

# Contents

## Foreword

xxiii

## Chapter 1: Introduction to BCRAN and Cisco Remote Access Solutions

1

Introduction 2

WAN Connection Requirements 2

WAN Topology and Specifications 3

Connection Types 4

Dedicated Connections 4

Circuit-Switched Connections 6

Packet-Switched Connections 10

WAN Encapsulation Protocols 11

SDLC 11

HDLC 11

SLIP 12

PPP 12

X.25 12

Frame Relay 13

ATM 13

Selecting Cisco Access Servers and Routers 14

700 Series 14

800 Series 14

900 Series 15

1000 Series 15

1400 Series 15

1600 Series 15

1700 Series 16

2500 Series 16

2600 Series 16

3000 VPN Concentrators 16

3600 Series 16

|                                                          |    |
|----------------------------------------------------------|----|
| AS5000 Series                                            | 17 |
| 7100, 7200, and 7500 Series                              | 17 |
| Considerations Before Installing a Remote Access Network | 17 |
| Network Planning and Design                              | 18 |
| Proper Analysis                                          | 18 |
| Identifying Suitable Equipment for Each Site             | 21 |
| Staging and Testing                                      | 23 |
| Remote Access Network Implementation Considerations      | 24 |
| Change Control Procedures                                | 24 |
| Backout Plans                                            | 24 |
| Minimizing Network Interruption                          | 25 |
| Coordination of Resources                                | 25 |
| Verifying and Troubleshooting Network Installation       | 25 |
| Summary                                                  | 25 |
| FAQs                                                     | 26 |

## **Chapter 2: Configuring Asynchronous Remote Access Connections      29**

|                                            |    |
|--------------------------------------------|----|
| Introduction                               | 30 |
| Modem Overview                             | 30 |
| Digital Modems                             | 32 |
| Modem Signaling and Cabling                | 32 |
| Cisco Console and AUX Port Cabling         | 33 |
| Modem Modulation Standards                 | 34 |
| Error Control and Data Compression Methods | 35 |
| Automatic Repeat Request (ARQ)             | 36 |
| Microcom Networking Protocol (MNP)         | 36 |
| Link Access Procedure for Modems (LAPM)    | 37 |
| Data Compression Protocols                 | 37 |
| Configuring an Asynchronous Connection     | 38 |
| Router Configuration                       | 39 |
| Modem Configuration                        | 48 |
| Manual Configuration                       | 48 |
| Automatic Configuration                    | 51 |
| Chat Scripts                               | 55 |
| Providing Asynchronous Dial-in             |    |
| Terminal Services                          | 56 |
| Terminal Services                          | 57 |
| The Autocommand Feature                    | 66 |
| Menus                                      | 67 |
| EXEC Callback                              | 69 |
| Summary                                    | 73 |
| FAQs                                       | 74 |

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>Chapter 3: Using PPP to Provide Remote Network Access</b> | <b>75</b> |
| Introduction                                                 | 76        |
| PPP Overview                                                 | 76        |
| PPP Features                                                 | 77        |
| Multiple Protocols per Communication Line                    | 77        |
| Authentication                                               | 77        |
| Link Configuration and Negotiation                           | 77        |
| Error Detection                                              | 77        |
| Header Compression                                           | 78        |
| Bonding of Communications Links                              | 78        |
| LCP                                                          | 79        |
| NCP                                                          | 81        |
| PPP vs. SLIP and ARAP                                        | 81        |
| Relevant RFCs                                                | 82        |
| Configuring PPP                                              | 83        |
| Autoselect                                                   | 84        |
| PPP Addressing Methods                                       | 84        |
| PPP Link Control Options                                     | 86        |
| PAP and CHAP Authentication                                  | 86        |
| Authentication Failures                                      | 91        |
| PPP Callback                                                 | 91        |
| MSCB                                                         | 93        |
| PPP Compression                                              | 93        |
| MPPC                                                         | 93        |
| Compression Effects                                          | 94        |
| Multilink PPP                                                | 94        |
| Multichassis Multilink PPP                                   | 96        |
| Verifying and Troubleshooting PPP                            | 99        |
| PPP and Cisco Access Servers                                 | 99        |
| PPP and ISDN Connections between Cisco Routers               | 99        |
| Providing Remote Access Services for                         |           |
| Microsoft Windows Clients                                    | 104       |
| Microsoft Specific PPP Options                               | 104       |
| Windows 95 Clients                                           | 105       |
| Windows 98 Clients                                           | 105       |
| Windows NT4 Clients                                          | 107       |
| Windows 2000 Clients                                         | 108       |
| Troubleshooting Microsoft Windows Connections                | 110       |
| Summary                                                      | 111       |
| FAQs                                                         | 112       |

|                                                                                                     |                |
|-----------------------------------------------------------------------------------------------------|----------------|
| <b>Chapter 4: Utilizing Virtual Private Network (VPN) Technology for Remote Access Connectivity</b> | <b>113</b>     |
| Introduction                                                                                        | 114            |
| VPN Technology                                                                                      | 114            |
| ISAKMP & IKE                                                                                        | 114            |
| IPSec                                                                                               | 115            |
| DES, Triple Pass DES & 3DES                                                                         | 116            |
| VPN Operation                                                                                       | 116            |
| Cisco VPN Terminology                                                                               | 117            |
| Site-to-Site VPN                                                                                    | 119            |
| An Intranet Solution                                                                                | 119            |
| Configuring ISAKMP/IKE                                                                              | 120            |
| Configuring IPSec                                                                                   | 123            |
| An Extranet Solution                                                                                | 126            |
| Remote Access VPN                                                                                   | 130            |
| Configuring IPSec on the Network Access Server                                                      | 131            |
| Service Provider Solution                                                                           | 135            |
| Configuring ISAKMP                                                                                  | 136            |
| Configuring IPSec                                                                                   | 137            |
| Configuring the VPN Client                                                                          | 138            |
| Verifying and Debugging VPN Operation                                                               | 140            |
| Advantages and Disadvantages of VPN                                                                 | 143            |
| Cisco's VPN Solutions                                                                               | 145            |
| FW Solution (HW Accelerator)                                                                        | 145            |
| 3000 Series Product Line                                                                            | 145            |
| Traditional Router with FW Feature Set                                                              | 147            |
| Policy Manager 2.x (VPN Configuration and Management)                                               | 147            |
| Summary                                                                                             | 148            |
| FAQs                                                                                                | 149            |
| <br><b>Chapter 5: Using ISDN and DDR to Enhance Remote Access Connectivity</b>                      | <br><b>151</b> |
| Introduction                                                                                        | 152            |
| ISDN Overview                                                                                       | 152            |
| Basic Rate Interface (BRI)                                                                          | 154            |
| BRI Call Setup                                                                                      | 154            |
| BRI Reference Points and Functional Groups                                                          | 155            |
| Primary Rate Interface (PRI)                                                                        | 156            |
| PRI Reference Points and Functional Groups                                                          | 157            |
| ISDN Protocol Layers                                                                                | 157            |
| U-plane                                                                                             | 158            |
| C-plane                                                                                             | 159            |

|                                             |     |
|---------------------------------------------|-----|
| ISDN Call Setup and Teardown                | 159 |
| Dial-on-Demand Routing (DDR)                | 159 |
| Interesting Traffic                         | 161 |
| Topologies                                  | 162 |
| Point-to-Point Topology                     | 162 |
| Fully Meshed Topology                       | 162 |
| Hub-and-Spoke Topology                      | 164 |
| Dialer Interfaces                           | 165 |
| Dialer Profiles                             | 166 |
| Dialer Rotary Groups                        | 166 |
| Dialer Addressing                           | 166 |
| Dialer Mapping                              | 166 |
| Encapsulation                               | 167 |
| Supported Interfaces                        | 167 |
| Configuring ISDN and DDR                    | 168 |
| Caller ID Screening                         | 179 |
| Routing Issues with DDR                     | 179 |
| Static and Default Routes                   | 180 |
| Snapshot Routing                            | 180 |
| OSPF On-demand Circuits                     | 181 |
| Route Redistribution                        | 182 |
| Monitoring and Troubleshooting ISDN and DDR | 182 |
| Monitoring the ISDN Interface               | 182 |
| Monitoring the Dialer                       | 186 |
| Monitoring PPP Multilink                    | 188 |
| Monitoring Snapshot Routing                 | 189 |
| Troubleshooting ISDN and DDR                | 190 |
| Walkthrough                                 | 195 |
| Summary                                     | 203 |
| FAQs                                        | 205 |

## **Chapter 6: Enabling Dial-on-Demand Routing (DDR) 209**

|                                  |     |
|----------------------------------|-----|
| Introduction                     | 210 |
| Dialer Rotary Groups             | 210 |
| Configuring Dialer Rotary Groups | 210 |
| Dialer Profiles                  | 213 |
| Physical Interface               | 214 |
| Dialer List                      | 214 |
| Dialer Interface                 | 214 |
| Dialer Pool                      | 214 |
| Map Class                        | 214 |
| Configuring Dialer Profiles      | 215 |

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| Virtual Profiles                                                                | 217 |
| Case 1: Create a Virtual Profile Using the Virtual Template                     | 218 |
| Configure a Virtual Profile Using Virtual Templates                             | 218 |
| Case 2: Create a Virtual Profile Using the AAA Server                           | 219 |
| Configure a Virtual Profile Using the AAA Server                                | 220 |
| Case 3: Create a Virtual Profile Using Both the Virtual Template and AAA Server | 221 |
| Configure a Virtual Profile Using Both the Virtual Template and AAA Server      | 222 |
| Fine Tuning Connections                                                         | 223 |
| Dialer Lists                                                                    | 223 |
| Dialer Timers                                                                   | 225 |
| Walkthrough                                                                     | 226 |
| Summary                                                                         | 231 |
| FAQs                                                                            | 232 |

## **Chapter 7: Configuring and Backing Up Permanent Connections 233**

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| Introduction                                                               | 234 |
| Configuring Point-to-Point Connections                                     | 234 |
| X.25 Connections                                                           | 237 |
| X.25 Overview                                                              | 237 |
| Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) | 238 |
| Frames in X.25                                                             | 238 |
| X.25 Virtual Circuits                                                      | 240 |
| X.25 Call Setup and Disconnection                                          | 240 |
| Configuring X.25                                                           | 241 |
| Verifying and Troubleshooting X.25 Connections                             | 245 |
| Frame Relay Connections                                                    | 248 |
| Frame Relay Overview                                                       | 248 |
| Frame Relay Topologies                                                     | 253 |
| Split Horizon and Poison Reverse                                           | 255 |
| Subinterfaces                                                              | 257 |
| Configuring Frame Relay                                                    | 259 |
| Verifying and Troubleshooting Frame Relay                                  | 263 |
| Loopback Tests                                                             | 266 |
| Local Loopback                                                             | 266 |
| Remote Loopback                                                            | 267 |
| Frame Relay Traffic Shaping (FRTS)                                         | 271 |
| Enable Frame Relay Traffic Shaping (FRTS) on the Interface                 | 272 |

|                                                  |     |
|--------------------------------------------------|-----|
| Configuring Traffic Shaping                      | 272 |
| Verifying Traffic Shaping                        | 280 |
| ATM Connections                                  | 290 |
| ATM Overview                                     | 290 |
| ATM Packet Format                                | 290 |
| ATM Adaptation Layer (AAL)                       | 291 |
| ATM Virtual Circuits                             | 292 |
| PVC Mapping and Circuit Buildup                  | 292 |
| Configuring ATM                                  | 293 |
| Verifying and Troubleshooting ATM Connections    | 297 |
| The debug atm packet Command                     | 300 |
| The debug atm state Command                      | 302 |
| The debug atm ilmi Command                       | 303 |
| Backing up Permanent Connections                 | 305 |
| Backup Interface                                 | 305 |
| The backup load Command                          | 308 |
| Floating Static Routes and Default Routes        | 309 |
| Frame Relay Configuration with ISDN backup       | 310 |
| Dialer Watch                                     | 315 |
| Configuring a Dialer Profile                     | 316 |
| Verifying and Troubleshooting Backup Connections | 317 |
| Routing Issues                                   | 321 |
| Redundant Hardware and Links/Design              |     |
| and Performance Issues                           | 321 |
| Load Balancing                                   | 322 |
| Summary                                          | 323 |
| FAQs                                             | 324 |

## **Chapter 8: Securing your Remote Access Network 325**

|                                            |     |
|--------------------------------------------|-----|
| Introduction                               | 326 |
| What is a Firewall?                        | 326 |
| Cisco IOS Firewall Feature Set             | 327 |
| Firewall Feature Set Benefits and Features | 327 |
| Phase I                                    | 327 |
| Phase I+                                   | 327 |
| Phase II (Full Features)                   | 327 |
| Key Benefits                               | 328 |
| AAA Overview                               | 328 |
| AAA Servers                                | 329 |
| CiscoSecure                                | 330 |
| Authentication                             | 331 |
| Authorization                              | 331 |

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| Accounting                                                                 | 332 |
| Method-Lists                                                               | 332 |
| Security Protocols                                                         | 333 |
| Remote Authentication Dial-in User Service (RADIUS)                        | 333 |
| Terminal Access Controller Access Control System Plus (TACACS+)            | 333 |
| Comparing TACACS+ and RADIUS                                               | 334 |
| Using RADIUS and TACACS+ for AAA Services                                  | 336 |
| Configuring AAA                                                            | 336 |
| Enabling AAA                                                               | 336 |
| Configuring the RADIUS or TACACS+ Parameters                               | 336 |
| Configuring TACACS+ Parameters                                             | 337 |
| Configuring RADIUS Parameters                                              | 338 |
| Configuring AAA Authentication                                             | 339 |
| The aaa authentication login Command                                       | 339 |
| The aaa authentication ppp Command                                         | 340 |
| The aaa authentication enable default Command                              | 341 |
| Configuring AAA Authorization                                              | 342 |
| Configuring AAA Accounting                                                 | 344 |
| Virtual Profiles and AAA                                                   | 346 |
| Scenario 1: Virtual Profiles Using Virtual Templates                       | 347 |
| Scenario 2: Virtual Profiles Using AAA Configuration                       | 348 |
| Scenario 3: Virtual Profiles Using Virtual Templates and AAA Configuration | 349 |
| Configuring Virtual Profiles                                               | 349 |
| Configuring Virtual Profiles Using Virtual Templates                       | 349 |
| Configuring virtual Profiles Using AAA Configuration                       | 352 |
| Configuring Virtual Profiles Using Virtual Templates and AAA Configuration | 352 |
| Per-User Configuration Example                                             | 354 |
| User 'Remote' RADIUS Configuration                                         | 354 |
| Network Access Server Configuration (central)                              | 355 |
| Monitoring and Verifying AAA Access Control                                | 358 |
| AAA Debug And Show Commands                                                | 358 |
| Walkthrough                                                                | 362 |
| Summary                                                                    | 368 |
| FAQs                                                                       | 368 |

## **Chapter 9: Optimizing Network Performance with Queuing and Compression      371**

|                     |     |
|---------------------|-----|
| Introduction        | 372 |
| Network Performance | 372 |
| Queuing Overview    | 373 |

|                                                          |     |
|----------------------------------------------------------|-----|
| Queuing Methods and Configuration                        | 373 |
| First-in, First-out Queuing (FIFO)                       | 374 |
| Weighted Fair Queuing (WFQ)                              | 375 |
| Priority Queuing (PQ)                                    | 383 |
| Custom Queuing (CQ)                                      | 387 |
| Class-Based Weighted Fair Queuing (CBWFQ)                | 390 |
| Selecting a Cisco IOS Queuing Method                     | 392 |
| Verifying Queuing Operation                              | 395 |
| Weighted Random Early Detection (WRED) Overview          | 395 |
| Tail Drop                                                | 396 |
| Weighted Random Early Detection (WRED)                   | 396 |
| Flow-based WRED                                          | 396 |
| Data Compression Overview                                | 397 |
| The Data Compression Mechanism                           | 397 |
| Header Compression                                       | 398 |
| Link and Payload Compression                             | 399 |
| Per-Interface Compression (Link Compression)             | 401 |
| Per-Virtual Circuit Compression<br>(Payload Compression) | 401 |
| Hardware Compression                                     | 401 |
| Selecting a Cisco IOS Compression Method                 | 402 |
| Verifying Compression Operation                          | 403 |
| Summary                                                  | 403 |
| FAQs                                                     | 404 |

## **Chapter 10: Requirements for Network Address Translation in Remote Access Networks 407**

|                                                 |     |
|-------------------------------------------------|-----|
| Introduction                                    | 408 |
| NAT Overview                                    | 408 |
| Terminology                                     | 409 |
| NAT Operation                                   | 411 |
| Traffic Types Supported                         | 412 |
| NAT Commands                                    | 413 |
| Translate Inside Source Addresses               | 414 |
| Dynamic Translation                             | 414 |
| Configuring Dynamic NAT                         | 416 |
| Dynamic NAT Translation Screen Captures         | 418 |
| Address Overloading                             | 421 |
| Configuring Address Overloading                 | 423 |
| Address Overloading Screen Captures             | 424 |
| Static Translation                              | 425 |
| Configuring Static NAT Translations             | 427 |
| Static NAT Translation Output                   | 428 |
| Dual Address Translation (Overlapping Networks) | 430 |

|                                               |     |
|-----------------------------------------------|-----|
| Configuring Overlapping Networks              | 434 |
| TCP Load Distribution                         | 436 |
| Configuring TCP Load Distribution             | 438 |
| Output Showing TCP Load Distribution          | 440 |
| Changing NAT Timeouts                         | 443 |
| NAT to an ISP                                 | 444 |
| NAT to an ISP using Easy IP                   | 445 |
| Easy IP Operation                             | 446 |
| PAT to an ISP Using a Cisco 700 Series Router | 449 |
| Walkthrough                                   | 450 |
| Summary                                       | 453 |
| FAQs                                          | 454 |

|                                                                         |            |
|-------------------------------------------------------------------------|------------|
| <b>Chapter 11: Private Addressing and Subnetting<br/>Large Networks</b> | <b>457</b> |
| Introduction                                                            | 458        |
| Strategies to Conserve Addresses                                        | 458        |
| Classless Inter-Domain Routing (CIDR)                                   | 459        |
| Variable-Length Subnet Mask (VLSM)                                      | 459        |
| Private Addresses                                                       | 459        |
| Addressing Economics                                                    | 460        |
| An Appeal                                                               | 462        |
| Public vs Private Address Spaces                                        | 463        |
| Can I Pick My Own?                                                      | 463        |
| RFC 1918—Private Network Addresses                                      | 465        |
| The Three Address Blocks                                                | 465        |
| Considerations                                                          | 466        |
| Which to Use When                                                       | 467        |
| Strategy for Subnetting a Class A Private Network                       | 468        |
| The Network                                                             | 469        |
| The Strategy                                                            | 470        |
| Address Assignment                                                      | 471        |
| The Headquarters LANs                                                   | 471        |
| The WAN Links from Headquarters to the<br>Distribution Centers          | 472        |
| The Distribution Center LANs                                            | 472        |
| The Store LANs                                                          | 473        |
| Results                                                                 | 474        |
| BGP Requirements                                                        | 475        |
| IBGP and EBGP Requirements                                              | 479        |
| Loopback Interfaces                                                     | 481        |
| Summary                                                                 | 482        |
| FAQs                                                                    | 482        |

|                                                                 |            |
|-----------------------------------------------------------------|------------|
| <b>Appendix: Implementing the Windows 2000 Servers</b>          | <b>485</b> |
| Introduction                                                    | 486        |
| Installing Windows 2000                                         | 487        |
| Overview of a Scripted Installation                             | 488        |
| Overview of Disk Duplication Methods                            | 491        |
| SYSPREP                                                         | 491        |
| RIPREP                                                          | 492        |
| Windows 2000 Setup Phases                                       | 495        |
| WINNT Phase                                                     | 496        |
| Text Mode                                                       | 496        |
| GUI Mode                                                        | 496        |
| Installing the Active Directory                                 | 497        |
| Which Domain First?                                             | 498        |
| Which Server First?                                             | 499        |
| DCPromo                                                         | 500        |
| Installing the Recovery Console                                 | 503        |
| Populating a Domain with Organizational Units (OUs) and Objects | 504        |
| Creating an OU                                                  | 505        |
| Create an OU for Hidden Objects                                 | 505        |
| Delegating Authority                                            | 506        |
| Creating a User Account                                         | 508        |
| Creating Groups                                                 | 511        |
| Publishing Printers                                             | 513        |
| Publishing Folders                                              | 514        |
| Applying a Group Policy                                         | 515        |
| Setting Up Sites                                                | 516        |
| Installing and Configuring Windows 2000 Components              | 519        |
| Configuring DNS                                                 | 519        |
| Configuring the Distributed File System                         | 521        |
| Public Key Infrastructure                                       | 522        |
| Internet Information Services                                   | 525        |
| Asynchronous Transfer Mode                                      | 527        |
| Terminal Services                                               | 527        |
| Configuring Routing and Remote Access Services                  | 534        |
| DHCP                                                            | 535        |
| WINS                                                            | 537        |
| Case Studies                                                    | 537        |
| ABC Chemical Company                                            | 537        |
| West Coast Accounting                                           | 539        |
| Summary                                                         | 540        |
| FAQs                                                            | 544        |
| <b>Index</b>                                                    | <b>547</b> |