | 7           |
| DNSSEC                                                                 | 7           |
| EDNS0                                                                  | 8           |
| Resource Registration Restriction                                      | 8           |
| <b>2.1/2.1.1</b> Planning a DNS Namespace                              | 8           |
| <b>2.1.1</b> Resolution Strategies                                     | 9           |
| Choosing Your First DNS Domain Name                                    | 10          |
| Internal Domains versus Internet Domains                               | 11          |
| Naming Standards                                                       | 12          |
| DNS Namespace and Active Directory Integration                         | 17          |
| How DNS Integrates with Active Directory                               | 18          |
| Benefits of Integration                                                | 19          |

|                        |                                                                                     |           |
|------------------------|-------------------------------------------------------------------------------------|-----------|
| <b>2.1.2/2.1.5</b>     | Zone Replication .....                                                              | 20        |
|                        | Transfer Types .....                                                                | 23        |
| <b>2.1.5</b>           | Non-Active Directory Integrated Zones .....                                         | 25        |
|                        | Configuring Stub Zones .....                                                        | 30        |
| <b>2.1.5</b>           | Using Windows DNS with Third-Party DNS Solutions .....                              | 31        |
|                        | Active Directory Integrated Zones .....                                             | 32        |
|                        | Zone Storage .....                                                                  | 33        |
|                        | Scopes .....                                                                        | 36        |
| <b>2.1.3</b>           | DNS Forwarding .....                                                                | 38        |
|                        | Understanding Forwarders .....                                                      | 39        |
|                        | Forwarder Behavior .....                                                            | 39        |
|                        | Conditional Forwarders .....                                                        | 41        |
|                        | Forward-Only Servers .....                                                          | 43        |
|                        | Directing Queries Through Forwarders .....                                          | 44        |
| <b>2.1.4</b>           | DNS Security .....                                                                  | 45        |
|                        | DNS Security Guidelines .....                                                       | 45        |
|                        | Levels of DNS Security .....                                                        | 47        |
|                        | Low-Level Security .....                                                            | 48        |
|                        | Medium-Level Security .....                                                         | 48        |
|                        | High-Level Security .....                                                           | 49        |
|                        | Understanding and Mitigating DNS Threats .....                                      | 49        |
|                        | DNS Spoofing .....                                                                  | 50        |
|                        | Denial of Service .....                                                             | 50        |
|                        | DNS Footprinting .....                                                              | 52        |
|                        | Using Secure Updates .....                                                          | 52        |
|                        | The DNS Security Extensions Protocol .....                                          | 54        |
|                        | Using DNSSEC .....                                                                  | 56        |
|                        | Summary of Exam Objectives .....                                                    | 58        |
|                        | Exam Objectives Fast Track .....                                                    | 58        |
|                        | Exam Objectives Frequently Asked Questions .....                                    | 60        |
|                        | Self Test .....                                                                     | 62        |
|                        | Self Test Quick Answer Key .....                                                    | 67        |
|                        | <b>Chapter 2 Planning and Implementing an Active Directory Infrastructure</b> ..... | <b>69</b> |
|                        | Introduction .....                                                                  | 70        |
| <b>6.2/6.2.1/6.2.2</b> | Designing Active Directory .....                                                    | 70        |

|                                     |                                                         |     |
|-------------------------------------|---------------------------------------------------------|-----|
|                                     | Evaluating Your Environment .....                       | 70  |
|                                     | Creating a Checklist .....                              | 76  |
|                                     | Expect the Unexpected .....                             | 78  |
| <b>6.2/6.2.1/<br/>6.2.2</b>         | Creating an Active Directory Hierarchy .....            | 78  |
|                                     | Before You Start .....                                  | 80  |
| <b>6.2.1</b>                        | Forest Root .....                                       | 81  |
| <b>6.2.2</b>                        | Child Domains .....                                     | 83  |
|                                     | Domain Trees .....                                      | 84  |
| <b>6.2.3/6.2.4/<br/>6.2.5/6.2.6</b> | Configuring Active Directory .....                      | 85  |
| <b>6.2.3</b>                        | Application Directory Partitions .....                  | 85  |
|                                     | Managing Partitions .....                               | 87  |
|                                     | Replication .....                                       | 87  |
| <b>6.2.4</b>                        | Domain Controllers .....                                | 88  |
|                                     | Establishing Trusts .....                               | 94  |
| <b>6.2.6</b>                        | Types of Trusts .....                                   | 94  |
|                                     | Evaluating Connectivity .....                           | 98  |
|                                     | Setting Functionality .....                             | 98  |
| <b>6.2.5</b>                        | Forest Functional Levels .....                          | 98  |
|                                     | Domain Functional Levels .....                          | 100 |
| <b>6.1/6.1.1/<br/>6.1.2</b>         | Global Catalog Servers .....                            | 101 |
| <b>6.1</b>                          | Planning a Global Catalog Implementation .....          | 102 |
|                                     | When to Use a Global Catalog .....                      | 104 |
| <b>6.1.1</b>                        | Creating a Global Catalog Server .....                  | 105 |
|                                     | Universal Group Membership Caching .....                | 106 |
| <b>6.1.2</b>                        | When to Use Universal Group Membership Caching .....    | 106 |
|                                     | Configuring Universal Group Membership Caching .....    | 107 |
|                                     | Adding Attributes to Customize the Global Catalog ..... | 108 |
|                                     | Effects on Replication .....                            | 109 |
|                                     | Security Considerations .....                           | 109 |
|                                     | Summary of Exam Objectives .....                        | 110 |
|                                     | Exam Objectives Fast Track .....                        | 111 |
|                                     | Exam Objectives Frequently Asked Questions .....        | 112 |
|                                     | Self Test .....                                         | 114 |
|                                     | Self Test Quick Answer Key .....                        | 119 |

|                                                                                              |            |
|----------------------------------------------------------------------------------------------|------------|
| <b>Chapter 3 Managing and Maintaining an Active Directory Infrastructure</b>                 | <b>121</b> |
| Introduction .....                                                                           | 122        |
| Choosing a Management Method .....                                                           | 122        |
| Using a Graphical User Interface .....                                                       | 122        |
| Using the Command-line .....                                                                 | 124        |
| Defining Commands .....                                                                      | 124        |
| Using Scripting .....                                                                        | 125        |
| <b>7.1/7.1.1/Managing Forests and Domains</b> .....                                          | <b>126</b> |
| <b>7.1.2/7.1.3</b>                                                                           |            |
| <b>7.1</b> Managing Domains .....                                                            | 126        |
| Creating a New Child Domain .....                                                            | 127        |
| Managing a Different Domain .....                                                            | 131        |
| Removing a Domain .....                                                                      | 132        |
| Deleting Extinct Domain Metadata .....                                                       | 133        |
| Raising the Domain Functional Level .....                                                    | 134        |
| Managing Organizational Units .....                                                          | 136        |
| Assigning, Changing, or Removing Permissions on Active Directory Objects or Attributes ..... | 138        |
| Managing Domain Controllers .....                                                            | 139        |
| <b>7.1/7.1.2</b> Managing Forests .....                                                      | 142        |
| Creating a New Domain Tree .....                                                             | 143        |
| Raising the Forest Functional Level .....                                                    | 145        |
| Managing Application Directory Partitions .....                                              | 147        |
| <b>7.1.2</b> Managing the Schema .....                                                       | 149        |
| <b>7.1.1</b> Managing Trusts .....                                                           | 152        |
| Creating a Realm Trust .....                                                                 | 154        |
| Managing Forest Trusts .....                                                                 | 157        |
| Creating a Shortcut Trust .....                                                              | 158        |
| Creating an External Trust With the Windows Interface ...                                    | 160        |
| Selecting the Scope of Authentication for Users .....                                        | 161        |
| Verifying a Trust .....                                                                      | 162        |
| Removing a Trust .....                                                                       | 163        |
| <b>7.1.3</b> Managing UPN Suffixes .....                                                     | 164        |
| <b>7.2</b> Restoring Active Directory .....                                                  | 165        |
| <b>7.2.2</b> Performing a Nonauthoritative Restore .....                                     | 166        |
| <b>7.2.1</b> Performing an Authoritative Restore .....                                       | 170        |

|                                                  |     |
|--------------------------------------------------|-----|
| Understanding NTDSUTIL Restore Options .....     | 171 |
| Performing a Primary Restore .....               | 172 |
| Summary of Exam Objectives .....                 | 173 |
| Exam Objectives Fast Track .....                 | 173 |
| Exam Objectives Frequently Asked Questions ..... | 175 |
| Self Test .....                                  | 176 |
| Self Test Quick Answer Key .....                 | 182 |

## **Chapter 4 Implementing PKI in a Windows Server 2003 Network      183**

|                                                        |     |
|--------------------------------------------------------|-----|
| Introduction .....                                     | 184 |
| An Overview of Public Key Infrastructure .....         | 184 |
| Understanding Cryptology .....                         | 185 |
| Encryption .....                                       | 185 |
| Benefits of Public Key Infrastructure .....            | 188 |
| Privacy .....                                          | 189 |
| Authentication .....                                   | 189 |
| Nonrepudiation .....                                   | 190 |
| Integrity .....                                        | 190 |
| Components of Public Key Infrastructure .....          | 190 |
| Digital Certificates .....                             | 190 |
| X.509 .....                                            | 191 |
| Certificate Authorities .....                          | 193 |
| Single CA Models .....                                 | 194 |
| Hierarchical Models .....                              | 194 |
| Web-of-Trust Models .....                              | 196 |
| Certificate Policy and Practice Statements .....       | 197 |
| Publication Points .....                               | 198 |
| Certificate Revocation Lists .....                     | 199 |
| Simple CRLs .....                                      | 199 |
| Delta CRLs .....                                       | 199 |
| Online Certificate Status Protocol .....               | 200 |
| Certificate Trust Lists .....                          | 200 |
| Key Archival and Recovery .....                        | 200 |
| Hardware Key Storage versus Software Key Storage ..... | 201 |
| Standards .....                                        | 202 |
| Windows PKI Components .....                           | 204 |
| Microsoft Certificate Services .....                   | 204 |

|              |                                                                     |     |
|--------------|---------------------------------------------------------------------|-----|
|              | Active Directory .....                                              | 205 |
|              | CryptoAPI .....                                                     | 205 |
|              | CAPICOM .....                                                       | 205 |
| <b>5.2</b>   | Planning the Windows Server 2003 Public Key Infrastructure .....    | 206 |
|              | The Certificate Templates MMC Snap-in .....                         | 206 |
|              | Certificate Autoenrollment and Autorenewal for All Subjects .....   | 207 |
|              | Delta CRLs .....                                                    | 207 |
|              | Role-Based Administration .....                                     | 207 |
|              | Key Archival and Recovery .....                                     | 208 |
|              | Event Auditing .....                                                | 208 |
|              | Qualified Subordination .....                                       | 208 |
|              | The Process for Designing a PKI .....                               | 208 |
|              | Defining Certificate Requirements .....                             | 209 |
|              | Creating a Certification Authority Infrastructure .....             | 211 |
|              | Extending the CA Infrastructure .....                               | 211 |
|              | Configuring Certificates .....                                      | 212 |
|              | Creating a Certificate Management Plan .....                        | 212 |
| <b>5.2.1</b> | Types of Certificate Authorities .....                              | 213 |
|              | Online versus Offline Certificate Authorities .....                 | 213 |
|              | Root versus Subordinate Certificate Authorities .....               | 213 |
|              | Enterprise CA versus Standalone CAs .....                           | 214 |
| <b>5.2.2</b> | Enrollment and Distribution .....                                   | 215 |
|              | Web Enrollment .....                                                | 215 |
|              | Autoenrollment .....                                                | 217 |
| <b>5.2.3</b> | Using Smart Cards .....                                             | 218 |
|              | Defining a Business Need .....                                      | 218 |
|              | Smart Card Usage .....                                              | 218 |
|              | Smart Card Certificate Enrollment .....                             | 219 |
| <b>5.1</b>   | Configuring Public Key Infrastructure within Active Directory ..... | 219 |
|              | Web Enrollment Support .....                                        | 223 |
|              | Creating an Issuer Policy Statement .....                           | 225 |
|              | Managing Certificates .....                                         | 226 |
|              | Managing Certificate Templates .....                                | 226 |
|              | Using Autoenrollment .....                                          | 226 |
|              | Importing and Exporting Certificates .....                          | 230 |
|              | Revoking Certificates .....                                         | 231 |
|              | Configuring Public Key Group Policy .....                           | 232 |
|              | Automatic Certificate Request .....                                 | 232 |

|                                                         |            |
|---------------------------------------------------------|------------|
| Managing Certificate Trust Lists .....                  | 233        |
| Common Root Certificate Authorities .....               | 233        |
| Publishing the CRL .....                                | 234        |
| Scheduled Publication .....                             | 234        |
| Manual Publication .....                                | 234        |
| Backup and Restoring Certificate Services .....         | 234        |
| Summary of Exam Objectives .....                        | 238        |
| Exam Objectives Fast Track .....                        | 238        |
| Exam Objectives Frequently Asked Questions .....        | 240        |
| Self Test .....                                         | 241        |
| Self Test Quick Answer Key .....                        | 246        |
| <b>Chapter 5 Managing User Authentication</b> .....     | <b>247</b> |
| Introduction .....                                      | 248        |
| <b>8.1.2 Password Policies</b> .....                    | 248        |
| Creating an Extensive Defense Model .....               | 249        |
| Strong Passwords .....                                  | 250        |
| System Key Utility .....                                | 250        |
| Defining a Password Policy .....                        | 253        |
| Applying a Password Policy .....                        | 253        |
| Modifying a Password Policy .....                       | 256        |
| Applying an Account Lockout Policy .....                | 256        |
| Modifying an Account Lockout Policy .....               | 259        |
| Password Reset Disks .....                              | 259        |
| Creating a Password Reset Disk .....                    | 259        |
| Resetting a Local Account .....                         | 260        |
| <b>8.1 User Authentication</b> .....                    | 262        |
| Need for Authentication .....                           | 263        |
| Single Sign-on .....                                    | 263        |
| Interactive Logon .....                                 | 264        |
| Network Authentication .....                            | 264        |
| Authentication Types .....                              | 265        |
| Kerberos .....                                          | 265        |
| Understanding the Kerberos Authentication Process ..... | 266        |
| Secure Sockets Layer/Transport Layer Security .....     | 267        |
| NT LAN Manager .....                                    | 268        |
| Digest Authentication .....                             | 269        |
| Passport Authentication .....                           | 270        |

|                                                                      |                                                  |            |
|----------------------------------------------------------------------|--------------------------------------------------|------------|
|                                                                      | Internet Authentication Service .....            | 273        |
|                                                                      | Using IAS for Dialup and VPN .....               | 275        |
|                                                                      | Creating Remote Access Policies .....            | 278        |
|                                                                      | Using IAS for Wireless Access .....              | 281        |
|                                                                      | Creating a User Authorization Strategy .....     | 282        |
|                                                                      | Educating Users .....                            | 284        |
| <b>8.1.1</b>                                                         | Using Smart Cards .....                          | 283        |
|                                                                      | When to Use Smart Cards .....                    | 285        |
|                                                                      | Implementing Smart Cards .....                   | 285        |
|                                                                      | PKI and Certificate Authorities .....            | 286        |
|                                                                      | Setting Security Permissions .....               | 287        |
|                                                                      | Enrollment Stations .....                        | 288        |
|                                                                      | Issuing Enrollment Agent certificates .....      | 289        |
|                                                                      | Requesting an Enrollment Agent Certificate ..... | 290        |
|                                                                      | Enrolling Users .....                            | 291        |
|                                                                      | Installing a Smart Card Reader .....             | 292        |
|                                                                      | Issuing Smart Card Certificates .....            | 292        |
|                                                                      | Assigning Smart Cards .....                      | 294        |
|                                                                      | Logon Procedures .....                           | 294        |
|                                                                      | Revoking Smart Cards .....                       | 294        |
|                                                                      | Planning for Smart Card Support .....            | 296        |
|                                                                      | Summary of Exam Objectives .....                 | 297        |
|                                                                      | Exam Objectives Fast Track .....                 | 297        |
|                                                                      | Exam Objectives Frequently Asked Questions ..... | 299        |
|                                                                      | Self Test .....                                  | 300        |
|                                                                      | Self Test Quick Answer Key .....                 | 307        |
| <b>Chapter 6 Developing and Implementing a Group Policy Strategy</b> |                                                  | <b>309</b> |
|                                                                      | Introduction .....                               | 310        |
| <b>9.1</b>                                                           | Developing a Group Policy Strategy .....         | 310        |
| <b>9.1.1</b>                                                         | Planning Group Policy with RSoP .....            | 311        |
|                                                                      | Group Policy Overview .....                      | 311        |
|                                                                      | The Planning Process .....                       | 316        |
|                                                                      | Using RSoP .....                                 | 318        |
|                                                                      | Queries .....                                    | 324        |
| <b>9.1.2</b>                                                         | Planning the User Environment .....              | 326        |
| <b>9.1.3</b>                                                         | Planning the Computer Environment .....          | 328        |

|                                                               |                                                       |            |
|---------------------------------------------------------------|-------------------------------------------------------|------------|
| <b>9.2</b>                                                    | Configuring the User Environment .....                | 330        |
| <b>9.2.1</b>                                                  | Distributing Software .....                           | 332        |
| <b>9.2.2</b>                                                  | Autoenrolling User Certificates .....                 | 335        |
| <b>9.2.3</b>                                                  | Redirecting Folders .....                             | 336        |
| <b>9.2.4</b>                                                  | User Security .....                                   | 340        |
|                                                               | Summary of Exam Objectives .....                      | 342        |
|                                                               | Exam Objectives Fast Track .....                      | 342        |
|                                                               | Exam Objectives Frequently Asked Questions .....      | 344        |
|                                                               | Self Test .....                                       | 345        |
|                                                               | Self Test Quick Answer Key .....                      | 351        |
| <b>Chapter 7 Managing Group Policy in Windows Server 2003</b> |                                                       | <b>353</b> |
|                                                               | Introduction .....                                    | 354        |
|                                                               | Managing Applications .....                           | 354        |
|                                                               | Managing Security Policies .....                      | 358        |
| <b>10.1</b>                                                   | Troubleshooting Group Policies .....                  | 360        |
|                                                               | Troubleshooting the Group Policy Infrastructure ..... | 361        |
|                                                               | Troubleshooting Software Installation .....           | 363        |
|                                                               | Troubleshooting Policy Inheritance .....              | 364        |
|                                                               | Using RSoP .....                                      | 365        |
|                                                               | Using RSoP in Logging Mode .....                      | 366        |
|                                                               | Using RSoP to Troubleshoot Security Settings .....    | 373        |
|                                                               | Using GPRresult.exe .....                             | 373        |
|                                                               | Other Troubleshooting Techniques .....                | 375        |
|                                                               | Using the Group Policy Management Console .....       | 377        |
|                                                               | Key Features and Benefits .....                       | 379        |
|                                                               | Delegating Control of a GPO via GPMC .....            | 381        |
|                                                               | Using Security Filtering in GPMC .....                | 382        |
|                                                               | Using GPMC as a Troubleshooting Tool .....            | 383        |
|                                                               | Creating a Group Policy Modeling Report .....         | 385        |
|                                                               | Managing Windows 2000 Domains .....                   | 386        |
|                                                               | Summary of Exam Objectives .....                      | 387        |
|                                                               | Exam Objectives Fast Track .....                      | 387        |
|                                                               | Exam Objectives Frequently Asked Questions .....      | 389        |
|                                                               | Self Test .....                                       | 390        |
|                                                               | Self Test Quick Answer Key .....                      | 399        |

**Chapter 8 Securing a Windows Server 2003 Network 401**

|                           |                                              |     |
|---------------------------|----------------------------------------------|-----|
|                           | Introduction .....                           | 402 |
|                           | Understanding Server Roles .....             | 402 |
|                           | File Servers .....                           | 403 |
|                           | Print Servers .....                          | 403 |
|                           | Application Servers .....                    | 404 |
|                           | Mail Servers .....                           | 404 |
|                           | Terminal Servers .....                       | 405 |
|                           | Remote Access and VPN Servers .....          | 406 |
|                           | Domain Controllers .....                     | 407 |
|                           | Operations Masters .....                     | 407 |
|                           | Global Catalog Servers .....                 | 408 |
|                           | DNS Servers .....                            | 408 |
|                           | DHCP Servers .....                           | 409 |
|                           | WINS Servers .....                           | 409 |
|                           | Streaming Media Servers .....                | 409 |
| <b>1.1/1.2/<br/>1.2.1</b> | Securing Servers by Roles .....              | 418 |
|                           | Securing File Servers .....                  | 424 |
|                           | Securing Print Servers .....                 | 425 |
|                           | Securing Application Servers .....           | 426 |
|                           | Web Servers .....                            | 427 |
|                           | Securing Mail Servers .....                  | 429 |
|                           | Secure Password Authentication .....         | 432 |
|                           | Securing Terminal Servers .....              | 433 |
|                           | Securing Remote Access and VPN Servers ..... | 434 |
|                           | Securing Domain Controllers .....            | 436 |
|                           | Securing DNS Servers .....                   | 437 |
|                           | Securing DHCP Servers .....                  | 438 |
|                           | Known Security Issues .....                  | 438 |
|                           | Securing WINS Servers .....                  | 439 |
| <b>1.2.2</b>              | Security Templates .....                     | 443 |
|                           | Creating Security Templates .....            | 449 |
|                           | Best Practices .....                         | 449 |
|                           | Modifying Existing Templates .....           | 450 |
|                           | Applying Templates .....                     | 450 |

|                                                           |                                                      |            |
|-----------------------------------------------------------|------------------------------------------------------|------------|
| <b>4.3.1/4.3/</b>                                         | Securing Data Transmission .....                     | 459        |
| <b>4.3.1/4.3.2</b>                                        |                                                      |            |
|                                                           | Need for Network Security .....                      | 459        |
|                                                           | Planning for Secure Data Transmission .....          | 459        |
| <b>4.3.2</b>                                              | IP Security .....                                    | 460        |
|                                                           | Overview .....                                       | 460        |
|                                                           | Deploying IPSec .....                                | 460        |
|                                                           | IPSec Management Tools .....                         | 461        |
| <b>5.3</b>                                                | Implementing and Maintaining Security .....          | 469        |
| <b>5.3.1</b>                                              | Security Monitoring .....                            | 470        |
| <b>5.3.2</b>                                              | Change and Configuration Management .....            | 471        |
| <b>5.4</b>                                                | Updating the Infrastructure .....                    | 473        |
|                                                           | Types of Updates .....                               | 473        |
|                                                           | Service Packs .....                                  | 473        |
|                                                           | Hotfixes .....                                       | 474        |
|                                                           | Deploying and Managing Updates .....                 | 475        |
|                                                           | Analyzing Your Computers .....                       | 476        |
|                                                           | Windows Update .....                                 | 492        |
|                                                           | Windows Update Catalog .....                         | 496        |
|                                                           | Software Update Services and Automatic Updates ..... | 499        |
|                                                           | Summary of Exam Objectives .....                     | 508        |
|                                                           | Exam Objectives Fast Track .....                     | 509        |
|                                                           | Exam Objectives Frequently Asked Questions .....     | 511        |
|                                                           | Self Test .....                                      | 512        |
|                                                           | Self Test Quick Answer Key .....                     | 518        |
| <b>Chapter 9 Planning Security for a Wireless Network</b> |                                                      | <b>519</b> |
|                                                           | Introduction .....                                   | 520        |
|                                                           | Wireless Concepts .....                              | 520        |
|                                                           | Communication in a Wireless Network .....            | 521        |
|                                                           | Radio Frequency Communications .....                 | 521        |
|                                                           | Spread-Spectrum Technology .....                     | 522        |
|                                                           | How Wireless Works .....                             | 523        |
|                                                           | Wireless Network Architecture .....                  | 526        |
|                                                           | CSMA/CD and CSMA/CA .....                            | 527        |
|                                                           | Wireless Standards .....                             | 528        |
|                                                           | Windows Wireless Standards .....                     | 529        |
|                                                           | IEEE 802.11b .....                                   | 530        |

|            |                                                      |     |
|------------|------------------------------------------------------|-----|
|            | IEEE 802.11a .....                                   | 531 |
|            | IEEE 802.11g .....                                   | 531 |
|            | IEEE 802.20 .....                                    | 532 |
|            | Wireless Vulnerabilities .....                       | 532 |
|            | Passive Attacks .....                                | 533 |
|            | War Driving to Discover Wireless Networks .....      | 533 |
|            | Sniffing .....                                       | 535 |
|            | Active Attacks .....                                 | 535 |
|            | Spoofing and Unauthorized Access .....               | 536 |
|            | Denial of Service and Flooding Attacks .....         | 539 |
|            | Man-in-the-Middle Attacks on Wireless Networks ..... | 540 |
|            | Hijacking and Modifying a Wireless Network .....     | 541 |
|            | Jamming Attacks .....                                | 542 |
|            | Fundamentals of Wireless Security .....              | 543 |
|            | Understanding and Using the                          |     |
|            | Wireless Equivalent Privacy Protocol .....           | 543 |
|            | Creating Privacy with WEP .....                      | 545 |
|            | Understanding WEP Vulnerabilities .....              | 548 |
|            | Using IEEE 802.1X Authentication .....               | 549 |
|            | RC4 Vulnerabilities .....                            | 550 |
|            | Planning and Configuring Windows                     |     |
|            | Server 2003 for Wireless Technologies .....          | 550 |
| <b>4.2</b> | Planning and Implementing Your                       |     |
|            | Wireless Network with Windows Server 2003 .....      | 551 |
|            | Planning the Physical Layout .....                   | 552 |
|            | Planning the Network Topology .....                  | 553 |
|            | Planning for Network Identification .....            | 553 |
|            | Planning for Wireless Security .....                 | 554 |
| <b>4.2</b> | Implementing Wireless Security                       |     |
|            | on a Windows Server 2003 Network .....               | 555 |
|            | Using Group Policy for Wireless Networks .....       | 555 |
|            | Defining Preferred Networks .....                    | 560 |
|            | 802.1X Authentication .....                          | 563 |
|            | User Identification and Strong Authentication .....  | 565 |
|            | Dynamic Key Derivation .....                         | 565 |
|            | Mutual Authentication .....                          | 565 |
|            | Per-Packet Authentication .....                      | 566 |
|            | Using RSoP .....                                     | 566 |

|                  |                                                                             |            |
|------------------|-----------------------------------------------------------------------------|------------|
|                  | Logging Mode Queries .....                                                  | 567        |
|                  | Planning Mode Queries .....                                                 | 567        |
|                  | Assigning and Processing Wireless<br>Network Policies in Group Policy ..... | 568        |
|                  | Wireless Network Policy Information<br>Displayed in the RSoP Snap-in .....  | 568        |
|                  | Viewing Wireless Computer Assignments .....                                 | 573        |
| <b>4.2</b>       | Securing a Windows Server 2003 Wireless Network .....                       | 574        |
|                  | Using a Separate Subnet for Wireless Networks .....                         | 577        |
|                  | Securing Virtual Private Networks .....                                     | 578        |
|                  | Using IPSec .....                                                           | 579        |
|                  | Implementing Stub Networks for Secure Wireless Networks .....               | 579        |
|                  | Monitoring Wireless Activity .....                                          | 580        |
|                  | Implementing the Wireless Monitor Snap-in .....                             | 580        |
|                  | Monitoring Access Point Data .....                                          | 582        |
|                  | Using Wireless Logging for Security .....                                   | 583        |
|                  | Summary of Exam Objectives .....                                            | 584        |
|                  | Exam Objectives Fast Track .....                                            | 586        |
|                  | Exam Objectives Frequently Asked Questions .....                            | 588        |
|                  | Self Test .....                                                             | 589        |
|                  | Self Test Quick Answer Key .....                                            | 594        |
|                  | <b>Chapter 10 Remote Management</b> .....                                   | <b>595</b> |
|                  | Introduction .....                                                          | 596        |
| <b>4.1/4.1.1</b> | Remotely Administering Client Computers .....                               | 596        |
|                  | Remote Assistance .....                                                     | 597        |
|                  | Configuring the Client .....                                                | 597        |
|                  | Setting Group Policy for Remote Assistance .....                            | 598        |
|                  | Requesting Help Using Remote Assistance .....                               | 604        |
|                  | Providing Help Using Remote Assistance .....                                | 611        |
|                  | Blocking Remote Assistance Requests .....                                   | 613        |
|                  | Securing Remote Assistance .....                                            | 615        |
|                  | Firewalls and Remote Assistance .....                                       | 619        |
| <b>4.1.2</b>     | Terminal Services Remote Administration .....                               | 621        |
|                  | New Features in Terminal Services .....                                     | 621        |
|                  | Audio Redirection .....                                                     | 622        |
|                  | Group Policy Integration .....                                              | 622        |
|                  | Resolution and Color Enhancements .....                                     | 623        |

|                                                                    |            |
|--------------------------------------------------------------------|------------|
| Remote Desktop for Server Administration .....                     | 624        |
| Understanding Remote Desktop for Administration .....              | 625        |
| Configuring Remote Desktop for Administration .....                | 626        |
| Deploying Remote Desktop for Server Administration .....           | 633        |
| Using Remote Desktop for Administration .....                      | 633        |
| Remote Desktop Snap-in .....                                       | 635        |
| Summary of Exam Objectives .....                                   | 638        |
| Exam Objectives Fast Track .....                                   | 639        |
| Exam Objectives Frequently Asked Questions .....                   | 640        |
| Self Test .....                                                    | 642        |
| Self Test Quick Answer Key .....                                   | 648        |
| <b>Chapter 11 Disaster Recovery Planning and Prevention</b>        | <b>649</b> |
| Introduction .....                                                 | 650        |
| <b>3.2.3</b> Understanding Disaster Recovery .....                 | 650        |
| Planning for Disaster Recovery .....                               | 651        |
| <b>3.2.3</b> Windows Disaster Recovery .....                       | 653        |
| Startup Options .....                                              | 653        |
| Recovery Console .....                                             | 658        |
| <b>3.2.3</b> Automated System Recovery .....                       | 660        |
| <b>3.2/3.2.1/3.2.2</b> Backup and Recovery .....                   | 663        |
| Establishing a Plan .....                                          | 664        |
| Tape Rotation .....                                                | 664        |
| Offsite Storage .....                                              | 665        |
| <b>3.2.1</b> Backup Strategies .....                               | 666        |
| Volume Shadow Copy .....                                           | 666        |
| The Need for Periodic Testing .....                                | 671        |
| Security Considerations .....                                      | 671        |
| Using Windows Clustering .....                                     | 672        |
| Clustering Technologies .....                                      | 672        |
| Availability and Features .....                                    | 673        |
| <b>3.1/3.1.1/3.1.2</b> Planning a High-Availability Solution ..... | 674        |
| <b>3.1.1</b> Clustering Services .....                             | 674        |
| Considerations .....                                               | 675        |
| Typical Deployments .....                                          | 676        |

|              |                                                  |            |
|--------------|--------------------------------------------------|------------|
|              | Installing a Server Cluster .....                | 676        |
|              | Securing a Server Cluster .....                  | 676        |
| <b>3.1.2</b> | Network Load Balancing .....                     | 676        |
|              | Sizing a Load-Balanced Cluster .....             | 677        |
|              | Typical Deployment .....                         | 678        |
|              | Installing Network Load Balancing .....          | 679        |
|              | Securing Network Load Balancing .....            | 683        |
|              | Summary of Exam Objectives .....                 | 684        |
|              | Exam Objectives Fast Track .....                 | 684        |
|              | Exam Objectives Frequently Asked Questions ..... | 686        |
|              | Self Test .....                                  | 687        |
|              | Self Test Quick Answer Key .....                 | 691        |
|              | <b>Self Test Appendix</b>                        | <b>693</b> |
|              | <b>Index</b>                                     | <b>785</b> |