CCNA Security
Official Exam Certification Guide

Master the IINS 640-553 exam with this official study guide
Assess your knowledge with chapter-opening quizzes
Review key concepts with Exam Preparation Tasks
Practice with realistic exam questions on the CD-ROM

Michael Watkins
Kevin Wallace, CCIE® No. 7945
CCNA Security
Official Exam Certification Guide

Michael Watkins
Kevin Wallace, CCIE No. 7945

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA
About the Authors

**Michael Watkins**, CCNA/CCNP/CCVP/CCSP, is a full-time senior technical instructor with SkillSoft Corporation. With 13 years of network management, training, and consulting experience, he has worked with organizations such as Kraft Foods, Johnson and Johnson, Raytheon, and the U.S. Air Force to help them implement and learn about the latest network technologies. In addition to holding more than 20 industry certifications in the areas of networking and programming technologies, he holds a bachelor of arts degree from Wabash College.

**Kevin Wallace**, CCIE No. 7945, is a certified Cisco instructor working full time for SkillSoft, where he teaches courses in the Cisco CCSP, CCVP, and CCNP tracks. With 19 years of Cisco networking experience, he has been a network design specialist for the Walt Disney World Resort and a network manager for Eastern Kentucky University. He holds a bachelor of science degree in electrical engineering from the University of Kentucky. He is also a CCVP, CCSP, CCNP, and CCDP, with multiple Cisco security and IP communications specializations.

About the Technical Reviewers

**Ryan Lindfield** is an instructor and network administrator with Boson. He has more than ten years of network administration experience. He has taught many courses designed for CCNA, CCNP, and CCSP preparation, among others. He has written many practice exams and study guides for various networking technologies. He also works as a consultant, where among his tasks are installing and configuring Cisco routers, switches, VPNs, IDSs, and firewalls.

**Anthony Sequeira**, CCIE No. 15626, completed the CCIE in Routing and Switching in January 2006. He is currently pursuing the CCIE in Security. For the past 15 years, he has written and lectured to massive audiences about the latest in networking technologies. He is currently a senior technical instructor and certified Cisco Systems instructor for SkillSoft. He lives with his wife and daughter in Florida. When he is not reading about the latest Cisco innovations, he is exploring the Florida skies in a Cessna.
Dedications

For their support and encouragement throughout this process, I dedicate my contribution to this book to my family.
—Michael

I dedicate my contribution to this book to my best friend (and wife of 14 years), Vivian.
—Kevin

Acknowledgments

From Michael Watkins:

I want to thank the team at Cisco Press for their direction and support throughout the writing process. For their support and encouragement throughout this process, I wish to thank and acknowledge Tom Warrick and the instructor team at SkillSoft. I also wish to thank Kevin Wallace, who brought his talent and experience to this project and was an enormous help each step of the way.

Finally, I want to thank my family for their continued support through this project, especially my children, Abigail, Matthew, and Addison, who are always an inspiration in all that I do.

From Kevin Wallace:

I wish to express my sincere thanks to the team at Cisco Press. You guys are a class act, and I’m honored to be associated with you. Also, I give a huge thank-you to Michael Watkins for inviting me to participate in writing this book.

On a personal note, I know all the good things in my life come from above, and I thank God for those blessings. Also, my wife, Vivian, and my daughters, Sabrina and Stacie, have become accustomed to seeing me attached to my laptop over the past few months. Thank you for your love and support throughout this process.
This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:
- Complete the brief registration form.
- Enter the coupon code 35C1-WTME-WMIT-F7ED-JNPY

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.
Contents at a Glance

| Foreword | xxvi |
| Introduction | xxvii |

**Part I  Network Security Concepts  3**
- Chapter 1  Understanding Network Security Principles  5
- Chapter 2  Developing a Secure Network  45
- Chapter 3  Defending the Perimeter  77
- Chapter 4  Configuring AAA  111
- Chapter 5  Securing the Router  155

**Part II  Constructing a Secure Infrastructure  205**
- Chapter 6  Securing Layer 2 Devices  207
- Chapter 7  Implementing Endpoint Security  251
- Chapter 8  Providing SAN Security  279
- Chapter 9  Exploring Secure Voice Solutions  297
- Chapter 10  Using Cisco IOS Firewalls to Defend the Network  319
- Chapter 11  Using Cisco IOS IPS to Secure the Network  385

**Part III  Extending Security and Availability with Cryptography and VPNs  427**
- Chapter 12  Designing a Cryptographic Solution  429
- Chapter 13  Implementing Digital Signatures  463
- Chapter 14  Exploring PKI and Asymmetric Encryption  491
- Chapter 15  Building a Site-to-Site IPsec VPN Solution  523

**Part IV  Final Preparation  589**
- Chapter 16  Final Preparation  577

**Part V  Appendixes  583**
- Appendix A  Answers to “Do I Know This Already?” Questions  585
- Appendix B  Glossary  595
- Appendix C  CCNA Security Exam Updates: Version 1.0  617
- Appendix D  Memory Tables  (CD only)
- Appendix E  Memory Tables Answer Key  (CD only)
- Index  620
Contents

Foreword xxvi
Introduction xxvii

Part I Network Security Concepts 3

Chapter 1 Understanding Network Security Principles 5

“Do I Know This Already?” Quiz 5

Foundation Topics 9

Exploring Security Fundamentals 9

Why Network Security Is a Necessity 9

Types of Threats 9

Scope of the Challenge 10

Nonsecured Custom Applications 11

The Three Primary Goals of Network Security 12

Confidentiality 12

Integrity 12

Availability 13

Categorizing Data 13

Classification Models 13

Classification Roles 15

Controls in a Security Solution 16

Responding to a Security Incident 17

Legal and Ethical Ramifications 18

Legal Issues to Consider 19

Understanding the Methods of Network Attacks 20

Vulnerabilities 20

Potential Attackers 21

The Mind-set of a Hacker 23

Defense in Depth 24

Understanding IP Spoofing 27

Launching a Remote IP Spoofing Attack with IP Source Routing 28

Launching a Local IP Spoofing Attack Using a Man-in-the-Middle Attack 29

Protecting Against an IP Spoofing Attack 30

Understanding Confidentiality Attacks 31

Understanding Integrity Attacks 33

Understanding Availability Attacks 36

Best-Practice Recommendations 40

Exam Preparation Tasks 41

Review All the Key Topics 41

Complete the Tables and Lists from Memory 42

Definition of Key Terms 42
Exam Preparation Tasks  201
Review All the Key Topics  201
Complete the Tables and Lists from Memory  201
Definition of Key Terms  202
Command Reference to Check Your Memory  202

Part II  Constructing a Secure Infrastructure  205

Chapter 6  Securing Layer 2 Devices  207

“Do I Know This Already?” Quiz  207

Foundation Topics  211
Defending Against Layer 2 Attacks  211

  Review of Layer 2 Switch Operation  211
  Basic Approaches to Protecting Layer 2 Switches  212
  Preventing VLAN Hopping  213
    Switch Spoofing  213
    Double Tagging  214
  Protecting Against an STP Attack  215
  Combating DHCP Server Spoofing  218
  Using Dynamic ARP Inspection  220
  Mitigating CAM Table Overflow Attacks  222
  Spoofing MAC Addresses  223

Additional Cisco Catalyst Switch Security Features  225

  Using the SPAN Feature with IDS  226
  Enforcing Security Policies with VACLs  226
  Isolating Traffic Within a VLAN Using Private VLANs  227
  Traffic Policing  228
    Notifying Network Managers of CAM Table Updates  228

Port Security Configuration  228
Configuration Recommendations  231

Cisco Identity-Based Networking Services  232

  Introduction to Cisco IBNS  232
  Overview of IEEE 802.1x  234
  Extensible Authentication Protocols  236
    EAP-MD5  236
    EAP-TLS  236
    PEAP (MS-CHAPv2)  238
    EAP-FAST  239
    Combining IEEE 802.1x with Port Security Features  239
    Using IEEE 802.1x for VLAN Assignment  240
    Configuring and Monitoring IEEE 802.1x  243

Exam Preparation Tasks  246
Review All the Key Topics  246
Complete the Tables and Lists from Memory  246
Definition of Key Terms  247
Command Reference to Check Your Memory  247
Chapter 7  Implementing Endpoint Security  251

“Do I Know This Already?” Quiz  251
Foundation Topics  254
Examining Endpoint Security  254
  Defining Endpoint Security  254
    Examining Operating System Vulnerabilities  255
    Examining Application Vulnerabilities  257
  Understanding the Threat of Buffer Overflows  258
    Buffer Overflow Defined  259
    The Anatomy of a Buffer Overflow Exploit  259
    Understanding the Types of Buffer Overflows  260
  Additional Forms of Attack  261
Securing Endpoints with Cisco Technologies  265
  Understanding IronPort  265
    The Architecture Behind IronPort  266
  Examining the Cisco NAC Appliance  266
  Working with the Cisco Security Agent  268
    Understanding Cisco Security Agent Interceptors  269
    Examining Attack Response with the Cisco Security Agent  272
Best Practices for Securing Endpoints  273
  Application Guidelines  274
  Apply Application Protection Methods  274
Exam Preparation Tasks  276
Review All the Key Topics  276
Complete the Tables and Lists from Memory  277
Definition of Key Terms  277

Chapter 8  Providing SAN Security  279

“Do I Know This Already?” Quiz  279
Foundation Topics  282
Overview of SAN Operations  282
  Fundamentals of SANs  282
  Organizational Benefits of SAN Usage  283
  Understanding SAN Basics  284
  Fundamentals of SAN Security  285
    Classes of SAN Attacks  286
Implementing SAN Security Techniques  287
  Using LUN Masking to Defend Against Attacks  287
  Examining SAN Zoning Strategies  288
    Examining Soft and Hard Zoning  288
    Understanding World Wide Names  289
  Defining Virtual SANs  290
    Combining VSANs and Zones  291
Chapter 9 Exploring Secure Voice Solutions 297

“Do I Know This Already?” Quiz 297

Foundation Topics 301

Defining Voice Fundamentals 301
  Defining VoIP 301
  The Need for VoIP 302
  VoIP Network Components 303
  VoIP Protocols 305

Identifying Common Voice Vulnerabilities 307
  Attacks Targeting Endpoints 307
  VoIP Spam 308
  Vishing and Toll Fraud 308
  SIP Attack Targets 309

Securing a VoIP Network 310
  Protecting a VoIP Network with Auxiliary VLANs 310
  Protecting a VoIP Network with Security Appliances 311
  Hardening Voice Endpoints and Application Servers 313
  Summary of Voice Attack Mitigation Techniques 316

Exam Preparation Tasks 317

Chapter 10 Using Cisco IOS Firewalls to Defend the Network 319

“Do I Know This Already?” Quiz 319

Foundation Topics 323

Exploring Firewall Technology 323
  The Role of Firewalls in Defending Networks 323
  The Advance of Firewall Technology 325
  Transparent Firewalls 326
  Application Layer Firewalls 327

Exam Preparation Tasks 329
Chapter 11 Using Cisco IOS IPS to Secure the Network 385

“Do I Know This Already?” Quiz 385

Foundation Topics 388

Examining IPS Technologies 388

IDS Versus IPS 388

IDS and IPS Device Categories 389

Detection Methods 389

Network-Based Versus Host-Based IPS 391

Deploying Network-Based and Host-Based Solutions 394

IDS and IPS Appliances 395

Cisco IDS 4215 Sensor 396

Cisco IPS 4240 Sensor 397

Cisco IPS 4255 Sensor 397

Cisco IPS 4260 Sensor 397

Signatures 398

Exploit Signatures 398

Connection Signatures 399

String Signatures 399

Denial-of-Service Signatures 399

Signature Definition Files 399

Alarms 400

Using SDM to Configure Cisco IOS IPS 401

Launching the Intrusion Prevention Wizard 401

IPS Policies Wizard 404

Creating IPS Rules 410

Manipulating Global IPS Settings 417

Signature Configuration 419

Exam Preparation Tasks 425

Review All the Key Topics 425

Complete the Tables and Lists from Memory 425

Definition of Key Terms 425
Chapter 13 Implementing Digital Signatures 463

“Do I Know This Already?” Quiz 463

Foundation Topics 466

Examining Hash Algorithms 466

Exploring Hash Algorithms and HMACs 466

Anatomy of a Hash Function 467

Application of Hash Functions 467

Cryptographic Hash Functions 468

Application of Cryptographic Hashes 469

HMAC Explained 470

MD5 Features and Functionality 471

Origins of MD5 472

Vulnerabilities of MD5 473

Usage of MD5 475

SHA-1 Features and Functionality 475

Overview of SHA-1 476

Vulnerabilities of SHA-1 477

Usage of SHA-1 478

Using Digital Signatures 478

Understanding Digital Signatures 480

Digital Signature Scheme 483

Authentication and Integrity 483

Examining RSA Signatures 483

Exploring the History of RSA 484

Understanding How RSA Works 484

Encrypting and Decrypting Messages with RSA 485

Signing Messages with RSA 485

Vulnerabilities of RSA 486

Exploring the Digital Signature Standard 487

Using the DSA Algorithm 487

Exam Preparation Tasks 488

Review All the Key Topics 488

Complete the Tables and Lists from Memory 489

Definition of Key Terms 489
Chapter 14 Exploring PKI and Asymmetric Encryption  491

“Do I Know This Already?” Quiz  491

Foundation Topics  494

Understanding Asymmetric Algorithms  494

Exploring Asymmetric Encryption Algorithms  494

Using Public-Key Encryption to Achieve Confidentiality  495

Providing Authentication with a Public Key  496

Understanding the Features of the RSA Algorithm  497

Working with RSA Digital Signatures  498

Guidelines for Working with RSA  499

Examining the Features of the Diffie-Hellman Key Exchange Algorithm  499

Steps of the Diffie-Hellman Key Exchange Algorithm  500

Working with a PKI  500

Examining the Principles Behind a PKI  501

Understanding PKI Terminology  501

Components of a PKI  501

Classes of Certificates  502

Examining the PKI Topology of a Single Root CA  502

Examining the PKI Topology of Hierarchical CAs  503

Examining the PKI Topology of Cross-Certified CAs  505

Understanding PKI Usage and Keys  506

Working with PKI Server Offload  506

Understanding PKI Standards  507

Understanding X.509v3  507

Understanding Public Key Cryptography Standards (PKCS)  508

Understanding Simple Certificate Enrollment Protocol (SCEP)  510

Exploring the Role of Certificate Authorities and Registration Authorities in a PKI  511

Examining Identity Management  512

Retrieving the CA Certificate  513

Understanding the Certificate Enrollment Process  513

Examining Authentication Using Certificates  514

Examining Features of Digital Certificates and CAs  515

Understanding the Caveats of Using a PKI  516

Understanding How Certificates Are Employed  517

Exam Preparation Tasks  519

Review All the Key Topics  519

Complete the Tables and Lists from Memory  519

Definition of Key Terms  520

Chapter 15 Building a Site-to-Site IPsec VPN Solution  523

“Do I Know This Already?” Quiz  523

Foundation Topics  527
Part IV Final Preparation  589

Chapter 16 Final Preparation  577

  Exam Engine and Questions on the CD  577
    Install the Software from the CD  578
  Activate and Download the Practice Exam  578
  Activating Other Exams  579

  Study Plan  579
    Recall the Facts  580
    Use the Exam Engine  580
      Choosing Study or Simulation Mode  580
      Passing Scores for the IINS Exam  581

Part V Appendixes  583

  Appendix A Answers to “Do I Know This Already?” Questions  585
  Appendix B Glossary  595
  Appendix C CCNA Security Exam Updates: Version 1.0  617
  Appendix D Memory Tables (CD only)
  Appendix E Memory Tables Answer Key (CD only)

Index  620
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that the user enters (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.

- Braces ( { } ) indicate a required choice.

- Braces within brackets ([{ }]) indicate a required choice within an optional element.
Foreword

*CCNA Security Official Exam Certification Guide* is an excellent self-study resource for the Cisco IINS (640-553) exam. Passing the IINS exam validates the knowledge and skills required to successfully secure Cisco network devices.

Gaining certification in Cisco technology is key to the continuing educational development of today’s networking professional. Through certification programs, Cisco validates the skills and expertise required to effectively manage the modern enterprise network.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in your field of expertise or to gain new skills. Whether used as a supplement to more traditional training or as a primary source of learning, these materials offer users the information and knowledge validation required to gain new understanding and proficiencies.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco, and they offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope that you find these materials to be an enriching and useful part of your exam preparation.

Erik Ullanderson
Manager, Global Certifications
Learning@Cisco
May 2008
Introduction

Congratulations on your decision to pursue a Cisco Certification! If you’re reading far enough to look at the introduction to this book, you likely already have a sense of what you ultimately would like to achieve—the Cisco CCNA Security certification. Achieving Cisco CCNA Security certification requires that you pass the Cisco IINS (640-553) exam. Cisco certifications are recognized throughout the networking industry as a rigorous test of a candidate’s knowledge of and ability to work with Cisco technology. Through its quality technologies, Cisco has garnered a significant market share in the router and switch marketplace, with more than 80 percent market share in some markets. For many industries and markets around the world, networking equals Cisco. Cisco certification will set you apart from the crowd and allow you to display your knowledge as a networking security professional.

Historically speaking, the first entry-level Cisco certification is the Cisco Certified Network Associate (CCNA) certification, first offered in 1998.

With the introduction of the CCNA Security certification, Cisco has for the first time provided an area of focus at the associate level. The CCNA Security certification is for networking professionals who work with Cisco security technologies and who want to demonstrate their mastery of core network security principles and technologies.

Format of the IINS Exam

The 640-553 IINS exam follows the same general format of other Cisco exams. When you get to the testing center and check in, the proctor gives you some general instructions and then takes you into a quiet room with a PC. When you’re at the PC, you have a few things to do before the timer starts on your exam. For instance, you can take a sample quiz, just to get accustomed to the PC and the testing engine. If you have user-level PC skills, you should have no problems with the testing environment. Additionally, Chapter 16 points to a Cisco website where you can see a demo of the actual Cisco test engine.

When you start the exam, you are asked a series of questions. You answer the question and then move on to the next question. The exam engine does not let you go back and change your answer. When you move on to the next question, that’s it for the earlier question.

The exam questions can be in one of the following formats:

- Multiple-choice (MC)
- Testlet
- Drag-and-drop (DND)
Simulated lab (Sim)

Simlet

The first three types of questions are relatively common in many testing environments. The multiple-choice format simply requires that you point and click a circle beside the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many answers. Testlets are questions with one general scenario, with multiple MC questions about the overall scenario. Drag-and-drop questions require you to click and hold, move a button or icon to another area, and release the mouse button to place the object somewhere else—typically in a list. For example, to get the question correct, you might need to put a list of five things in the proper order.

The last two types both use a network simulator to ask questions. Interestingly, these two types allow Cisco to assess two very different skills. Sim questions generally describe a problem, and your task is to configure one or more routers and switches to fix the problem. The exam then grades the question based on the configuration you changed or added. Interestingly, Sim questions are the only questions that Cisco (to date) has openly confirmed that partial credit is given for.

The Simlet questions may well be the most difficult style of question on the exams. Simlet questions also use a network simulator, but instead of answering the question by changing the configuration, the question includes one or more MC questions. The questions require that you use the simulator to examine the current behavior of a network, interpreting the output of any `show` commands that you can remember to answer the question. Whereas Sim questions require you to troubleshoot problems related to a configuration, Simlets require you to analyze both working networks and networks with problems, correlating `show` command output with your knowledge of networking theory and configuration commands.

What's on the IINS Exam?

Cisco wants the public to know both the variety of topics and the kinds of knowledge and skills that are required for each topic, for every Cisco certification exam. To that end, Cisco publishes a set of exam topics for each exam. The topics list the specific subjects, such as ACLs, PKI, and AAA, that you will see on the exam. The wording of the topics also implies the kinds of skills required for that topic. For example, one topic might start with “Describe...”, and another might begin with “Describe, configure, and troubleshoot...”. The second objective clearly states that you need a thorough and deep understanding of that topic. By listing the topics and skill level, Cisco helps you prepare for the exam.

Although the exam topics are helpful, keep in mind that Cisco adds a disclaimer that the posted exam topics for all its certification exams are guidelines. Cisco makes an effort to
keep the exam questions within the confines of the stated exam topics. I know from talking
to those involved that every question is analyzed to ensure that it fits within the stated exam
topics.

IINS Exam Topics

Table I-1 lists the exam topics for the 640-553 IINS exam. Although the posted exam topics
are not numbered at Cisco.com, Cisco Press does number the exam topics for easier
reference. Notice that the topics are divided among nine major topic areas. The table also
notes the part of this book in which each exam topic is covered. Because it is possible that
the exam topics may change over time, it may be worthwhile to double-check the exam
topics as listed on Cisco.com (http://www.cisco.com/go/certification). If Cisco later adds
exam topics, you may go to http://www.ciscopress.com and download additional
information about the newly added topics.

Table I-1  640-553 IINS Exam Topics

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Exam Topic</th>
<th>Book Part(s) Where Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Describe the security threats facing modern network infrastructures</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Describe and mitigate the common threats to the physical installation</td>
<td>I</td>
</tr>
<tr>
<td>1.2</td>
<td>Describe and list mitigation methods for common network attacks</td>
<td>I</td>
</tr>
<tr>
<td>1.3</td>
<td>Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks</td>
<td>II</td>
</tr>
<tr>
<td>1.4</td>
<td>Describe the main activities in each phase of a secure network lifecycle</td>
<td>I</td>
</tr>
<tr>
<td>1.5</td>
<td>Explain how to meet the security needs of a typical enterprise with a comprehensive security policy</td>
<td>I</td>
</tr>
<tr>
<td>1.6</td>
<td>Describe the Cisco Self Defending Network architecture</td>
<td>I</td>
</tr>
<tr>
<td>1.7</td>
<td>Describe the Cisco security family of products and their interactions</td>
<td>I, II, III</td>
</tr>
<tr>
<td>2.0</td>
<td>Secure Cisco routers</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Secure Cisco routers using the SDM Security Audit feature</td>
<td>I</td>
</tr>
<tr>
<td>2.2</td>
<td>Use the One-Step Lockdown feature in SDM to secure a Cisco router</td>
<td>I</td>
</tr>
<tr>
<td>2.3</td>
<td>Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements</td>
<td>I</td>
</tr>
<tr>
<td>2.4</td>
<td>Secure administrative access to Cisco routers by configuring multiple privilege levels</td>
<td>I</td>
</tr>
<tr>
<td>2.5</td>
<td>Secure administrative access to Cisco routers by configuring role based CLI</td>
<td>I</td>
</tr>
<tr>
<td>Reference Number</td>
<td>Exam Topic</td>
<td>Book Part(s) Where Topic Is Covered</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>2.6</td>
<td>Secure the Cisco IOS image and configuration file</td>
<td>I</td>
</tr>
<tr>
<td><strong>3.0</strong></td>
<td>Implement AAA on Cisco routers using local router database and external ACS</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Explain the functions and importance of AAA</td>
<td>I</td>
</tr>
<tr>
<td>3.2</td>
<td>Describe the features of TACACS+ and RADIUS AAA protocols</td>
<td>I</td>
</tr>
<tr>
<td>3.3</td>
<td>Configure AAA authentication</td>
<td>I</td>
</tr>
<tr>
<td>3.4</td>
<td>Configure AAA authorization</td>
<td>I</td>
</tr>
<tr>
<td>3.5</td>
<td>Configure AAA accounting</td>
<td>I</td>
</tr>
<tr>
<td><strong>4.0</strong></td>
<td>Mitigate threats to Cisco routers and networks using ACLs</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets</td>
<td>II</td>
</tr>
<tr>
<td>4.2</td>
<td>Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI</td>
<td>II</td>
</tr>
<tr>
<td>4.3</td>
<td>Configure IP ACLs to prevent IP address spoofing using CLI</td>
<td>II</td>
</tr>
<tr>
<td>4.4</td>
<td>Discuss the caveats to be considered when building ACLs</td>
<td>II</td>
</tr>
<tr>
<td><strong>5.0</strong></td>
<td>Implement secure network management and reporting</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Describe the factors to be considered when planning for secure management and reporting of network devices</td>
<td>I</td>
</tr>
<tr>
<td>5.2</td>
<td>Use CLI and SDM to configure SSH on Cisco routers to enable secured management access</td>
<td>I</td>
</tr>
<tr>
<td>5.3</td>
<td>Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server</td>
<td>I</td>
</tr>
<tr>
<td>5.4</td>
<td>Describe SNMPv3 and NTPv3</td>
<td>I</td>
</tr>
<tr>
<td><strong>6.0</strong></td>
<td>Mitigate common Layer 2 attacks</td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features</td>
<td>II</td>
</tr>
<tr>
<td><strong>7.0</strong></td>
<td>Implement the Cisco IOS firewall feature set using SDM</td>
<td></td>
</tr>
<tr>
<td>7.1</td>
<td>Describe the operational strengths and weaknesses of the different firewall technologies</td>
<td>II</td>
</tr>
<tr>
<td>7.2</td>
<td>Explain stateful firewall operations and the function of the state table</td>
<td>II</td>
</tr>
<tr>
<td>7.3</td>
<td>Implement Zone Based Firewall using SDM</td>
<td>II</td>
</tr>
<tr>
<td><strong>8.0</strong></td>
<td>Implement the Cisco IOS IPS feature set using SDM</td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>Define network based vs. host based intrusion detection and prevention</td>
<td>II</td>
</tr>
</tbody>
</table>
Another way to get some direction about the topics on the exams is to look at the course outlines for the related courses. Cisco offers one authorized CCNA Security-related course: Implementing Cisco IOS Network Security (IINSv1.0). Cisco authorizes Certified Learning Solutions Providers (CLSP) and Certified Learning Partners (CLP) to deliver these classes. These authorized companies can also create unique custom course books using this material, in some cases to teach classes geared toward passing the 640-553 IINS exam.

### About the CCNA Security Official Exam Certification Guide

As mentioned earlier, Cisco has outlined the topics tested on the 640-553 IINS exam. This book maps to these topic areas and provides some background material to give context and to help you understand these topics.

This section lists this book’s variety of features. A number of basic features included in this book are common to all Cisco Press Official Exam Certification Guides. These features are designed to help you prepare to pass the official certification exam, as well as help you learn relevant real-world concepts and procedures.

### Objectives and Methods

The most important and somewhat obvious objective of this book is to help you pass the 640-553 IINS exam. In fact, if the primary objective of this book were different, the book’s title would be misleading! However, the methods used in this book to help you pass the exams are also designed to make you much more knowledgeable about how to do your job.
This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. The CCNA Security certification is the foundation of the professional level Cisco certification in security, the CCSP, so it is important that this book also help you truly learn the material. This book is designed to help you pass the CCNA Security exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD

**Book Features**

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **“Do I Know This Already?” quiz:** Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.

- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.

- **Exam Preparation Tasks:** At the end of the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter.

  — **Review All the Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All the Key Topics activity lists the Key Topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each Key Topic, so you should review these.

  — **Complete the Tables and Lists from Memory:** To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list.
— **Definition of Key Terms**: Although the exam may be unlikely to ask a question such as “Define this term,” the CCNA exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.

— **Command Reference Tables**: Some chapters cover a large number of configuration and EXEC commands. These tables list and describe the commands introduced in the chapter. For exam preparation, use these tables for reference, but also read them when performing the Exam Preparation Tasks to make sure you remember what all the commands do.

■ **CD-based practice exam**: The companion CD contains an exam engine (From Boson software, http://www.boson.com), that includes two question databases. One database has a copy of all the “Do I Know This Already?” quiz questions from the book, and the other has unique exam-realistic questions. To further help you prepare for the exam, you can take a simulated IINS exam using the CD.

**How This Book Is Organized**

This book contains 15 core chapters—Chapters 1 through 15. Chapter 16 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the IINS exam. The core chapters are organized into parts. They cover the following topics:

■ **Part I: Network Security Concepts**

— **Chapter 1, “Understanding Network Security Principles”**: This chapter explains the need for network security and discusses the elements of a secure network. Additionally, legal and ethical considerations are discussed. You are also introduced to various threats targeting the security of your network.

— **Chapter 2, “Developing a Secure Network”**: This chapter explains the day-to-day procedures for deploying, maintaining, and retiring information security components. You are also provided with considerations and principles for authoring a security policy, in addition to creating user awareness of the security policy. Finally, this chapter describes the Cisco Self-Defending Network, which is Cisco’s vision for security systems.

— **Chapter 3, “Defending the Perimeter”**: This chapter describes methods of securely accessing a router prompt for purposes of administration. Additionally, you are given an overview of the Cisco Integrated Services Router (ISR) line of routers. In this chapter you also examine the Cisco Security Device Manager (SDM) interface. The graphical interface provided by SDM allows administrators to configure a variety of router features using a collection of wizards, which use best-practice recommendations from the Cisco Technical Assistance Center (TAC).
— Chapter 4, “Configuring AAA”: This chapter explores the uses of AAA, including the components that make it up, as well as the steps necessary to successfully configure AAA using the local database. The role of Cisco ACS is also examined as it relates to configuring AAA, including a discussion of working with both RADIUS and TACACS+.

— Chapter 5, “Securing the Router”: This chapter discusses various router services that attackers might target. To help you harden the security of a router, this chapter also describes the AutoSecure feature and Cisco SDM’s One-Step Lockdown feature. Next the chapter focuses on securing and monitoring router access using syslog, SSH, and SNMPv3 technologies. Finally, this chapter distinguishes between in-band and out-of-band network management and how to use Cisco SDM to configure a variety of management and monitoring features.

■ Part II: Constructing a Secure Infrastructure

— Chapter 6, “Securing Layer 2 Devices”: This chapter explains how Cisco Catalyst switches can be configured to mitigate several common Layer 2 attacks. Then you are introduced to how Cisco Identity-Based Networking Services (IBNS) uses IEEE 802.1x, RADIUS, and Extensible Authentication Protocol (EAP) technologies to selectively allow access to network resources based on user credentials.

— Chapter 7, “Implementing Endpoint Security”: This chapter examines a variety of threats faced by endpoints in a network environment and introduces a series of techniques that can be used to help safeguard systems from common operating system vulnerabilities. This chapter also explores various Cisco-specific technologies that may be used to defend endpoints from a variety of attacks. Specifically, technologies such as IronPort, the Cisco NAC Appliance, and the Cisco Security Agent are discussed.

— Chapter 8, “Providing SAN Security”: This chapter outlines the basics of SAN operation and looks at the benefits that a SAN brings to the enterprise as a whole. A variety of security mechanisms, such as LUN masking, SAN zoning, and port authentication, are also explored as steps that may be taken to safeguard data in a SAN environment.

— Chapter 9, “Exploring Secure Voice Solutions”: This chapter introduces you to voice over IP (VoIP) networks. You learn what business benefits VoIP offers, in addition to the components and protocols that support the transmission of packetized voice across a data network. You are made aware of specific threats targeting a VoIP network. Some threats (such as toll fraud) are found in traditional telephony networks, but others are specific to VoIP.
Finally, this chapter identifies specific actions you can take to increase the security of VoIP networks. For example, you will consider how to use firewalls and VPNs to protect voice networks and how to harden the security of Cisco IP Phones and voice servers.

— *Chapter 10, “Using Cisco IOS Firewalls to Defend the Network”*: This chapter begins by exploring the evolution of firewall technology and the role of firewalls in constructing an overall network defense. This chapter also examines how to use access control lists (ACL) to construct a static packet-filtering mechanism for the enterprise environment. Finally, zone-based firewalls are discussed because they represent a significant advance in firewall technology. Their role in defending the network is examined.

— *Chapter 11, “Using Cisco IOS IPS to Secure the Network”*: This chapter distinguishes between intrusion detection and intrusion prevention. Various Intrusion Prevention System (IPS) appliances are introduced, and the concept of signatures is discussed. Also, this chapter examines how to configure a Cisco IOS router to act as an IPS sensor, as opposed to using, for example, a dedicated IPS appliance. Specifically, the configuration discussed uses a wizard available in the Cisco SDM interface.

### Part III: Extending Security and Availability with Cryptography and VPNs

— *Chapter 12, “Designing a Cryptographic Solution”*: This chapter initially explores the basics of cryptographic services and looks at their evolution. This chapter also examines the use of symmetric encryption, including a variety of symmetric algorithms such as DES, 3DES, AES, SEAL, and various Rivest ciphers. This chapter concludes with a discussion of the encryption process and what makes for a strong, trustworthy encryption algorithm.

— *Chapter 13, “Implementing Digital Signatures”*: This chapter begins with a look at hash algorithms and explores their construction and usage. This includes a discussion of their relative strengths and weaknesses in practical application. The components that make up a digital signature are also explored in depth, along with a discussion of their application as a means of proving a message’s authenticity.

— *Chapter 14, “Exploring PKI and Asymmetric Encryption”*: This chapter looks at the use of asymmetric algorithms in a PKI and examines the features and capabilities of RSA specifically. The Diffie-Hellman (DH) algorithm is also discussed, as to how it is used for key exchange. This chapter also explores the makeup of the PKI infrastructure and discusses the various components and topologies that may be employed.
Chapter 15, “Building a Site-to-Site IPsec VPN Solution”: This chapter introduces you to an IPsec virtual private network (VPN) and its components. Additionally, you explore specific devices in the Cisco VPN product family. Then you are presented with Cisco best-practice recommendations for VPNs. This chapter then walks you through the process of configuring an IPsec site-to-site VPN on an IOS router, using both the command-line interface and the Cisco Security Device Manager (SDM) interface.

Part IV: Final Preparation

Chapter 16, “Final Preparation”: This chapter identifies tools for final exam preparation and helps you develop an effective study plan.

Part V: Appendixes

Appendix A, “Answers to the ‘Do I Know This Already?’ Questions”: Includes the answers to all the questions from Chapters 1 through 15.

Appendix B, “Glossary”: The glossary contains definitions of all the terms listed in the “Definition of Key Terms” section at the conclusion of Chapters 1 through 15.

Appendix C, “CCNA Security Exam Updates: Version 1.0”: This appendix provides instructions for finding updates to the exam and this book when and if they occur.

Appendix D, “Memory Tables”: This CD-only appendix contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams. This appendix is available in PDF format on the CD; it is not in the printed book.

Appendix E, “Memory Tables Answer Key”: This CD-only appendix contains the answer key for the memory tables in Appendix D. This appendix is available in PDF format on the CD; it is not in the printed book.

How to Use This Book to Prepare for the IINS Exam

Using this book to prepare for the IINS exam is pretty straightforward—read each chapter in succession, and follow the study suggestions in Chapter 16, “Final Preparation.”

For the core chapters of this book (Chapters 1 through 15), you do have some choices about how much of the chapter you read. In some cases, you may already know most or all of the information covered in a given chapter. To help you decide how much time to spend on each chapter, the chapters begin with a “Do I Know This Already?” quiz. If you get all the quiz questions correct, or you miss just one question, you may want to skip to the end of the
chapter and the “Exam Preparation Tasks” section, and do those activities. Figure I-1 shows the overall plan.

**Figure I-1  How to Approach Each Chapter of This Book**

When you have completed Chapters 1 through 15, you can use Chapter 16 for exam preparation guidance. That chapter includes the following suggestions:

- Check [http://www.ciscopress.com](http://www.ciscopress.com) for the latest copy of Appendix C, which may include additional topics for study.
- Repeat the tasks in all the chapters’ “Exam Preparation Tasks” chapter-ending section.
- Review all DIKTA questions using the exam engine.
- Practice for the exam using the exam engine.

This book is broken into parts and chapters that address the key areas of the IINS exam. Each chapter begins with a series of “Do I Know This Already?” questions. You should work through these to get a sense of your current knowledge of the subject matter being discussed. Each chapter contains memory tables that you should work through. At the end of each chapter is a list of all the key topics, as well as terms central to the topic. It is a good idea to focus on these key topic areas and to be familiar with all the terms listed in each chapter. After you have completed this book, you may further prepare for the exam and test your knowledge by working through the practice exam on the CD. Tracking your score on the practice exam and noting areas of weakness will allow you to review these areas in the text to further solidify your knowledge before the actual IINS exam.

**For More Information**

If you have any comments about this book, you can submit them at [http://www.ciscopress.com](http://www.ciscopress.com). Just go to the website, click Contact Us, and enter your message.

IINS exam topics covered in this part:

- Describe and mitigate the common threats to the physical installation
- Describe and list mitigation methods for common network attacks
- Describe the main activities in each phase of a secure network lifecycle
- Explain how to meet the security needs of a typical enterprise with a comprehensive security policy
- Describe the Cisco Self Defending Network architecture
- Describe the Cisco security family of products and their interactions
- Secure Cisco routers using the SDM Security Audit feature
- Use the One-Step Lockdown feature in SDM to secure a Cisco router
- Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
- Secure administrative access to Cisco routers by configuring multiple privilege levels
- Secure administrative access to Cisco routers by configuring role-based CLI
- Secure the Cisco IOS image and configuration file
- Explain the functions and importance of AAA
- Describe the features of TACACS+ and RADIUS AAA protocols
- Configure AAA authentication
- Configure AAA authorization
- Configure AAA accounting
- Describe the factors to be considered when planning for secure management and reporting of network devices
- Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
- Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server
- Describe SNMPv3 and NTPv3
This chapter covers the following topics:

**ISR overview and providing secure administrative access:** This section describes methods of securely accessing a router prompt for purposes of administration. Additionally, this section provides an overview of the Cisco Integrated Services Router (ISR) line of routers.

**Cisco Security Device Manager overview:** This section examines the Cisco Security Device Manager (SDM) interface. The graphical interface provided by SDM allows administrators to configure a variety of router features using a collection of wizards and other configuration aids, which use best-practice recommendations from the Cisco Technical Assistance Center (TAC).
In addition to Cisco firewall, virtual private network (VPN), and intrusion prevention system (IPS) appliances that can sit at the perimeter of a network, Cisco IOS routers offer perimeter-based security. For example, the Cisco Integrated Services Routers (ISR) can be equipped to provide high-performance security features, including firewall, VPN termination, and IPS features, in addition to other services such as voice and quality-of-service (QoS) services. This chapter introduces various ISR models.

Because perimeter routers can be attractive targets for attack, they should be configured to secure administrative access. Therefore, this chapter also discusses specific approaches to “harden” administrative access to ISRs.

Configuring advanced ISR router features can be a complex process. Fortunately, many modern Cisco routers can be configured using the graphical Cisco Security Device Manager (SDM) interface. SDM contains multiple wizard-like configuration utilities, which are introduced in this chapter.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz helps you determine your level of knowledge of this chapter’s topics before you begin. Table 3-1 details the major topics discussed in this chapter and their corresponding quiz questions.

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR Overview and Providing Secure Administrative Access</td>
<td>1 to 10</td>
</tr>
<tr>
<td>Cisco Security Device Manager Overview</td>
<td>11 to 13</td>
</tr>
</tbody>
</table>
1. Which of the following are considered IOS security features? (Choose four.)
   a. Stateful firewall
   b. MARS
   c. IPS
   d. VRF-aware firewall
   e. VPN
   f. ACS

2. Some ISRs include a USB port, into which a flash drive can connect. What are three common uses for the flash drive? (Choose three.)
   a. Storing configuration files
   b. Storing a digital certificate
   c. Storing a copy of the IOS image
   d. Storing a username/password database

3. The enable secret password appears as an MD5 hash in a router’s configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption service is not enabled). Why does Cisco still support the use of both enable secret and enable passwords in a router’s configuration?
   a. Because the enable secret password is a hash, it cannot be decrypted. Therefore, the enable password is used to match the password that was entered, and the enable secret is used to verify that the enable password has not been modified since the hash was generated.
   b. The enable password is used for IKE Phase I, whereas the enable secret password is used for IKE Phase II.
   c. The enable password is considered to be a router’s public key, whereas the enable secret password is considered to be a router’s private key.
   d. The enable password is present for backward compatibility.

4. What is an IOS router’s default response to multiple failed login attempts after the `security authentication failure` command has been issued?
   a. The login process is suspended for 10 seconds after 15 unsuccessful login attempts.
   b. The login process is suspended for 15 seconds after 10 unsuccessful login attempts.
   c. The login process is suspended for 30 seconds after 10 unsuccessful login attempts.
   d. The login process is suspended for 10 seconds after 30 unsuccessful login attempts.
5. What line configuration mode command would you enter to prevent a line (such as a console, aux, or vty line) connection from timing out because of inactivity?
   a. no service timeout
   b. timeout-line none
   c. exec-timeout 0 0
   d. service timeout default

6. An IOS router’s privileged mode, which you can access by entering the **enable** command followed by the appropriate password, has which privilege level?
   a. 0
   b. 1
   c. 15
   d. 16

7. How is a CLI view different from a privilege level?
   a. A CLI view supports only commands configured for that specific view, whereas a privilege level supports commands available to that level and all the lower levels.
   b. A CLI view can function without a AAA configuration, whereas a privilege level requires AAA to be configured.
   c. A CLI view supports only monitoring commands, whereas a privilege level allows a user to make changes to an IOS configuration.
   d. A CLI view and a privilege level perform the same function. However, a CLI view is used on a Catalyst switch, whereas a privilege level is used on an IOS router.

8. To protect a router’s image and configuration against an attacker’s attempt to erase those files, the Cisco IOS Resilient Configuration feature keeps a secure copy of these files. What are these files called?
   a. The bootset
   b. The configset
   c. The backupset
   d. The backup-config
9. When you configure Cisco IOS login enhancements for virtual connections, what is the “quiet period”?
   a. The period of time between successive login attempts
   b. A period of time when no one is attempting to log in
   c. The period of time in which virtual login attempts are blocked, following repeated failed login attempts
   d. The period of time in which virtual logins are blocked as security services fully initialize

10. In the banner motd # command, what does # represent?
    a. A single text character that will appear as the message of the day
    b. A delimiter indicating the beginning and end of a message of the day
    c. A reference to a system variable that contains a message of the day
    d. The enable mode prompt from where the message of the day will be entered into the IOS configuration

11. What Cisco IOS feature provides a graphical user interface (GUI) for configuring a wide variety of features on an IOS router and also provides multiple “smart wizards” and configuration tutorials?
    a. QPM
    b. SAA
    c. SMS
    d. SDM

12. What are two options for running Cisco SDM? (Choose two.)
    a. Running SDM from a router’s flash
    b. Running SDM from the Cisco web portal
    c. Running SDM from within CiscoWorks
    d. Running SDM from a PC

13. Which of the following are valid SDM configuration wizards? (Choose three.)
    a. Security Audit
    b. VPN
    c. ACS
    d. NAT
    e. STP
Foundation Topics

ISR Overview and Providing Secure Administrative Access

This section begins by introducing the security features offered in the Cisco line of ISR routers. Additional hardware options for these routers are also discussed. Then, with a foundational understanding of the underlying hardware, you will learn a series of best practices for security administrative access to a router. For example, a router can be configured to give different privilege levels to different administrative logins.

IOS Security Features

Although they are not a replacement for dedicated security appliances in large enterprise networks, modern Cisco routers, such as the ISR series, offer multiple integrated security features. Table 3-2 provides examples of these features, which vary by IOS feature set.

Table 3-2  IOS Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful firewall</td>
<td>The Cisco IOS firewall feature allows an IOS router to perform stateful inspection of traffic (using Context-Based Access Control [CBAC]), in addition to basic traffic filtering using access control lists (ACL).</td>
</tr>
<tr>
<td>Intrusion Prevention System</td>
<td>The IOS Intrusion Prevention System (IPS) feature can detect malicious network traffic inline and stop it before it reaches its destination.</td>
</tr>
<tr>
<td>VPN Routing and Forwarding-aware (VRF-aware) firewall</td>
<td>A VRF-aware firewall maintains a separate routing and forwarding table for each VPN, which helps eliminate issues that arise from more than one VPN using the same address space.</td>
</tr>
<tr>
<td>Virtual private networks</td>
<td>Cisco IOS routers can participate in virtual private networks (VPN). For example, a router at a headquarters location and at a branch office location could interconnect via an IPsec-protected VPN. This approach would allow traffic to pass securely between those sites, even if the VPN crossed an “untrusted” network, such as the Internet.</td>
</tr>
</tbody>
</table>

Cisco Integrated Services Routers

Cisco offers a series of routers called *Integrated Services Routers* (ISR). As their name suggests, these routers integrate various services (such as voice and security services) into
the router architecture. Although Cisco offers a wide range of router platforms, ISR models are easy to identify, because the last three digits of their model begin with the number 8. As shown in Figure 3-1, the ISR family of routers includes the 800 series, 1800 series, 2800 series, and 3800 series.

**Figure 3-1 800 Series, 1800 Series, 2800 Series, and 3800 Series ISRs**

**Cisco 800 Series**
The Cisco 800 series of ISRs is designed for teleworkers and small-office environments. These routers can connect to the Internet via a cable modem or DSL modem connection and offer secure connections over the Internet. Table 3-3 contrasts some of the features available in the Cisco 850 and 870 series of ISRs.

**Table 3-3 Cisco 800 Series of ISRs**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco 850 Series</th>
<th>Cisco 870 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN technology support</td>
<td>ADSL Annex A (Cisco 857)</td>
<td>ADSL Annex B (Cisco 876), ADSL Annex A (Cisco 877), G.SHDSL (Cisco 878)</td>
</tr>
<tr>
<td>Built-in routed/WAN Ethernet</td>
<td>One 10/100 WAN (Cisco 851)</td>
<td>One 10/100 WAN (Cisco 871)</td>
</tr>
<tr>
<td>Integrated cryptographic hardware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum flash memory</td>
<td>20 MB</td>
<td>52 MB</td>
</tr>
<tr>
<td>Maximum SRAM</td>
<td>64 MB</td>
<td>256 MB</td>
</tr>
<tr>
<td>Support for Cisco Security Device Manager (SDM)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco 1800 Series

The Cisco 1800 series of ISRs is designed for small businesses and smaller enterprise branch offices. These routers are designed for connectivity via cable modem/DSL, Metro Ethernet, and wireless technologies. Table 3-4 contrasts some of the features available in the Cisco 1800 and 1841 series of ISRs.

Table 3-4  Cisco 1800 Series of ISRs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco 1800 Series (Fixed Interface)</th>
<th>Cisco 1841 Series (Modular)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN technology support</strong></td>
<td>ADSL Annex A (Cisco 1801), ADSL Annex B (Cisco 1802), G.SHDSL (Cisco 1803)</td>
<td>ADSL and optional G.SHDSL WICs</td>
</tr>
<tr>
<td><strong>Built-in routed/WAN Ethernet</strong></td>
<td>One 10/100 (Cisco 1801-1803)</td>
<td>Two 10/100</td>
</tr>
<tr>
<td></td>
<td>Two 10/100 (Cisco 1811, 1812)</td>
<td></td>
</tr>
<tr>
<td><strong>Integrated cryptographic hardware</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Maximum flash memory</strong></td>
<td>128 MB</td>
<td>128 MB</td>
</tr>
<tr>
<td><strong>Maximum SRAM</strong></td>
<td>384 MB</td>
<td>384 MB</td>
</tr>
<tr>
<td><strong>Support for Cisco Security Device Manager (SDM)</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Maximum number of VPN tunnels</strong></td>
<td>50</td>
<td>800</td>
</tr>
<tr>
<td><strong>Stateful firewall support</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Intrusion Prevention System (IPS) support</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco 2800 Series

The Cisco 2800 series of ISRs is designed for small-to-medium businesses and enterprise branch offices. These routers can securely provide voice, data, and video services. Table 3-5 contrasts some of the features available in the Cisco 2801, 2811, 2821, and 2851 series of ISRs.

### Table 3-5  Cisco 2800 Series of ISRs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco 2801 Series</th>
<th>Cisco 2811 Series</th>
<th>Cisco 2821 Series</th>
<th>Cisco 2851 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN technology support</strong></td>
<td>ADSL and optional G.SHDSL WICs</td>
<td>ADSL and optional G.SHDSL WICs</td>
<td>ADSL and optional G.SHDSL WICs</td>
<td>ADSL and optional G.SHDSL WICs</td>
</tr>
<tr>
<td><strong>Built-in routed/WAN Ethernet</strong></td>
<td>Two 10/100</td>
<td>Two 10/100</td>
<td>Two 10/100/1000</td>
<td>Two 10/100/1000</td>
</tr>
<tr>
<td><strong>Integrated cryptographic hardware</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Maximum flash memory</strong></td>
<td>128 MB</td>
<td>256 MB</td>
<td>256 MB</td>
<td>256 MB</td>
</tr>
<tr>
<td><strong>Maximum SRAM</strong></td>
<td>384 MB</td>
<td>769 MB</td>
<td>1024 MB</td>
<td>1024 MB</td>
</tr>
<tr>
<td><strong>Support for Cisco Security Device Manager (SDM)</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Maximum number of VPN tunnels</strong></td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
</tr>
<tr>
<td><strong>Stateful firewall support</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Intrusion Prevention System (IPS) support</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Cisco 3800 Series

The Cisco 3800 series of ISRs is designed for medium to large businesses and enterprise branch offices. These routers offer multiple security, IP telephony, video, network analysis, and web application features. Table 3-6 contrasts some of the features available in the Cisco 3825 and 3845 series of ISRs.
ISR Enhanced Features

Although traditional Cisco routers (that is, non-ISRs) offer features similar to those highlighted in the preceding tables, ISRs are unique in that they contain integrated hardware components (that vary by platform) to enhance performance. For example, most ISR models include the following enhancements:

- **Integrated VPN acceleration**: By using dedicated hardware for VPN encryption, ISRs reduce the overhead placed on a router’s processor, thereby increasing VPN performance and scalability. Specifically, the built-in VPN acceleration hardware supports 3DES and Advanced Encryption Standard (AES).

- **Dedicated voice hardware**: IP telephony applications often use digital signal processors (DSP) to mix multiple voice streams in a conference. They also encrypt voice packets and convert between high-bandwidth and low-bandwidth codecs (that is, a coder/decoder, such as G.711 and G.729, which specify how voice samples are digitally represented in a voice packet). Voice traffic uses Real-time Transport Protocol (RTP), a Layer 4 protocol, to transport voice in a network. For increased security, Secure RTP (SRTP) can be used, which provides AES encryption for voice. However, because of the processor overhead required for SRTP’s encryption, dedicated DSP hardware is required. Fortunately, ISRs can use packet voice DSP modules (PVDM) to take over the processing of such tasks.

The Cisco 2800 series of ISRs can use PVDM2 modules with onboard voice interface cards (VIC). Additionally, PVDM2 modules can be inserted into Cisco High-Density Analog (HDA) network modules and the Cisco Digital Extension Module for Voice and Fax, which can be inserted into the Cisco 2821, 2851, 3825, and 3845 ISR models.
**Advanced Integration Modules**: Cisco offers a variety of Advanced Integration Modules (AIM), which can offload processor-intensive tasks from a router’s processor. For example, AIMs can be used for VPN processing, including a variety of standards for encryption, authentication, and data integrity. The following are some AIM models:

- **AIM-VPN/BPII-PLUS**: Used in Cisco 1800 series ISRs, which can support a single AIM
- **AIM-VPN/EPII-PLUS**: Used in Cisco 2800 series ISRs and the Cisco 3825 ISR, all of which can accommodate two AIMs
- **AIM-VPN/HPII-PLUS**: Used in the Cisco 3845 ISR, which supports two AIMs

**USB port**: All Cisco ISRs, with the exception of the Cisco 850 ISR, include one or two Universal Serial Bus (USB) ports. These ports can be used with a USB flash drive to store IOS images or configuration files. Also, from a security perspective, a USB eToken containing a signed digital certification can be inserted for VPN use.

WAN connectivity network modules such as the WIC-2T, WIC-1B, and VWIC-1MFT offer flexibility in how various ISRs connect to the WAN. Here are some examples of other network modules supported on various ISR models:

- **Cisco HWIC-AP**: An IEEE 802.11 wireless module supporting a variety of wireless standards.
- **Cisco IDS Network Module**: Includes a hard drive containing multiple signatures of well-known attacks. Can be used to detect and subsequently prevent malicious traffic.
- **Cisco Content Engine**: Includes either a 40-GB or 80-GB hard drive for caching web content. This makes it available for quick retrieval by local clients, as opposed to the client’s having to retrieve all the information from the web.
- **Cisco Network Analysis Module (NAM)**: Provides a detailed analysis of traffic flow.

**Password-Protecting a Router**

Administrators can access a router for administrative purposes in a variety of ways. For example, as shown in Figure 3-2, a PC running terminal emulation software can telnet into a router. The Telnet connection is considered to be using a vty line (a “virtual tty” line). Alternatively, a PC using terminal emulation software can connect directly to a router’s console (“con”) line over a serial connection. For remote administrative access, many Cisco routers also have an auxiliary line (“aux”) that might connect to a modem.
Telnet sends data in clear text. Therefore, if an attacker intercepted a series of Telnet packets, he could view their contents, such as usernames and passwords. For a more secure connection, administrators might choose to use Secure Shell (SSH) for access over a vty line. Modern Cisco routers also offer a graphical interface called Cisco Security Device Manager (SDM), which is accessible over the network using HTTP or HTTPS.

However, regardless of how an administrator chooses to access a router, the router typically challenges the administrator to provide either a password or a username/password combination before access is granted. As soon as an administrator is granted access to the router, she might be in user mode, where she has a limited number of commands she can issue. However, most router administration is performed from privileged mode. To access privileged mode from user mode, the administrator enters the enable command. Typically, the administrator then is prompted to enter another password, sometimes called the enable password. Interestingly, by default, a router has no password protection of any kind.

To protect a router from unauthorized access, a “strong” password should be selected. A strong password is one that is difficult for an attacker to guess or compromise by launching a dictionary attack or brute-force attack. A dictionary attack occurs when an attacker tries to use passwords from a file containing commonly used passwords. A brute-force attack occurs when an attacker tries all combinations of characters until a match is found. Recommended Cisco guidelines for selecting a strong router password include the following:

■ Select a password that is at least ten characters long. The security password min-length 10 global configuration mode command can be used to enforce this password length recommendation.
- Use a mixture of alphabetic (both uppercase and lowercase), numeric, and special characters.
- The password should not be a common word found in a dictionary.
- Create a policy that dictates how and when passwords are to be changed.

**NOTE** A space is a valid special character that can be used in a password. However, any leading space (that is, one or more spaces at the beginning of the password) is ignored.

When an administrator initially either sets up a router from the factory and chooses to run the setup script or issues the `setup` command, the System Configuration dialog appears. The administrator is prompted to enter basic router configuration parameters, including the passwords described in Table 3-7.

**Table 3-7 Passwords Configured During the SETUP Script**

<table>
<thead>
<tr>
<th>Password Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable secret password</td>
<td>This password is used to permit access to a router’s privileged mode. The password is stored in the router’s configuration as an MD5 hash value, making it difficult for an attacker to guess and impossible to see with the naked eye.</td>
</tr>
<tr>
<td>Enable password</td>
<td>This password is not encrypted (or hashed) by default. Therefore, the enable password is considered weaker than the enable secret password. However, Cisco IOS still supports the enable password for backward compatibility. For example, if the IOS version on a router were rolled back to a version that supported the enable password but not the enable secret password, the enable password would offer some level of security.</td>
</tr>
<tr>
<td>vty password</td>
<td>When an administrator connects to a router over a network connection (such as a Telnet or SSH connection), she might be prompted to enter a vty password to have access to the virtual tty line to which she is connecting.</td>
</tr>
</tbody>
</table>

Even after the System Configuration dialog completes, and the router is functioning in a production environment, administrators can still change the router passwords. For example, the `enable secret password` global configuration mode command can be used to set the router’s enable secret password. Consider Example 3-1, which shows an enable secret password being set to Cisc0Pr3$$. Notice how the enable secret password then appears in the running configuration. The string of characters shown is not an *encrypted* version of the password. Rather, the string is the result of an MD5 hash function, which always yields a 128-bit hash value that is also known as a “digest.”
To configure a password for a router’s console, the administrator enters line configuration mode for `con 0` and specifies a password with the `password` command. Then, to force console connections to require a password, the `login` command is issued, as shown in Example 3-2.

Similarly, you can set a password for the auxiliary port. Enter line configuration mode for `aux 0` and specify a password and require a login, like the console port configuration illustrated in Example 3-3.

In addition to physically connecting to a router via the console or auxiliary port, administrators can connect to a router using a Telnet or SSH connection. Instead of connecting to physical ports, these types of connections use virtual ports. Specifically, by default a router has five virtual tty lines (that is, “vty”), vty 0 to vty 4, over which administrators can remotely connect. Similar to the console and auxiliary ports, passwords can be assigned to these vty lines, as shown in Example 3-4.
The enable secret password appears in the running configuration as an MD5 hash value. However, the console, auxiliary, and vty line passwords appear in the running configuration as plain text, as shown in Example 3-5.

Example 3-5  Line Passwords Appearing in Plain Text

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line con 0</td>
<td>password 1mA$3cr3t login</td>
</tr>
<tr>
<td>line aux 0</td>
<td>password @uxP@$w0rd login</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>password MyP@$w0rd login</td>
</tr>
</tbody>
</table>

To better secure these passwords, a password encryption service can be enabled on the router. This service uses a Cisco-proprietary algorithm that is based on a Vigenere cipher. This algorithm is far from secure. Its password can be easily compromised with downloadable utilities freely available on the Internet (such as the GetPass utility from Boson Software). However, enabling the password encryption service does help prevent someone from obtaining a password from the casual inspection of a router’s configuration.

The password encryption service is enabled in global configuration mode using the service password-encryption command. After enabling this service, the console, auxiliary, and vty line passwords appear in an encrypted format. The 7 that appears after the password command indicates that the password has been encrypted using this Cisco-proprietary encryption algorithm, as shown in Example 3-6.

Example 3-6  Cisco-Proprietary Password Encryption Results

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1(config)# service password-encryption</td>
<td></td>
</tr>
<tr>
<td>R1(config)# show run</td>
<td></td>
</tr>
<tr>
<td>! line con 0</td>
<td>password 7 091D43285D561405818 login</td>
</tr>
<tr>
<td>line aux 0</td>
<td>password 7 06261A397C6E4D5D1247000F login</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>password 7 09615739394153055B1E00 login</td>
</tr>
</tbody>
</table>
Aside from having a single password for all administrators, individual user accounts can be used to give different login credentials (that is, username/password combinations) to different administrators. Although an external user database (such as a Cisco Secure Access Control Server [ACS]) could be used, a simple way to configure a user database is to add the username/password combinations to a router’s configuration. Example 3-7 shows the addition of a username and password using the `username kevinw secret $up3r$3cr3t` command. The password will appear in the router’s configuration as an MD5 hash value.

Example 3-7  Configuring a Local User Database

```
R1(config)# username kevinw secret $up3r$3cr3t
R1(config)# end
R1# show run

! username kevinw secret 5 $1$geU5$vc/uDRS5dWi0rpQJTimBw/
```

**NOTE**  If you already know the MD5 hash value of the password you are setting for a user, you can enter the hash value, instead of the password, using the `username username secret 5 hash_value` command. The 5 indicates that the string you are entering for the password is the result of an MD5 hash of the password, as opposed to the plain-text password. You could optionally indicate the plain-text password with a 0 in place of the 5.

If an attacker gains physical access to a router, he could connect to the router’s console port and reboot the router. During the bootup process, the attacker could generate a break sequence, causing the router to enter ROM monitor (ROMMON) mode. From ROMMON mode, the attacker could reset the router’s password and thereby gain access to the router’s configuration.

Although the ability to perform this type of password recovery often proves useful to administrators, if the router’s physical security cannot be guaranteed, this feature opens a vulnerability for attackers. To mitigate this threat, an administrator can disable the password recovery feature by issuing the `no service password-recovery` command in global configuration mode. After entering this command, the administrator is cautioned not to execute this command without another plan for password recovery, because ROMMON will no longer be accessible.
Limiting the Number of Failed Login Attempts
If an attacker uses a brute-force attack or a dictionary attack when attempting to log in to a
device, such as a router, multiple login attempts typically fail before the correct credentials
are found. To mitigate these types of attacks, a Cisco IOS router can suspend the login
process for 15 seconds, following a specified number of failed login attempts. By default,
a 15-second delay is introduced after ten failed login attempts. However, the `security
authentication failure rate number_of_failed_attempts log` configuration command
(issued in global configuration mode) can be used to specify the maximum number of failed
attempts (in the range of 2 to 1024) before introducing the 15-second delay.

Example 3-8 illustrates setting the maximum number of attempts to five. Also, notice the
`log` command, which causes a TOOMANY_AUTHFAILS syslog message to be written to
a syslog server.

Example 3-8  Setting the Number of Failed Login Attempts

```
R1# conf term
R1(config)# security authentication failure rate 5 log
R1(config)# end
```

Setting a Login Inactivity Timer
After an administrator provides appropriate credentials and successfully logs into a router,
the router could become vulnerable to attack if the administrator walks away. To help
prevent an unattended router from becoming a security weakness, a 10-minute inactivity
timer is enabled by default. However, Cisco recommends that inactivity timers be set to no
more than 3 minutes. Fortunately, administrators can adjust the inactivity windows with the
`exec-timeout` command, issued in line configuration mode. Consider
Example 3-9, which shows setting the inactivity timer for the console, auxiliary, and vty
lines to 2 minutes and 30 seconds.

Example 3-9  Setting an Inactivity Timer

```
R1# conf term
R1(config)# line con 0
R1(config-line)# exec-timeout 2 30
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# exec-timeout 2 30
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 2 30
```
Configuring Privilege Levels
Larger enterprise environments might need to support multiple administrative privilege levels for router configuration. For example, help desk staff might need access to a subset of the IOS commands available to the primary router configuration team.

Cisco IOS routers normally use two of the 16 supported privilege levels. Specifically, Cisco IOS routers support privilege levels in the range 0 to 15. By default, when you attach to a router, you are in user mode, which has a privilege level of 1. After entering the enable command and providing appropriate credentials, you are moved to privileged mode, which has a privilege level of 15.

However, for a finer granularity of administrative privileges, you can configure privilege levels in the range 1 to 14 using the privilege mode {level level command | reset command} command in global configuration mode. reset is used to reset the privilege level of a command to its original privilege level. To illustrate, Example 3-10 shows how to configure the debug command to be a privilege level 5 command and how to set the enable secret password for level 5 administrative access.

Example 3-10 Configuring a Privilege Level

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1# config term</td>
</tr>
<tr>
<td>R1(config)# privilege exec level 5 debug</td>
</tr>
<tr>
<td>R1(config)# enable secret level 5 L3v3l5P055</td>
</tr>
<tr>
<td>R1(config)# end</td>
</tr>
</tbody>
</table>

After additional privilege levels are configured, an administrator can specify the privilege level she wants to change to using the enable level command. For example, for an administrator to switch to the previously configured privilege level of 5, she would enter the enable 5 command. After switching to a privilege level of 5, the administrator would have access to all commands associated not only with privilege level 5, but also all lower privilege levels.

Creating Command-Line Interface Views
Similar to making different commands available to different administrators using privilege levels, role-based command-line interface (CLI) views can be used to provide different sets of configuration information to different administrators. However, unlike making commands available via privilege levels, using role-based CLI views you can control
exactly what commands an administrator has access to. Following are the steps required to configure these views:

**Step 1** **Enable AAA**: Authentication, authorization, and accounting (AAA) is discussed in detail in Chapter 4, “Configuring AAA.” For now, just realize that AAA must be enabled to support views. Example 3-11 shows how to enable AAA on an IOS router.

**Example 3-11  Enabling AAA**

```
R1# conf term
R1(config)# aaa new-model
R1(config)# end
```

**Step 2** **Enable the root view**: The root view is represented by the set of commands available to an administrator logged in with a privilege level of 15. You might be required to provide the enable secret password to enable the root view, as shown in Example 3-12.

**Example 3-12  Enabling the Root View**

```
R1# enable
Password:
R1#
```

**Step 3** **Create a view**: Use the `parser view name` command to create a new view, as shown in Example 3-13.

**Example 3-13  Creating a View**

```
R1# conf term
R1(config)# parser view HELPDESK
R1(config-view)#
```

**Step 4** **Set a password for the view**: Use the `secret 0 password` command to set the password required to invoke the view. The 0 in the command indicates that the password provided is in plain text, as opposed to an MD5 hash value. Example 3-14 shows how to configure a view’s password.

**Example 3-14  Setting a Password for a View**

```
R1(config-view)# secret 0 H3lpD3skP@55
R1(config-view)#
```
**Step 5** Add available commands to the view: The `commands parser_mode {include | include-exclusive | exclude} [all] [interface interface_identifier | command]` command, issued in view configuration mode, allows an administrator to specify a command (or interface) available to a particular view. Example 3-15 shows how to specify that the `copy` command (followed by any keywords), the `traceroute` command, and the `ping` command will be available to a specific view (HELPDESK in this example).

**Example 3-15** Specifying Commands Available to a View

```
R1(config-view)# commands exec include all copy
R1(config-view)# commands exec include traceroute
R1(config-view)# commands exec include ping
```

**Step 6** Verify the role-based CLI view configuration: After creating a view, you can switch to that view with the `enable view name` command. After switching to the new view, you enter a `?`, for context-sensitive help, to see what commands are available in your new view, as demonstrated in Example 3-16.

**Example 3-16** Confirming Role-Based CLI Configuration

```
R1# enable view HELPDESK
Password:
R1#?
Exec commands:
  <1-99>  Session number to resume
  copy    Copy from one file to another
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  show    Show running system information
  traceroute    Trace route to destination
```

**Protecting Router Files**

To protect a router’s image and configuration from an attacker’s attempt to erase those files, the Cisco IOS Resilient Configuration feature keeps a secure copy of these files. These files are called the `bootset`. Table 3-8 details the steps required to configure Cisco IOS Resilient Configuration.
Enabling Cisco IOS Login Enhancements for Virtual Connections

Administrators, and therefore attackers, can create virtual connections to an IOS router using Telnet, SSH, and HTTP. Because an attacker does not need physical access to a router to attempt one of these “virtual” connections, you should further secure these connection types using the Cisco IOS Login Enhancements feature. This feature adds the following requirements to the login process:

- Create a delay between repeated login attempts.
- Suspend the login process if a denial-of-service (DoS) attack is suspected.
- Create syslog messages upon the success and/or failure of a login attempt.

These login enhancements are not enabled by default. To enable the login enhancements with their default settings, you can issue the `login block-for` command in global configuration mode. The default login settings specify the following:

- A delay of 1 second occurs between successive login attempts.
- No virtual connection (that is, a connection using Telnet, SSH, or HTTP) can be made during the “quiet period,” which is a period of time in which virtual login attempts are blocked, following repeated failed login attempts.

You, as an administrator, might want to alter the supported virtual login parameters to better detect and protect against DoS and/or dictionary attacks. Table 3-9 provides a command reference for these parameters.

---

### Table 3-8 Cisco IOS Resilient Configuration Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Enable image resilience</td>
<td>The <code>secure boot-image</code> command, issued in global configuration mode, secures the Cisco IOS image. The secured image is hidden so that it does not appear in a directory listing of files.</td>
</tr>
<tr>
<td>Step 2: Secure the boot configuration</td>
<td>The <code>secure boot-config</code> command, issued in global configuration mode, archives the running configuration of a router to persistent storage.</td>
</tr>
<tr>
<td>Step 3: Verify the security of the bootset</td>
<td>The <code>show secure bootset</code> command can be used to verify that Cisco IOS Resilient Configuration is enabled and that the files in the bootset have been secured.</td>
</tr>
</tbody>
</table>
Consider the enhanced support for virtual logins configuration shown in Example 3-17. After entering global configuration mode, the `login block-for 30 attempts 5 within 10` command is used to block login attempts for 30 seconds after five failed login attempts occur within a 10-second time period. If logins are then blocked based on the first command, the period of time that logins are blocked is called the quiet period. However, in this example, the `login quiet-mode access-class 101` command specifies that during the quiet period, traffic permitted by ACL 101 still is allowed to log in via Telnet, SSH, or HTTP. The delay between successive login attempts is configured to 3 seconds with the `login delay 3` command. This configuration specifies that log messages should be generated upon every failed or successful login attempt using the `login on failure log` and `login on-success log` commands. Finally, the `show login` command is issued to confirm the configuration of these virtual login parameters.
Creating a Banner Message

When someone connects to one of your routers, he sees some sort of message or prompt. For legal reasons, Cisco suggests that a banner message be displayed to warn potential attackers not to attempt a login. For example, you wouldn’t want to use a banner message that says, “Welcome! You are connected to Router 1.” An attacker could use such a message as part of his legal defense, stating that he was told that he was welcomed to your router.

Please consult competent legal counsel when phrasing the banner message. However, as soon as you have the appropriate verbiage for your banner message, you can apply the message to your router with the `banner motd delimiter message_body delimiter command. The `motd` parameter stands for “message of the day,” and the `delimiter` is a character you choose to indicate the beginning and end of the banner message. Therefore, you should choose a delimiter that will not appear in the message body. Example 3-18 shows how to create a banner message. Notice that the `$` character is used as the delimiter. Example 3-19 shows the new banner message presented to a user who just connected to the router via Telnet.
Cisco Security Device Manager Overview

Cisco IOS routers support many features (including security features) that require complex configurations. To aid in a number of these configuration tasks, Cisco introduced the Cisco Security Device Manager (SDM) interface. This section introduces SDM, discusses how to configure and launch SDM, and how to navigate the SDM wizards.

Introducing SDM
Cisco SDM provides a graphical user interface (GUI) for configuring a wide variety of features on an IOS router, as shown in Figure 3-3. Not only does SDM offer multiple “smart wizards,” but configuration tutorials also are provided. Even though SDM stands for Security Device Manager, several nonsecurity features also can be configured via SDM, such as routing and quality-of-service (QoS) features.

Example 3-18  Creating a Message-of-the-Day Banner

```
R1# conf term

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# banner motd $

Enter TEXT message. End with the character '$'.
WARNING: This router is the private property of Cisco Press.
    Disconnect now if you are not an authorized user.
    Violators will be prosecuted.
$
R1(config)#end
```

Example 3-19  Login Prompt with a Banner Message

```
WARNING: This router is the private property of Cisco Press.
    Disconnect now if you are not an authorized user.
    Violators will be prosecuted.

User Access Verification

Password:
```
Some newer Cisco routers come with SDM preinstalled, but SDM needs to be installed on other supported platforms. Go to http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm to download the current version of SDM and its release notes. Cisco SDM offers the following benefits:

- SDM’s smart wizards use Cisco TAC best-practice recommendations for a variety of configuration scenarios.
- SDM intelligently determines an appropriate security configuration based on what it learns about a router’s configuration (for example, a router’s interfaces, NAT configuration, and existing security configuration).
- SDM supports multiple security features such as wizard-based VPN configuration, router security auditing, and One-Step Lockdown configuration.
- SDM, which is supported in Cisco IOS 12.2(11)T6 and later, does not impact a router’s DRAM or CPU.
Preparing to Launch Cisco SDM

If you plan to run SDM on a router that does not already have SDM installed, you need to install SDM either from a CD accompanying the router or from a download from the Cisco IOS Software Center. The installation is wizard-based. You are prompted to install SDM either on an administrator’s PC, in the router’s flash, or both.

SDM can connect to the managed router using secure HTTP (that is, HTTPS). The commands shown in Table 3-10 can be used to configure the router for HTTP support. Example 3-20 illustrates the use of these commands.

Table 3-10  HTTPS Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# ip http server</td>
<td>Enables an HTTP server on a router</td>
</tr>
<tr>
<td>Router(config)# ip http secure-server</td>
<td>Enables a secure HTTP (HTTPS) server on a router</td>
</tr>
<tr>
<td>Router(config)# ip http authentication local</td>
<td>Configures a local authentication method for accessing the HTTPS server</td>
</tr>
<tr>
<td>Router(config)# username name privilege 15 secret 0 password</td>
<td>Configures a username and password to be used for authentication local to the router</td>
</tr>
</tbody>
</table>

Example 3-20  HTTPS Server Configuration for R1

```
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip http authentication local
R1(config)# username kevin privilege 15 secret 0 cisco
```

To verify that the required SDM files are installed on a router, you can issue the `show flash` command. The output of this command should show, at a minimum, the following SDM files:

- `sdmconfig-router_platform.cfg`
- `sdm.tar`
- `es.tar`
- `common.tar`
- `home.shtml`
- `home.tar`
If you run SDM from a router’s flash, as opposed to running SDM from a PC, the first time you connect to the router via a browser, you are taken to the Cisco SDM Express interface. Specifically, on a new router that has SDM installed, you point your browser to http://10.10.10.1. Alternatively, on an existing router, you point your browser to an active IP address on the router. Cisco SDM Express guides you through the initial SDM configuration on a router. Subsequent connections to your router via a browser take you directly to SDM, as opposed to Cisco SDM Express. However, if you run SDM from a PC, you can launch Cisco SDM by choosing Start > Programs > Cisco Systems > Cisco SDM.

Exploring the Cisco SDM Interface

Notice the toolbar across the top of the SDM page, as highlighted in Figure 3-4. You can use this toolbar to navigate between the Home, Configure, and Monitor views.

The Home view provides summary information about the router platform. For example, this summary information shows you the router model, memory capacity, flash capacity, IOS version, and an interface summary.
After clicking the **Configure** button, you see a screen similar to the one shown in Figure 3-5. Notice the wizards available in the Tasks bar. Available configuration wizards are described in Table 3-11.

**Figure 3-5  Configuration Tasks Bar**

![Tasks Bar](image)

**Table 3-11  Cisco SDM Wizards**

<table>
<thead>
<tr>
<th>Cisco SDM Wizard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces and Connections</td>
<td>Helps you configure LAN and WAN interfaces</td>
</tr>
<tr>
<td>Firewall and ACL</td>
<td>Supports the configuration of basic and advanced IOS-based firewalls</td>
</tr>
<tr>
<td>VPN</td>
<td>Helps you configure a secure site-to-site VPN, Cisco Easy VPN Server, Cisco Easy VPN Remote, and DMVPN</td>
</tr>
<tr>
<td>Security Audit</td>
<td>Identifies potential security vulnerabilities in a router’s current configuration and tweaks the router’s configuration to eliminate those weaknesses</td>
</tr>
</tbody>
</table>

*continues*
In addition to the configuration wizards, notice the **Additional Tasks** button, as shown in Figure 3-6.

**Figure 3-6  Additional Tasks Button**
Advanced administrators can use graphical interfaces to configure these additional tasks. Examples of these tasks are DHCP configuration, DNS configuration, and AAA configuration.

After clicking the **Monitor** button, you see a screen similar to the one shown in Figure 3-7. Clicking the various buttons in the Tasks bar allows you to monitor the status of various router features. Examples are firewall status, VPN status, and IPS status.

**Figure 3-7  Monitoring Tasks**

This chapter has introduced SDM. Subsequent chapters will detail how you can leverage SDM to configure a variety of security options. For exam purposes, you should be comfortable with navigating the various SDM screens and performing basic configuration tasks.
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, denoted with the Key Topic icon. Table 3-12 lists these key topics and the page where each is found.

Table 3-12  Key Topics for Chapter 3

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 3-2</td>
<td>IOS security features</td>
<td>81</td>
</tr>
<tr>
<td>List</td>
<td>ISR enhancements</td>
<td>85</td>
</tr>
<tr>
<td>Table 3-7</td>
<td>Passwords configured during the SETUP script</td>
<td>88</td>
</tr>
<tr>
<td>Table 3-8</td>
<td>Cisco IOS Resilient Configuration steps</td>
<td>96</td>
</tr>
<tr>
<td>List</td>
<td>Requirements added by Cisco IOS Login Enhancements for Virtual Connections</td>
<td>96</td>
</tr>
<tr>
<td>Example 3-18</td>
<td>Creating a message-of-the-day banner</td>
<td>99</td>
</tr>
<tr>
<td>List</td>
<td>Cisco SDM benefits</td>
<td>100</td>
</tr>
<tr>
<td>Table 3-11</td>
<td>Cisco SDM wizards</td>
<td>103-104</td>
</tr>
</tbody>
</table>

Complete the Tables and Lists from Memory

Print a copy of Appendix D, “Memory Tables,” (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists so that you can check your work.

Definition of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

Integrated Services Router (ISR), dictionary attack, brute-force attack, privilege level, role-based command-line interface (CLI) view, bootset, Cisco Security Device Manager (SDM)
Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. To see how well you have memorized the commands as a side effect of your other studies, cover the left side of the table with a piece of paper, read the descriptions on the right side, and see whether you remember the commands.

Table 3-13  Chapter 3 Configuration Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable secret password</td>
<td>A global configuration mode command that configures a router’s enable secret password</td>
</tr>
<tr>
<td>password password</td>
<td>A line configuration mode command that configures a password for a line (such as a con, aux, or vty line)</td>
</tr>
<tr>
<td>login</td>
<td>A line configuration mode command that configures a line to require a login</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>A global configuration mode command that encrypts plain-text passwords in a router’s configuration</td>
</tr>
<tr>
<td>exec-timeout minutes [seconds]</td>
<td>A line configuration mode command that specifies an inactivity period before logging out a user</td>
</tr>
<tr>
<td>security authentication failure rate number_of_failed_attempts log</td>
<td>A global configuration mode command used to specify the maximum number of failed attempts (in the range of 2 to 1024) before introducing a 15-second delay; also generates a log message if the specified threshold is exceeded</td>
</tr>
<tr>
<td>privilege mode {level level command</td>
<td>reset command}</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>A global configuration mode command used to enable authentication, authorization, and accounting (AAA)</td>
</tr>
<tr>
<td>parser view view_name</td>
<td>A global configuration mode command used to create a new view</td>
</tr>
<tr>
<td>secret 0 password</td>
<td>A view configuration mode command used to set the password required to invoke the view</td>
</tr>
<tr>
<td>commands parser_mode {include</td>
<td>include-exclusive</td>
</tr>
</tbody>
</table>

continues
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure boot-image</td>
<td>A global configuration mode command used to enable image resilience</td>
</tr>
<tr>
<td>secure boot-config</td>
<td>A global configuration mode command that archives the running configuration of a router to persistent storage</td>
</tr>
<tr>
<td>login block-for</td>
<td>A global configuration mode command that specifies the number of failed login attempts (within a specified time period) that trigger a quiet period, during which login attempts will be blocked</td>
</tr>
<tr>
<td>login quiet-mode</td>
<td>A global configuration mode command that specifies an ACL that identifies exemptions from the previously described quiet period</td>
</tr>
<tr>
<td>login delay seconds</td>
<td>A global configuration mode command that specifies a minimum period of time that must pass between login attempts</td>
</tr>
<tr>
<td>login on-failure log</td>
<td>A global configuration mode command that creates log messages for failed login attempts</td>
</tr>
<tr>
<td>login on-success log</td>
<td>A global configuration mode command that creates log messages for successful login attempts</td>
</tr>
<tr>
<td>banner motd</td>
<td>A global configuration mode command that configures a message to be displayed when a user administratively connects to a router</td>
</tr>
<tr>
<td>ip http server</td>
<td>A global configuration mode command that enables an HTTP server on a router</td>
</tr>
<tr>
<td>ip http secure-server</td>
<td>A global configuration mode command that enables a secure HTTP (HTTPS) server on a router</td>
</tr>
<tr>
<td>ip http authentication local</td>
<td>A global configuration mode command that configures a local authentication method for accessing the HTTPS server</td>
</tr>
<tr>
<td>username name privilege 15 secret 0 password</td>
<td>A global configuration mode command that configures a username and password to be used for authentication local to the router</td>
</tr>
</tbody>
</table>
### Table 3-14 Chapter 3 EXEC Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable view</td>
<td>Enables the root view, which is represented by the set of commands available to an administrator logged in with a privilege level of 15</td>
</tr>
<tr>
<td>enable view</td>
<td>Switches to the specific view (after the required credentials are provided)</td>
</tr>
<tr>
<td>show secure bootset</td>
<td>Used to verify that Cisco IOS Resilient Configuration is enabled and that the files in the bootset have been secured</td>
</tr>
<tr>
<td>show login</td>
<td>Can be used to verify that enhanced support for virtual logins is configured and to view the login parameters</td>
</tr>
</tbody>
</table>
Index

Numerics
3DES, 450
800 series ISR, 82–83
1800 series ISR, 83
1999 Gramm-Leach-Bliley Act (GLBA), 19
2800 series ISR, 84
3800 series ISR, 84–86

A
AAA
configuring, 115–116
for routers, 116–125
using SDM, 127–128
using Cisco Secure ACS, 128–131
RADIUS, 141–143
TACACS+, 138–141
configuring, 144–147
troubleshooting on routers, 126–127
AAA (authentication, authorization, and accounting), 267
aaa accounting command, 125
academic hackers, 22
access, disabling IP phone web access, 316
access control, 256
ACLs
applying to interface, 352
configuring, 349–350
developing, 351
functions, grouping, 362
ICMP traffic, restricting, 358–359
IP address spoofing, mitigating, 357–358
router service traffic, filtering, 360–361
RIPv2, 361–362
SNMP, 361
static packet filters, creating, 347–348
traffic filtering, 354–357
Turbo ACLs, 350–351
acquisition and development phase (SDLC), 49
activating practice exam, 578–579
active attacks, 23
adaptive chosen ciphertext attacks, 486
administrative controls, 16
administrative law, 18
advancements in firewall technology, 325–326
AES (Advanced Encryption Standard), 451–452
aggressive mode (IKE), 530
AH (Authentication Header), 531
AIM (Advanced Integration Modules), 86, 538
AIP-SSM (Advanced Inspection and Prevention Security Services Module), 392
alerts, 366–367
algorithms
asymmetric encryption, 494
DH Key Exchange, 499–500
public-key encryption, 494–497
RSA, 497–499
Digital Signature Algorithm. See DSA
digital signatures, 482
hash, 466
HMAC, 470–471
MD5, 471–473, 475
SHA-1, 475–478
symmetric encryption, 441–443
anatomy
buffer overflows, 259–260
hash functions, 467
worms, 263–264
anomaly-based detection, 390
application inspection firewalls, 338–342
application layer
attacks, 398
firewalls, 327–333
application servers
VoIP, 304
VoIP protection, 315
applications
nonsecure custom, 11
protection methods, 274–275
security guidelines, 274
vulnerabilities, 257–258
applying
ACLs to router interface, 352
certificates, 517–518
architecture
Cisco Security Agent, 268–269
IronPort, 266
ARO (annualized rate of occurrence), 61
ASA 5500 Security Appliance, 342–343
asymmetric algorithms, 494
DH Key Exchange, 499–500
public-key encryption, 494–495
authentication, 496–497
confidentiality, 495–496
RSA
digital signatures, 498–499
features, 497
guidelines, 499
asymmetric encryption algorithms, 443–444, 480
attackers
hackers, compared, 20
prosecuting, 17–18
attacks, 23
adaptive chosen ciphertext, 486
application layer, 398
availability, 36–39
branch prediction analysis, 486
confidentiality, 31–33
DDoS, 37
DoS, 36
electrical disturbance, 38
elevation of privileges, 258
heap overflows, 259
ICMP, 37
integrity, 33–36
IP spoofing, 27–28
IP source routing, 28–29
man-in-the-middle attacks, 29
protection against, 30–31
man-in-the-middle, 309
message tampering, 309
network layer, 399
password, 35
physical environment, 39
registration hijacking, 309
responses to, 272–273
salami, 34
SIP, 309–310
Smurf, 37
TCP SYN floods, 37
timing, 486
transport layer, 398
Trojan horses, 262
types of, 438–439
viruses, 262-264
VoIP targets, 307–308
vulnerabilities, 20–21
worms, 261
anatomy, 263–264
compared to viruses, 264
AUP (acceptable use policies), 57
authentication, 540
  CAs, 514
digital signatures, 483
EAP-MD5, 236
EAP-TLS, 236–237
PEAP, 238
PEAP-FAST, 239
phone image, 314
public-key encryption, 496–497
RADIUS, 141–143
TACACS+, 138–141
configuring, 144–147
authentication, authorization, and accounting. See AAA
AutoSecure feature (Cisco IOS Software), 161–165
auxiliary VLANS, VoIP protection, 310–311
AV (asset value), 61
availability, 13
availability attacks, 36–39
awareness training, 66

B
backup sites, 56
banner messages, creating, 98–99
Belaso, Giovan Batista, 435
benefits of VoIP, 302–303
birthday attacks, 439
black hat hackers, 22
blended threats, 66
blind spoofing, 28
block ciphers, 444–445
botnets, 36
BPA (branch prediction analysis) attacks, 486
BPDU Guard, 217–218
brute-force attacks, 87, 439
brute-force password attack, 35
buffer overflows, 258
anatomy, 259–260
definition, 259
Trojan horses, 262
types, 260
viruses, 262–264
worms, 261
anatomy, 263–264
compared to viruses, 264
business continuity planning, disaster recovery, 55
  backup sites, 56
disruption categories, 56

C
call agents, 304
calling search spaces, toll fraud, 309
CAM (Content Addressable Memory) table
overflow attacks, mitigating, 222–223
CAs (certificate authorities), 478, 501
authentication, 514
certificates, applying, 517–518
cross-certified, 505
hierarchical, 503, 505
identity management, 512
PKI roles, 511–512
  authentication, 514
certificate enrollment, 513–514
certificate retrieval, 513
digital certificates, 515–516
identity management, 512
single root CA trust topology, 502–503
categorizing data, 13
  classification models, 13–14
classification roles, 15
CBAC (Context-Based Access Control), 368–369
CBC mode (DES), 448
certificate authority. See CAs
certificates, 501
  applying, 517–518
  authentication, 514
classes, 502
digital, 515–516
enrollment, 513–514
PKI, 506
retrieving, 513
CHAP (Challenge Handshake Authentication Protocol), 292
checking for updated information, 617–618
checksum, 468
chosen ciphertext attacks, 438
chosen plain-text attacks, 438
ciphers
- block ciphers, 444–445
- stream ciphers, 445
- substitution cipher, 434–435
- transposition ciphers, 436
- Vigenère cipher, 435

ciphertext, 485

ciphertext-only attacks, 439

CIR (committed information rate), 228
Cisco 500 series PIX Security Appliances, 538
Cisco ASA 5500 Series Adaptive Security Appliance, 342–343, 536–537
Cisco Catalyst switches
- Cisco IBNS, 232–233
- port security, 228–231
- PVLANs, configuring, 227
- security features, 225–226
- VACLs, configuring, 227
Cisco IBNS (Identity-Based Networking Services), 232–233
Cisco IDS 4215 Sensor, 396
Cisco IOS firewalls, 364
- alerts, 366–367
- configuring, 370–371
- SPI, 367–369
- traffic filtering, 365
- traffic inspection, 366
Cisco IOS Resilient Configuration, 95–96
Cisco IOS Software, AutoSecure feature, 161–165
Cisco IOS zone-based firewalls, 369–370
- banners, creating, 98–99
- class maps, 378–379
- configuring, 363–364
- policies, 376–377
- privilege levels, configuring, 93
- verifying configuration, 379
- zone membership rules, 371–372
- zone pairs, 375–376
- zone restrictions, 373–374
Cisco IPS 4240 Sensor, 397
Cisco IPS 4255 Sensor, 397
Cisco IPS 4260 Sensor, 397
Cisco MDS 9000 SAN-OS, 286
Cisco PIX appliances, 326

Cisco SDM (Security Device Manager), 69
99–100
- AAA, troubleshooting, 127–128
- installation, verifying, 101–102
- interface, 102–103
- management features, configuring, 185–190
- NTP, configuring, 194–195
- routers, locking down, 166–171
- SNMP, configuring, 190–193
- SSH, configuring, 196–200
- wizards, 103–105
Cisco SDM VPN wizard, 548
- Quick Setup wizard, site-to-site VPNS, configuring, 550–558
- Step-by-Step wizard, site-to-site VPNS, configuring, 559–570
Cisco Secure ACS, configuring AAA, 128–131
Cisco Secure ACS for Windows, installing, 132–137
Cisco Secure ACS Solution Engine, 115
Cisco Security Agent, 268–269
- architecture, 268–269
- attack responses, 272–273
- interceptors, 269–272
Cisco Security MARS, 70
Cisco Self-Defending Networks, 66
- constructing, 67–68
- integrated security products, 70–71
Cisco VPN 3000 series concentrators, 535–536
civil law, 18
class maps, 378–379
classes of SAN attacks, 286
classification models, 13
- characteristics, 14
- government/military, 13
- organizational, 14
classification roles, 15
CLI views, creating, 93–95
close-in attacks, 23
cold sites, 56
command and control interface, IDS/IPS sensors, 396
commands
  aaa accounting, 125
  debug aaa authentication, 126
  exec-timeout, 92
  service password-encryption, 90
  setup, 88
  shutdown, 158
community strings, 181
components
  of PKI, 501–502
  of VoIP, 303, 305
Computer Fraud and Abuse Act, 19
computer security hackers, 22
Computer Security Institute (CSI), 9
confidential data category, 14
confidentiality, 12
  public-key encryption, 495–496
  SANs, 293
confidentiality attacks, 31–33
configuration interceptors, 271
configuring
  AAA, 115–116
    on routers, 116–125
    using Cisco Secure ACS, 128–131
    using SDM, 127–128
  ACLs, 349–350
  Cisco IOS firewalls, 370–371
  firewalls, Cisco IOS zone-based firewalls, 363–364
  IEEE 802.1x, 243–245
  IOS-based IPS with SDM
    Add a Rule screen, 412
    Add an Extended Rule Entry screen, 412
    command delivery to router, 416
    Edit IPS on an Interface screen, 410–411
    filter configuration verification, 417
    fragment checking, enabling, 414
    global settings, 417–418
  IPS configuration screen, 403
  IPS Policies Wizard, 404–410
  launching SDM, 401
  ordered list of rules, 414
  rule entry confirmation, 412
  rule permitting all traffic, 414
  SDEE notification screen, 403
  SDEE subscription screen, 404
  SDM configuration screen, 401
  signatures, 419, 422–423
  IPsec site-to-site VPNs, 543–547
  management features with Cisco SDM, 185–190
  NTP with SDM, 194–195
  port security, 228–231
  privilege levels, 93
  PVLANs, 227
  signatures, 419, 422–423
  site-to-site VPNs, 559–570
    with Cisco SDM Quick Setup wizard, 550–558
  SNMP with SDM, 190–193
  SPAN ports, 226
  SSH
    on routers, 183–185
    with SDM, 196–200
  syslog, 175–178
  VACLs, 227
connection signatures, 399
close, embryonic, 399
closed ports, 234
close, administrative, 16
close, detective, 17
close, deterrent, 17
close, physical, 16
close, preventive, 17
close, technical, 16
closed networks, 297
close
  ACLs, 353–354
    banner messages, 98–99
  CLI views, 93–95
    firewall policies, 345–347
criminal law, 18
CRLs (Certificate Revocation Lists), 540
cross-certified CAs, 505
cryptoanalysis, 438–439
cryptographic hash functions, 468–469
  application, 469–470
cryptographic hashes, 455
cryptographic keys, 441
cryptography

asymmetric encryption, 443–444, 480

dh key exchange, 499–500

digital signatures, 478, 480

algorithms, 482

authentication, 483

dss, 487

implementations, 482

integrity, 483

legality, 482

private keys, 482

public key distribution, 482

rsa, 483–486

schemes, 483

users, 482

encryption algorithms, 437, 440–441

key management, 456–458

selecting, 453–454

hash algorithms, 466

hash functions

anatomy, 467

application, 467–468

cryptographic, 468–470

history of, 434

HMAC, overview, 470–471

MD5, 471–472

functionality, 475

origins, 472–473

vulnerabilities, 473

one-time pad, 436

SHA-1, 476

features, 475

functionality, 478

vulnerabilities, 477–478

substitution cipher, 434–435

symmetric encryption, 441–453

cryptology, 433

CSI (Computer Security Institute), 9

CTLs (Certificate Trust Lists), 540

custodian role, 15

data, categorizing

classification models, 13–14

classification roles, 15

data didding, 34

dDoS (Distributed Denial of Service) attacks, 37

dbug aaa authentication command, 126

decrypting messages, RSA, 485

Defense in Depth design philosophy, 24–26

Denial of Service (DoS) attacks, 36

deploying IDS/IPS network-based/host-based solutions, 394–395

DES, 447–448

stream cipher modes, 449

designing secure networks, 63

complexity, 64

privileges, minimizing, 63

detectoral controls, 17

deterrent controls, 17

developing ACLs, 351

DH (Diffie-Hellman) Key Exchange Algorithm, 499–500

DHCHAP (Diffie-Hellman Challenge Handshake Authentication Protocol), 292

DHCP server spoofing, 218–220

dictionary attacks, 35, 87

digests, 88

digital certificates, 515–516

digital signatures, 478, 480

algorithms, 482

authentication, 483

DSS, 487

dsa, 487

integrity, 483

legality, 482

private keys, 482

public key distribution, 482

rsa, 483, 498–499

message encryption/decryption, 485

origins, 484

overview, 484

signing messages, 485–486

vulnerabilities, 486

schemes, 483

users, 482
direct application attacks, 257

disabling
  GARP, 316
  IP phone web access, 316
  unneeded services, 316

disaster recovery, 55
  backup sites, 56
  disruption categories, 56

disposition phase (SDLC), 51

Distributed Denial of Service (DDoS)
  attacks, 37

distribution attacks, 23

DMVPN (Dynamic Multipoint VPN), 534

DMZ (demilitarized zone), 344

DoS (Denial of Service) attacks, 36
  signatures, 399

double tagging, 213–214

DSA (Digital Signature Algorithm), 487

DSCP (Differentiated Services Code Point), 228

dsniff, 223

DSS (Digital Signature Standard), 487
dumpster diving confidentiality attacks, 32

DVS (Dynamic Vectoring and Streaming)
  engine, 266

E

EAP-MD5 (Extensible Authentication Protocol Message Digest 5), 236

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), 236–237

ECB mode (DES), 448

Economic Espionage Act of 1996, 19

EF (exposure factor), 61
electrical disturbances, 38

elevation of privileges attack, 258

embryonic connections, 399

EMI (electromagnetic interference)
  interception, 32

enable passwords, 88

enable secret passwords, 88

enabling SSH on routers, 183–185

encrypting messages, RSA, 485

encryption, 437, 440–441, 453–454

  asymmetric, 443–444
    DH Key Exchange, 499–500
    public-key encryption, 494–497
    RSA, 497–499
  
  key management, 456–458
  public-key, 494–495
    authentication, 496–497
    confidentiality, 495–496

  symmetric, 441–445
    3DES, 450
    AES, 451–452
    DES, 447–449
    key lengths, 446
    Rivest ciphers, 452–453
    SEAL, 452

endpoint security

  application vulnerabilities, 257–258
  buffer overflows, 258
    anatomy, 259–260
    definition, 259
    Trojan horses, 262
    types, 260
    viruses, 262–264
    worms, 261–264

  Cisco Security Agent, 268–269
    architecture, 268–269
    attack responses, 272–273
    best practices, 273–274
    interceptors, 269, 271–272
  
  defining, 254
  endpoint protection, 254
  IronPort, 265
    architecture, 266

  NAC Appliance, 254, 266–268
  NAC framework, 267
  network infection containment, 254
  operating system vulnerabilities, 256–257
  secure software, 255
  VoIP protection, 313–314

end-user policies, 59

the Enigma, 434

enterprise networks, SANs, 283–284

ESP (Encapsulating Security Payload), 531
  incorporating in SANs, 294
establishing
IPsec site-to-site VPNs, 542
SSL tunnels, 459
ethics codes of conduct, 18
evaluating network security, 52–54
exam, preparing for, 577–580
exam engine, 580
exec-timeout command, 92
execution space interceptors, 271
Executive Order 12958, 14
exploits, 20
signatures, 398
extended ACLs, 349
Extended Authentication. See XAUTH
external threats, 10

F
FAC (Forced Authorization Code), 309
fail open, 63
fail-closed mode, 63
FCAP (Fibre Channel Authentication Protocol), 292
FCPAP (Fibre Channel Password Authentication Protocol), 293
FC-SP (Fibre Channel Security Protocol), 294
Fiber Channel
WWN, 289
zoning, 288
file system interceptors, 271
files, signature definition, 399–400
firewalls, 323–324
application inspection, 338–342
application layer, 327–333
Cisco IOS firewalls, 364
alerts, 366–367
configuring, 370–371
SPI, 367–369
traffic filtering, 365
traffic inspection, 366
Cisco IOS zone-based, 369–370
class maps, 378–379
configuring, 363–364
policies, 376–377
verifying configuration, 379
zone membership rules, 371–372
zone pairs, 375–376
zone restrictions, 373–374
packet-filtering, 333–335
policies, creating, 345–347
role in layered defense strategy, 343–345
stateful packet-filtering, 335–338
technology advancements, 325–326
transparent, 326–327
VoIP protection, 311–312
FISMA (Federal Information Security Management Act) of 2002, 19
Forced Authorization Code (FAC), 309
functions, hash
anatomy, 467
application, 467–468
cryptographic, 468–470

G
GARP (gratuitous ARP), 29, 220
disabling, 316
gatekeepers, 304
gateways, 304
goals of security, 12
availability, 13
confidentiality, 12
integrity, 12
governing policies, 58
government/military classification model, 13
Gramm-Leach-Bliley Act (GLBA) of 1999, 19
grey hat hackers, 22
GRE tunnels, 532
grouping ACL functions, 362
guidelines, 59

H
H.248 protocol, 306
H.323 protocol, 306
hackers
attackers, compared, 20
mind-set, 23–24
types, 21–22
hacktivists, 22
hard zoning, 289
hardening
endpoints, VoIP protection, 313–314
routers, 158–160
software, 255
hardware acceleration modules, 538–539
hash algorithms, 466. See also hash functions, 467
  HMAC, overview, 470–471
  MD5
    functionality, 475
    origins, 472–473
    overview, 471–472
    vulnerabilities, 473
  SHA-1
    features, 475
    functionality, 478
    overview, 476
    vulnerabilities, 477–478
hash functions
  anatomy, 467
  application, 467–468
  cryptographic, 468–470
hashing, 455
Health Insurance Portability and Accountability Act (HIPAA) of 2000, 19
heap overflows, 259
hierarchical CAs, 503, 505
hijacking TCP sessions, 36
HIPAA (Health Insurance Portability and Accountability Act) of 2000, 19
HIPS (Host-based Intrusion Prevention System), 254
deploying, 394
history of cryptology, 434–436
HMAC (Hash-based Message Authentication Code), 470–471
hobby hackers, 22
honey pot detection, 390
host-based IDS/IPS solutions, deploying, 254, 391–395
hot sites, 56

ICMP attacks, 37
ICMP traffic, restricting with ACLs, 358–359
identifying router vulnerabilities, 158–160
identity management, CAs, 512
IDS (intrusion detection systems), 226
  IPS, compared, 388–389
  malicious traffic detection methods, 389–391
    anomaly-based, 390
honey pot, 390
  policy-based, 390
  signature-based, 389
network-based solutions, deploying, 394–395
sensors, 395
  Cisco IDS 4215, 396
  interfaces, 396
  network-based, 392–394
  operating modes, 396
signatures, 398
  connection, 399
  definition files, 399–400
  DoS, 399
  exploit, 398
  firing responses, 400–401
  string, 399
IDS Network Module (NM-CIDS), 393
IDSM-2 (Intrusion Detection System Module 2), 393
IEEE 802.1x, 234–235
  combining with port security features, 239–240
  configuring, 243–245
  VLAN assignment, 240–241
IETF (Internet Engineering Task Force), 507
IINS exam, scoring, 581
IKE (Internet Key Exchange), 529-531
ILOVEYOU virus, 262
implementation phase (SDLC), 50
in-band management, 173–175
incident responses, 17–18
indirect application attacks, 257
initiation phase (SDLC), 49
inline mode (sensors), 396
insider attacks, 23
installing
  enclosed CD, 578
  Cisco Secure ACS for Windows, 132–137
integrity, 12
  digital signatures, 483
integrity attacks, 33–36
interceptors, Cisco Security Agent, 269–272
interfaces, IDS/IPS sensors, 396
internal threats, 10
international jurisdiction issues, 19
Intrusion Detection System Module 2. See IDSM-2
IOS-based IPS, configuring with SDM
Add a Rule screen, 412
Add an Extended Rule Entry screen, 412
command delivery to router, 416
Edit IPS on an Interface screen, 410–411
filter configuration verification, 417
fragment checking, enabling, 414
global settings, 417–418
IPS configuration screen, 403
IPS Policies Wizard, 404, 407, 409–410
launching SDM, 401
ordered list of rules, 414
rule entry confirmation, 412
rule permitting all traffic, 414
SDEE notification screen, 403
SDEE subscription screen, 404
SDM configuration screen, 401
signatures, 419, 422–423
IP address spoofing
mitigating with ACLs, 357–358
IP phones, 304
IP source routing, 28–29
IP spoofing attacks, 27–28
IP source routing, 28–29
man-in-the-middle attacks, 29
protection against, 30–31
types, 28
IP telephony, 301
IPS (intrusion prevention systems), 81. See also IOS-based IPS, configuring with SDM
host-based, 391, 394
IDS, compared, 388–389
malicious traffic detection methods,
389–391
anomaly-based, 390
honey pot, 390
policy-based, 390
signature-based, 389
network-based, 391
network-based solutions, deploying,
394–395
sensors, 395
Cisco IPS 4240, 397
Cisco IPS 4255, 397
Cisco IPS 4260, 397
interfaces, 396
network-based, 392–394
operating modes, 396
signatures, 398
connection, 399
definition files, 399–400
DoS, 399
exploit, 398
firing responses, 400–401
string, 399
IPS Policies Wizard, 404–409
Add a Rule screen, 412
Add an Extended Rule Entry screen, 412
command delivery to router, 416
Edit IPS on an Interface screen, 410–411
filter configuration verification, 417
fragment checking, enabling, 414
ordered list of rules, 414
rule entry confirmation, 412
rule permitting all traffic, 414
IPsec, 529
AH, 531
best practices, 540–541
ESP, 531
IKE, 529, 531
site-to-site VPNs
configuring, 543–558
establishing, 542
IPSec tunnels, VoIP protection, 312
IronPort, 265
architecture, 266
ISAKMP sessions, 530
isolation between processes, 257
ISR (Integrated Security Routers), 81–82
1800 Series, 83
2800 Series, 84
3800 Series, 84–86
800 Series, 82–83
J–K
Jefferson, Thomas, 434
Julius Ceasar, 435
key management, 456–458
keyloggers, 35
keys. See also PKI
key pair combinations, 506
private, digital signatures, 482
public, distribution, 482
public-key encryption, 494–495
  authentication, 496–497
  confidentiality, 495–496

keys, 456–457
known plain-text attacks, 439

L
launching SDM, 401
Layer 2 switching, 211
  CAM table overflow attacks, mitigating, 222–223
  DAI, 220–221
  DHCP server spoofing, 218–220
  double tagging, 214
  IEEE 802.1x, 234–235
  MAC address spoofing attacks, preventing, 223–225
  port security, configuring, 228–230
  securing, 212–213
  security best practices, 231
  STP attacks, 215–217
layered defense strategy, 343–345
least-privilege concept, 256
legal guidelines, 18
  administrative, 18
  civil law, 18
  criminal law, 18
  international jurisdiction, 19
  U.S. information security laws/regulations, 19
legality of digital signatures, 482
limitations of PKI, 516–517
local user database (AAA)
  configuring, 116–125
  troubleshooting, 126–127
locking down routers, 160–171
logging, configuring syslog, 175–178
login activity timers, setting, 92
login enhancements, enabling for virtual connections, 96–98
loose IP source routing, 29
lost passwords, recovering, 91
LUN (Logical Unit Member) masking, 287

M
MAC address spoofing attacks, preventing, 223–225
MAC address table, 211
main mode (IKE), 530
malicious traffic detection methods, IDS/IPS devices, 389, 391
  anomaly-based, 390
  honey pot, 390
  policy-based, 390
  signature-based, 389
  summary, 391
managed node SNMP entity, 182
management features, configuring with Cisco SDM, 185–190
man-in-the-middle attacks, 29, 221
  VoIP, 309
MARs (machine access restrictions), 131
Maubourne, Joseph, 436
MCUs (multipoint control units), 304
MD5 (Message Digest 5)
  functionality, 475
  origins, 472–473
  overview, 471–472
  vulnerabilities, 473
MD5 (Message Digest algorithm 5), 471
meet-in-the-middle attack, 439
Megaco, 306
memory protection/isolation, 256
Message Digest algorithm 5. See MD5
message tampering, 309
messages
  encrypting/decrypting with RSA, 485
  RADIUS, 142
  signing with RSA, 485–486
  SNMP, 180
metacharacters, 399
method lists, defining, 119–120
MGCP (Media Gateway Control Protocol), 306
MIB, 180
microengines, 398
military/government classification model, 13
minimizing privileges, 63
mitigating
  CAM table overflow attacks, 222–223
  IP address spoofing with ACLs, 357–358
monitoring IEEE 802.1x, 243–245
N

NAC (Network Admission Control) framework, 254
endpoint security, 266–268
overview, 267
NAFs (network access filters), 132
NAP (network access profiles), 131
NAT (network address translation), best practices, 541
network infection containment, 254
network interceptors, 271
network layer attacks, 399
network management. See secure management and reporting
network security, evaluating, 52–54
network security policies, 57
end-user policies, 59
governing policies, 58
responsibilities, 59
risk analysis
example of, 61
qualitative analysis, 61
quantitative analysis, 60
technical policies, 58
user awareness and training, 64, 66
network-based IDS/IPS solutions
deploying, 394–395
sensors, 392–394
NIDS (network-based IDS), 25, 395
NIPS (network-based IPS), 25, 391, 394
NIST (National Institute of Standards and Technology), 458, 475
Nmap security scanner, evaluating network security, 54
NM-CIDS (IDS Network Module), 393
nonblind spoofing, 28
nonsecure custom applications, 11
NTP (Network Time Protocol), configuring with SDM, 194–195
numbered ACLs, 349–350

O
one-step lockdown feature (Cisco SDM), 166–171
one-time pad, 436

OOB (out-of-band), 172–175
operating modes, IDS/IPS sensors, 396
operating system vulnerabilities, 255–257
operations and maintenance phase (SDLC), 50
operations security recommendations, 51–52
organizational classification model, 14

P
packet capture confidentiality attacks, 32
packet captures, 35
packet-filtering firewalls, 333–335
stateful, 335–338
PACs (protected access credentials, 239
paralyze phase (worms), 264
partitions, toll fraud, 309
passing scores for IINS exam, 581
passive attacks, 23
password attacks, 35
password encryption, 90
password-protecting routers, 86–91
paths, trusted, 256
payloads, 263
PEAP (Protected Extensible Authentication Protocol), 238–239
penetration phase (worms), 264
persist phase (worms), 264
phishing, 308
phone image authentication, 314
phreakers, 22
physical controls, 16
physical environment attacks, 39
ping of death, 37
ping sweep confidentiality attacks, 32
ping sweeps, 399
PKCS (Public Key Cryptography Standards), 508–510
PKI (Public Key Infrastructure), 500
CAs, 501
authentication, 514
certificate enrollment, 513–514
certificate retrieval, 513
certificates, applying, 517–518
cross-certified, 505
digital certificates, 515–516
directional, 503–505
PKI (Public Key Infrastructure X.509), 507
point solutions, 67
policy-based detection, 390
polyalphabetic ciphers, Vigenère, 435
Port 80, 66
port authentication protocols
  CHAP, 292
  DHCHAP, 292
port scan confidentiality attacks, 32
port scans, 10
port security, 228–231
  combining with IEEE 802.1x, 239–240
practice exam, activating, 578–579
preparing for exam, 577
  study plan, 579–580
preventing
  DHCP server spoofing, 218–220
  double tagging, 214
  MAC address spoofing attacks, 223–225
  STP attacks, 215–217
  VLAN hopping, 213
preventive controls, 17
Privacy Act of 1974, 19
private data category, 14
private keys, digital signatures, 482
privileged context of execution, 256
privileged mode, 87
privileges
  elevation of privileges attack, 258
  minimizing, 63
  switching, 256
probe phases (worms), 264
procedures, 59
process memory protection and isolation, 256
processes, isolating, 257
promiscuous mode (sensors), 396
propagate phase (worms), 264
prosecuting attackers, 17–18
protection
  applications, 274–275
  endpoint, 254
  endpoints
    Cisco Security Agent, 268–273
    IronPort, 265–266
    NAC Appliance, 266–268
    NAC framework, 267
    operating system vulnerabilities, 256–257
  IP spoofing attacks, 30–31
  memory, 256
  VoIP
    application servers, 315
    auxiliary VLANs, 310–311
    endpoints, hardening, 313–314
    firewalls, 311–312
    IPsec tunnels, 312
    summary, 316
proxy servers, 331
PSTN (public switched telephone network), 301
public data category, 14
public keys, digital signatures, 482
public-key encryption, 494–495
  authentication, 496–497
  confidentiality, 495–496
PVLANs (Private VLANs), 227
Quick Setup wizard (Cisco SDM VPN wizard), 549
  site-to-site VPNs, configuring, 550–558
RADIUS, 137, 141–143
Rail Fence Cipher, 436
rainbow tables, 473
RAs (registration authorities), 506
Real-time Transport Protocol (RTP), 306
recovering lost passwords, 91
reference monitors, 257
registration authorities. See RAs
registration hijacking, 309
remote-access VPNs, 528
responding to incidents, 17–18
responses to attacks by Cisco Security Agent, 272–273
restricted VLANs, 242
restricting ICMP traffic with ACLs, 358–359
Rijmen, Vincent, 451
Rijndael cipher, 451
RIPv2, filtering traffic, 361–362
risk analysis, 60–61
risk avoidance, 62
risk management, 62
risk mitigation, 62
risks, 20
Rivest ciphers, 452–453
Rivest, Ronald, 472
roles
  of CA in PKI, 511–512
    authentication, 514
    certificate enrollment, 513–514
    certificate retrieval, 513
    digital certificates, 515–516
    identity management, 512
  classification, 15
ROMMON mode, 91
root bridge, 215
Root Guard, 217
root port, 215
rooting a system (quotes), 260
router service traffic
  filtering with ACLs, 360–361
  RIPv2, filtering with ACLs, 361–362
  SNMP, filtering with ACLs, 361
routers
  AAA
    configuring, 116–125
    troubleshooting, 126–127
  ACLs, applying to interface, 352
  hardening, 159–160
  locking down, 160–171
  password-protecting, 86–91
  SSH, configuring, 183–185
  VPN-enabled, 533–535

RSA (Rivest, Shamir, Adleman), 483, 491, 497–499
  digital signatures, 498–499
  message encryption/decryption, 485
  origins, 484
  overview, 484
  signing messages, 485–486
  vulnerabilities, 486
RSPAN (Remote SPAN), 226
RTCP (RTP Control Protocol), 306
RTP (Real-time Transport Protocol), 306
S
SAFE (Security and Freedom through Encryption) Act, 19
salami attacks, 34
salt, 473
SANs (storage area networks), 282
  attack classes, 286
  data confidentiality, 293
  ESP, incorporating, 294
  LUN masking, 287
  organizational benefits, 283–284
  port authentication protocols, 292
  SCSI communications model, 284
  virtual SANs, 290–291
  VSANs, combining with zones, 291
  zoning strategies, 288–289
SANS Institute Top 20 vulnerabilities website, 273
Sarbanes-Oxley (SOX) Act of 2002, 19
SBU (sensitive but unclassified) data category, 14
SCCP (Skinny Client Control Protocol), 306
SCEP (Simple Certificate Enrollment Protocol), 510–511
schemes, digital signatures, 483
Scherbius, Arthur, 434
scoring simulated exam, 581
script kiddies, 22
SCSI communications model, 284
SDEE (Security Device Event Exchange), 399
SDLC (System Development Life Cycle), 49
  acquisition and development phase, 49
  disposition phase, 51
  implementation phase, 50
  initiation phase, 49
  operations and maintenance phase, 50
SDM (Security Device Manager), 401
AAA, configuring, 127–128
configuration page, 401
IOS-based IPS configuration
   Add a Rule Screen, 412
   Add an Extended Rule Entry Screen, 412
   command delivery to router, 416
   Edit IPS on an Interface Screen, 410–411
   filter configuration verification, 417
   fragment checking, enabling, 414
   global settings, 417–418
   IPS configuration Screen, 403
   IPS Policies Wizard, 404–410
   launching SDM, 401
   ordered list of rules, 414
   rule entry confirmation, 412
   rule permitting all traffic, 414
   SDEE notification Screen, 403
   SDEE subscription Screen, 404
   SDM configuration Screen, 401
   signatures, 419, 422–423
launching, 401
management features, configuring, 185–190
SEAL, 452
secret data category, 14
secure management and reporting, 172–175
   NTP, configuring, 194–195
   SNMP, configuring, 190–193
   SNMPv3, 179, 181–182
   SSH, configuring, 196–200
secure network design, 63
   complexity, 64
   privileges, minimizing, 63
Secure Socket Layer. See SSL
secure software, 255
security, goals of, 12–13
Security and Freedom through Encryption (SAFE) Act, 19
Security Device Event Exchange (SDEE), 399
security levels, 181–182
security models, 182
security policies, 57
   end-user policies, 59
   governing policies, 58
   responsibilities, 59
risk analysis
   example of, 61
   qualitative analysis, 61
   quantitative analysis, 60
   technical policies, 58
   user awareness and training, 64–66
security zones, 373
selecting encryption algorithms, 453–454
sensitive but unclassified (SBU) data category, 14
sensitive data category, 14
sensors, IDS/IPS, 395
   Cisco IDS 4215, 396
   Cisco IPS 4240, 397
   Cisco IPS 4255, 397
   Cisco IPS 4260, 397
   interfaces, 396
   operating modes, 396
service password-encryption command, 90
services, unneeded, disabling, 316
setting login activity timers, 92
setup command, 88
SHA-1 (Secure Hash Algorithm 1), 475
   features, 475
   functionality, 478
   overview, 476
   vulnerabilities, 477–479
shutdown command, 158
signature-based detection, 389
signatures, 398
   configuring, 419, 422–423
   connection, 399
definition files, 399–400
digital, 478–480
   algorithms, 482
   authentication, 483
   DSS, 487
   implementations, 482
   integrity, 483
   legality, 482
   private keys, 482
   public key distribution, 482
   RSA, 483–486, 498–499
   schemes, 483
   users, 482
DoS, 399
exploit, 398
firing responses, 400–401
string, 399
simulation mode (exam engine), 580–581
single root CA trust topology, 502–503
SIP (Session Initiation Protocol), 306
SIP attacks, 309–310
site-to-site VPNS, 527–528
  configuring, 543–547
  establishing, 542
Skinny Client Control Protocol (SCCP), 306
SLAP (Switch Link Authentication Protocol), 292
Smurf attacks, 37
SNMP (Simple Network Management Protocol), 179–182
  community strings, 181
  configuring with SDM, 190–193
  messages, 180
  service filtering, 361
  traps, 228
social engineering, 33
soft zoning, 289
software
  hardening, 255
  secure, 255
SOX (Sarbanes-Oxley) Act of 2002, 19
spam, 308
SPAN (Switch Port Analyzer), 216
  ports, configuring, 226
SPI (stateful packet inspection), 367–369
SPIT (spam over IP telephony), 308
spoofing, 213
SRP (Secure Remote Password), 293
SRTP (Secure RTP), 306
SSH (Secure Shell), configuring, 183–185
  with SDM, 196–200
SSL (Secure Socket Layer), 517
SSL VPNS, 458–459
  tunnels, establishing, 459
standard ACLs, 348
standards, 59
  PKI, 507
    PKCS, 508, 510
    SCEP, 510–511
    X.509v3, 507–508
stateful packet-filtering firewalls, 335–338
static packet filters, creating, 347–348
static packet-filtering firewalls, 333–335
steganography, 33
Step-by-Step wizard (Cisco SDM VPN wizard), configuring site-to-site VPNS, 559–570
sticky secure MAC addresses, 225
STP attacks, 215–217
stream cipher modes (DES), 449
stream ciphers, 445
strict IP source routing, 29
string signatures, 399
study mode (exam engine), 580
studying for exam, 579–580
substitution cipher, 434–435
switch spoofing, 213
switches
  securing, 211–213
  voice-enabled, 305
  VPN-enabled, 533–535
symmetric encryption, 445
  3DES, 450
  AES, 451–452
  DES, 447–449
  key lengths, 446
  Rivest ciphers, 452–453
  SEAL, 452
symmetric encryption algorithms, 441–443
syslog, configuring, 175–178

T

TACACS+, 137–141
  configuring, 144–147
TCP (Transmission Control Protocol)
  session hijacking, 36
  SYN floods, 37
  three-way handshake process, 27

technical controls, 16
technical policies, 58
threats to security, 66
  buffer overflows, 258
    anatomy, 259–260
    definition, 259
    Trojan horses, 262
  types, 260
  viruses, 262, 264
  worms, 261, 263–264
  external, 10
  internal, 10
timing attacks, 486
toll fraud, 309
toolbar (SDM), 102–103
top-secret data category, 14
traffic filtering with ACLs, 354–357
traffic policing, 228
transparent firewalls, 326–327
transport layer attacks, 398
transport mode, 532
transposition ciphers, 436
traps, 228
Trojan horses, 35, 262
troubleshooting AAA on routers, 126–127
trust relationship exploitation, 35
trusted code, 255
trusted paths, 256
TSL (Transport Layer Security), 458
tunnel mode, 533
tunnels, 527
Turbo ACLs, 350–351

U
U.S. information security laws/regulations, 19
UCM (Unified Communications Manager), 314
unclassified data category, 14
uncontrolled ports, 234
unneeded services, disabling, 316
updates for ICND1 exam, 617–618
user mode, 87
user role, 15

V
VACLs (VLAN access control lists), 226–227
verifying
SDM installation, 101–102
zone-based firewall configuration, 379
Vernam cipher, 436
Vernan, Gilbert, 436
videoconference stations, 305
Vigenère cipher, 90, 435
virtual connections, enabling login
enhancements, 96–98
viruses, 262
compared to worms, 264
ILOVEYOU, 262
vishing, 308
VLAN assignment using IEEE 802.1x, 240–241
VLAN hopping, preventing, 213
VLANs, 211
auxiliary, VoIP protection, 310–311
double tagging, preventing, 214
restricted, 242
STP attacks, preventing, 215–217
voice-enabled switches, 305
VoIP (voice over IP), 297
benefits, 302–303
components of, 303–305
IP telephony, compared, 301
overview, 301
protecting
application servers, 315
auxiliary VLANs, 310–311
endpoints, hardening, 313–314
firewalls, 311–312
IPsec tunnels, 312
summary, 316
protocols, 305–306
vulnerabilities, 307
design considerations, 539–541
site-to-site, 527–528
configuring, 543–547, 550–558
establishing, 542
SSL VPNs, 458–459
VRF-aware firewall, 81
VSANs (virtual SANs), 290–291
vty passwords, 88
vulnerabilities, 20–21
  applications, 257–258
  identifying, 158–160
  MD5, 473
  operating systems, 255, 257
    endpoint protection, 256–257
  RSA, 486
  SANS Institute Top 20 website, 273
  SHA-1, 477–478
  VoIP, 307
    endpoint attacks, 307–308
    SIP attacks, 309–310
  spam, 308
  toll fraud, 309
  vishing, 308

W
  warm sites, 56
  web access, disabling on IP phones, 316
  websites
    2007 CSI/FBI Computer Crime and Security Survey, 10
    Executive Order 12958, 14
    NIST, 458
    PKIX, 507
    SANS Institute Top 20 vulnerabilities, 273
    Wireshark, 32
  white hat hackers, 22
  Windows, installing Cisco Secure ACS, 132–137
  Wireshark, 32
  wiretapping, 33
  wizards, IPS Policies, 404, 407–410
    Add a Rule page, 412
    Add an Extended Rule Entry page, 412
    command delivery to router, 416
    Edit IPS on an Interface page, 410–411
    filter configuration verification, 417
    fragment checking, enabling, 414
    ordered list of rules, 414
    rule entry confirmation, 412
    rule permitting all traffic, 414
  worms, 261
    anatomy, 263–264
    compared to viruses, 264
  WWN (World Wide Names), 289

X-Y-Z
  X.509v3 standard, 507–508
  XAUTH (Extended Authentication), 517
  Zenmap, 54
  zone-based firewalls, 369–370
    class maps, 378–379
    policies, 376–377
    verifying configuration, 379
    zone membership rules, 371–372
    zone pairs, 375–376
    zone restrictions, 373–374
  zoning strategies for SANs, 289